

**T.C.**  
**İSTANBUL AYDIN ÜNİVERSİTESİ**  
**LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ**



**BLOKZİNCİR TEKNOLOJİSİNE DAYALI, ŞİFRELEME VE  
STEGANOĞRAFİ TEKNİKLERİ KULLANILAN, YÜKSEK  
GÜVENLİKLİ BİLGİ DEĞİŞİM ALGORİTMASI**

**DOKTORA TEZİ**

**Mustafa TAKAOĞLU**

**Bilgisayar Mühendisliği Anabilim Dalı**  
**Bilgisayar Mühendisliği Programı**

**MAYIS, 2022**



**T.C.**  
**İSTANBUL AYDIN ÜNİVERSİTESİ**  
**LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ**



**BLOKZİNCİR TEKNOLOJİSİNE DAYALI, ŞİFRELEME VE  
STEGANOĞRAFİ TEKNİKLERİ KULLANILAN, YÜKSEK  
GÜVENLİKLİ BİLGİ DEĞİŞİM ALGORİTMASI**

**DOKTORA TEZİ**

**Mustafa TAKAOĞLU**  
**(Y1615.610006)**

**Bilgisayar Mühendisliği Anabilim Dalı**  
**Bilgisayar Mühendisliği Programı**

**Tez Danışmanı: Prof. Dr. Naim Mahmood Musleh AJLOUNI**

**Eş Danışman: Prof. Dr. Ali Güneş**

**MAYIS, 2022**



## ONAY FORMU





## ONUR SÖZÜ

Doktora tezi olarak sunduğum “Blokzincir Teknolojisine Dayalı, Şifreleme ve Steganografi Teknikleri Kullanılan, Yüksek Güvenlikli Bilgi Değişim Algoritması” adlı çalışmanın, tezin proje safhasından sonuçlanmasına kadarki bütün süreçlerde bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurulmaksızın yazıldığını ve yararlandığım eserlerin Bibliyografya’da gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve onurumla beyan ederim.  
(16/05/2022)

Mustafa TAKAOĞLU



## ÖNSÖZ

Bilginin istenmeyen taraflarca ele geçirilmesinin engellenmesi için tarih boyunca çeşitli yöntemler geliştirilmiştir: Bilginin gizlenmesi yani insan gözüyle fark edilemez hale getirilmesi için steganografi denilen gizli yazı yazma anlamına gelen çalışma konusu ortaya çıkmıştır. Bilginin korunması için geliştirilen bir diğer yöntem ise şifreleme algoritmalarıdır. Kriptoloji yani şifre bilimi olarak herkesçe bilinen bu çalışma konusunda matematiksel algoritmalara dayalı verinin korunması gerçekleştirilmektedir. 2014 yılı itibariyle blokzincir isminin kullanılmaya başlandığı ve 2009 yılında kullanıma sunulan Bitcoin kripto parasının yaratıcı gücü olan blokzincir teknolojisi ise verinin gerçek anlamda dağıtık, değiştirilemez ve güvenli olarak kaydedilmesine imkân tanımaktadır. Tez çalışmamızda veri güvenliğinin sağlanmasında steganografi ve şifreleme algoritmalarının blokzincir teknolojisinin en önemli parçalarından biri olan özet algoritmalarından yararlanılarak güvenliğin yüksek seviyede sağlandığı ve saldırılara karşı dayanıklı bir yöntem geliştirilmiştir.

Tez konusunun seçilmesinde, akademik yayın çalışmalarında ve kişisel gelişimimde yol gösteren kıymetli büyüğüm ve tez danışmanım Prof. Dr. Naim Mahmood Musleh Ajlouni'ye özel teşekkürlerimi sunmak istiyorum. Ayrıca tez çalışmamın jürisinde bulunan kıymetli hocalarım Prof. Dr. Zafer ASLAN ve Dr. Ali Hamitoğlu'na göstermiş oldukları ilgi, destek ve sabır için ayrıca teşekkürlerimi sunmak istiyorum. İstanbul Aydın Üniversitesi Bilgisayar Mühendisliği Ana Bilim Dalı Başkanı kıymetli hocam Prof. Dr. Ali Güneş'e tez çalışmama ve akademik kariyerime vermiş olduğu destekler için teşekkür ve saygılarımı sunmak istiyorum. Ayrıca Dr. Adem Özyavaş'a bu süreçte şahsıma ve akademik çalışmalarımıza sağlamış olduğu paha biçilemez destekler için teşekkür ve saygılarımı sunmak istiyorum. Son olarak tüm bu çalışmaların sebebi olan kıymetli aileme teşekkürlerimi sunarım.

Mayıs, 2022

Mustafa TAKAOĞLU



# **BLOKZİNCİR TEKNOLOJİSİNE DAYALI, ŞİFRELEME VE STEGANOĞRAFI TEKNİKLERİ KULLANILAN, YÜKSEK GÜVENLİKLİ BİLGİ DEĞİŞİM ALGORİTMASI**

## **ÖZET**

Veri güvenliğinin şifreleme yöntemleriyle sağlanmasında simetrik ve asimetrik anahtarlı şifreleme algoritmaları kullanılmaktadır. Verinin dijitalleşmesi neticesinde şifreleme algoritmalarının matematiksel hesaplamalarının tamamıyla bilgisayar ortamında uygulanabilmesi sayesinde şifreleme süreci dijitalleşmiştir. İlk güvenlik standardı olarak kabul edilen DES algoritmasının kullanımı sonrasında görülen güvenlik açıkları sebebiyle AES şifreleme algoritmasının veri şifreleme standardı olarak kabul görmüştür. Simetrik şifrelemeye örnek olan bu algoritmalar günümüzde halen çokça kullanılan simetrik anahtarlı şifreleme algoritmalarıdır. Bir diğer simetrik şifreleme algoritması olan Vernam şifreleme algoritması tezimizde seçilmiş ve kullanılmıştır. Vernam şifreleme algoritmasının diğer simetrik şifreleme algoritmalarından farklı olarak şifrelenecek dosya boyutu kadar anahtar kullanması sebebiyle ve sahip olduğu algoritmik karmaşıklık sayesinde kuantum sonrası dönem için güvenli kabul edilen algoritmalarından biri olarak karşımıza çıkmaktadır. Vernam algoritmasında karşılaşılan ve geliştirilmeye açık çalışma konuları arasında anahtar üretiminin gerçek rastgele olması ve anahtarın paylaşımının güvence altına alınması bulunmaktadır. Bu sebeple tez çalışmamızda tüm dosya türlerinin güvenli bir şekilde alıcıya iletilmesini sağlayan modüler bir algoritma geliştirilmiştir. İlk modül olarak geliştirilen manipülasyon algoritması, tüm dosyaların tek bir formata dönmesine, anlamlandırılabilir bir bilgiye ulaşılmasının engellenmesine, steganografinin gerçekleştirilebilmesine imkân tanıyacak şekilde geliştirilmiştir. İkinci modülde anahtar havuzları üzerinde gerçekleştirilen değişiklik sonucunda rastgeleliğin artırılması sağlanmıştır. Elde edilen yeni anahtar havuzundan dosya büyüklüğü kadar anahtar seçimi gerçekleştirilmiştir. Bu seçilen anahtar Vernam algoritması kullanılarak manipüle edilmiş dosya şifrelenmiştir. Üçüncü modülde anahtar havuzunun rastgele olarak yeniden oluşturulmasında kullanılan sıra bilgisi ve

anahtarın yeni anahtar havuzundan seçildiđi noktanın bilgisi alınarak manipölasyon modölü sayesinde steganografi yapılabilmesi kolaylaşan şifrelenmiş dosya üzerine gizlenmişlerdir. Dördündü modölde ise blokzincir teknolojisinin en önemli parçalarından olan özütleme algoritmalarından SHA256 kullanılarak dosyalar özütleştir. Bu özütleme değeri alıcı ve gönderici arasında doğrulama amaçlı olarak kullanılmış ve veri iletimi esnasında gerçekleşebilecek saldırı yahut çevresel faktörler sebebiyle meydana gelebilecek değışikliklerin engellenmesi sağlanmıştır.

**Anahtar Kelimeler:** Şifreleme, Steganografi, Blokzincir Teknolojisi, Özütleme Algoritmaları, Anahtar Dağıtım, Vernam Şifreleme Algoritması



# **HIGHLY SECURED INFORMATION EXCHANGE ALGORITHM USING ENCRYPTION AND STEGANOGRAPHY TECHNIQUES, BASED ON BLOCKCHAIN TECHNOLOGY.**

## **ABSTRACT**

Symmetric and asymmetric key encryption algorithms are used to ensure data security with encryption methods. As a result of the digitization of the data, the encryption process has been digitized as the mathematical calculations of encryption algorithms can be applied completely in the computer environment. Due to the security vulnerabilities seen after the use of the DES algorithm, which is accepted as the first security standard, it has been accepted as the data encryption standard of the AES encryption algorithm. These algorithms, which are examples of symmetric encryption, are symmetric-key encryption algorithms that are still widely used today. Vernam encryption algorithm, another symmetric encryption algorithm, was selected and used in our thesis. Unlike other symmetric encryption algorithms, Vernam encryption algorithm is one of the algorithms that is considered safe for the post-quantum period, due to its algorithmic complexity and the fact that it uses as many keys as the size of the file to be encrypted. Among the working issues encountered and open to improvement in the Vernam algorithm are the true randomness of key generation and securing the sharing of the key. For this reason, in our thesis, a modular algorithm has been developed that ensures safe transmission of all file types to the receiver. The manipulation algorithm developed as the first module has been developed in a way that allows all files to be converted into a single format, to prevent access to meaningful information, and to perform steganography. As a result of the change made on the key pools in the second module, the randomness was increased. Key selection was carried out according to the file size from the new key pool obtained. This selected key has been manipulated using the Vernam algorithm and the file has been encrypted. In the third module, the sequence information used in the random regeneration of the key pool and the information of the point where the key was selected from the new key pool were taken and they were hidden on the

encrypted file, which made steganography easier thanks to the manipulation module. In the fourth module, files were hashed using SHA256, one of the most important parts of blockchain technology, hash algorithms. These hash values have been used for verification purposes between the receiver and the sender, and it has been ensured that changes that may occur due to attacks or environmental factors during data transmission are prevented.

**Keywords:** Cryptography, Steganography, Blockchain Technology, Hash Algorithms, Key Distribution, Vernam Encryption Algorithm



# İÇİNDEKİLER

## Sayfa

|                                                                              |           |
|------------------------------------------------------------------------------|-----------|
| ÖNSÖZ.....                                                                   | iii       |
| ÖZET.....                                                                    | v         |
| ABSTRACT .....                                                               | vii       |
| İÇİNDEKİLER.....                                                             | ix        |
| KISALTMALAR .....                                                            | xi        |
| ÇİZELGELER LİSTESİ.....                                                      | xv        |
| ŞEKİLLER LİSTESİ.....                                                        | xvii      |
| <b>I. GİRİŞ.....</b>                                                         | <b>1</b>  |
| A. Literatür Taraması .....                                                  | 7         |
| B. Problem Tanıtımı .....                                                    | 25        |
| C. Önerilen Yöntem.....                                                      | 26        |
| D. Tezin Bilime Katkısı .....                                                | 27        |
| <b>II. DOSYA TÜRLERİ VE DOSYA MANİPÜLASYONU ALGORİTMASI ....</b>             | <b>29</b> |
| A. Dosya Türleri .....                                                       | 30        |
| B. Önerilen Dosya Manipülasyonu Algoritması .....                            | 31        |
| C. Manipülasyonu Testleri .....                                              | 33        |
| 1. PDF Dosya Türü Manipülasyonu ve Tersine Manipülasyonu .....               | 34        |
| 2. JPG Dosya Türü Manipülasyonu ve Tersine Manipülasyonu .....               | 39        |
| 3. DOC Dosya Türü Manipülasyonu ve Tersine Manipülasyonu.....                | 43        |
| 4. XLSX Dosya Türü Manipülasyonu ve Tersine Manipülasyonu .....              | 46        |
| D. Manipülasyonu Sonuçlarının Analizi .....                                  | 49        |
| E. Sonuç .....                                                               | 50        |
| <b>III. ŞİFRELEME .....</b>                                                  | <b>51</b> |
| A. İleri Şifreleme Standardı (Advanced Encryption Standard, AES).....        | 54        |
| B. Vernam Şifreleme Algoritması .....                                        | 54        |
| C. Üçlü Veri Şifreleme Standardı (Triple Data Encryption Standard, TDES) ... | 55        |
| D. Önerilen Algoritma .....                                                  | 56        |

|                                           |            |
|-------------------------------------------|------------|
| E. Test ve Analiz .....                   | 61         |
| F. Sonuç.....                             | 65         |
| <b>IV. STEGANOGRAFI .....</b>             | <b>67</b>  |
| A. Önerilen Steganografi Algoritması..... | 69         |
| B. Sonuç.....                             | 72         |
| <b>V. BLOKZİNCİR TEKNOLOJİSİ.....</b>     | <b>73</b>  |
| A. Önerilen Blokzincir Algoritması .....  | 78         |
| B. Sonuç.....                             | 80         |
| <b>VI. ANALİZ VE TARTIŞMA .....</b>       | <b>83</b>  |
| <b>VII. SONUÇ VE ÖNERİLER .....</b>       | <b>87</b>  |
| <b>VIII. KAYNAKÇA.....</b>                | <b>89</b>  |
| <b>EKLER .....</b>                        | <b>99</b>  |
| <b>ÖZGEÇMİŞ.....</b>                      | <b>169</b> |

## KISALTMALAR

- .3gp** : Third Generation Partnership Project (Üçüncü Nesil Ortaklık Projesi)
- .7z** : Compressed Archive File Format (Sıkıştırılmış Arşiv Dosya Formatı)
- .asp** : Active Server Pages (Aktif Sunucu Sayfası)
- .aspx** : Active Server Page Extended (Aktif Genişletilmiş Sunucu Sayfası)
- .avi** : Audio Video Interleaved (Ses Video Interleaved)
- .bmp** : Simple Raster Graphics Image File Format (Basit Raster Grafik Görüntü Dosyası Formatı)
- .dat** : Data file (Veri Dosyası)
- .dic** : Dictionary File (Sözlük Dosyası)
- .doc** : Word Processing Document Format (Word İşlem Belge Formatı)
- .docx** : Microsoft Word Document (Microsoft Word Dosyası)
- .exe** : Executable (Yürütülebilir)
- .flv** : File Format Used by Adobe Flash Player and Adobe AIR (Adobe Flash Player ve Adobe AIR Tarafından Kullanılan Dosya Biçimi)
- .gif** : Graphics Interchange Format (Grafik Değişim Formatı)
- .html** : HyperText Markup Language (Hiper Metin İşaretleme Dili)
- .jpg** : Digital Image Format Which Contains Compressed Image Data (Sıkıştırılmış Görüntü Verilerini İçeren Dijital Görüntü Formatı)
- .mdb** : Microsoft Access MDB File Format (Microsoft Access MDB Dosya Biçimi)
- .mdbx** : Access Based Database Files (Erişim Tabanlı Veritabanı Dosyalarına)
- .mid** : Musical Instrument Digital Interface File (Müzik Aleti Dijital Arayüz Dosyası)
- .mkv** : Matroska Multimedia Container (Matroska Multimedya Konteyneri)
- .mov** : QuickTime Video Format (QuickTime Video Formatı)
- .mp3** : MPEG-1 Audio Layer III (MPEG-1 Ses Katmanı III)
- .mp4** : Digital Multimedia Container Format (Dijital Multimedya Konteyner Formatı)

**.odt** : Open Document Text (Open Belge Metni)

**.ogg** : Ogg Vorbis Compressed Audio File (Ogg Vorbis Sıkıştırılmış Ses Dosyası)

**.ott** : OASIS' OpenDocument Standard Format (OASIS' OpenDocument Standart Formatı)

**.pdf** : Portable Document Format (Taşınabilir Döküman Formatı)

**.php** : HyperText Preprocessor (Hiper Metin Ön İşlemcisi)

**.png** : Portable Graphics Format (Taşınabilir Grafik Formatı)

**.ppt** : PowerPoint Presentation (PowerPoint Sunumu)

**.pptx** : Microsoft PowerPoint Open XML (Microsoft PowerPoint Açık XML)

**.psd** : The Native File Format of Adobe Photoshop (Adobe Photoshop'un Yerel Dosya Biçimi)

**.rar** : Roshal Archive Compressed File (Roshal Arşivi Sıkıştırılmış Dosya)

**.rtf** : Rich Text Format (Zengin metin formatı)

**.tar** : Tape Archive (Teyp Arşivi)

**.txt** : Text (Metin)

**.uot** : Uniform Office Document (Tekdüze Ofis Belgesi)

**.wav** : Waveform Audio File Format (Dalga Formu Ses Dosyası Formatı)

**.wmv** : Windows Media Video (Windows Medya Video)

**.xls** : Microsoft Excel's Workbook File (Microsoft Excel Çalışma Kitabı Dosyası)

**.xlsx** : Standard Extension for the Modern Microsoft Excel Spreadsheet Files (Modern Microsoft Excel Elektronik Tablo Dosyaları için Standart Uzantı)

**.zip** : Archive File Format (Arşiv Dosya Biçimi)

**AES** : Advanced Encryption Standard (İleri Şifreleme Standardı)

**AHCI** : Arts and Humanities Citation Index (Sanat ve Beşerî Bilimler Atıf Dizini)

**BPP** : Bits Per Pixel (Piksel Başına Bit Sayısı)

**BTC** : Bitcoin

**CNN** : Convolutional Neural Network (Evrişimli Sinir Ağı)

**CP-ABE**: Ciphertext-Policy Attribute-Based Encryption (Şifreli Metin İlkesi Öznitelik Tabanlı Şifreleme)

**DCT** : Discrete Cosine Transform (Ayrık Kosinüs Dönüşümü)

**DES** : Data Encryption Standard (Veri Şifreleme Standardı)

**DWT** : Discreate Wavelet Transform (Ayrık Dalgacık Dönüşümü)

**ETH** : Ethereum

**GAN** : General Adversarial Network (Üretken Düşman Ağları)

**IoT** : Internet of Things (Nesnelerin İnterneti)  
**KB** : Kilobayt  
**LFSR** : Linear Feedback Shift Register (Doğrusal Geri Besleme Kaydırma Kaydı)  
**MB** : Megabayt  
**MD5** : Message-Digest Algorithm 5 (Mesaj Özeti Algoritması 5)  
**MÖ** : Milattan Önce  
**ms** : Milisaniye  
**MSE** : Mean Squared Error (Ortalama Kare Hatası)  
**NCC** : Normalized Cross Correlation (Normalleştirilmiş Çapraz Korelasyon)  
**NFC** : Near Field Communication (Yakın Alan İletişimi)  
**NSA** : National Security Agency (Ulusal Güvenlik Ajansı)  
**OMR** : Optical Mark Recognition (Optik İşaret Tanıma)  
**OTA** : Ozyavas-Takaoglu-Ajlouni  
**OTP** : One Time Pad (Tek Seferlik Şerit)  
**PEKS** : Public Key Encryption with Keyword Search (Anahtar Kelime Arama ile Açık Anahtar Şifreleme)  
**PoW** : Proof-of-Work (İş Kanıtı)  
**PoW-BC**: Proof-of-Work-and-Block-Compression (İş Kanıtı ve Blok Sıkıştırma)  
**PSNR** : Peak Signal Noise Ratio (Tepe Sinyal Gürültü Oranı)  
**RBML**: Rule Based Machine Learning (Kural Tabanlı Makine Öğrenimi)  
**RSA** : Rivest-Shamir-Adleman  
**SCI** : Science Citation Index (Bilim Alıntı Endeksi)  
**SCI-E** : Science Citation Index Expanded (Science Citation Index Genişletildi)  
**SGX** : Software Guard Extension (Yazılım Koruma Uzantısı)  
**SSCI** : Social Sciences Citation Index (Sosyal Bilimler Atıf İndeksi)  
**SSMI** : Structural Smilarity Index Measure (Yapısal Benzerlik İndeksi Ölçüsü)  
**TÜBİTAK** : Türkiye Bilimsel ve Teknolojik Araştırma Kurumu  
**UIQI** : Universal Image Quality Index (Evrensel Görüntü Kalitesi İndeksi)  
**URL** : Uniform Resource Locator (Tekdüzen Kaynak Bulucu)  
**VANET**: Vehicular Ad Hoc Network (Araç Özel Ağı)  
**YÖK** : Yükseköğretim Kurulu



## ÇİZELGELER LİSTESİ

### Sayfa

|                                                                                 |    |
|---------------------------------------------------------------------------------|----|
| Çizelge 1 Şifreleme ve şifre çözme süreleri (ms).....                           | 62 |
| Çizelge 2 AES, 3DES ve önerilen yöntem şifreleme ve şifre çözme sonuçları ..... | 63 |





## ŞEKİLLER LİSTESİ

### Sayfa

|                                                                            |    |
|----------------------------------------------------------------------------|----|
| Şekil 1 Manipülasyon ve tersine manipülasyon blok diyagramı.....           | 33 |
| Şekil 2 PDF bayt tekniğiyle manipülasyon grafiği.....                      | 35 |
| Şekil 3 PDF arabelleğe alma yöntemiyle manipülasyon grafiği .....          | 36 |
| Şekil 4 PDF tersine bayt manipülasyonu grafiği.....                        | 37 |
| Şekil 5 PDF tersine ara bellek tekniği manipülasyonu grafiği.....          | 38 |
| Şekil 6 JPG bayt tekniğiyle manipülasyon grafiği .....                     | 39 |
| Şekil 7 JPG arabelleğe alma yöntemiyle manipülasyon grafiği.....           | 40 |
| Şekil 8 JPG tersine bayt manipülasyonu grafiği.....                        | 41 |
| Şekil 9 JPG tersine ara bellek tekniği manipülasyonu grafiği.....          | 42 |
| Şekil 10 DOC bayt tekniğiyle manipülasyon grafiği.....                     | 43 |
| Şekil 11 DOC arabelleğe alma yöntemiyle manipülasyon grafiği .....         | 44 |
| Şekil 12 DOC tersine bayt manipülasyonu grafiği.....                       | 44 |
| Şekil 13 DOC tersine ara bellek tekniği manipülasyonu grafiği.....         | 45 |
| Şekil 14 XLSX bayt tekniğiyle manipülasyon grafiği.....                    | 46 |
| Şekil 15 XLSX arabelleğe alma yöntemiyle manipülasyon grafiği .....        | 47 |
| Şekil 16 XLSX tersine bayt manipülasyonu grafiği .....                     | 47 |
| Şekil 17 DOC tersine ara bellek tekniği manipülasyonu grafiği.....         | 48 |
| Şekil 18 Simetrik anahtarlı şifreleme çalışma prensibi.....                | 53 |
| Şekil 19 Yeni anahtar havuzu elde edilme yöntemi .....                     | 58 |
| Şekil 20 Önerilen algoritma gönderici tarafı blok diyagramı .....          | 59 |
| Şekil 21 Önerilen algoritma alıcı tarafı blok diyagramı .....              | 60 |
| Şekil 22 Önerilen algoritma şifreleme sonuçları grafiği.....               | 62 |
| Şekil 23 Önerilen algoritma şifre çözme sonuçları grafiği .....            | 63 |
| Şekil 24 Steganografi ve tersine steganografi diyagramları.....            | 71 |
| Şekil 25 SHA256 algoritması ile şifrelenmiş dosya özütlenmesi.....         | 78 |
| Şekil 26 Blokzincir eklentisi alıcı ve gönderici için akış diyagramı ..... | 80 |
| Şekil 27 Önerilen algoritma modülleri .....                                | 84 |



## I. GİRİŞ

Bilgi tarih boyunca hep kıymetli olmuş ve korunması için çeşitli uğraşlar verilmiştir. Bilgi yani dijital haliyle verinin başkaları tarafından fark edilmemesi üzerine ve tespit edilse de erişilememesi üzerine çalışmalar yürütülmektedir. Bu hususta üzerinde durulması gereken iki nokta steganografi ve kriptoloji kavramlarıdır. Steganografi kelime kökü olarak Yunancadan gelen ve gizli yazı anlamına gelen bir çalışma prensibidir. Steganografide yapılmaya çalışılan şey verinin çeşitli yöntemler kullanılarak gizlenmesidir (Şahin vd., 2021). Gizlenen yani başkaları tarafından tespit edilemeyen bir şeyin elde edilmesi için dikkat harcanmasına gerek yoktur. Tarih boyunca düzgün uygulanmış ve insanlar tarafından tespit edilemeyen bir steganografi çalışmasının veriyi koruma başarısı hep yüksek olmuştur. İlk örnekleri olarak kabul edilen MÖ 440 yılında yaşandığı Herodot tarafından aktarılan ve iki Yunan kralının birbirine güvendikleri bir kölenin saçlarını kazıtıp yazdıkları bilgiyi kölenin saçlarının uzaması sonrasında diğer krala göndererek gerçekleştirmişlerdir. Yine Antik Yunanda balmumu tabletleri kullanılarak bilgi gönderimi yapıldığı bilinmektedir. Örnekleri verilen bu steganografi çalışmaları fiziksel steganografi olarak bilinmektedir (Basuki ve Rosiyadi, 2019). Diğer bir steganografi çalışması ise dijital steganografidir. Bilgisayar teknolojisinin yaygınlaşması neticesinde sahip olunan imkanlar kullanılarak, dijitalleşen veri dijital ortamda gizlenmeye çalışılmıştır. Bit seviyesinde yapılan bu gizleme çalışmaları zamanla geliştirilmiş tüm dosya türlerinde kullanılacak şekilde yeni yöntemler geliştirilmiştir (Ajlouni vd., 2021).

Dijital verinin gizlenmesinde kullanılan dosya türünün seçilecek yöntem açısından önemi bulunmaktadır. Ses, video, metin, görüntü gibi dosya türlerinde veri gizleme yöntemleri geliştirilmiştir. Steganografi uygulanması kolay, üzerinde akademik çalışmaların yapılması ekonomik bir çalışma prensibidir. Ortalama bir bilgisayar gücü ile kolaylıkla gizlenmek istenen veriler kapak-multimedya diye isimlendirilen verinin gizlendiği dosya türlerinde saklanır. Bu

sebeple özellikle geliřmekte olan ÷lkelerde yahut teknolojiye ulaşmanın pahalı olduđu coğrafyalarda steganografi konusu çokça çalışılmaktadır (Giron vd., 2021).

Steganografik ürünler yani stego-multimedya diye isimlendirilen ve içinde gizlenmiş veri olan dosyaların tespit edilmesi için çeşitli yöntemler kullanılmaktadır. Bu yöntemlere steganaliz yöntemleri denilmektedir (Kasapbasi, 2019). Özetle steganaliz yöntemlerinde yapılan işlem, elde edilebilmişse orijinal dosya ile ellerine geçen dosyayı karşılaştırmak ve bit seviyesinde gör÷len deęişikliklerin tespit edilmesidir. Yahut histogram analizleri kullanarak steganografik ürünlerde farklılık tespit edilmektedir (Mohsin vd., 2021). Anlaşılacağı üzere birçok steganografi teknięi olduđu için bu tekniklere uygun steganaliz ve histogram analiz yöntemleri geliştirilmektedir. Doğal olarak bu tarz tespit yöntemlerinin devlet seviyesinde desteklenen resmi organizasyonlarca sürdür÷ldüğü düşün÷ldüğ÷nde ve internetin dahi anlık olarak taranması ile gerçekleştirilmeye çalışıldığı düşün÷ldüğ÷nde, steganografi yahut şifreleme yöntemleriyle gizlenen ve korunan verilere gösterilen ilginin ne kadar yüksek olduđu anlaşılabilir.

Amerikan Ulusal Güvenlik Ajansı (National Security Agency, NSA) gibi kuruluşlar interneti anlık ve sürekli inceleyebilme imkanlarına sahip oldukları için veri gizlenmiş birçok stego-multimedya çalışmasını tespit etmekte ve gizlenen veriyi elde etmek için çeşitli analiz çalışmaları yürütmektedirler (Takaoğlu ve Takaoğlu, 2019).

Bir dięer veri koruma yöntemi ise şifreleme algoritmalarıdır (Lin, 2019). Şifrelemenin ilk örnekleri MÖ 1900 yıllarında antik Mısır'da gör÷lmüştür. Anlaşılacağı üzere şifreleme bilimi yahut çalışmaları insanlık tarihi ile yaşıt bir konumdadır. Antik Yunan ve Roma imparatorluğu dönemlerinde de gör÷len şifreleme çalışmaları genellikle askeri amaçlarla kullanılmıştır. Yine verinin dijitalleşmesi neticesinde şifreleme çalışmaları bilgisayar ortamında sürdür÷lmeye başlanmış ve bu alanda çok ciddi tecrübeler elde edilmiştir. Günümüzde sahip olunan hesaplama gücü kullanılan bilgisayarlarda çok daha hızlı işlem yapabilme katkısı sağlamasının yanı sıra asıl şifreleme ve matematiksel hesaplamalarda büyük katkı sağlamaktadır. Verinin güç olarak kabul edildięi 21 yüzyılda veri güvenliği çok büyük bir önem taşımaktadır. Veri

güvenliğinin sağlanmasında şifreleme ve özüt (hash) algoritmalarından faydalanılmaktadır. Şifreleme algoritmalarının gücü sahip oldukları algoritmik karmaşıklık ve anahtar paylaşımının güvenliğine dayanır. Bu sayede işlem gücü artan bilgisayarlarca yapılan kaba kuvvet ataklarına karşı korunaklı bir ortam sağlanmış olur (Li vd., 2021).

Bilgisayarlarda kullanılan işlemciler üzerine düşünülmesi gerekmektedir. Bilindiği üzere kuantum fiziği doğurmuş olduğu yeni soruların yanı sıra insanlığın ihtiyaç duyduğu birçok soruya cevap getirmekte ve insanlığa katkı sağlamaktadır. Günümüzde satın alınan bilgisayarların tamamı silikon bazlı işlemcilere sahiptir. Silikon bazlı işlemciler için Gordon Moore tarafından tanıtılan ve Moore Kanunu olarak bilinen bir durum söz konusudur (Moore, 1965). Kısaca Moore kanunu işlemci içindeki transistör sayısının her iki yılda bir iki katına çıkacağını ve işlemci boyutunun da ufalacağını, maliyetlerin ise aynı kalacağını hatta azalacağını ifade eden bir kanundur. Günümüzde kullanılan işlemciler ve sahip oldukları boyut ve transistör miktarları incelendiğinde Moore kanununa göre silikon bazlı işlemcilerin sahip olabilecekleri hesaplama gücünün sonlarına yaklaşıldığı kabul edilmektedir. Bu şu anlama gelir, günümüzde kullanılan süper bilgisayarlar da dahil olmak üzere tüm silikon bazlı işlemci kullanılan bilgisayarlarda elde edilen işlem gücünün arttırılabilmesi için yeni donanımlara veya yeni yöntemlere ihtiyaç duyulacaktır. Dağıtık hesaplama yöntemleri bu amaçla birçok farklı metot kullanarak çözümler getirmiş, paralel hesaplama ve dağıtık mimarilerle umut vadeden çalışmalar ortaya koyulmuştur. Ancak kuantum fiziği prensiplerinden faydalanılarak üretilen kuantum bilgisayarları, önerildikleri ve geliştirildikleri ilk hallerinden çok daha kullanıma erişilebilir bir hal almıştır. Bu sebeple günümüzde birçok kuantum bilgisayarını geliştiren firma, kendi sistemlerine erişimi ücretsiz ve serbest bırakmakta ve akademik yahut ilgili kişilerin istedikleri çalışmaları yapmalarına imkân sağlamak için ücretsiz hizmetler sunmaktadırlar. Kuantum hesaplama ya da kuantum bilgisayarları, sahip oldukları mimari ve foton yani ışık kullanılması sebebiyle çok hızlı çalışabilen bilgisayarlardır. Şifreleme algoritmaları ise daha önce ifade edildiği üzere algoritmik karmaşıklık ve anahtar dağıtımının güvenlik seviyesi kadar güvenli kabul edilmektedir. Bu sebeple günümüz süper bilgisayarlarının yıllar içerisinde

kaba kuvvetle kırabileceği düşünölen şifreleme algoritmalarını kuantum hesaplama sayesinde saniyeler içerisinde kırılabilir bir hale gelmektedir. Khirshoff'a göre geliştirilen ve algoritması kimseyle paylaşılmayan bir şifreleme algoritmasının dahi nasıl çalıştığının herkesçe bilindiğı düşünölerek hareket edilmesi ve güvenlik katmanlarının buna göre geliştirilmesi gerekmektedir. Bu sebeple kuantum hesaplama gücüne karşı verinin korunması için kullanılacak şifreleme algoritmalarının çok doğru seçilmesi, geliştirilecekse post kuantum dönem diye adlandırılan döneme dayanıklı olacak şekilde geliştirilmesi gerekmektedir. Algoritmik karmaşıklık olarak post kuantum dönem için dayanıklı olduğı düşünölen Advanced Encryption Standard, AES256 ve One-time-pad, OTP gibi şifreleme algoritmalarının şimdiden geliştirilen sistemlerde güvenliğin sağlanmasında kullanılması düşünölebilir (Lin vd., 2021). Bu algoritmalarda ise önemli olan husus anahtar paylaşımıdır. Anahtarı istenmeyen bir tarafın eline geçmiş şifreli verinin güvenliğınden söz etmek mümkün değildir. Bu sebeple anahtar paylaşımının güvenliğınin sağlanmasında gerek kuantum anahtar dağıtım yöntemleri gerekse de Diffie-Hellman gibi anahtar paylaşım yöntemleri kullanılmaktadır (Liang vd., 2021).

Verinin korunması hususunda bir diğör yöntem ise blokzincir teknolojisidir. Blokzincir teknolojisi aslında kriptoloji (şifreleme) ve bilgisayar bilimlerinin ortak çalışma konusudur (Takaoğlu ve Güneş, 2019). Blokzincir diye adlandırabileceğimiz ilk örnek 90'lı yıllarda Stuart Haber ve W. Scott Stornetta isimli iki kriptografin dosya arşivlemek için geliştirdikleri zaman damgası (timestamp) yöntemi kabul edilebilir. Ardından dijital paralar (e-Cash gibi), oyun paraları gibi çeşitli çalışmalar olmuştur. Ralph C. Merkle'nin 70'lerde tanıtmış olduğı Merkle ağacı algoritması ve hash algoritmalarında görölen yenilikler, blokzincir teknolojisinin bu denli ilgi çekmesinde en önemli etken olarak kabul edilen Bitcoin (BTC) kripto parasının tüm bu bilgi birikimlerinin doğru birleştirilmesi sonucunda elde edilmesini sağlamıştır. Nedir bu Bitcoin sorusundan önce neden Bitcoin çıktı sorusunu sormak daha doğru olacaktır. Satoshi Nakamoto sessizliğe gömölmeden önce Bitcoin'in tanıtımı için yapmış olduğı çalışmalarda birçok soruya cevap vermiş ve önermiş olduğı fikri tanıtmaya çalışmıştır. Bilindiğı üzere dünya birçok ekonomik kriz yaşamış ve bu krizlerin birçoğı da Amerika kökenli krizler olmuştur. Yaşanan krizler

incelendiğinde gerek II. Dünya Savaşında altın temelli para basımı prensibinin terk edilmesi ve karşılıksız para basılması ve bu durumun kamu ile çok geç paylaşılması, 2008-2012 yıllarında yaşanan Amerikan konut kredilerinde görülen çöküş sebebiyle dünyayı derinden etkileyen krizde de bankaların insanlara paylaştığı verilerin doğru olmaması sebep olmuştur.

Çünkü paylaşılan veriler incelendiğinde hiçbir sorun gözükmediği gibi insanların konut kredi fonlarına yatırım yapmalarını teşvik edecek veriler paylaşılmış, ayrıca alım gücü olmayan insanlara çok kolay bir şekilde konut kredileri verilmiştir. Kredilerin tahsislerinde karşılaşılan olumsuzluklar dahi doğru bir şekilde kamu ile paylaşılmamıştır. Birçok ekonomik krizde benzer sebepler büyük sorunlara sebebiyet vermiştir (İşler vd., 2019). Satoshi bu sebeple merkezi otoriteyi aradan çıkartmak ki bu örnekte merkezi otorite olarak bankacılık sistemini dikkate alabiliriz, yerine ademi merkeziyetçi bir sistem getirilmesini önermiştir. Bitcoin arada resmi bir otorite olmadan insanlar tarafından değerli olduklarını kabul ettikleri dijital bir kripto para transferi neticesinde alışveriş yapılmasını sağlamaktadır. Kara para ve illegal aktivitelerin finanse edilmesi amacıyla geliştirildiği ileri sürülse de önerilen fikrin bilimsel açıdan incelenmesinde tarafsız olunması gerekmektedir. Geline nokta Satoshi'nin önermiş olduğu merkezi otoriteyi ortadan kaldıran ve insanların söz sahibi olduğu, her şeyin şeffaf ve anonim olduğu bir evren tasviri aslında çökmüştür. Çünkü birçok finansal kuruluş ve bankalar kripto paraları aynı altın ya da döviz gibi bir değer olarak kabul edip, vermiş oldukları hizmetlerin arasına kripto para çözümlerini de ekleyerek bu yeniliğe ayak uydurmuştur (Takaoğlu vd., 2019). Devletlerin de gerekli hukuksal düzenlemeleri yapmaya başlaması ve kendi ekonomilerini, milli paralarını bu platforma çekmek suretiyle bu değişime ayak uydurmaları teoride Satoshi'nin elde etmek istediği dünya düzenine erişmesini imkânsız bir hale getirmiştir. Peki dünya ekonomisini bu denli değiştiren Bitcoin kripto parasının bizi yani bilgisayar bilimlerini ilgilendiren kısmı nedir?

Bitcoin kripto parasını üreten akla blokzincir teknolojisi denilmektedir. Blokzincir teknolojisi insanlığa dağıtık ve güvenli bir veri tabanı hizmeti sunmaktadır. Bilindiği üzere günümüzde kullanılan veri tabanlarının bulut tabanlı olanları dahil birçoğu merkezi yapıdadır. Nihayetinde hedef alınabilecek

bir veri tabanı bulunmakta ve güvenlik katmanlarını aşabilecek güçte bir saldırı yöntemi kullanan kişilerce elde edilebilir yahut kullanılamaz hale getirilebilir yapıdadır. Blokzincir teknolojisi bloklardan oluşan ve güvenliğinin özüt (hash) algoritmalarıyla sağlandığı bir mimariye sahiptir. Blokzincir teknolojisini dağıtık defter teknolojisi de denilmektedir. Çünkü aynı bir defterin sayfalarında olduğu gibi her bir blok bir sayfa gibi gerçekleştirilen işlemlerin kayıtlarıyla doldurulmakta ve bu defter sisteme erişim hakkı olan tüm düğümlerde bulunmaktadır. Bitcoin blokzincir sisteminde her bir blok 1 MB boyutunda tasarlanmıştır. Daha sonra görülen ölçeklenebilirlik sorunları sebebiyle 2 MB'a çıkartılan blok boyutları her bir coin gönderimi sırasında oluşan ve işlem diye adlandırılan ve bloklara kaydedilen yaklaşık 258 baytlık bir veri üretimi söz konusudur. Bu veriler blokzincire erişim hakkı olan düğümlerce %51 oranında kabul edildikten sonra blok yani deftere kaydedilir ve defterin son hali tüm düğümlerle paylaşarak verinin dağıtıklığı sağlanmış olmaktadır (Yu vd., 2020).

Blokzinciri oluşturan bloklar birbirleriyle özüt algoritması kullanılarak bağlanmaktadır. Bilinenin aksine blokzincir sistemlerinin korunmasında şifreleme algoritmalarından daha çok hash algoritmalarına güvenilmektedir. Çünkü özüt algoritmaları girilen bir veri için tek yönlü olarak benzersiz bir değer üreten algoritmalarlardır. Örneğin SHA256 özüt algoritması kullanılarak “Merhaba Dünya!” özütlendiğinde elde edilen değer ile “MERHABA DÜNYA!” cümlesinden elde edilecek değer farklı olacaktır. Girilen veride yapılan en ufak değişiklik farklı bir özüt değeri elde edilmesine neden olmaktadır. Bu sebeple hash algoritmaları blokzincir sistemlerine kurcalanamamazlık, İngilizce tabiri ile tamper-proof bir yapı kazandırmaktadır. Bloklar bu özüt değerleri kullanılarak birbirlerine bağlanmaktadır. Bir önceki blokta gerçekleşen en ufak bir değişiklikte o blok, zincir dışına çıkartılmakta ve eski haline gelmeden sisteme dahil edilmemektedir. Bu sebeple blokzincir sistemlerine kaydedilen bir verinin değiştirilebilme mümkün olmamakta, gönderilen bir kripto para da geri alınamamaktadır (Wang ve Li, 2021).

Blokzincir sistemleri Bitcoin örneğinde olduğu gibi halka açık yani public olabileceği gibi gizli yani private yapıda da olabilir. Ayrıca konsorsiyum ve karma blokzincir yapılarında da olabilir. Bu bize verinin blokzincir sisteminde

kaydedilmesi sonrasında başkaları tarafından incelenebilmesinin engellenmesini sağlar. Günümüzde 2009 yılından bu yana gerçekleşmiş tüm Bitcoin işlem geçmişini halka açık bir halde incelenmeye müsait bir yapıdadır. Bu durum verinin gizlenmesi gerektiği durumlarda sorun olarak karşımıza çıkmaktadır. Blokzincir teknolojisi kripto para ve finans ile sınırlı olmayan bir yapıda olduğu için farklı alanlarda blokzincir teknolojisi uygulandığında şeffaflık yahut anonimlik bir sorun oluşturabilmektedir (Partala, 2018).

Günümüzde blokzincir teknolojisi akla gelebilecek her alanda uygulanmaya çalışılmaktadır. Çünkü Ethereum platformu başta olmak üzere birçok blokzincir geliştirme platformu insanlığın hizmetine sunulmuş ve akıllı sözleşmeler gibi yenilikler sayesinde blokzincir sistemleri statik yapıdan daha dinamik bir hal almaya başlamıştır. Doğal olarak blokzincir teknolojisi birçok alanda kullanılabilir bir hal almaya başlamıştır. Teknolojinin her yeni uygulama alanı tecrübe edildiğinde yeni sorunlar ortaya çıkmakta ve yeni çözüm yöntemlerine ihtiyaç duyulmaktadır. Hali hazırdaki sistemlere blokzincir sistemi bir katman olarak eklenebilir yapıdadır ayrıca tümüyle blokzincir teknolojisinden faydalanarak sistemler geliştirmek de mümkündür (Pranto vd., 2021).

Blokzincir teknolojisi aynı steganografi ve şifreleme algoritmalarında sağlanan veri gizlenmesi ve veri güvenliği konusunda yenilikçi çözümler sunmaktadır. Bu sebeple tez çalışmamızda blokzincir teknolojisinden, steganografi ve şifreleme tekniklerinden faydalanılarak yüksek güvenli bir veri iletim algoritması üzerinde durulmuştur. Tez çalışmamızın ilerleyen bölümlerinde gerçekleştirilen çalışmalar ve elde edilen sonuçlar ayrıntılı olarak paylaşılmıştır.

#### **A. Literatür Taraması**

Tez çalışma süreci YÖK tarafından belirlenen maksimum 6 yıl 12 dönemlik süreçte tamamlanabilmiştir. Bu süreç içerisinde tezimizde konu alınan blokzincir, steganografi ve şifreleme üzerine 10 adet çeşitli çalışmalar yapılmıştır. Bu çalışmaların hepsi literatüre katkı sağlamış bazıları kendi alanlarında ilk olma özelliği taşımaktadır. Gerçekleştirmiş olduğumuz tez çalışmasının bir başka benzeri bulunmamaktadır. Bu sebeple birçok katmandan

oluşan algoritmamızın tanıtımı sırasında modüler yapıda geliştirdiğimiz algoritmanın daha iyi tanıtılması için hem gerçekleştirmiş olduğumuz akademik yayın çalışmalarını paylaşmak hem de bu çalışmaları gerçekleştirirken literatürde bulunan benzer çalışmaları paylaşmayı hedeflemiş bulunmaktayız.

A Novel and Robust Hybrid Blockchain and Steganography Scheme (Takaoğlu vd., 2021) isimli çalışma tezimizden üretilmiş olup Q2 dereceli SCI-E bir dergide yayınlanmıştır. Bu çalışmada literatüre blokzincir steganografisi kavramı kazandırılmıştır. Steganografide kullanılan steganaliz yöntemleri tümüyle işlevsiz hale getirilmiş ve herhangi bir kapak-multimedya (cover-multimedia) içine istenilen boyutlarda bilgi gizlenmesine imkân sağlamaktadır. Bu kazanımların sağlanmasında en önemli etken geliştirmiş olduğumuz Ozyavas, Takaoğlu, Ajlouni yani OTA algoritmasıdır. OTA algoritması iki ayaaktan oluşmaktadır. İlk ayağında kapak-multimedya içerisine gizlenecek bilgiler geliştirilen yeni işaretleme yöntemi ile kaydedilir. 1 KB'lık dizilerin doldurularak yapıldığı bu tekrarlamalı işlem sonucunda saklanmak istenen bilgi çeşitli arama türlerinden arzu edileni kullanılarak gizlenir. 2, 3, 4, ..., 9 bitlik arama örgüleri kullanılarak gizlenmek istenen veri kapak-multimedya içine gizlenir/işaretlenir. Bu işaretleme işlemlerinin adresleri dizilerde saklanır ve bu diziler blokzincir sistemi gizli (private) yapıda olmasına rağmen diğer düğümlerce görülmesin diye şifrelenir. OTA algoritmasının ikinci ayağı ise OTA blokzincir aşamasıdır. Bu gizli blokzincir sisteminde en küçük transfer edilebilen coin miktarı 1 OTA coindir. Her bir transferde kendi geliştirdiğimiz blok yapısı sayesinde 1 KB'lık veri girişi imkânı olmaktadır. Şifrelenmiş 1 KB'lık diziler 1 OTA coin harcanarak alıcıya iletilir. Blok yapısında ayrıca URL bilgisinin girildiği bir bölüm bulunmaktadır. URL bilgisi kapak-multimedya alıcı ile paylaşılırken çevresel etkenlerden etkilenmesin diye gizli bir serverda saklanarak blokzincir üzerinden alıcıya iletilir. Serverda saklanan kapak-multimedya başkalarının eline geçerse hiçbir güvenlik riski doğurmaz çünkü saklanan kapak-multimedya üzerinde gizlenmiş hiçbir bilgi bulunmamaktadır. Bir başka deyişle kapak-multimedya üzerinde steganaliz yöntemlerinin tespit edebileceği herhangi bir değişiklik yapılmamaktadır. Tüm steganografik bilgiler blokzincir sisteminde saklanmakta olup başkalarının ulaşamayacağı bir yapıdadır. Tüm bu sistem steganografiye blokzincir

steganografisi adı altında yeni bir çalışma konusu eklemiş olup, sadece steganografi amacıyla geliştirilmiş ilk blokzincir sistemi olması açısından da ayrı bir öneme sahiptir. Yapılan steganografik işlemin tespit edilebilmesi ve gizlenen verinin elde edilebilmesi mümkün değildir.

Sarkar ve arkadaşları önermiş oldukları Stego-chain isimli çalışmalarında (Sarkar vd., 2020) Robert's edge detection yöntemi ile birlikte blokzincir sistemi önermişlerdir. Bu çalışmadaki amaçları resimdeki köşe alanları genişleterek gizleme kapasitesini arttırmaktır. Steganografi işlemi sonrası elde edilen stego-resim AES ile şifrelenmiştir. Daha sonra bu dosya ufak karelere bölünüp blokzincir üzerinden alıcıya gönderilmiştir. Alıcı da elde ettiği karelerden stego-resmi elde ettikten sonra anahtarı kullanarak tersine adımları izleyip bilgiye ulaşmaktadır. Bu alanda önerilmiş sayılı çalışmalardan biri olsa da blokzincir teknolojisinin imkanları tam olarak kullanılmıştır diyemeyiz. Çünkü elde edilen stego-resimin AES ile şifrelenmesi düzgün planlanmış bir gizli blokzincirde gereksiz bir işlemdir. Stego-resmin gizli bir blokzincirde, düğümlerin sadece kendi işlemlerini görebildikleri bir ortamda, geleneksel steganografi kurallarına uyarak iletimini sağlamak çok verimli bir yol olmayabilir. Bir stego-resmin ufak matrixlere bölünerek alıcıya iletilmesi hem oluşacak işlem sayısı olarak hem de harcanacak süre ve enerji dikkate alındığında tercih edilebilir bir yöntem olmayabilir. Ayrıca tanıtılan stego-chain blokzincir sistemiyle ilgili teknik bilgiler yeterli değildir. Gerçekleşen işlemlerin diğer düğümler tarafından onaylanıp blokzincire kaydedilmesi süreciyle ilgili ve ödül ve önerdikleri güvenilirlik mantığı ile ilgili yeterli teknik bilgiler paylaşılmamıştır. Çalışmanın blokzincir kısmı ile ilgili paylaşılan tablo ve görseller tatmin edici seviyede değildir. Steganografi kısmının çok daha kuvvetli olduğu bu çalışmanın blokzincir steganografi alanında yayınlanan sayılı indeksli çalışmalardan biri olması sebebiyle önemi büyüktür.

Mohsin ve arkadaşlarının önermiş oldukları particle swarm optimizasyonu algoritması (Mohsin vd., 2021) üzerinde ufak değişiklikler yapılarak, COVID19 verilerinin blokzincir teknolojisi vasıtasıyla güvenli bir şekilde korunması ve iletimi amaçlanmıştır. Birden fazla kapak-resim kullanılmış ve her kapak-resimde en optimal veri saklanacak yerler seçilerek hareket edilmiştir. Steganografi yapılan stego-resimlere özüt değerleri eklenmiş ve kurcalama

yapılıp yapılmadığı bu özüt değerleri kontrol edilerek incelenmiştir. Blokzincir steganografi çalışması olması ve pandemi sürecinde COVID19 verileri ile çalışması planlanan bir çalışma olmasına rağmen bazı konularda akıl karıştırıcı bilgiler paylaşılmıştır. Blokzincir kullanılan bir sistemde stego-resimleri özüt ile kurcalanamaz hale getirmek aynı işi iki kere yapmaktan ve karmaşıklığı arttırmaktan başka bir işe yaramayacaktır. Blokzincir düğümleri tarafından onaylanmış bir işlemin üzerinde değişiklik yapılması durumunda sistemden uzaklaştırıldığı herkesçe bilinen bir özelliktir. Ayrıca makalenin iddialar ve limitler kısımlarında paylaşılan 1. ve 2. madde doğru sayamayacağımız bilgiler paylaşılmaktadır. 1. Maddede ifade edilen özüt algoritmasının covid verisini saklarken kullanılmasının data bütünlüğü güvence altına aldığı ve literatürde kendi önerdikleri yöntem gibi covid verilerinin bütünlüğüne odaklanmış çalışma olmadığı bilgisi isabetli değildir. Çünkü gerek özüt fikirleri daha önce ifade edildiği üzere mantıklı bir fikir değildir, gerekse de literatürde salgın öncesi sağlık verilerinin bütünlüğünün sağlanması üzerine yayınlanmış birçok çalışma bulunmaktadır. Hatta önerilen sistemler o kadar kapsayıcıdır ki gizlenen verinin COVID19 verisi olup olmadığının hiçbir önemi bulunmamaktadır. Ayrıca 2. Maddede ifade edildiği üzere literatürdeki tüm steganografi metotlarının veriyi bir host resimde sakladığı bilgisi de kesin olarak doğru değildir. Literatürde birden fazla kapak-resim kullanarak bilgi gizlenen birçok çalışma bulunmaktadır. Bu tarz çok temel konularda isabetsiz bilgiler paylaşılması ve gerçek veriyle sistemlerini test etmemeleri dışında Blokzincir Steganografi üzerine yayınlanmış ilk indeksli bir çalışmalardan olması sebebiyle değerlidir.

Basuki ve Rosiyadi önermiş oldukları işlem steganografisi ve resim steganografisi yöntemleriyle (Basuki ve Rosiyadi, 2019) gizli ve güvenli bir veri iletim sistemini elde etmeyi başarmışlardır. Ethereum sistemini kullanarak geliştirdikleri yöntem ile şifrelenmiş gizli bilgi ile geleneksel görüntü steganografisi yapılmaktadır. Bu aşamada partition number, image url ve access time gibi bilgiler oluşturulmaktadır. Bu bilgiler kullanılarak işlem steganography dedikleri aşamaya geçilmektedir. Transaction field selection, embedding method ve parsing method olmak üzere üç aşamada uygulanan işlem steganografisi ile blokzincir steganografisi olarak örnek gösterilecek emsalsiz bir çalışma gerçekleştirmişlerdir. Yazarlar çalışmalarında hem steganografi hem

de blokzincir sistemlerini çok doğru incelemiş ve önerdikleri sistemde kullanma başarıları göstermişlerdir.

Partala (Partala, 2018) önermiş olduğu cover communication çalışmasında blokzincir ve least significant bit, LSB kullanarak kuvvetli bir sistem önermiştir. Göndericinin her işlemde 1 bit veri gizlemesi yaparak gönderilecek bilgiyi bir dizi işlem sonucunda karşı tarafa iletmesi sonucunda gerçekleşen bu sistemde hem blokzincir sistemi doğru tasarlanmış hem de veri gizlenmesi başarıyla gerçekleşmiştir. Bu çalışmada zayıflık olarak öne sürülecek tek şey süredir. Yaklaşık olarak 1 bayt veri gönderimi için 1 saatten daha fazla veri zaman harcanmaktadır. Her bir bit için 1 işlem yapılması da ayrıca büyük boyutlu bir veride çok ciddi işlem sayılarına ulaşılmasına ve sistemin uzun süreli kullanımında blokzincirde ölçekleme sorunlarına sebebiyet verebilir. Ancak teorik olarak önerilen sistem mükemmel en yakın şekilde çalışan ve literatürde görülen en iyi çalışmalardan biridir.

Hornig ve arkadaşları önerdikleri yöntemiyle (Hornig vd., 2021) belirledikleri kapak-resimleri blok permutasyonu kullanarak şifrelemişlerdir. Şifreledikleri hasta verilerini de histogram shifting yöntemini kullanarak şifreledikleri kapak-resim içine gizlemişlerdir. Blokzincir sisteminde gerçekleştirilen bu yöntem ile hem güvenli veri iletimi sağlanmış hem de gömme oranı 0.8 bpp gibi bir seviyede sağlanmıştır. Çalışmalarında önerdikleri yöntem blokzincir steganografisi için çok güzel bir örnektir. Ancak hastane gibi çok sayıda hasta verilerinin bulunduğu bir ortamda gizlenen görüntülerin çözünürlüklerinin yüksek olması, bir başka deyişle gizlenen verinin boyutunun büyük olduğu bir veri setinde önerilen sistemde blokzincir sisteminin çalışma süresi, şifreleme süreçleri ve steganografi adımlarının gerçekleştirilmesi çok ciddi zamanlar alacak ve gerçek hayatta önerilen sistemin hastanelerin sahip oldukları teknolojik altyapı ve imkanlar göz önüne alındığında kullanılabilirliği olası gözükmemektedir.

Xu ve arkadaşları çalışmalarında (Xu vd., 2018) açık blokzincir işlemleri üzerinden geliştirdikleri yöntemle steganografi yöntemi önermişlerdir. Göndericinin blokzincir madencisi olması gerektiği ifade edilmiştir. Seçilen işlemler üzerinde bir seri işlemler yaparak yeni bir blok oluşturulması ve bu steganografik bilgilerin bu blokta kaydedilmesi önerilmiştir. Bu çalışmanın

realitede uygulanabilirliđi çok büyük soru işaretleri taşımaktadır. Çünkü günümüzde açık/genel blokzincir olan birçok sistemde madencilerin çok güçlü bir işlem gücüne sahip olmaması durumunda blok oluşturabilmeleri mümkün değildir. Hepsinden önemlisi, çalışmalarında önerdikleri tarzda bir blok oluşturup bir açık (public) blokzincirin yeni bloku olarak kaydetmeleri de pek mümkün değildir. Çünkü her blokzincirin yaratılış (genesis) blokunda tanıtılan özellikler doğrultusunda yeni işlem bilgileri oluşturulur ve kayıt işlemi gerçekleştirilir. Mazdutt ve arkadaşlarının yapmış oldukları çalışmada (Mazdutt vd., 2018) Bitcoin blokzincirinde sistemin ürettiđi verilere benzemeyen 1600 işlem kaydının yapıldığını ortaya koymuştur. Bu veri girişleri kolaylıkla tespit edilebildiđi gibi bu tarz veri kayıtlarının engellenmesi için çalışmalar sürdürölmektedir. Xu ve arkadaşları oluşturdukları steganografik verileri açık bir blokzincirin blok yapısında fark edilmeden nasıl kaydedeceklerini ifade etmemişlerdir. Steganografinin fark edilmeme ilkesine uygun olmayan bu yöntemin realitede gerçekleşebilme ihtimali çok düşüktür.

Giron ve arkadaşları blokzincirleri steganografik analiz yöntemi (Giron vd., 2021) önererek incelemişlerdir. Çalışmalarında blokzincir sistemi üzerinde steganografi teknikleri kullanarak veri gizleme yöntemlerinin tespit edilmesine çalışılmıştır. Ancak yapmış oldukları kapsamlı araştırma ve incelemeler sonucunda açık blokzincir sistemleri üzerinde steganografi yapıldığına dair bir delil bulamamışlardır. Ancak literatürde önerilen blokzincir steganografisi çalışmalarında görölen steganografinin yanlış kullanılması üzerine tespitlerde bulunulmuştur. Sequential analysis ve Clustering analysis dedikleri steganaliz yöntemlerini 625,941 bitcoin ve 6 milyon ethereum bloku ve 98 milyon bitcoin kümesi üzerinde denemişlerdir. Yapılan çalışma bu alanda daha fazla çalışmanın yapılmasına ihtiyaç duyulduđunu gözler önüne sermiştir.

Doktora eğitimi sürecinde yapılan bir diđer çalışma ise steganografi konusunun ayrıntılı bir şekilde araştırılması ve elde edilen bilgilerin alan yazın formatında yayınlanmasıdır. Bu amaçla Review of the Literature on the Steganography Concept (Şahin vd., 2021) isimli makale Amerikan ve hakemli bir dergide yayınlanmıştır. Çalışmada steganografinin tarihçesi ve farklı alanlardaki uygulamaları incelenmiştir. Görüntü, video, ses, metin ve protokol steganografisi incelenmiştir. Steganografi teknikleri iki başlık altında

incelenmiştir. Protokol steganografisi; ayrık Fourier dönüşümü tekniği, ayrık kosinüs dönüşümü tekniği ve ayrık dalgacık dönüşümü tekniği başlıklarında incelenmiştir. Uzamsal alan yöntemleri; en az önemli bitler, optimal piksel ayarlama prosedürü, piksel değer farkı, kenar tabanlı veri gömme yöntemleri başlıklarında incelenmiştir.

A Survey of Artificial Intelligence Driven Blockchain Technology: Blockchain Intelligence (Ajlouni vd., 2021) isimli çalışma İngiliz bir hakemli dergide yayımlanmıştır. Bu çalışmada blokzincir teknolojisi ayrıntılı olarak anlatılmış ve yapay zekâ ile blokzincir teknolojisinin birlikte kullanımı üzerinde durulmuştur. Blokzincir zekâsı kavramı literatüre sunulan yeni kavramlardan biridir ve akademik çalışmalarda üzerinde durulan sayılı çalışmalardan biri olarak bizim çalışmamızda ele alınmıştır. Yapay zekanın blokzincir sistemlerine nasıl uygulanabileceği ve elde edilebilecek kazanımlar üzerinde görüşlerimiz paylaşılmıştır.

Blokzincir Temelli Milli Bağış Zinciri Projesi (Takaoglu vd., 2021) isimli akademik çalışmamız hakemli bir uluslararası bir konferansta sözlü olarak sunulmuştur. Önermiş olduğumuz fikir anonimliğin çok yüksek olduğu ve ihtiyaç sahipleri ile yardımseverleri bir araya getiren yardımlaşma platformudur. Kamu kuruluşlarıyla birlikte yürütülmesi zorunlu olan bu proje fikrinde ihtiyaç sahiplerinin bilgileri resmi kamu kuruluşlarından gelecek olup hazırlanan web sitesinde yardımseverlerin önüne kripto cüzdan numarası çıkartan bir arama motoru şeklinde düşünülmüştür. Aylık asgari ücret seviyesini geçen yardım alan cüzdanların geliştirmiş olduğumuz mekanizma sayesinde arama motorunca ön plana çıkartılmayacağı ve yardım almayan cüzdanların ön planda tutulacağı bir sistemdir. Kripto para ve kripto cüzdanların blokzincir teknolojisi ile sağlandığı, kullanıcı ile etkileşimin web sitesi üzerinden gerçekleştiği sosyal yardımlaşma projesidir. Proje fikri ilgili bakanlık tarafından incelenmesi amacıyla iletilmiş ancak maalesef olumlu bir geri dönüş alamamıştır. İstanbul Büyükşehir Belediyesi'nin açmış olduğu proje duyusuna gönderilmiş, ilk aşamayı geçmiş ancak ülkemizde gerçekleştirilebilmesi noktasında yeterli altyapı ve gelişmişliğin olmaması sebebiyle kabul edilmemiştir. İlerleyen süreçte bu proje fikrinin uygulanabilmesi için yeni girişimlerimiz olacaktır.

AviChainDB: Blockchain Integration on Aviation Databases (Takaoğlu vd., 2021) isimli çalışma OSTIV Meteorological Panel’de sözlü olarak tanıtılmıştır. Havacılık sektöründe gerek ülkemizin sivil havacılık kurumları gerekse de askeri amaçlı kullanımlarında dünyanın önde gelen havacılık yazılım firmalarından hizmetler alınmaktadır. Çoğunlukla Amerikan olan bu yazılım firmalarının kuruldukları ülkenin Amerika olması ve Vatanseverlik Kanunu gereği talep edilmesi halinde ellerinde tuttukları verileri Amerikan ilgili devlet teşkilatları ile paylaşmak zorunda olmaları sebebiyle Türkiye olarak kendi havacılık veri tabanımızın olması gerekmektedir. TUSAŞ bu konu ile ilgili bir proje toplama duyurusu yapmış bu bağlamda üniversitemiz adına blokzincir teknolojisi ile havacılık veri tabanı önerisi geliştirilip bu duyuruya katılım sağlanmıştır. Yapılan çalışma sırasında önermiş olduğumuz yöntemlerden TUSAŞ’a gönderilmemiş olan bu panelde kısaca tanıtılmış ve akademik bir yayın haline getirilmiştir. Özetle önerilen sistem karma bir çözüm sunmaktadır ve fikrin geliştirilebilmesi için havacılık veri tabanları üzerine çalışan ilgili birimlerle birlikte çalışılması gerekmektedir.

Yazıcı Steganografisi ve Sarı Nokta Analizinin Günümüzde Geçerliliği (Takaoğlu ve Takaoğlu, 2020) makalesi ve Yazıcı Steganografisi, Sarı Nokta Analizi – Bir Mini Derleme (Takaoğlu ve Takaoğlu, 2019) isimli makalede fiziki steganografi olarak adlandırılan günümüz yazıcılarında uygulanan steganografi ele alınmıştır. Her iki dergi de hakemli ve uluslararası yapıda olup Dergipark sistemi üzerinde tanıtılan dergilerdir. Yazıcı steganografisi yazıcılarda halen uygulanmaya devam eden ve çıktı alınan kağıtlarda fark edilmeyecek şekilde iz bırakarak yapılan bir işlemdir. İlk olarak sahte para üretimine engel olmak için yapıldığı ileri sürülse de yakın süreçte Amerika’da basına sızdırılan devlet sırlarının kim tarafından basınla paylaşıldığının tespitinde çıktı alınmış kâğıt incelenerek hangi yazıcıdan alındığı bulunmuş ve yazdırma emrini veren kişiye ulaşılmıştır. Her yazıcı firmasının kendi standartlarında uygulamış olduğu bu tahrifat öncelikle etik olmamakla birlikte çeşitli güvenlik kaygılarını da birlikte getirmektedir. Her iki çalışmamızda bu konular üzerinde durulmuş ve ayrıntılı bilgi paylaşımı yapılmıştır.

Blokzinciri Teknolojisi ve Türkiye’deki Muhtemel Uygulanma Alanları (Takaoğlu vd., 2019) isimli çalışmamız hakemli ve uluslararası Dergipark’ta

taranan bir dergide yayınlanmıştır. Blokzincir teknolojisi için 2019 yılına kadar yapılmış çalışmaların ayrıntılı bir şekilde ele alındığı ve Türkiye'nin blokzincir uygulamalarına nasıl dahil olabileceği ve güçlü, zayıf, geliştirilmeye açık yönlerinin ele alındığı bir araştırma makalesidir. Çok sayıda atıf alan bu çalışmamızda yapmış olduğumuz tespitlerin ne denli isabetli olduğu 2022 yılı şartları altında incelendiğinde daha iyi anlaşılmaktadır.

Blokzinciri ve Kripto Paraların İnsanlığa Etkileri (İşler vd., 2019) isimli makalede kripto paralar ve blokzincir teknolojisi geniş bir şekilde tanıtılmış ve insanların göstermiş oldukları ilgi üzerine çalışma yürütülmüştür. Bilim felsefesi konusunda çalışmalar yürüten Ufuk Fatih Küçükali Hocamızın da katkıları ile birlikte blokzincir teknolojisinin ve kripto paraların insanlara etkisi felsefi bir boyutta ele alınmıştır. Doktora çalışmalarında, özellikle mühendislik konularında yapılan tez çalışmalarında görülen tek boyutlu çalışmaların değişmesi ve geniş kapsamlı araştırmaların yapılabilmesi açısından tezimiz için önemli bir çalışma olmuştur.

Yükseköğretimde Blokzincir Teknolojisi (Takaoğlu ve Güneş, 2019) isimli çalışmamız uluslararası bir konferansta sözlü olarak tanıtılmıştır. Üniversitelerin sistemlerine blokzincir sistemlerinin entegrasyonu üzerinde durulan bu çalışmamızda 2019 yılına kadar yapılmış veya önerilmiş teorik ve uygulamalı örnekler ele alınarak neler yapılabileceği üzerine bilgiler paylaşılmıştır. 2022 yılında dahi birçok üniversitede blokzincir konusu üzerine çalışan öğrenci kulüpleri, araştırma merkezleri ve hatta devlet araştırma merkezlerinde bulunan stratejik öneme sahip organizasyonlarda bu alanda yapılan çalışmalar maalesef yeterli seviyenin çok uzağındadır. Bu bağlamda yapmış olduğumuz çalışmanın ülkemizdeki üniversitelerin blokzincir teknolojisini nasıl kendi sistemlerine entegre edebilecekleri üzerine bilgi paylaşması açısından önem taşımaktadır.

(Kasapbaşı, 2019) çalışmasında, Huffman veri sıkıştırma algoritmasıyla kodlanmış ve sıkıştırılmış Türkçe metinleri gizlemek için yeni fraktal akış şifreleme algoritması kullanılarak yeni bir uzaysal alan kaotik steganografi şeması sunulmaktadır. Hem şifreleme hem de steganografinin birlikte kullanılması açısından önemli bir çalışmadır. Ayrıca çalışmada elde edilen Peak Signal Noise Ratio, PSNR, Stractural Smilarity Index Measure, SSIM,

Universal Image Quality Index, UIQI, Mean Squared Error, MSE ve histogram analizi sonuçları emsal çalışmalara kıyasla umut verici seviyededir.

(Tabares-Soto vd., 2021) yapmış oldukları çalışmada dijital resim steganografisinde kullanılan steganaliz yöntemlerinin doğruluğunu Convolutional Neural Network, CNN algoritmaları kullanarak arttırmayı amaçlamışlardır. Çalışmalarında eğitim süresini 6 saatten aşağıda tutmuşlar ve iyileştirme olarak da %2 ile %10 arasında iyileştirme sağlamışlardır. Steganaliz yöntemlerinin nasıl çalıştığının anlaşılmasında ve iyileştirilmesi hususunda yapılabileceklerin daha iyi anlaşılabilmesi açısından bu çalışma büyük bir öneme sahiptir.

(Kaito ve Miyata, 2021) yapmış oldukları çalışmada Shamir sır paylaşım yöntemini kullanarak şifrelenmiş gizli veriyi korelasyon temelli, spread spectrum yöntemi ve analizi ile birlikte kullanarak steganografik olarak gizlemektedir. Elde ettikleri sonuçları SSMI verileri üzerinden değerlendirmişlerdir.

(Subramanian vd., 2021) görüntü steganografisi üzerine yapmış oldukları alan yazın çalışmasında steganografi konusu ayrıntılı bir şekilde tanıtmışlardır. Özellikle derin öğrenme algoritmalarının görüntü steganografisi üzerinde uygulanabilirlikleri üzerine odaklanmışlardır. Convolutional Neural Network, CNN, General Adversarial Network, GAN ve geleneksel yöntemleri üzerinde durulmuştur. Elde edilen sonuçlar özet bir şekilde paylaşılmıştır.

(Setiadi vd., 2017) çalışmalarında Discrete Cosine Transform, DCT yani ayırık kosinüs dönüşünü algoritması ile OTP şifreleme algoritmasını birlikte kullanarak veri gizleme işlemi gerçekleştirmişlerdir. Çalışmanın sonuçları incelendiğinde elde edilen PSNR ve Normalized Cross Correlation, NCC değerleri kabul edilebilir seviyelerde çıkmıştır. Her ne kadar önerilen algoritma ileri seviyede olmasa dahi şifreleme ve gizleme işlemlerinin birlikte yapılması açısından güzel bir örnektir.

(Saad vd., 2021) önermiş oldukları yeni algoritmalarıyla steganaliz yöntemlerine karşı dayanıklı ve kapaksız (coverless) diye tanıttıkları görüntü Optical Mark Recognition, OMR ve Rule Based Machine Learning, RBML algoritmalarının birlikte kullanımı ile oluşturulmuş algoritmalarını test

etmişlerdir. Yenilikçi ve akıllıca bir çözüm önerilen çalışmanın incelenmesi bu alana ilgi duyan akademisyenler açısından faydalı olacaktır.

(Wahab vd., 2021) önermiş oldukları algoritmalarında Rivest-Shamir-Adleman, RSA şifreleme algoritması ve steganografi sıkıştırma tekniklerini kullanarak bir çalışma gerçekleştirmişlerdir. Huffman kodlaması yani kayıpsız sıkıştırma algoritmasından faydalanılmıştır. Discrete Wavelet Transform, DWT yani dağıtık dalgacık dönüşümü algoritmasından faydalanılmıştır. Denedikleri yöntem güzel olmakla birlikte, PSNR gibi başarı kriterlerine göre çok yüksek bir başarı elde edildiğini söylemek pek mümkün değildir.

(Li vd., 2020) yapmış oldukları çalışmada kablosuz iletişimin şifrelenmesinde OTP şifreleme algoritması ve anahtar üretimi üzerine odaklanmıştır. Ağlara yöneltilen çeşitli saldırı modelleri tanıtılmıştır. Anahtar üretim süreçleri hakkında bilgi verilmiş ve kendi kullanmış oldukları algoritma tanıtılmıştır. OTP algoritmasının farklı alanlarda kullanımının incelenmesi ve anahtar üretim ve paylaşım süreçleriyle ilgili paylaşılan bilgiler açısından faydalı bir çalışmadır.

(Boakye-Boateng vd., 2019) çalışmalarında OTP algoritmasını temel olarak emsal çalışmalarla kıyaslandığında paket kaybı olmayan, daha kısa zaman ve enerji harcayan bir algoritma üzerinde çalışmışlardır. Algoritmalarını kablosuz ağlarda test etmişlerdir. OTP kullanımında da rastgele numara üreticiden faydalanmışlardır. Elde ettikleri sonuçlar olumlu yönde değerlendirilebilir.

(Gebremichael vd., 2019) önermiş oldukları yöntemle kaynak sıkıntısı olan IoT ağlarında kullanılmak üzere güvenli bir anahtar oluşturma algoritması önermektedirler. Eliptik eğri kriptografisinden ve tek yönlü kriptografik akümülatörlerden faydalanılmıştır. Üretilen anahtarların güvenliğinin nasıl sağlanacağıyla ilgili de bilgiler paylaşılmıştır.

(Raj vd., 2020) çalışmalarında multilayer linear feedback shift register (LFSR) şifreleme algoritmasını kullanarak veri güvenliğini sağlamayı amaçlamışlardır. Sinyal iletiminde kullanılmak üzere çok katmanlı olarak One-Time-Pad algoritması kodlanmıştır. Simülasyon neticesinde elde ettikleri sonuçlar çalışmalarında paylaşılmıştır.

(Manucom vd., 2019) çalışmalarında OTP şifreleme algoritması için büyük bir önem taşıyan anahtar üretimi ve üretilen anahtarın gerçek rastgele olması durumu üzerinde durmuşlardır. Anahtar üretimi için kendi algoritmalarını önermişlerdir. Bu algoritma özetle gerçek anahtar üretim algoritması ve Fisher-Yates karıştırma algoritmasını kullanmaktadır. Yapmış oldukları test ve analizler sonucunda önermiş oldukları algoritmanın karmaşıklık ve tekrar edilmeme yani gerçek rastgele olma durumuna daha yakın olduğunu göstermiştir. Tam bir rastgelelik için günümüzde fiziki cihazlar kullanılmaktadır. Bu cihazlarda doğa olayları taklit edilerek gerçek bir rastgele anahtar üretimi yapılmaktadır. Fiziki bir cihaz desteği olmadan rastgele bir numara üretmek ve bunu güvenlik sistemlerinde anahtar olarak kullanmak risk taşımaktadır. Bu sebeple anahtar üretim hususunda algoritmik seviyede karmaşıklığı arttıracak eklentiler yapılması gerekmektedir. Yapılan çalışma literatürde bu alanda yapılan az sayıdaki çalışmalardan biridir. Tezimizde de benzer sorunun giderilmesi için çalışılmıştır.

(Hamid ve Abdullah, 2015) yapmış oldukları çalışmalarında fiziksel kimlik doğrulamasında rastgele numara üretilen ve OTP algoritması temel alınarak çalışan bir algoritma önermişlerdir. Rastgele anahtar üretimi ve OTP algoritmasının fiziksel bir uygulamada test edilmesi ve sonuçlarının paylaşılması açısından önem arz etmektedir.

(Pablos vd., 2020) çalışmalarında kuantum sonrası dönem için anahtar değişim algoritması önermişlerdir. Kyber isimli bu algoritma ile kuantum hesaplama gücüyle yapılabilecek saldırılarla karşı dayanıklı bir ortam oluşturmak amaçlanmıştır. Kyber algoritmasında 4 turlu bir grup kimliği doğrulanmış anahtar değişimi geliştirilmiştir. Elde ettikleri simülasyon sonuçları emsal çalışmalarla karşılaştırılmıştır.

(Ejaz vd., 2021) çalışmalarında simetrik blok şifreleri için güvenli bir protokol geliştirmiş ve dinamik permutasyonlar kullanarak simetrik blok şifreleri tasarlamışlardır. Elde ettikleri sonuçları ülkelerinin Ulusal Teknoloji ve Standartlar Enstitüsünün belirlemiş olduğu test ve istatistikleri kullanarak paylaşmış ve olumlu yönde sonuçlar almışlardır. Geliştirmiş oldukları sistemin 192 ya da 256 bitlik anahtar boyutları için de geliştirilebilir olduğunu paylaşmışlardır.

(Furtak, 2020) çalışmasında kriptolojik anahtar üretimi ve yenilenmesi üzerine bir sistem önermiştir. Önerilen bu sistem nesnelerin interneti ağında bulunan düğümlerce kullanılacak şekilde geliştirilmiştir. Bir konsept olarak önerildiği için çok yaygın bir uygulama alanı yoktur ancak yeni bir fikrin planlanması, geliştirilmesi ve tanıtımı açısından güzel bir çalışmadır.

(Belghazi vd., 2019) çalışmalarında kablosuz ağların güvenli hale getirilmesi için akıllı bir ortamda nesnelerin interneti cihaz-cihaz iletişimini önermiş oldukları anahtar değişim algoritmasını kullanarak yapmayı amaçlamışlardır. QR kod, Diffie-Hellman anahtar paylaşım algoritması ve SHA256 özüt algoritması kullanılmıştır.

(Stulman ve Stulman, 2019) çalışmalarında MANET’lerde bulunan dalgalı topolojiyi kullanarak anahtar paylaşım tekniği üzerinde çalışmışlardır. Önermiş oldukları algoritma saldırılara karşı sahip olduğu dinamik ve sürekli değişen topolojik yapısı sayesinde yüksek seviyede dayanıklıdır.

(Aliyev vd., 2020) yapmış oldukları çalışmada araçlar arasında iletişimin sağlanmasında ölçeklenebilir ve güvenli grup anahtar yönetim ve paylaşım algoritması önermişlerdir. Önermiş oldukları algoritma emsal çalışmalarla karşılaştırıldığında %80 oranda daha hızlı çalışmıştır.

(Choudhary vd., 2020) çalışmalarında sanayi nesnelerin interneti için hızlı kimlik doğrulama ve anahtar değişim protokolü üzerine çalışmışlardır. Önermiş oldukları algoritmanın diğerlerinden daha iyi olduğunu iddia etmekte ve enerji tüketimi ve saldırılara karşı güvenli olması açısından elde ettikleri sonuçların emsallerinden daha iyi olduğunu açıklamışlardır. Bu ve benzeri çalışmalar anahtar dağıtım sürecinde karşılaşılan sorunlar ve giderilmesi için yürütülen çalışmaların görülmesi açısından tezimiz için öneme sahiptir.

(Roy ve Khatwani, 2017) çalışmalarında eliptik eğri kriptolojisi temel olarak kimlik doğrulama ve anahtar değişimi protokolü önermiş ve bunun kriptanalizini yapmışlardır. Bu doğrultuda denial of service, man in the middle, weak authentication ve SQL injection gibi saldırılara dayanıklı olacak bir algoritma geliştirmeye çalışmışlardır.

(Lee ve Lee, 2018) yapmış oldukları çalışmada dinamik grup kimlik doğrulaması ve anahtar değişimi algoritması önermişlerdir. Türkçeye

çevrildiğinde şeylerin interneti diye isimlendirilebilecek IoT İngilizce kavramını sır paylaşım eşiği temel alınarak ölçülebilir akıllı ortamlar için geliştirmişlerdir.

(Liu vd., 2018) çalışmalarında grup anahtar paylaşımı algoritması geliştirmişlerdir. Bu algoritma da VANET ağı için geliştirilen literatürdeki güzel çalışmalardan biridir. Önermiş oldukları algoritmanın güvenlik ve verim açısından kendilerinden daha düşük sonuçlar almış çalışmalara göre karşılaştırılması yapılmıştır.

(Mihalkovich vd., 2020) çalışmalarında deterministik olmayan tam karar vermek problemi temel alınarak grup arasında iletişimin olmadığı bir anahtar dağıtım algoritması üzerinde durmuşlardır. Geliştirdikleri algoritmanın diğer birçok benzer çalışmada eksik olan kuantum kriptanaliz yöntemlerine karşı kendi çalışmalarında önlem almışlardır.

(Alvarez vd., 2017) araştırmalarında kullanılan anahtar dağıtım algoritmalarını incelemişlerdir. Kullanılan algoritmaların performans ve gereksinimleri üzerinden bir araştırma yapılmış ve elde edilen sonuçlar paylaşılmıştır.

(Kim vd., 2020) çalışmalarında sağlık sektöründe kullanılmak üzere kablosuz iletişim ağında parola doğrulamalı anahtar değişim algoritması geliştirmişlerdir. Aslında geliştirdikleri algoritma daha önce yapılmış bir çalışmada bulunan eksikliklerin iyileştirilmesi sayesinde olmuştur. Elde edilen yöntem güvenlik açısından kendisinden öndeki algoritmaya göre daha başarılıdır.

(Wang ve Li, 2021) yapmış oldukları çalışmada hastane verilerini korumak için Healthchain ismiyle bir blokzincir sistemi geliştirmişlerdir. Gizlilik ihtiyaçlarının sağlandığı teorik olarak ispatlanan bu ve benzeri birçok sağlık alanındaki blokzincir çalışmalarının tasarımsal ve gerçek hayat uygulamalarından uzak kalan gereksinim analizleri sebebiyle uygulanabilir olması pek mümkündür değildir. Özellikle sağlık sektöründe üretilen verilerin boyutlarında karşılaşılan büyük alan ihtiyaçları sadece blokzincir sisteminden ziyade karma sistemlerin düşünülmesi gerekliliğini doğurmaktadır.

(Yoon vd., 2020) yapmış oldukları ve SPEKS ismini verdikleri çalışmada public key encryption with keyword search, PEKS diye bilinen yönteme SGX

yani software guard extension ismi verilen ortamını ekleyerek yapmışlardır. %80'lik bir hesaplama süresinde iyileştirme görülmüştür.

(Lin, 2019) yapmış olduğu çalışmada sosyal ağlarda kullanılmak üzere ikili doğrulamalı şifreleme algoritması üzerinde durmuştur. Eliptik eğri şifrelemesi ve Diffie-Hellman anahtar dağıtımı konuları esas alınarak ilgili çalışma gerçekleştirilmiştir. Önermiş olduğu algoritmanın güvenlik değerlendirmelerini teorik ve simülasyon sonuçlarını paylaşarak yapmıştır.

(Park vd., 2021) çalışmalarında sağlık verilerinin paylaşımında karşılaşıldığını iddia ettikleri güvenlik açıklığı ve veri sızdırılması durumuna çözüm getirmek amaçlı proxy bir server kurup bu server üzerinden şifreli metinleri tekrar şifreleyerek güvenlik sorununun giderilmesini amaçlamışlardır. Daha önceki birçok sağlık üzerine blokzincir entegrasyonu çalışmalarında görüldüğü üzere bu çalışmada da sorun tespiti ve çözümü hususunda getirilen yöntemin geçerliliği tartışmaya açık bir konudur. Blokzincir teknolojisi üzerine dergilerde hakemlik yapan akademisyenlerin bu alanda çok yetkin kişilerden oluşmaması sebebiyle günümüzde SCI, SCI-E, AHCI ve SSCI gibi birçok indeksli dergide yapılan yayınlarda kalite sorunu görülmektedir. Tezimizde bu doğrultuda yapılan yayın çalışmalarında maalesef gerçekçi olmayan akademik makaleler ile karşılaşılmış ve bu alanda yeni olan akademisyenlerin aklını karıştıracak nitelikte hataların olduğu görülmüştür.

(Yeom vd., 2021) yapmış oldukları çalışmada işveren ve çalışan arasında sözleşmelerin yönetildiği bir blokzincir sistemi geliştirmişlerdir. Sözleşme ayrıntıları ve çalışan bilgilerinin gizli tutulması için şifreli anahtar kelime mekanizması geliştirmişlerdir. Bu sayede gizli tutulmak istenen verilerin güvenliği sağlanarak erişimi gerçekleştirilebilir bir hal almıştır.

(Yuan vd., 2020) çalışmalarında Türkçe çevirisi Heterojen Kablosuz Algılayıcı Ağlar için Eşleşmesiz Kimlik Tabanlı Dijital İmza Algoritmasına Dayalı Bir Anahtar Yönetim Şeması olan önerilerini tanıtmışlardır. Algoritmalarında eliptik eğri kriptolojisinden faydalanmışlardır. Önerilen algoritmanın simülasyon ve test sonuçları paylaşılmıştır.

(Chen vd., 2018) çalışmalarında dinleme ve takip etme saldırılarına karşı güvenli bir sistem önermişlerdir. Kablosuz sensor ağlarında sizli anahtar

dağıtımı ve işaretleme tekniklerinden faydalanılarak saldırganlara karşı dayanıklı bir sistem önermişlerdir. Teorik analizi ve simülasyon testlerinde elde edilen sonuçlar paylaşılmıştır.

(Hussein vd., 2020) çalışmalarında akıllı kablosuz sensor ağlarında kullanılmak üzere dağıtık anahtar yönetim sistemi önermişlerdir. Önermiş oldukları bu yöntem ile eliptik eğiri kriptolojisinden de faydalanarak IoT temelli kablosuz sensor ağlarının güvenliğinin arttırılması amaçlanmıştır.

(Goumide vd., 2021) çalışmalarında araç bulut hesaplaması için maliyeti düşük, güvenli doğrulama ve anahtar dağıtımı yöntemi önermişlerdir. Çalışmalarında CP-ABE algoritması anahtar dağıtımında kullanılmıştır. Algoritmalarını AVISPA yazılımını kullanarak test etmiş ve elde edilen sonuçları paylaşmışlardır.

(Meng ve Li, 2021) yapmış oldukları çalışmalarında katmanlı bir veri paylaşım mekanizması için geliştirmiş oldukları çözüm önerisini tanıtmışlardır. Özel bir blokzincir sistemi geliştirmişlerdir. Aidiyet temelli şifreleme algoritmasından faydalanmışlardır. Ayrıca sistemdeki cihazların daha rahat tespit edilebilmesi için cihaz kapasite sistemi geliştirmişlerdir. Önermiş oldukları algoritmalarını çeşitli testlere tabi tutarak elde ettikleri sonuçları paylaşmışlardır.

(Lin vd., 2021) çalışmalarında kaos temelli senkron dinamik anahtar üretimi ve bu anahtarların görüntü dosyalarının şifrelemesinde AES algoritması için kullanımını önermişlerdir. Önermiş oldukları algoritmanın anahtar depolamada karşılaşılan sorunlara karşı çözüm getirdiğini açıklamaktadırlar. Bu iddialarını çeşitli istatistiksel analizler kullanarak kanıtlamışlardır.

(Rivero-Garcia vd., 2017) yapmış oldukları çalışmada hastaların kullanması ön görülen NFC bilekliklerin hasta bakıcıların mobil uygulamalarınca izlenebildiği katmanlı bir sistem önerilmiştir. Bunun yapılabilmesi için kimlik temelli doğrulama ve anahtar paylaşım sistemi geliştirmişlerdir. Özütleme algoritmalarından da faydalanılarak doğrulama süreci gerçekleştirilmiştir.

(Pranto vd., 2021) çalışmalarında nesnelerin interneti ve akıllı tarım uygulamalarda kullanılmak üzere blokzincir ve akıllı sözleşme kullanımından

faydalananarak bir sistem önermişlerdir. Blokzincir teknolojisinin kullanılması şeffaf, güvenli ve sağlam bir platform elde edilmesini sağlamıştır.

(Hussein vd., 2019) çalışmalarında tıbbi verilerin yönetimi için geliştirilen blokzinciri sistemi tanıtılmıştır. Diğer birçok sağlık üzerine yapılan blokzincir çalışmalarında görülen benzeri, teoriden öteye geçmesi çok güç, gereksinim analizi ve gerçek hayat uygulamasının iyi düşünülmediği çalışmalardan biridir. Simülasyon ortamında düşük gecikme hızı elde edildiği görülmüş bu durumda sağlık sektöründe önemli bir fark doğuracağı paylaşılmıştır.

(Yu vd., 2020) yapmış oldukları araştırmada PoW algoritması esas alarak blok sıkıştırma ekleyerek yeni bir algoritma önermişlerdir. Önerdikleri algoritmaya Pow-BC ismini vermişlerdir. Bu sayede blok boyutlarının ufaltılması ve bu sayede işlem veriminin artırılmasını enerji kullanımının düşürüleceğini düşünmüşlerdir. Yaptıkları testler ile bu görüşlerini destekleyici argümanlar üretmek istemişlerdir. Ancak benzer bir durum Bitcoin örneğinde yaşanmış, Bitcoin ekibi blok boyutunu arttırma yolunu seçmiştir. Bu makalede blok boyutunun düşürülmesi fikri daha çok blok üretimine sebebiyet verecek, bu durum ölçeklenebilirlik sorununu karşımıza çıkartacaktır. Bu sebeple önerilen algoritmanın uygun olacağı blokzincir sistemleri olabilir ancak her durum için uygun bir konsensüs algoritması olduğunu söylemek çok mümkün değildir.

(Rodriguez-Garcia vb., 2021) yaptıkları çalışmada sağlık sektöründe kullanılmak üzere blokzincir sistemi geliştirmişlerdir. Kullanıcıların yani hastaların verilerine erişim izinlerinin de düşünüldüğü, gizlilik, anonimite, güvenlik gibi kaygıların dikkate alınarak geliştirildiği gizli/özel bir blokzincir platformudur. Emsal çalışmalara göre çok daha iyi planlanarak hazırlanılmış bir çalışmadır.

(Javed vd., 2021) çalışmalarında blokzincir teknolojisinden faydalananarak geliştirmiş oldukları katmanlı mimari sayesinde sistemlerinde gizlilik, güvenlik ve sistem işletme maliyetlerini optimal seviyede tutmaya çalışmışlardır. Bu sistem dağıtık araç ağlarında kullanılmak üzere tasarlanmıştır. Elde edilen simülasyon ve test sonuçları makul seviyelerdedir.

(Belkhouja vd., 2018) yapmış oldukları çalışmada simetrik şifreleme yapısına sahip kaotik Henon sistemini kullanarak donanımların da dahil

olabileceği kablosuz ağlarda tıbbi amaçlı kullanılan cihazların güvenliğini amaçlamaktadır. Daha önce kendi araştırma konularımızdan biri olarak sıraya aldığımız ve sağlık verileri için güvenli blokzinciri sistemi konusuna çok yakın olan bu çalışmada, blokzincir teknolojisi kullanılmadan sağlık sistemlerinde veri iletimini koruma altına almaya çalışmışlardır. Dana önce yabancı bir devlet bakanına yapılan siber saldırı neticesinde kalp pili bilgileri saldırganların elinde olması sebebiyle hastanın kalp pili hedef alınmış ve kalp pili sisteminin durdurulması başarılmıştır. Bu saldırı sonucunda söz konusu bakan hastaneye yetiştirilip tedavi altına alınmış olsa da bu tür siber saldırıların yapılması durumunda insanların ne kadar çaresiz kalacakları aşîkardır. Bu sebeple literatür taramasında inceleme fırsatı bulduğumuz bu çalışma ele aldığı konu ve veri iletimini güvence altına almaya çalışması sebebiyle kıymetli bir çalışmadır.

(Li vd., 2018) çalışmalarında otonom araç bulutlarında mesaj iletimi için güvenli bir anahtar yönetim protokolü üzerinde çalışmışlardır. İki katmanlı bir mimari geliştirmişler bu geliştirmiş oldukları mimariyi çalışmalarında tanıtmışlardır. Hali hazırda bulunan bulut sistemlerinin genel bir incelenmesi ve elde edilen bilgiler neticesinde kendi yöntemlerini teorik olarak tanıtmış ve çeşitli saldırı durumlarına karşı güvenlik durumunu analiz etmişlerdir.

(Chuang ve Tseng, 2021) yapılan çalışmada beşinci nesil ağlarını kullanan akıllı şehir sistemlerinde kullanılmak üzere doğrulama ve anahtar değişim protokolü üzerine çalışmışlardır. Eliptik eğri şifrelemesi ile Diffie-Hellman anahtar dağıtım algoritmasından faydalanmışlardır. Üçüncü bir taraf olmadan doğrulama ve anahtar paylaşımı gerçekleştirilmesi amaçlanmıştır. Tezimizde bizim geliştirdiğimiz algoritmanın elde etmek istediği sonuca akıllı şehir uygulamalarında fiziksel kopyalanamaz değişkenler kullanarak ulaşmayı amaçlamışlardır. Uygulanabilirliği zamanla anlaşılabilir bu algoritmanın aksine tezimizde geliştirmiş olduğumuz algoritma anahtar paylaşımı yapmadan şifrelenmiş dosyaların geliştirmiş olduğumuz blokzincir temelli sistem sayesinde gerçekleştirmektedir.

Tez çalışmasının gerçekleştiği 6 yıl içerisinde sadece blokzincir konusu altında konferans ve çeşitli indekslerde yayın yapan dergilerin 1000'den fazla makalesi incelenmiştir. Benzer bir çalışma steganografi ve şifreleme konularında da gerçekleştirilmiştir. Yayınlatılan 10 akademik çalışmanın yanı

sıra tezin teslim edildiği bu süreçte hakem incelemesinde olan SCI ve SCI-E indeksli iki makale çalışması daha gönderilmiştir. Gerçekleştirilen tez çalışmasında elde edilen bilgi birikimi neticesinde İstanbul Demir ve Demir Dışı Metaller İhracatçıları Birliği tarafından yürütülen kitap çalışmasında teknik destek sağlanmış ve kitabın teşekkür bölümünde bu destek belirtilmiştir. Ayrıca İstanbul Aydın Üniversitesi Blokzincir Uygulama ve Araştırma Merkezinde yönetici olarak görevlendirilen tez sahibi Mustafa Takaoğlu, bu görevlendirme neticesinde birçok ulusal ve uluslararası Blockchain Talks isimli çeşitli konularda merkez danışma kurulu başkanı Erol User beyefendi ile birlikte webinarların gerçekleştirilmesinde katkı sağlamıştır. Ayrıca yine bu tez çalışmasında yapılan literatür taramaları neticesinde elde edilen bilgiler, İstanbul Aydın Üniversitesinin bünyesinde gerçekleştirilen ve BİL Kolejlerinin Türkiye geneli tüm öğrencilerini içeren webinarlarda paylaşılmıştır. Sonuç olarak tezimizden üretilen çalışmalar literatüre katkı sağladığı gibi bu konularda yapılabilecek yeni çalışmalara ihtiyaç duyulduğu için ilerleyen süreçte yeni konuların incelenmesine ve literatüre yani bilim dünyasına katkı sağlayacak nitelikte yeni çalışmaların yapılmasına imkân sağlamaktadır.

## **B. Problem Tanıtımı**

Tez çalışmamızda seçmiş olduğumuz konunun belirlenmesinde, güncel teknolojik gelişmelerinin, hali hazırda geliştirilmek amacıyla üzerine çalışılan konulara yenilikçi bir bakış açısı ve yöntemle uygulanması ve karşılaşılan sorunlara çözüm getirilmesi amaçlanmıştır. Bu sebeple veri iletimi konusunda karşılaşılan sorunlar ele alınmıştır. Bir verinin güvenli bir şekilde alıcı tarafına iletebilmesi için yapılması gereken çeşitli çalışmalar bulunmaktadır. Verinin şifrelenmesi ya da ağın güvence altına alınması gibi yapılan birçok çalışmanın ortak sorunu şifreleme amaçlı kullanılan algoritmanın anahtarının paylaşımı esnasında karşılaşılan güvenlik açıklarıdır. Bu sebeple tezimizde anahtar paylaşımı konusunda yeni bir algoritma geliştirme gerekliliği üzerinde mutabık kalınmıştır. Ayrıca kendi sistemimizde veri türü olarak seçilecek her türde dosya türünü kapsayacak şekilde ele alan ve yeni bir dosya formatına çeviren bir yöntem gerekliliği olduğu görülmüştür. Ek bir güvenlik katmanı olan bu manipülasyon çalışması sayesinde sistemimizde gönderimi yapılan tüm

türlerdeki dosyalar tek bir formata çevrilmekte ve dosyanın geliştirmiş olduğumuz şifreleme ve anahtar paylaşımı algoritmasını aşması durumunda ek bir güvenlik katmanı olması sağlanmıştır. Geliştirilen bu yeni dosya türü sayesinde yapılabilecek herhangi bir analiz yönteminde elde edilmeye çalışılan desen tespiti yapılabilmesi mümkün değildir. Yani kriptanaliz yöntemlerini bir sorun olarak kabul edersek, bu soruna çözüm getirmek amaçlanmıştır. Son olarak bir diğer sorun da veri iletimi esnasında dosyaların ele geçirilmesi ve üzerinde değişiklik yapılması durumudur. Bu sorunun önüne geçilmesi için de geliştirmiş olduğumuz blokzincir temelli veri iletim ağında özüt algoritmalarından faydalanarak veri bütünlüğünün ve kurcalama girişimlerinin önüne geçilmesi amaçlanmıştır.

Özetle tezimizde veri iletiminde güvenliğin üst düzeyde tutulabilmesi için veri türlerinin tamamında çalışan ve hiçbir dosya okuyucu tarafından açılmayacak bir formata sahip manipüle edilmiş yeni bir dosya türü elde edilmektedir. Bu dosya türü geliştirmiş olduğumuz şifreleme ve anahtar paylaşımı algoritması sayesinde alıcıya güvenli bir şekilde iletilebilmektedir. Geliştirilen bu algoritma manipüle edilen dosyayı şifrelediği için şifrelenmiş dosya üzerinde yapılacak her türlü kriptanaliz tekniğinin bir desen bulmasına engel olacak şekilde geliştirilmiştir. Ayrıca anahtar paylaşımını steganografiden faydalanarak gerçekleştirilen tez çalışmamızda, manipüle edilmiş ve şifrelenmiş dosyaların alıcı tarafına güvenle ulaştığından emin olmak için özüt algoritmalarından faydalanarak kurcalanamaz ve değiştirilemez bir yapıya kavuşması sağlanmıştır. Tezimizde ele alınan konunun seçilmesinde etken olan problem tanıtımı bu üç sorunun giderilmesi üzerine kurulmuştur.

### **C. Önerilen Yöntem**

Doktora tez çalışması 3 akademik dönemi kapsayacak şekilde planlanmıştır. Bu süreçlerin gerçekleştirilebilmesi için gerek doktora yeterlilik sınavı gerekse de doktora tez konusu seçimi ve savunması süreçlerinde yoğun bir teknik ve teorik bilgilerin hatırlanması üzerine çalışmalar yapılmış ve blokzinciri teknolojisi, steganografi bilimi, şifreleme algoritmaları ve anahtar paylaşımı algoritmaları gibi konular üzerine derinlemesine bilgi birikimi oluşturulması için literatür taraması yapılmıştır.

Belirtilmiş olan 3 dönemlik planlamada ele alınan tez konusunun gerçekleştirilebilmesi için gerekli olan modüllerin tamamlanması öngörülmüştür. İlk modül olarak veri manipülasyonu belirlenmiş ve Ocak 2020-2021 Güz döneminde yapılan Tez İzleme Jürisinde elde edilen sonuçlar tez izleme heyetimizle paylaşılmıştır. Sonrasında gerçekleştirilen ve tezimizin ikinci modülü olan steganografi bilimi esas alınarak yapılan şifreleme ve anahtar paylaşımı algoritması 2020-2021 Bahar döneminde yapılan Tez İzleme Jürisinde tanıtılmış ve elde edilen sonuçlar paylaşılmıştır. Üçüncü ve son modülde ise blokzincir teknolojisinden yola çıkarak özüt algoritmalarını veri iletim ağında kullanarak, veri iletimi güvenliği ve dosya kurcalanmasına karşı güvenliği sağlanmıştır. 2021-2022 Güz döneminde geliştirilen yöntem tanıtılmış ve sonrasında tez yazım sürecine başlanmıştır.

Blokzincir Teknolojisine Dayalı, Şifreleme ve Steganografi Teknikleri Kullanılan, Yüksek Güvenlikli Bilgi Değişim Algoritması ismiyle hazırlamış olduğumuz tez çalışmamızda veri/bilgi değişimini 4 katmanlı olarak (dosya manipülasyonu, şifreleme ve steganografi temelli anahtar paylaşımı ve blokzincir entegrasyonu) önermiş olduğumuz yöntemle gerçekleştirmiş bulunmaktayız. Tezimizin ilerleyen bölümlerinde ilgili katmanlar sırayla ele alınmış ve her başlık altında elde edilen sonuçlar paylaşılmıştır.

#### **D. Tezin Bilime Katkısı**

Gerçekleştirilen tez çalışmasında geliştirilen algoritma bilime çeşitli katkılar sağlamıştır. Öncelikle dosya manipülasyonu sürecinde elde edilen yeni dosya türü sayesinde yeni bir metin steganografisi yapılabilir hale gelmiştir. Normal şartlarda metin steganografisi gerçekleştirmesi zor ve tespit edilebilmesi kolay yöntemlerdir. Ancak tezimizde geliştirilen manipülasyon algoritması sayesinde dosya türlerinin tamamı anlamlandırılmaz bir formata dönüşmesi ve gizlenmek istenen bilgilerin bu sayede kolaylıkla tespit edilemeyecek şekilde gizlenmesi sağlanmıştır. Manipülasyon sürecinde elde edilen kazanımlardan bir diğeri de veri iletim ağının dinlenmesi ve küçük parçalar halinde verilerin okunabilmesi durumunda elde edilecek bilgilerin anlamlandırılabilir olmayan yapıda olmasıdır.

Çalışmanın ikinci modülü olan şifreleme ve anahtar paylaşımı kısmında geliştirilen yöntem alanında bir başka benzeri görülmemiş yapıdadır. Tezimizde OTP şifreleme algoritması için geliştirilen bu yöntem, anahtar seçiminin rastgele olarak yapılması gereken tüm şifreleme sistemlerinde uygulanabilir yapıda olmasının yanısıra sahip olduğu anahtar havuzu mimarisi sayesinde anahtar rastgeleliğini üst seviyede sağlamaktadır. Gönderici ve alıcı arasında önceden paylaşılmış anahtar havuzunun 16 alt parçaya bölünmesi ve sonrasında her anahtar seçiminde rastgele olacak şekilde tekrar birleştirilmesi sonucunda elde edilen yeni anahtar havuzundan anahtar seçilerek rastgele anahtar seçimi gerçekleşmektedir. Bu seçilen rastgeleliği arttırılmış anahtar ile şifrelenen dosyanın içine yeni oluşturulan havuzun sıralama bilgisi ve şifrenin bu havuzdan seçildiği noktanın bilgisi saklanmıştır. Üçüncü steganografi modülü sayesinde gerçekleştirilen bu gizleme işlemi sayesinde, anahtar paylaşımı açık kanallar kullanılmadan, geleneksel yöntemlerden destek almadan gerçekleştirilmektedir. Bir başka deyişle anahtar paylaşımı sürecinin anahtar paylaşımsız olarak gerçekleştirildiği ifade edilebilir. Çünkü dosyaya gizlenen havuz oluşturma bilgisi ve bu yeni havuzdan seçilen anahtarın başlangıç noktası bilgisi elde edilse dahi havuz bilgisi saldırganlarda olmadığı için sistemin güvenliği açısından bir risk teşkil etmemektedir. Anahtar paylaşımının steganografi ve geliştirmiş olduğumuz mimari ile yapıldığı başka bir çalışma literatürde bulunmamaktadır.

Dördüncü modülde geliştirilen blokzincir teknolojisi temelli algoritma sayesinde diğer üç modülde gerçekleştirilen manipülasyon, şifreleme ve steganografi adımlarının güvenliği ve sistemin bütünlüğü gerçekleştirilecek her türlü saldırı ve çevresel etkilerin engellenmesi amacıyla SHA256 özüt algoritması kullanılarak korunmaktadır. SHA256 algoritması ile özütlenen dosyanın alıcıya iletilmesi sonucunda; alıcı tarafında elde edilen özüt değeriyle karşılaştırılması neticesinde karşılaşılan duruma göre veri iletim hattının değiştirilmesi yahut onay verilip dosyanın açılması sürecine başlanmaktadır. Blokzincir bloklarında görülen özüt değerlerinin işaretlenmesi mantığına benzer bir şekilde kurgulanan bu eklenti sayesinde geliştirilen güvenlik ve gizleme katmanlarının kurcalanmaya karşı dayanıklı hale gelmesi sağlayarak bilime katkıda bulunmaktadır.

## II. DOSYA T RLER  VE DOSYA MAN P LASYONU ALGOR TMASI

Tezimizde dosya t rleri  zerine ayrıntılı arařtırmalar yapılmıřtır. Elde etmek istediĐimiz sonu ; dosya t rlerinin tamamını kapsayacak bir manip lasyon algoritması elde etmektir.      manip le edilmemiř bir dosyanın, řifrelendiĐi algoritmanın bir řekilde (kuantum sonrası d nem gibi) kırılması yahut řifre anahtarının saldırgan tarafından ele ge irilmesi durumunda g venliĐin sonlanıyor olması sebebiyle bu alanda ekstra bir g venlik katmanı geliřtirilmesi ihtiya ı olduĐu d ř n lm řt r.

řifreleme algoritmalarının  oĐu algoritmik karmařıklıĐı sayesinde ger ekleřtirilebilecek saldırılara karřı dayanıklı olarak geliřtirilmektedir (Belkhouja vd., 2018). Kırılan řifreleme algoritmaları  rnekleri ge miřte mevcuttur ama bu zafiyetlerin sebebi; geliřtirilen algoritmaların algoritmik seviyede ilkel kalmasından kaynaklanmaktadır. Bir diĐer sorun ise řifreleme algoritması her ne kadar geliřmiř hatta kuantum hesaplama g c ne karřı dahi g venilir yapıda olsa da anahtar paylařımı noktasında karřılařılan g venlik a ıkları sebebiyle g venlik a ıklarıyla karřılařılmaktadır. Bu sebeple anahtar paylařımının g venli halde yapılabilmesi i in bir ok y ntem  nerilmiřtir. G n m zde en  ok kullanılan y ntem Diffie-Hellman anahtar paylařım algoritmasıdır (Belghazi vd., 2019). Kuantum anahtar paylařımı algoritması da g n m zde  ok a tercih edilmektedir. T m bu g venlik  abalarına raĐmen řifrelenmiř dosyalar, anahtar alıcıya g venli bir řekilde teslim edilse dahi g nderici/alıcı tarafındaki kullanıcı hataları sebebiyle saldırganların eline ge ebilir ve ele ge irilen anahtar bilgisi sayesinde kolayca a ılabilirler. Nihayetinde řifreleme algoritmaları, anahtarın g vende tutulabildiĐi oranda korunaklıdır. Bu t r fiziki hataların da giderilebilmesi i in ek bir g venlik katmanına ihtiya  duyulmaktadır. Bu sebeple tezimizde t m iřletim sistemlerinde kullanılan her t rdeki dosyaların řifreleme algoritmasında yařanacak bir g venlik a ıĐı sebebiyle ele ge irilmesi durumunda anlamlı bir veriye ulařılmaması i in farklı bir yapıya d n řt r lmesine  alıřılmıřtır. Ayrıca veri iletimi esnasında aĐın dinlenmesi durumunda řifrelenmiř

verilerin belirli ve genellikle küçük parçalarına saldırganlarca erişim sağlanabilmektedir. Bu sebeple yöntemimiz, manipüle edilmiş bir dosyadan elde edilen bilgi parçacıklarının anlamlandırılabilir bir yapıda olmayacağı için kriptanaliz yöntemlerini işlevsiz hale getirmekte katkı sağlayacaktır. Ayrıca şu husus düşünüldüğünde AES, OTP ya da eliptik eğri şifreleme algoritması ile şifrelenmiş bir dosyanın kaba kuvvet yöntemiyle kırılması durumunda elde edilen dosyada yapılan manipülasyon çok büyük bir güvenlik kalkanı olarak düşünülemez. Ancak geliştirmiş olduğumuz bu manipülasyon katmanı sayesinde anahtar kaybından kaynaklanan güvenlik açıklarının önlenmesi amaçlanmıştır. Son olarak belirtmekte fayda vardır ki, Khirshoff'a göre algoritma geliştirilirken; oluşturulan algoritma karmaşıklığının başkaları tarafından bilinmediği düşünülerek hareket edilemez. Yani günümüzde çokça kullanılan AES, OTP, DES, 3DES gibi algoritmalar, sahip oldukları algoritmanın başkaları tarafından bilinmediği için değil sahip oldukları algoritmik mimarinin sağlamlığı sayesinde güvenlik sağlamakta ve tercih edilmektedirler (Georgieva-Tsaneva vd., 2022).

Özetle geliştirmiş olduğumuz dosya manipülasyonu modülü metin steganografisinin yapılmasına olanak sağlamakta, kriptanaliz ve steganaliz yöntemlerinin işe yaramamasına katkı sağlamakta, hat dinlenmesi durumlarında saldırganların anlamlandırılabilir bir bilgiye ulaşmasına engel olmakta ve incelenen dosyanın türü hakkında saldırganların bir fikir sahibi olmamasını sağlamaktadır.

## **A. Dosya Türleri**

Dosya kavramı dijitalleşen verilerin bilgisayar diski üzerinde saklanabilmesi için geliştirilen veri yapılarıdır. Hafızada her dosyanın bir başlangıç ve bitiş işaretçisi vardır. Dosya tipi ise kullanılan işletim sistemine uygun olarak geliştirilmiş ve dosyanın nasıl okunacağını yani dosyanın türünü belirten ve noktadan sonra kısaltma harflerle belirtilen yapılardır. Bir başka deyişle bu uzantılar dosyanın hangi programla açılacağını ve hangi işletim sisteminde kullanılabileceğini ifade etmektedir.

Örneğin Microsoft Windows işletim sisteminde bulunan Not Defteri uygulamasını açarak yazılmaya başlanan bir internet sayfası kodları, dosyanın uzantısı .html olarak kaydedilmesi durumunda işletim sistemi kullanım ekranında

web sayfası ve varsayılan internet yürütücüsü programının logosuyla gözükecek ve bu dosyanın açılması durumunda da bir internet sayfası karşımıza gelecektir.

Günümüzde birçok dosya uzantısı bulunmaktadır. İşletim sistemi ayrımı yapmaksızın yazı dosyaları için .txt, .dic, .odt, .ott, .rtf, .uot, .dic uzantıları, video dosyaları için .avi, .mp4, .mkv, .wmv, .flv, .3gp, .dat, .mov, ses dosyaları için .ogg, .mp3, .wav, .mid, resim dosyaları için .jpg, .png, .bmp, .psd, .gif (hareketli resim), Microsoft Office programlarının .doc, .docx, .xls, .xlsx, .ppt, .pptx, .mdb, .mdbx, website kodlamaları için .html, .php, .aspx, .asp, sıkıştırılan dosyalar için .rar, .zip, .tar, .7z, elektronik kitap ya da evraklar için .pdf ve uygulama yazılımları için de .exe uzantıları kullanılmaktadır (Marjai vd., 2022).

## **B. Önerilen Dosya Manipülasyonu Algoritması**

Tezimizde öncelikle çokça kullanılan .doc, .pdf, .xlsx, .jpg gibi dosya türlerinin manipüle edilmesi üzerine çalışılmıştır. Yaklaşık 1 aylık süreç sonrasında seçilen dosya türleri üzerinde yapılacak fiziksel müdahaleler ile geri alınabilir dosya bozulmalarının yapılabilmesi için denenen yöntemlerin her dosya türü için uygulanabilir seviyede olmadığı görülmüştür. Harcanan emek ve elde edilmek istenen sonuç ve bu süreçte programın karmaşıklığı dikkate alındığında daha kesin bir çözüm ihtiyacı olduğu görüşmüştür. Bu sebeple tüm dosya türlerinin dijital bir veri olması ve ikili (binary) formatta bilgisayarlarca işlendiği düşünülerek sistemimizde kullanılmak istenen tüm dosya türlerini bayt seviyesinde ve ara belleğe (buffer) alarak manipüle eden ve sonrasında gerçekleşen şifreleme ve veri iletimi işlemleri neticesinde alıcının elde ettiği dosyayı tersine adımlar takip ederek dosyanın manipüle edilmiş haline gelecek şekilde açılması ve manipülasyon algoritmamızın tersine çalıştırılması neticesinde kayıpsız bir şekilde gönderilen dosyaya ulaşılması sağlanmıştır. Bayt seviyesinde ve ara belleğe alarak yapılan aynı işlemler neticesinde farklı sürelerde aynı sonuçlara ulaşılmıştır.

Önerilen dosya manipülasyonu algoritması ile tüm dosya türleri Java programlama dili kullanılarak bayt seviyesinde okunabilmektedir. Tezimizde seçmiş olduğumuz .doc, .pdf, .xlsx ve .jpg dosya türleri bu amaçla test edilmek için seçilmiş ve testlerde kullanılmıştır. Bayt seviyesinde okunan bu dosyalarda geri alınabilecek şekilde değişiklik/manipülasyon yapılmıştır. Yapılan manipülasyon yöntemi, doktora tezinden üretilen yazılımın ürün/hizmet olarak kullanılmasına karar verildiği için

ayrıntılı olarak tanıtılmamaktadır. Ancak geliştirilen algoritmanın test sonuçları ilerleyen başlıklarda paylaşılmıştır.

Önerilen manipülasyon algoritması, anahtar kayıplarında karşılaşılan güvenlik açıklarının azaltılmasında katkı sağlamasının dışında üretilen manipüle edilmiş yeni dosyanın bayt seviyesinde tüm formatı bozulduğu için elde edilen yeni dosya türü sayesinde gönderilen dosya hakkında saldırganın hiçbir fikri bulunmamaktadır. Yani tüm türlerde manipüle edilen dosyalar tek bir okunamaz formata dönüşmektedir. Bu yeni dosya türü sayesinde kriptanaliz yöntemleri uygulanırken elde edilmeye çalışılan ve tekrar eden benzer durumların tespiti ve bu tespit edilen durumlar işaretlenerek dosya genelinde bir desen arayışında bulunulması ve sonrasında da şifreyi yahut doğru dosya formatını elde etme çalışmalarına yahut spesifik olarak bir dosya türü arandığında hedef olarak seçilmiş verilerde sınıflandırma yapılması mümkün olmayan bir hal almaktadır. Ayrıca steganografi sürecinde gerçekleştirilen manipülasyon işleminin büyük katkısı bulunmaktadır.

Aşağıda paylaşılan sözde kodda manipülasyon süreci paylaşılmıştır:

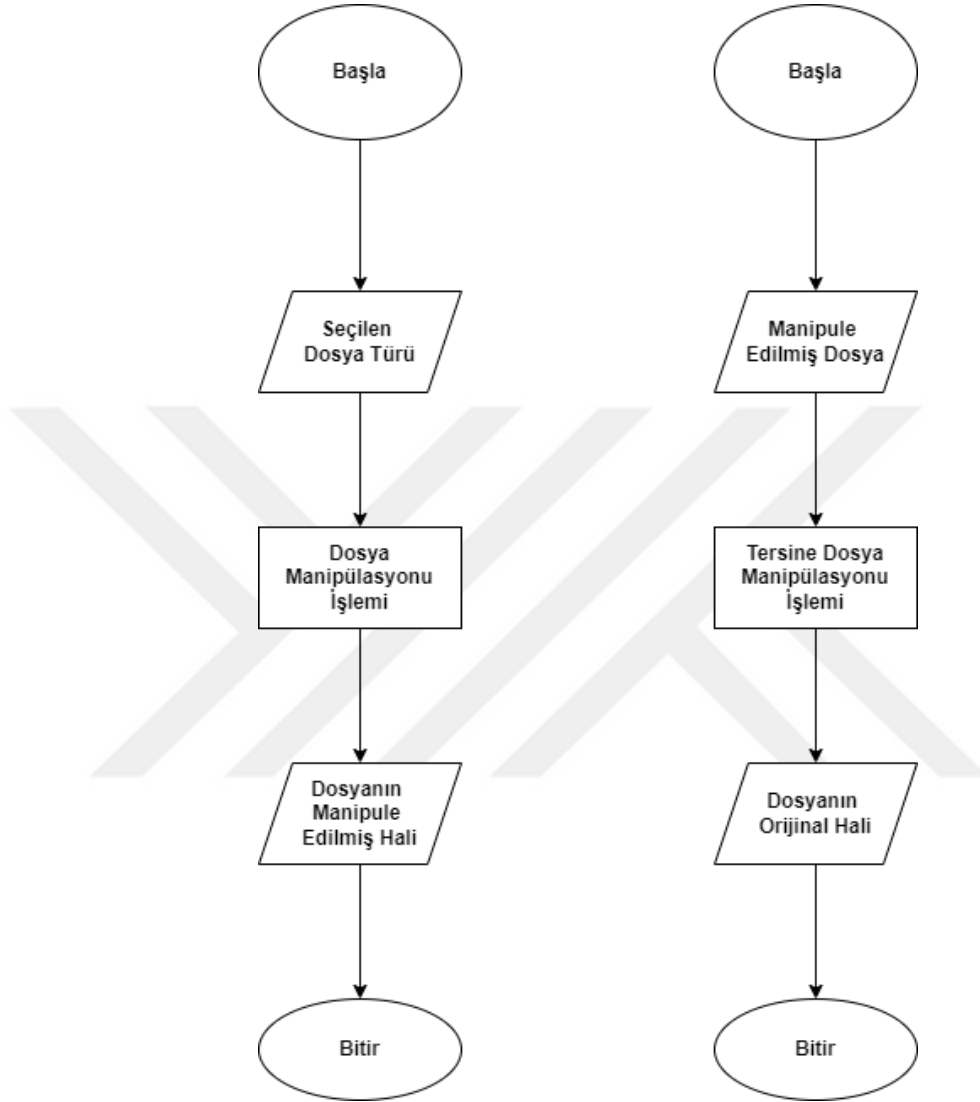
- Başla
- Herhangi bir seçilen dosya türünü (X) bayt seviyesinde OKU.
- Baytlarda belirlenen değişikliği ( $X=X'$ ) UYGULA.
- Yeni dosya halini ( $X'$ ) YAZDIR.
- Bitir

Aşağıda paylaşılan sözde kodda tersine manipülasyon süreci paylaşılmıştır:

- Başla
- Manipüle edilmiş dosyayı ( $X'$ ) OKU.
- Baytlarda yapılan değişikliği ( $X' = X$ ) tersine UYGULA.
- Dosyanın orijinal halini (X) YAZDIR.
- Bitir.

Şekil 1’de manipülasyon ve tersine manipülasyon sürecini ifade eden blok diyagramı paylaşılmıştır. Bayt ve ara bellek teknikleri manipüle edilecek verilerin

okunmasında uygulanan yöntemler olması sebebiyle blok diyagramında ayrıntılı olarak gösterilmemiştir.



Şekil 1 Manipülasyon ve tersine manipülasyon blok diyagramı

Önerilen manipülasyon algoritmasının uygulanması sonucunda manipüle edilmiş yeni dosyaların eski haline getirilebilmesi için tersine manipülasyon algoritması geliştirilmiştir. Basitçe tanıtmak gerekirse, dosya türlerinin bayt seviyesinde değiştirilen bitleri eski haline alınarak dosya eski haline getirilmektedir.

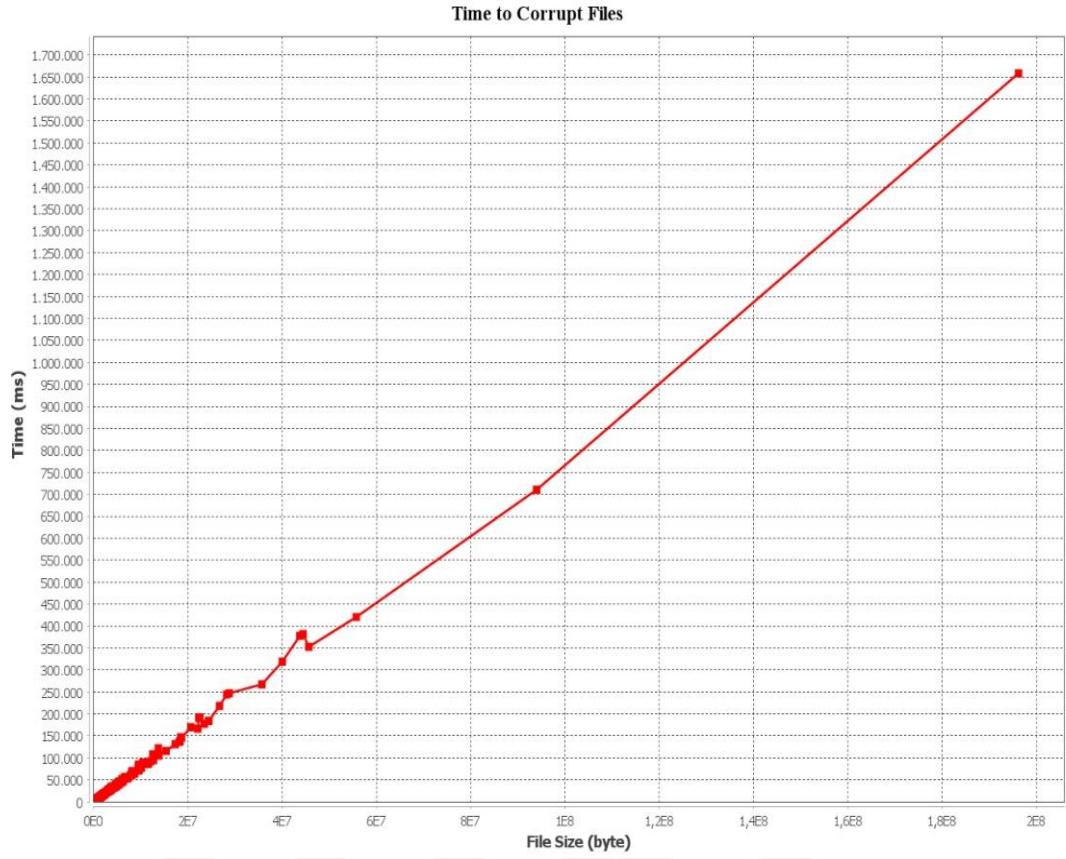
### C. Manipülasyonu Testleri

Tezimizin bu aşamasında tahrifat yapılacak dosya Java Programlama Dili kullanılarak okunmuştur. Okunan dosyalarda bazı bitler de tahrifat yapılmıştır. Bu

işler bayt seviyesinde olarak yapıldığı gibi arabelleğe alınarak da yapılmıştır. Aynı şekilde tahrifat yapılmış dosyalar eski hallerine her iki yöntem de kullanılarak getirilmiştir. Tezimizde 4 farklı dosya türü kullanılmıştır. Bu dosya uzantıları .doc, .pdf, .xlsx ve .jpeg olarak seçilmiştir. Tekrar ifade etmekte fayda vardır ki geliştirmiş olduğumuz algoritma tüm dosya türlerinde uygulanabilir yapıdadır. Test aşamasında, dosya türü fark etmeksizin, tahrifat yapılan dosya okunurken, dosya boyutu kaydedilmiş ve tahrifat işleminin ne kadar sürdüğü hesaplanmıştır. Elde edilen sonuçlar aşağıdaki alt başlıklarda paylaşılmıştır.

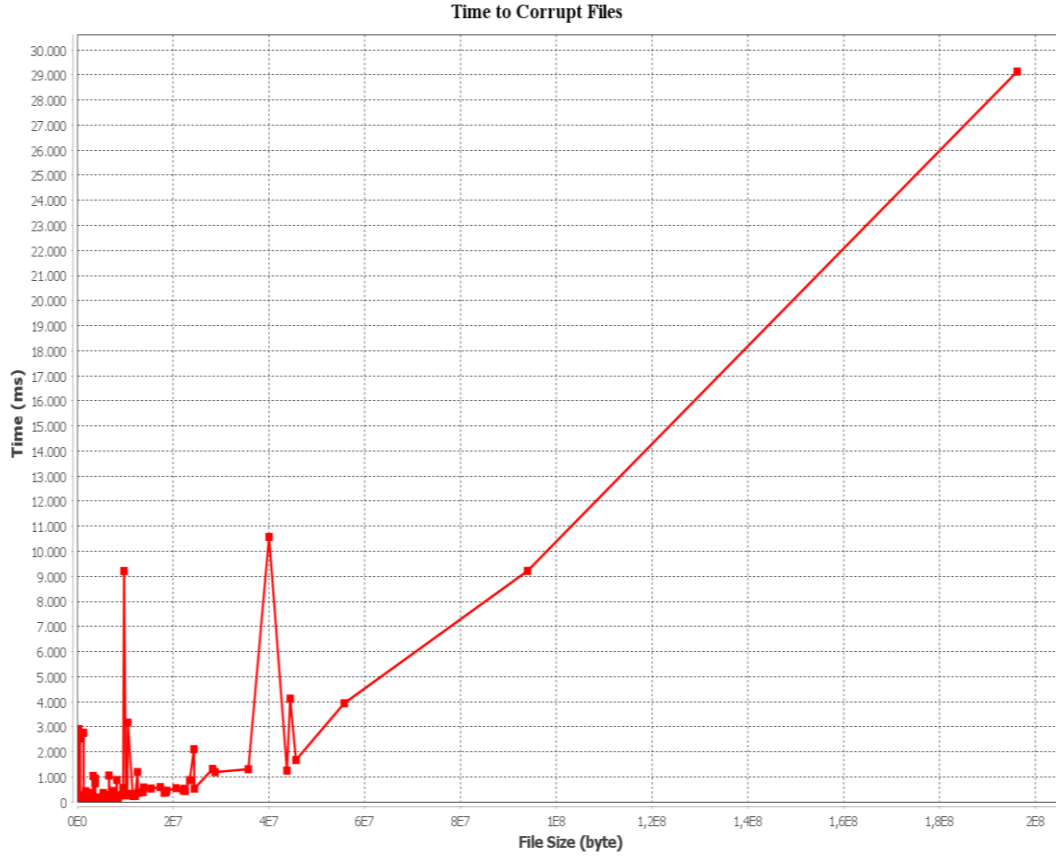
## **1. PDF Dosya Türü Manipülasyonu ve Tersine Manipülasyonu**

Bu test için veri seti olarak 607 farklı .pdf uzantılı dosya kullanılmıştır. Kullanılan veri tabanının toplam boyutu 1.69 GB büyüklüğündedir. Bayt seviyesinde ve ara bellek teknikleri kullanılarak algoritmamız uygulanmıştır. Aşağıda paylaşılan Şekil 2’de bayt tekniğiyle yapılan manipülasyon işlemi sonucunda elde edilen verilerle oluşturulmuş grafik bulunmaktadır. Bayt tekniği diye isimlendirdiğimiz yöntemde dosyalar baytlar halinde işleme alınmakta ve manipüle işleminin o baytta tamamlanması sonrasında yeni bayta geçilerek gerçekleştirilmektedir. Bu yöntem tezimizde incelenen .pdf dosya uzantısı dışındaki diğer üç dosya uzantısında da aynı şekilde uygulanmıştır.



Şekil 2 PDF bayt tekniğiyle manipölasyon grafiğı

Şekil 2'in oluşturulması için kullanılan veriler EK-1'de PDF dosyalarının bayt tekniğiyle manipölasyon sonuçları isimli bölümde paylaşılmıştır. Aşağıda paylaşılan Şekil 3'de ise ara belleğe alınarak manipöl edilen dosyalardan elde edilen boyut-zaman grafiğı gösterilmektedir. Ara belleğe alınma tekniğinde işleme alınan bayt sayısı bilgisayarın arabelleğı seviyesinde yüksek bir miktarda işlenmiş ve aynı sonuç yani manipöl edilmiş dosya elde edilmiştir. Diğer dosya türlerinde de ara belleğe alma tekniğı kullanılarak elde edilen sonuçlar grafikler halinde paylaşılmıştır.

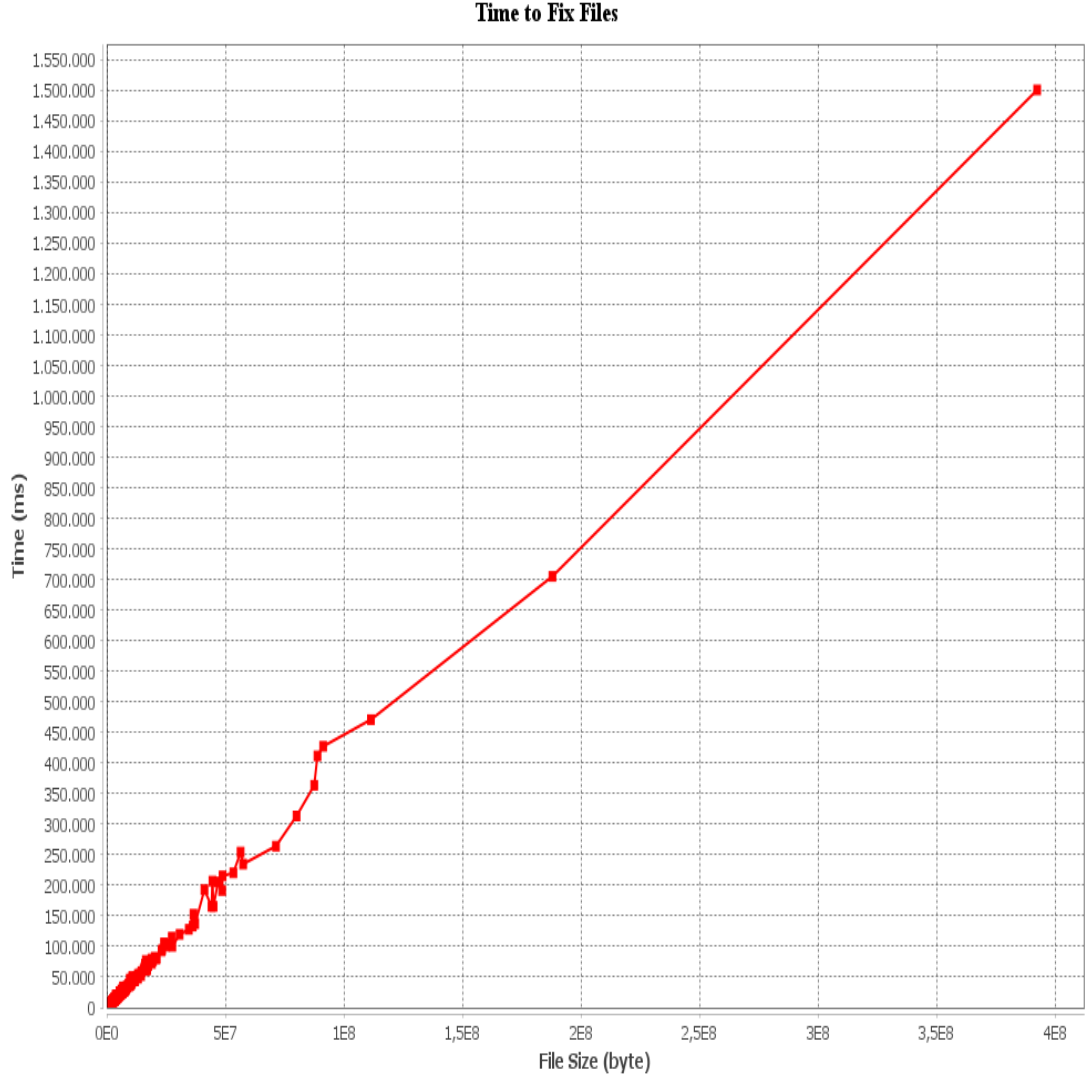


Şekil 3 PDF arabelleğe alma yöntemiyle manipölasyon grafiğı

Şekil 3'nin oluşturulmasında kullanılan dosya boyutu-zaman verileri EK-2: PDF dosyasının ara belleğe alınarak manipölle edilmesinin sonuçları isimli bölümde paylaşılmıştır.

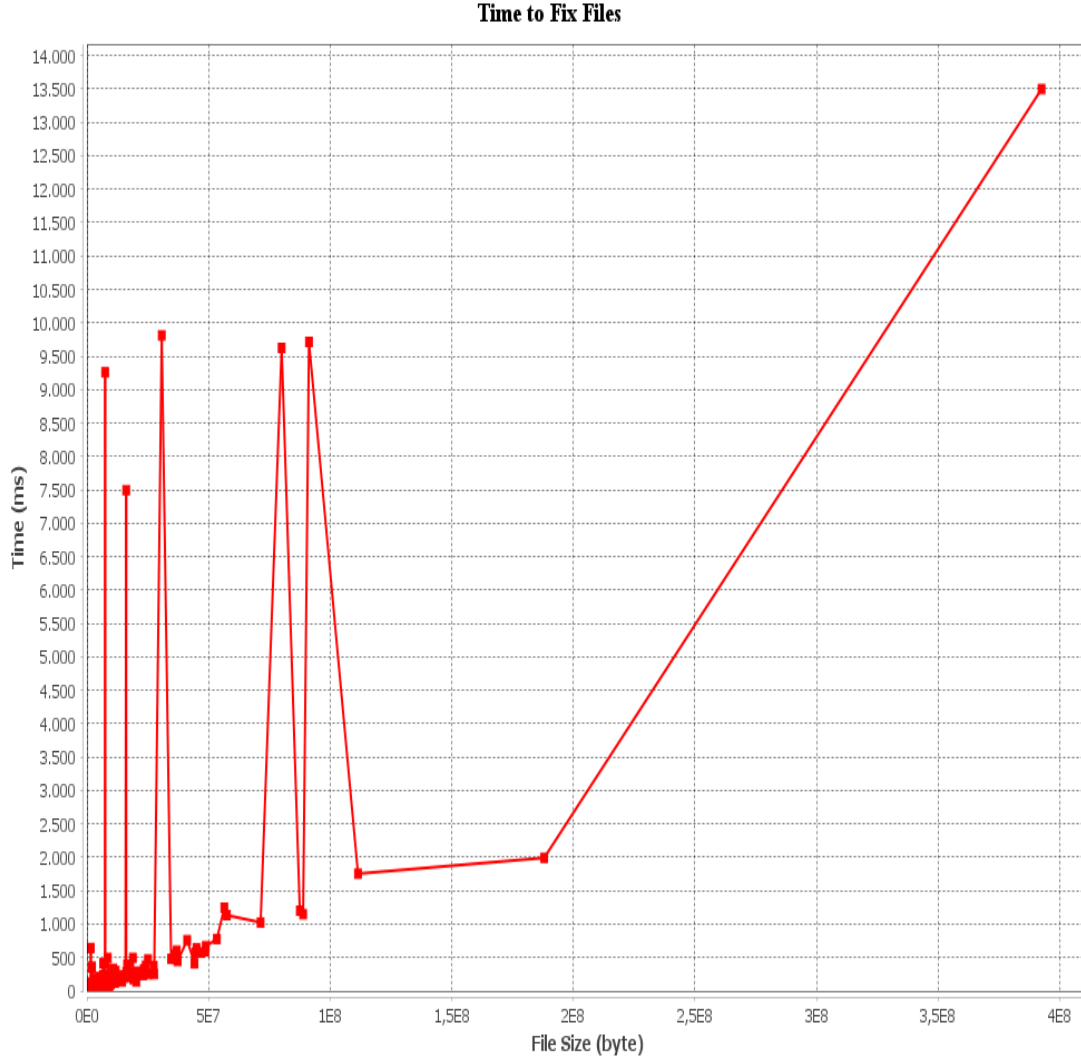
Göröldüğü üzere bayt tekniğı ve ara bellek tekniğı arasında zaman açısından çok büyük bir fark bulunmaktadır. Ancak ortak olan durum, dosya boyutu ile zaman ilişkisinin doğrusal olmasıdır. Özellikle Şekil 3'de paylaşılan grafik incelendiğinde Şekil 2'den farklı olarak bazı sıçramalar olduğunu göstermektedir. Kullanmış olduğumuz bilgisayarın kişisel bilgisayar seviyesinde olması ve bilgisayar zamanlayıcısında (scheduler) başka işlemlerin araya alınması sebebiyle milisaniye seviyesinde oynaklıklar görölmesi normaldir. Benzer bir sıçrama çok az olmak kaydıyla Şekil 2'de de görölmemektedir.

Şekil 4'de bayt tekniğıyle manipölle edilmiş dosyaların eski haline dönüştürölmesi sürecinde harcanan zaman grafiğı paylaşılmıştır. İlgili grafiğın oluşturulmasında kullanılan veriler EK-3: PDF dosyası tersine bayt manipölasyonu verileri bölümünde paylaşılmıştır.



Şekil 4 PDF tersine bayt manipölasyonu grafiğı

Şekil 5’de tersine ara belleğı alma tekniğıyle manipöle edilmiş dosyaların eski haline getirildiğı grafik paylaşılmıştır. Grafiğın oluşturulmasında EK-4: PDF dosyası tersine ara bellek manipölasyonu verileri bölümünde paylaşılmıştır.



Şekil 5 PDF tersine ara bellek tekniği manipölasyonu grafiđi

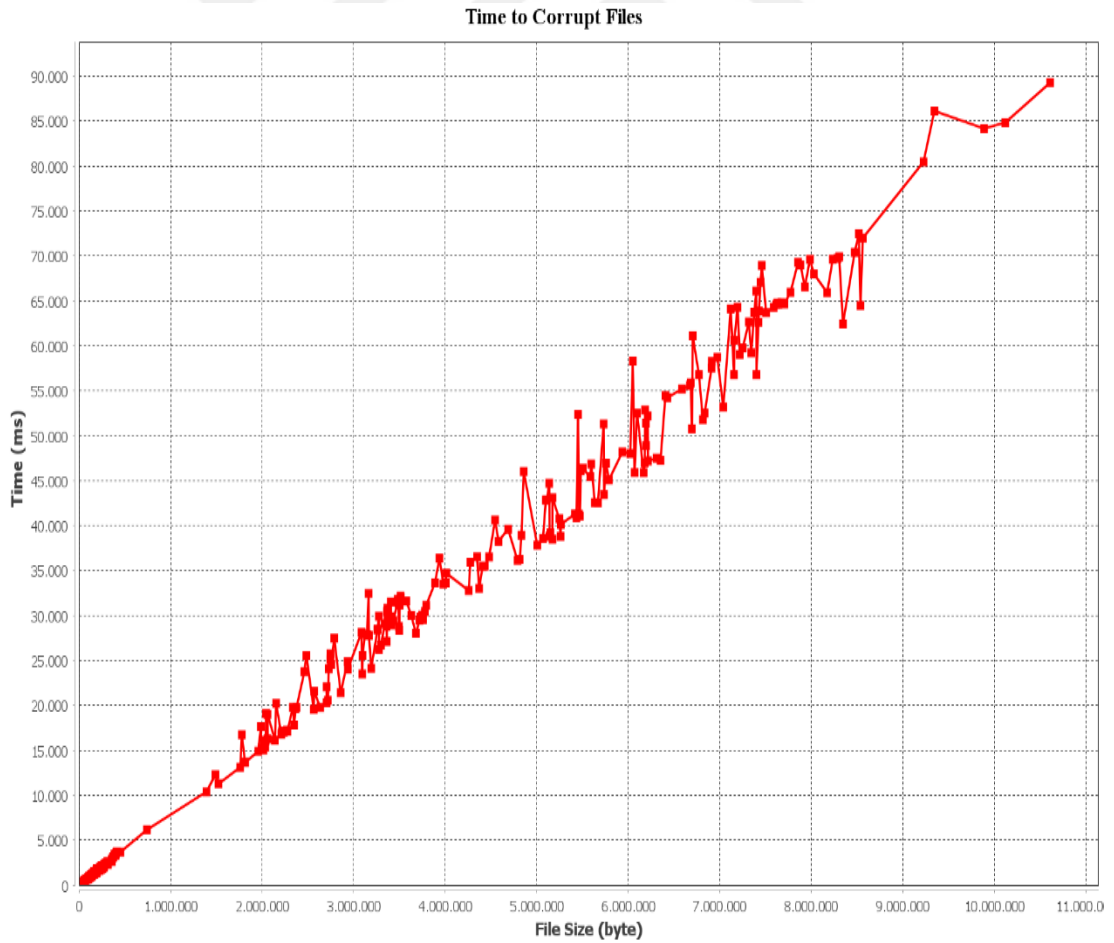
Şekil 4 ve Şekil 5 incelendiđinde tersine manipölasyon sürecinde hem bayt hem de ara bellek yönteminde elde edilen sonuçların hız olarak manipölasyon sürecinde gereken miktardan daha az olduđu görüřmüştür. Şekil 5’de paylaşılan ara bellek yönteminde yapılan tersine manipölasyon yönteminde elde edilen sonuçların manipölasyon sürecinde elde edilen ve zamanlayıcı (scheduler) sebebiyle oynaklıkların görölmesine sebebiyet veren durumun bir benzerinin yaşandıđı görölmektedir. Özellikle ara belleđe alma tekniđinde bu sıçramaların daha fazla görölmesinin sebebi aynı anda çok sayıda manipölasyon işlemi gerçekleştirildiđi için bilgisayarın aynı anda gerçekleştirdiđi diđer işlemleri de araya alması sebebiyle milisaniye seviyesinde görölen bu sıçramalarla karşılaşılmaktadır.

Elde edilen manipölasyon ve tersine manipölasyon sonuçları incelendiđinde, .pdf uzantılı dosyalar için yapılan işlemlerde harcanan zamanın dosya boyutu ile

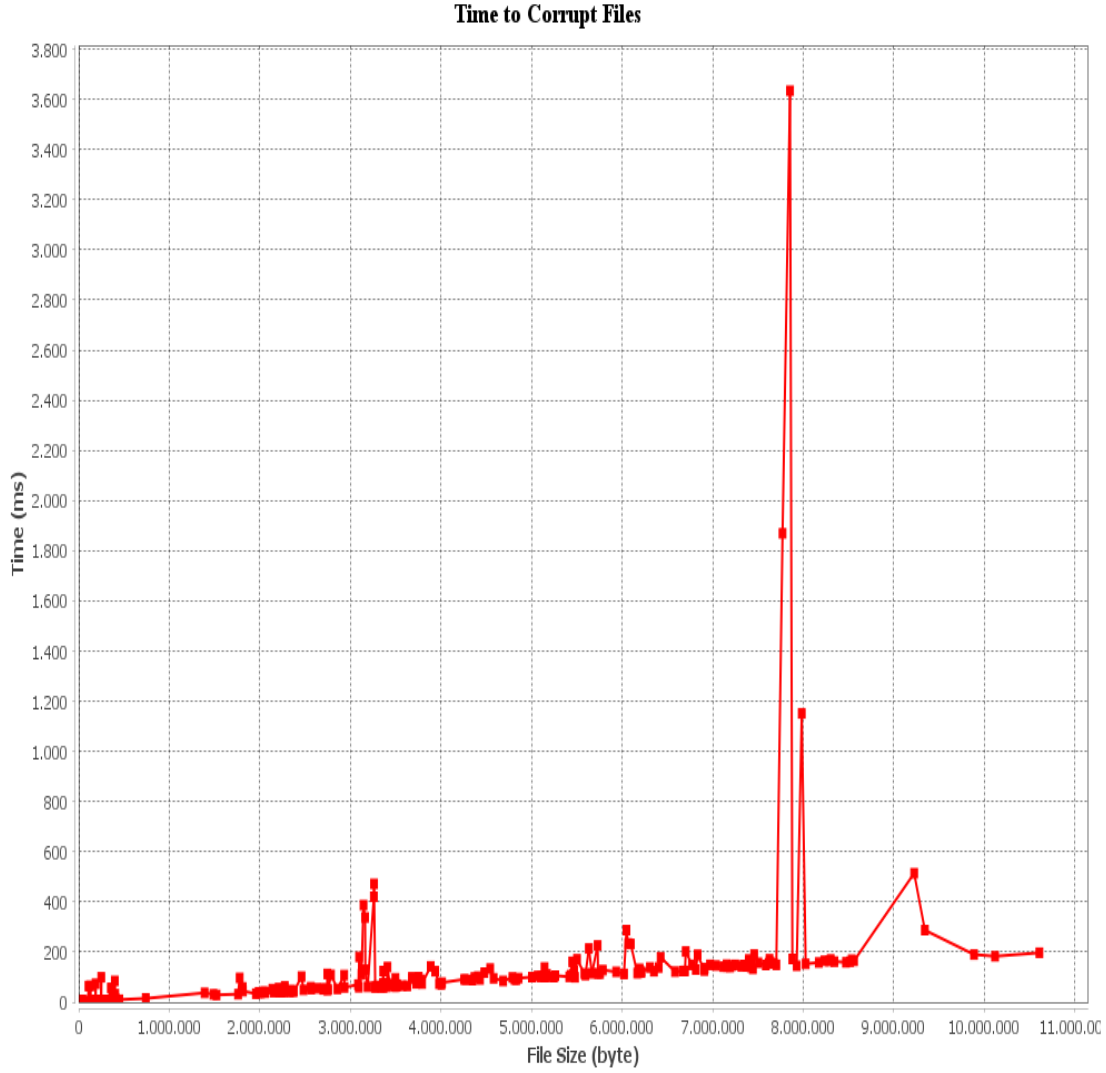
doğru orantılı olduğu görülmektedir. Yukarıda paylaşılan PDF dosya uzantısı için oluşturulmuş grafiklerde kullanılan veriler tezimizin bu bölümünde çok yer kapladığı ve sonuçların anlaşılmasında çok büyük bir önemi olmadığı için tezimizin ekler bölümünde paylaşılmıştır. Dört test için de kullanılan veriler tablo halinde paylaşılmış olup dosya boyutu (bayt) ve harcanan zaman (ms) şeklinde oluşturulmuştur. Sonuç olarak ara belleğe alma tekniği beklenildiği üzere hız açısından çok daha başarılı sonuçlar vermektedir.

## 2. JPG Dosya Türü Manipülasyonu ve Tersine Manipülasyonu

JPG dosya türünde yapılan test çalışmaları için veri seti olarak kullanılan 594 farklı jpg dosyası toplam 992 MB boyutundadır. Verilerimiz bayt tekniği ve ara belleğe alma tekniğiyle manipüle edilmiş ve daha sonrasında tersine manipülasyon işlemi yapılarak dosyaların orijinal hali elde edilmiştir. Şekil 6 ve Şekil 7’da bayt ve ara belleğe alma teknikleri kullanılarak elde edilen boyut (bayt) – zaman (ms) grafikleri EK-5 ve EK-6’da paylaşılan veriler kullanılarak elde edilmiştir.



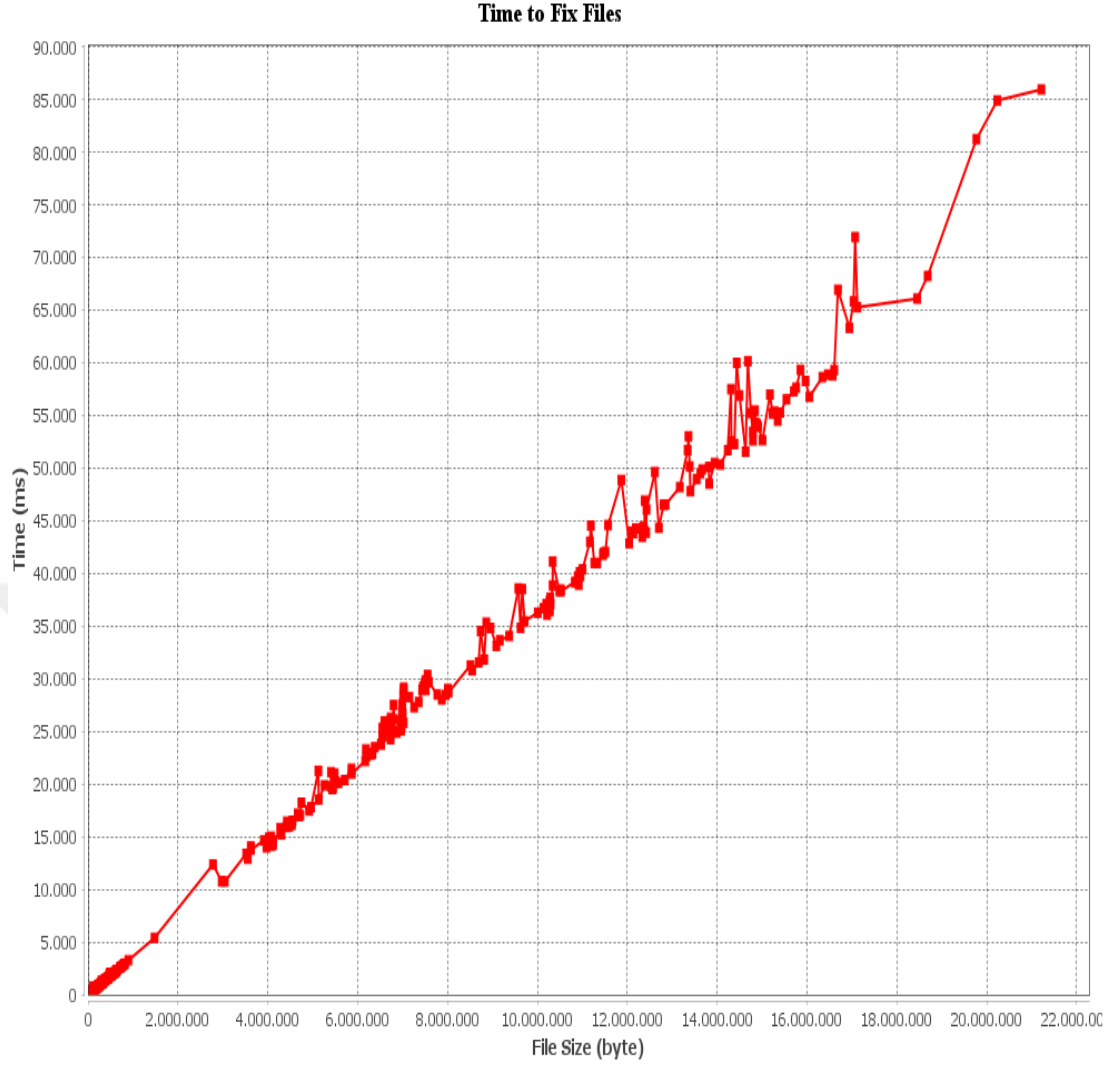
Şekil 6 JPG bayt tekniğiyle manipülasyon grafiği



Şekil 7 JPG arabelleğe alma yöntemiyle manipölasyon grafiğı

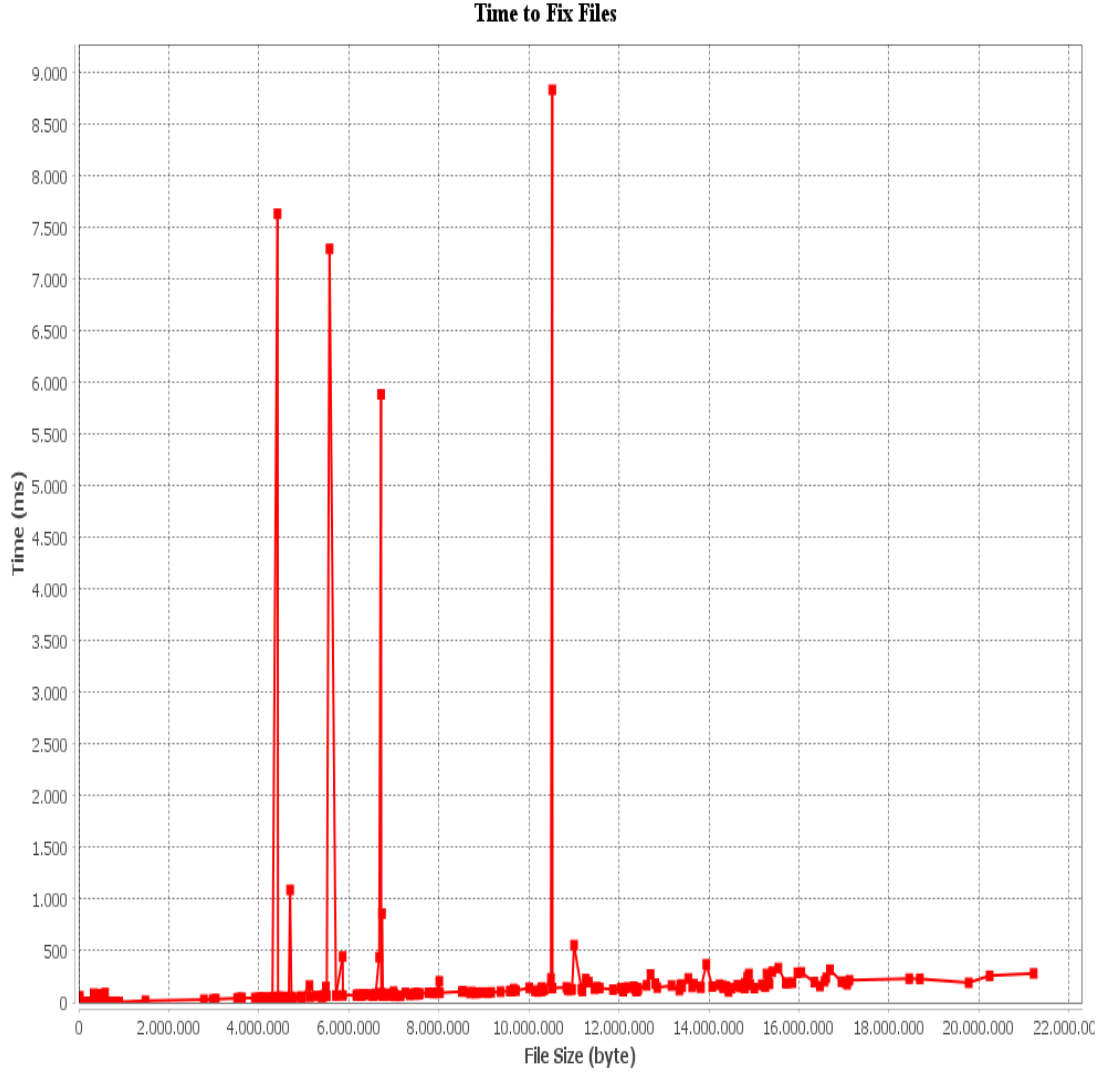
Şekil 6 ve Şekil 7 incelendiğinde kullanılan veriler de dikkate alınarak dosya manipölasyon hızının Şekil 6’de PDF çalışmasında görölen grafıklere benzer olarak doğru orantılı olacak şekilde gerçekleştiğı görölmektedir. Şekil 7’da ise ara belleğe alarak manipölasyon yapılması durumunda elde edilen grafik incelendiğinde zamanlayıcı (scheduler) sıçramaları dışında, dosya manipölasyonunun çok hızlı yapıldığı görölmektedir. Ara bellek tekniğı kullanılarak yapılan çalışmalarda genellikle sıçramalar görölmektedir. Bunun sebebi daha önceki PDF çalışmasında ifade edilmiştir.

Şekil 8 ve Şekil 9’de tersine manipölasyon işlemleri paylaşılmaktadır. Şekil 8’de tersine bayt manipölasyonu tekniğı uygulanması sonucunda EK-7’de paylaşılan boyut (bayt) – zaman (ms) verileri kullanılarak elde edilen grafik paylaşılmıştır.



Şekil 8 JPG tersine bayt manipölasyonu grafiğı

Şekil 9’de ise tersine ara bellek tekniğı kullanılarak elde edilen EK-8’deki boyut (bayt) – zaman (ms) verilerinin kullanılmasıyla elde edilen grafik paylaşılmıştır.

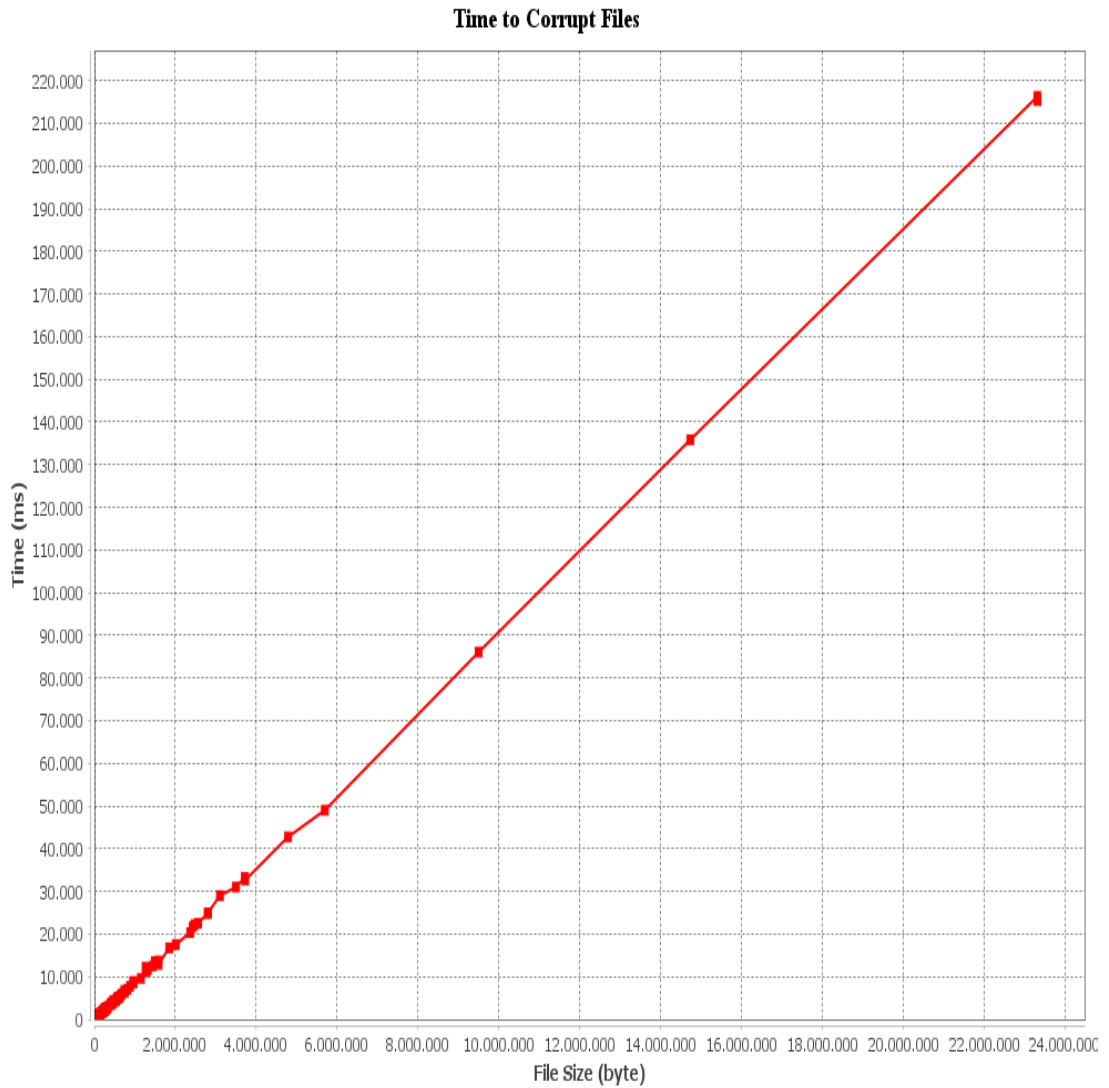


Şekil 9 JPG tersine ara bellek tekniği manipölasyonu grafiği

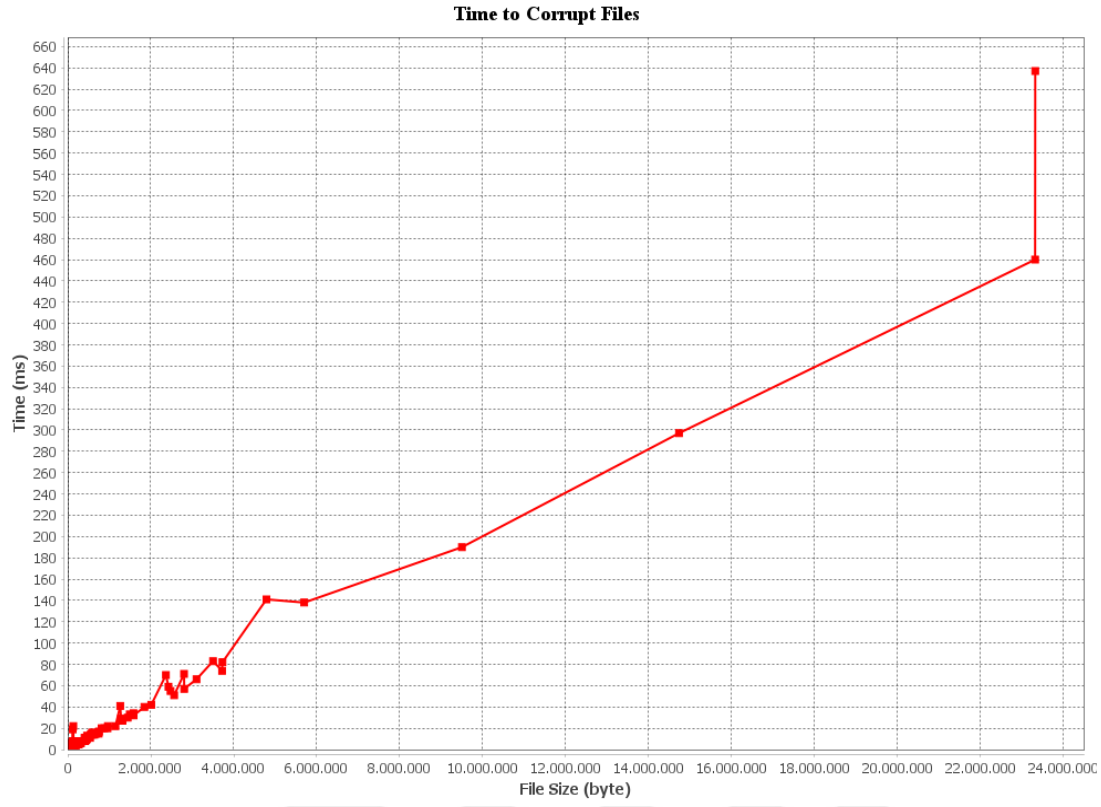
Şekil 8 incelendiğinde elde edilen verilerin tersine bayt tekniği kullanılması sebebiyle Şekil 9’de paylaşılan tersine ara bellek tekniğinden daha yavaş gerçekleşmesi neticesinde elde edilen grafikte doğru orantılı bir sonuç görülmektedir. Şekil 9’de ise tersine ara bellek tekniğinin çok hızlı çalışması sebebiyle elde edilen grafikte zamanlayıcı (scheduler) sıçramaları dışında neredeyse anlık bir performans sergilediği görülmektedir. Çok daha büyük bir JPG veri seti kullanılarak aynı işlemler gerçekleştirilme yoluna gidilseydi elde edilecek grafik yine doğru orantılı bir görüntüye sahip olacaktır. Aynı PDF çalışmasında olduğu gibi JPG dosyalarında da gerçekleştirilen manipölasyon ve tersine manipölasyon sonucunda dosyalar eski haline getirilmiş ve çalışır halde olup, elde edilen sonuçlar dikkate alındığında algoritmanın dosya türüne göre değil dosya boyutuna göre performans gösterdiği ve doğru orantılı bir sonuç elde edildiği görülmüştür.

### 3. DOC Dosya Türü Manipülasyonu ve Tersine Manipülasyonu

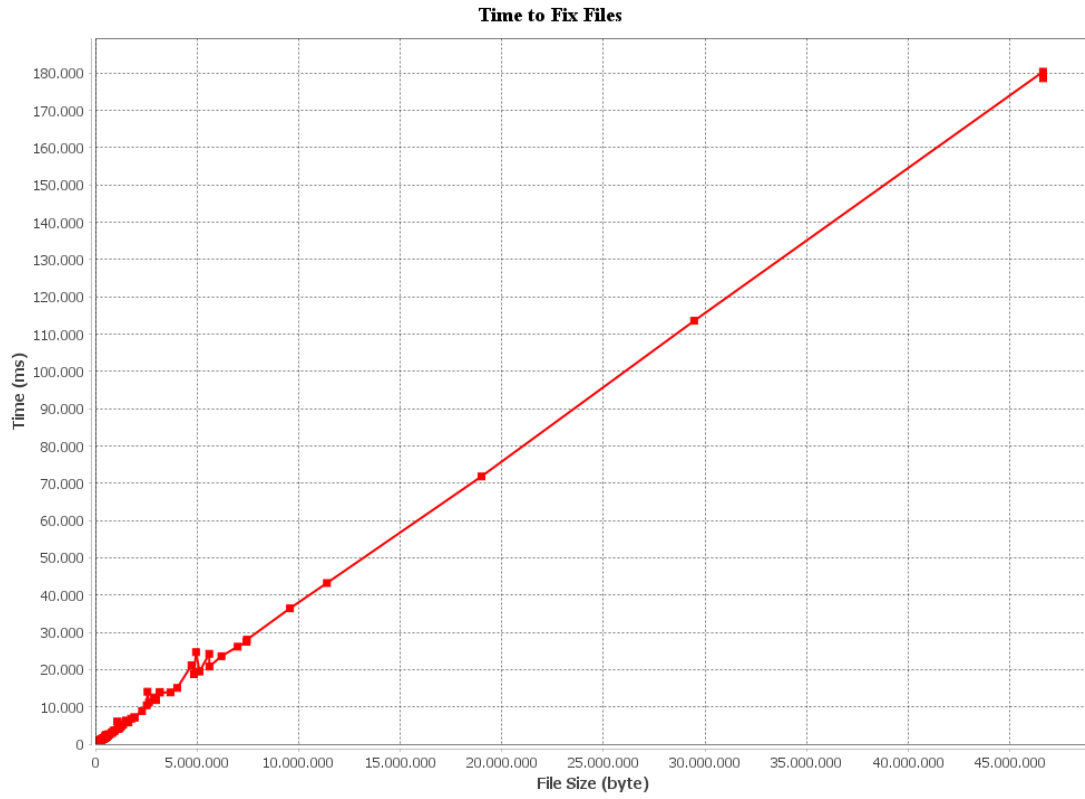
533 farklı .doc uzantılı dosya veri seti olarak kullanılmıştır. Kullanılan veri setinin toplam büyüklüğü 176 MB olarak ölçülmüştür. Daha önce PDF ve JPG dosya türlerinde yapıldığı üzere bayt ve ara bellek teknikleri dosya manipülasyonu için kullanılmıştır. Elde edilen boyut (bayt) – zaman (ms) verileri EK-9 ve Ek-10’da paylaşılmış olup Şekil 10 ve Şekil 11’de elde edilen grafik paylaşılmıştır. Aynı şekilde tersine manipülasyon teknikleri kullanılarak Ek-11 ve Ek-12’de paylaşılan veriler elde edilmiş ve bu verilerin kullanılması neticesinde Şekil 12 ve Şekil 13’de paylaşılan boyut (bayt) – zaman (ms) grafikleri elde edilmiştir.



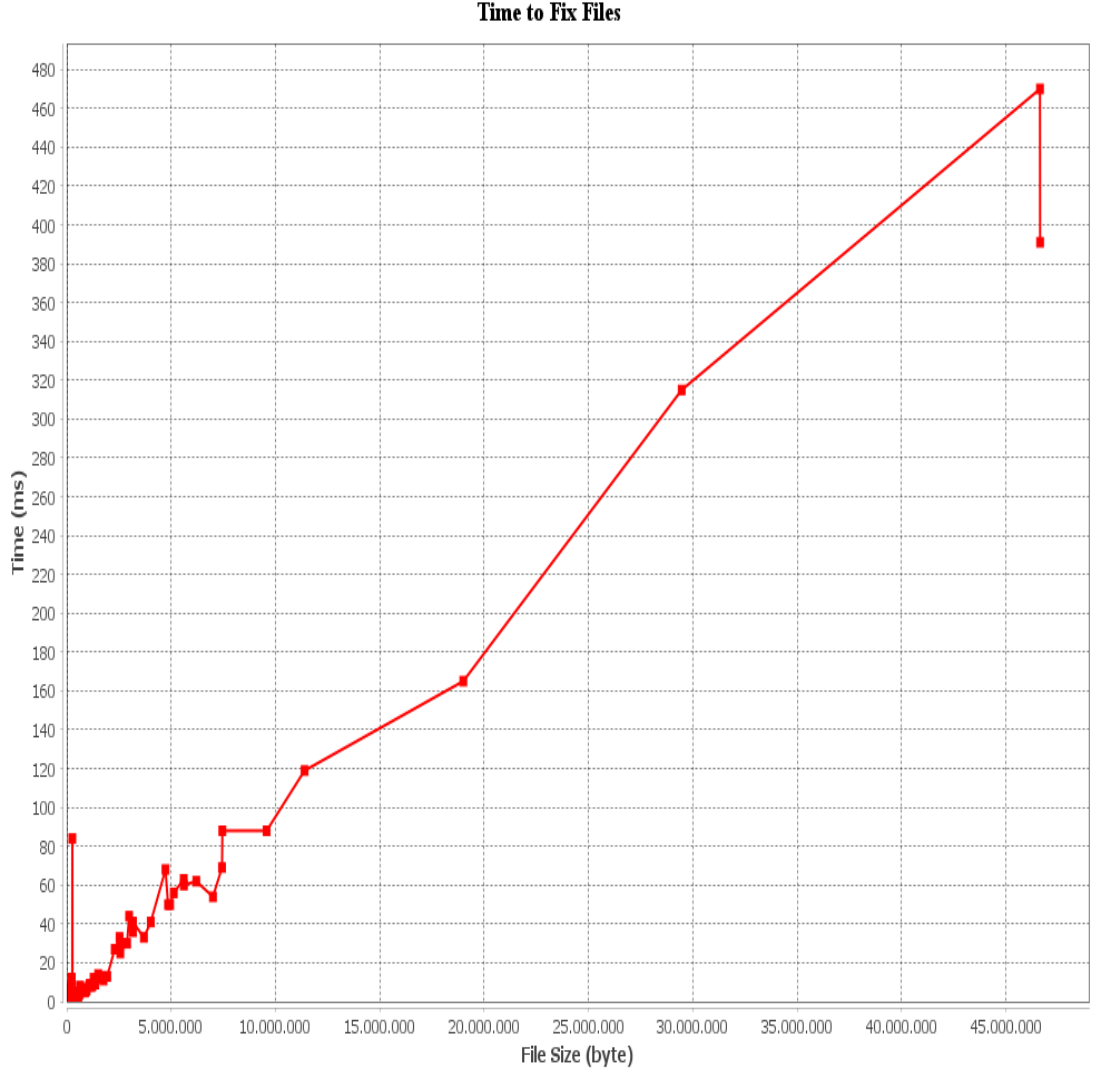
Şekil 10 DOC bayt tekniğiyle manipülasyon grafiği



Şekil 11 DOC arabelleğe alma yöntemiyle manipölasyon grafiğı



Şekil 12 DOC tersine bayt manipölasyonu grafiğı

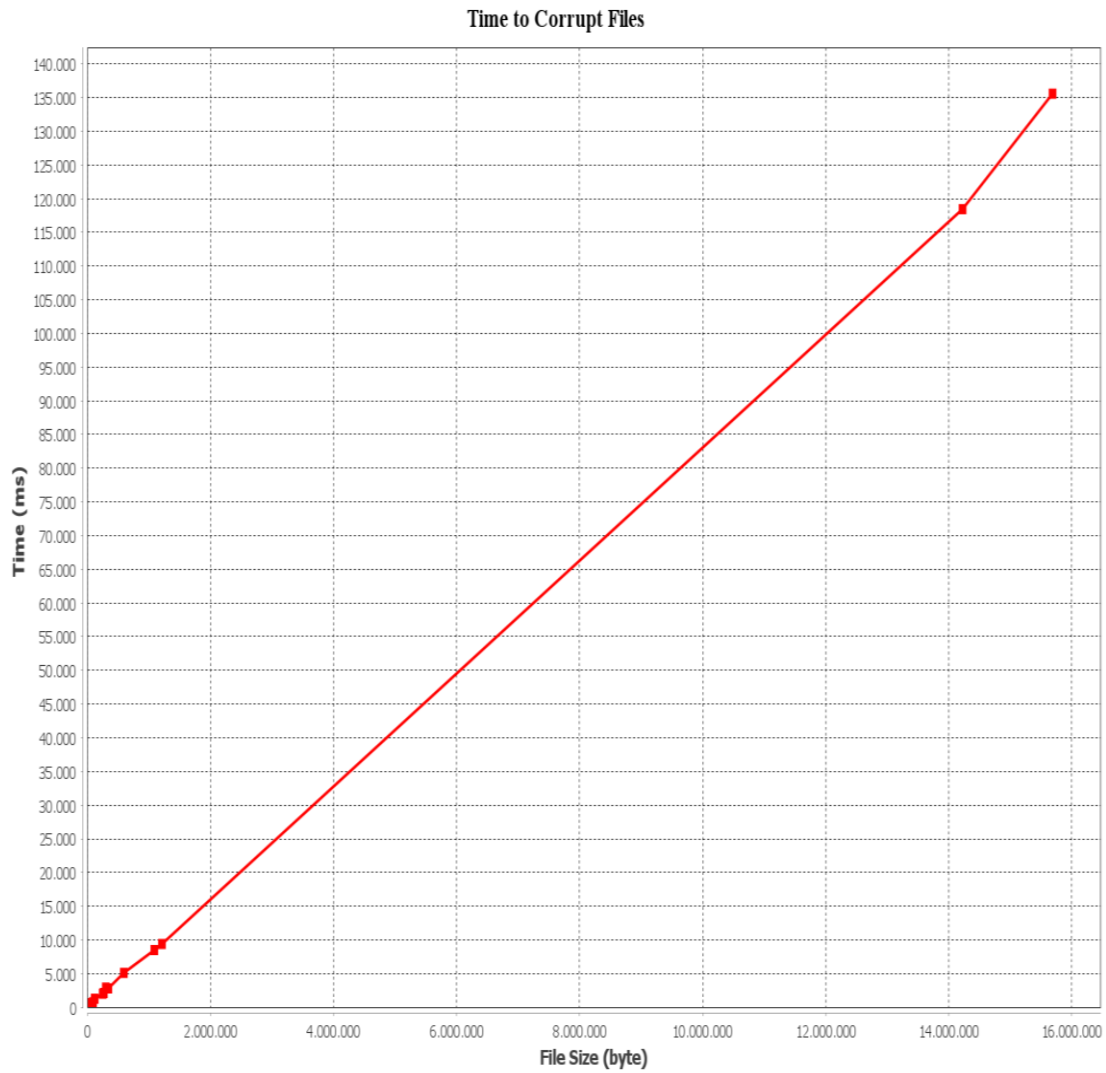


Şekil 13 DOC tersine ara bellek tekniği manipölasyonu grafiđi

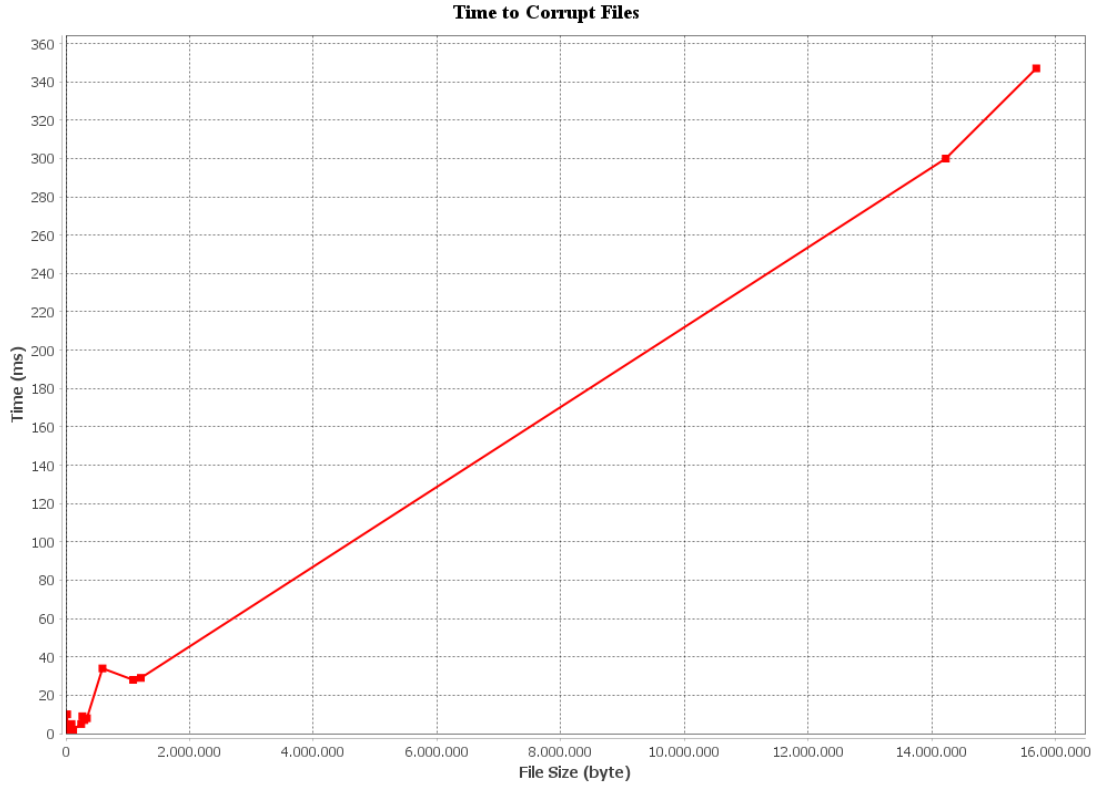
Şekil 12 ve Şekil 13’de paylaşılan grafikler incelendiğinde dosya boyutu ile doğru orantılı bir boyut-zaman grafiđi görölmektedir. Ara belleđe alarak verilerin manipöle edilmesi beklendiđi üzere hız olarak çok daha olumlu sonuçlar vermiştir. Şekil 14 ve Şekil 15’de elde edilen sonuçlar incelendiğinde tersine manipölasyon sonucunda beklenen hız farkının yanı sıra özellikle Şekil 15’de paylaşılan ara bellek tekniğinde görölen ufak sıçramalar bulunmaktadır. Ayrıca kullanılan veri tabanındaki dosyaların boyutları benzer ve uyumlu oldukları için elde edilen grafiklerde dosya boyutu (bayt) ile zaman (ms) grafiklerinde doğru orantılı bir sonuç elde edildiđi görölmektedir. DOC dosya türünde elde edilen sonuçlar aynı PDF ve JPG dosya türlerinde elde edilen sonuçlarla benzer nitelikte olmuştur. Manipölasyon ve tersine manipölasyon süreçlerinde hiçbir sorun ile karşılaşılmamış ve orijinal dosya tekrardan elde edilmiştir.

#### 4. XLSX Dosya Türü Manipülasyonu ve Tersine Manipülasyonu

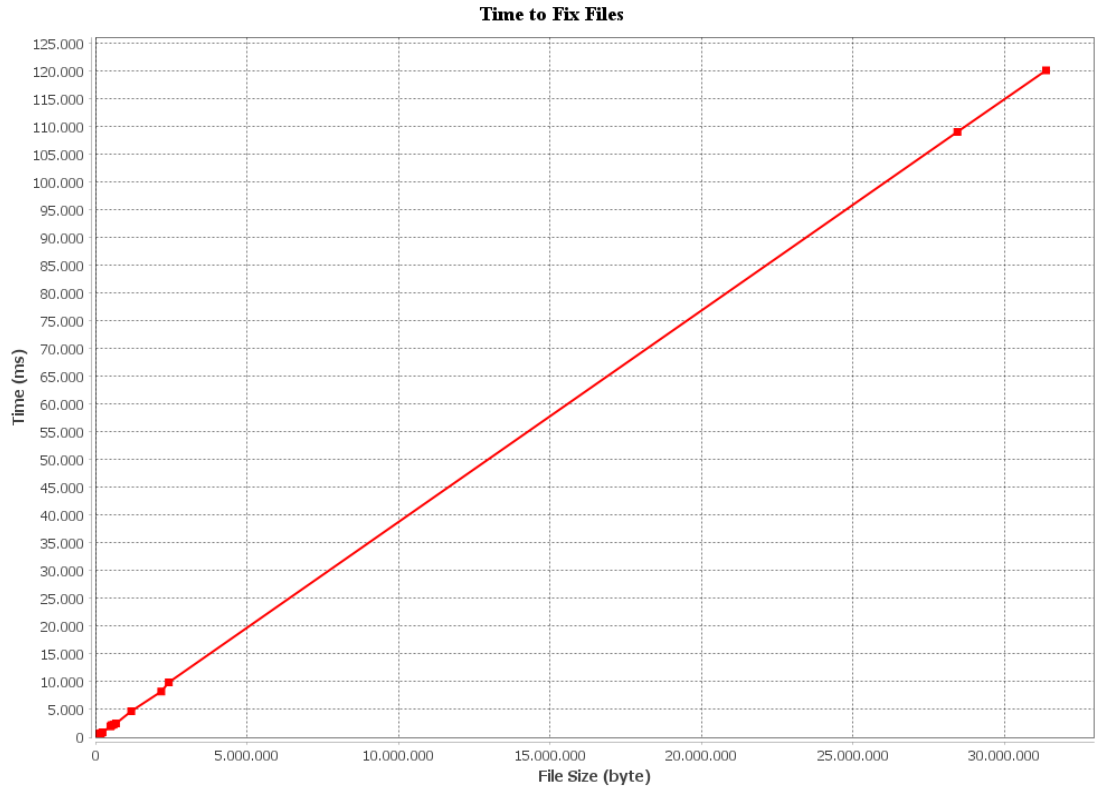
136 farklı .xlsx dosyası veri tabanı olarak oluşturulmuştur. Veri tabanının toplam büyüklüğü 32.2 MB seviyelerindedir. Daha önceki dosya türlerinde yapılan manipülasyon ve tersine manipülasyon işlemleri bayt ve ara bellek teknikleri için yapılmıştır. Sırası ile Ek-13, Ek-14, Ek-15, Ek-16’da paylaşılan boyut (bayt) – zaman (ms) verileri kullanılarak aşağıda paylaşılan Şekil 14, Şekil 15, Şekil 16 ve Şekil 17 elde edilmiştir.



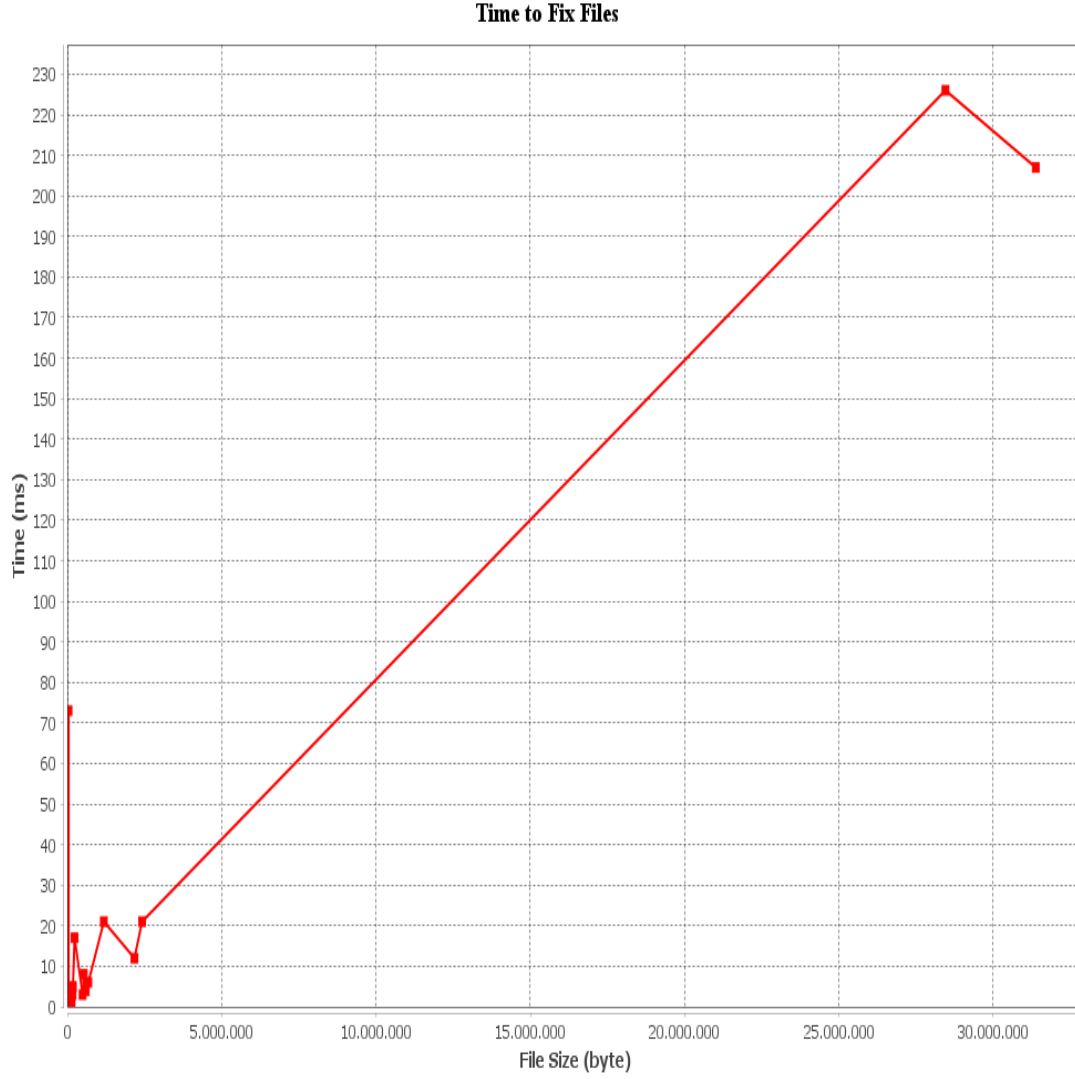
Şekil 14 XLSX bayt tekniğiyle manipülasyon grafiği



Şekil 15 XLSX arabelleğe alma yöntemiyle manipülasyon grafiği



Şekil 16 XLSX tersine bayt manipülasyonu grafiği



Şekil 17 DOC tersine ara bellek tekniği manipölasyonu grafiđi

Şekil 14 ve Şekil 15’de paylaşılan grafiklerde paylaşılan sonuçlar incelendiđinde ara bellek yönteminin çok daha hızlı bir şekilde aynı işlemi gerçekleştirdiđi görölmektedir. Grafiklerden de anlaşılacağı üzere dosya boyutu arttıkça gereken süre de artmaktadır. Şekil 15’de ara bellek yönteminin grafiđi tekrardan incelendiđinde elde edilen sonuçlarda sıçrama olarak kabul edeceğimiz bir uyumsuzluđun olmadığı görölmektedir. Bunun en büyük sebebi kullanılan veri setimizin özellikle PDF veri setine nazaran daha ufak boyutlarda olmasıdır.

Şekil 16 ve Şekil 17’da elde edilen tersine manipölasyon grafikleri incelendiđinde benzer durumun olduđu anlaşılmaktadır. Ancak Şekil 17’da zamanlayıcı (scheduler) sebebiyle ufak bir sıçramanın olduđu görölmektedir.

#### **D. Manipülasyonu Sonuçlarının Analizi**

Tüm dosya türleri üzerinde uygulanabilecek yapıda olan manipülasyon algoritmamız bayt tekniği ve ara bellek tekniği kullanılarak seçilen dört dosya türünde uygulanmıştır. Şekil 2, Şekil 6, Şekil 10, Şekil 14’de bayt tekniği kullanılarak dosya türleri üzerinde manipülasyon yapılması sonucunda elde edilen boyut (bayt) – zaman (ms) formundaki Ek-1, Ek-5, Ek-9, Ek-13’de paylaşılan veriler kullanılarak elde edilmiş grafikler paylaşılmıştır. Paylaşılan bu grafiklerin ortak noktası zaman açısından çok ciddi sürelerle mal olmasıdır. Ancak yapılan manipülasyonun başarı ile gerçekleşmesi ve manipüle edilmiş dosyanın geliştirmiş olduğumuz sistemde bir ağ dinleme saldırısı olması halinde saldırganlara anlamlı bir veri kaybı yaşatmayacağı için büyük bir öneme sahiptir. Ayrıca tüm veri türlerinden elde edilen grafikler incelendiğinde doğrusal bir yapı yani dosya boyutu arttıkça gereken zaman miktarının arttığı görülmektedir. Bayt tekniği tez çalışmamızda geliştirilen sistemde kullanılmamaktadır. Bunun yerine ara bellek tekniği dediğimiz verilerin ara belleğe çok sayılarda işleme alınıp hızlıca yapılmasını sağlayan yöntem tercih edilmiştir. Şekil 3, Şekil 7, Şekil 11 ve Şekil 15’de paylaşılan görseller Ek-2, Ek-6, Ek-10, Ek-14’de ara bellek tekniğinin kullanılması sonucunda elde edilen veriler kullanılarak hazırlanmıştır. Test etmiş olduğumuz tüm dosya türlerinde elde edilen grafikler incelendiğinde doğrusal ilerleyişi bozan bazı sıçramalar olduğu görülmektedir. Bu sıçramaların sebebi bilgisayar zamanlayıcısı (scheduler) olup ara belleğin sıkça kullanılması durumunda görülen bir durumdur. Test işlemleri sürecinde bu durumun daha iyi anlaşılabilmesi için dosya türlerinin veri tabanları değişken boyutlarda tercih edilmiştir. En büyük veri kümesi olarak PDF seçilmiş ardından JPEG, DOC ve XLSX dosya türleri veri tabanı büyüklüğüne göre sıralanmıştır. Küçük kabul edilebilecek veri setlerinde zamanlayıcı (scheduler) sıçramaları yok denecek kadar az karşımıza çıkmıştır. Ara bellek tekniği beklenildiği üzere hız açısından geliştirmiş olduğumuz algoritmaya uygun kabul edilecek seviyelerdedir. Bu sebeple manipülasyon yöntemi olarak ara bellek tekniği tercih edilmiştir.

Yapılan manipülasyon işlemi sonrasında geliştirmiş olduğumuz algorithmada şifreleme ve anahtar paylaşımı çalışmaları yapılmaktadır. Alıcı tarafına blokzincir temelli geliştirilen güvenli iletim ağından ulaştıktan sonra şifre çözülecek ve manipüle edilmiş dosyaya erişilecektir. Şekil 4, Şekil 8, Şekil 12, Şekil 16’de

paylaşılan grafikler Ek-3, Ek-7, Ek-11, Ek-15’de bulunan boyut (bayt) – zaman (ms) veriler kullanılarak oluşturulmuştur. Bu grafiklerde bayt tekniğiyle manipüle edilmiş dosyaların tersine manipülasyonundan elde edilen veriler kullanılarak paylaşılmıştır. Hız açısından oldukça başarısız olan bu teknik tersine manipülasyon sürecinin tamamlanması neticesinde orijinal dosyaya ulaşmamızı sağlamıştır. Şekil 5, Şekil 9, Şekil 13, Şekil 17’da Ek-4, Ek-8, Ek-12, Ek-16’da paylaşılan veriler kullanılarak oluşturulmuş boyut (bayt) – zaman (ms) grafiklerinde tersine ara bellek manipülasyonu işlemlerinin sonuçları gösterilmektedir. Görüleceği üzere zamanlayıcı (scheduler) sıçramaları tüm veri türlerinde görülmektedir. Süreç sonucunda elde edilen dosyalar zarar görmemiş ve orijinal hallerindedirler.

## **E. Sonuç**

Sonuç olarak manipülasyon ve tersine manipülasyon algoritmamızın sağlamış olduğu en önemli farklılıklardan birisi de tahrifat edilen dosya türlerinin birbirinden ayırt edilmesinin imkânsız hale gelmesidir. Bu özellik sayesinde iletim ağının saldırganlar tarafından dinlenmesi durumunda iletilen verinin türü hakkında fikir sahibi olmasının önüne geçilmektedir. Ayrıca okunamaz hale gelen dosyaların sahip oldukları bu hal sayesinde steganografi ile veri gizlenmesi sağlanabilmektedir. Son olarak anahtarın çeşitli sebeplerle kaybı durumunda ele geçen dosyanın anlamlı ve açılabilir bir yapıda olmaması sayesinde ek bir koruma katmanı sağlayacaktır. Tez çalışmamızın ilk aşaması olan dosya manipülasyonu süreci başarı ile tamamlanmıştır.

### III. ŞİFRELEME

Kriptoloji yani şifreleme bilimi insanlığın asırlardır üzerine çalıştığı bir veri koruma konusudur. İlk örneği antik Mısırda görülen kriptoloji, milattan önce 5. yüzyılda Spartalı savaşçılar tarafından ilk olarak askeri amaçla kullanılmıştır. Kriptoloji tamamen matematiksel formüllerden oluşmaktadır ve iki alt başlıkta incelenmektedir. Bunlar kriptografi yani şifreli yazı yazma ve kriptanaliz yani şifre çözme çalışmalarıdır. Bilgisayar teknolojisinin insanlığın kullanımına sunulması ile birlikte ve verilerin dijitalleşmesi sayesinde şifreleme çalışmaları dijital ortamda yapılmaya başlamıştır. Şifreleme algoritmaları denilince akla 3DES, OTP, SNOW, RSA, AES, Blowfish, Twofish, MD5 gibi algoritmalar gelmektedir (Sudhakar vd., 2015).

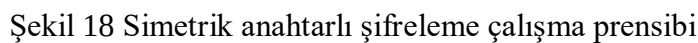
Kullanılmakta olan birçok farklı şifreleme algoritması bulunmaktadır. Daha önce de belirtildiği üzere Kerckhoffs'a göre geliştirilen tüm şifreleme algoritmalarının herkesçe algoritmik seviyede bilindiği düşünülerek hareket edilmelidir. Bu sebeple geliştirilen şifreleme algoritmaları her ne kadar karmaşıktırılır ve kırılması zor bir hale getirilse dahi geliştirilen algoritmanın herkesçe bilindiği düşünülerek güvenlik katmanları eklenmektedir; daha önemlisi anahtar paylaşımı da dahil olmak üzere tüm olasılıklar düşünülerek güvenli bir sistem geliştirilmelidir (Takaoğlu vd., 2021).

Günümüzde kullanmakta olduğumuz bilgisayarlar silikon bazlı işlemcilerle çalışmaktadır. Moore kanununa göre silikon bazlı işlemcilerin ulaşabileceği maksimum hız-boyut oranı bulunmaktadır. Kısaca ifade etmek gerekirse her 18 ayda bir donanım boyutu ufalırken hızı ise iki kat artacak ve maliyeti ise aynı kalacak ya da düşme trendinde olacak şeklinde tanımlanan bir kanundur. Kullanıcılar tarafından kolaylıkla alınabilen i9 10. nesil işlemcili yüksek hızda performans sunan bilgisayarlar bu hesaplama gücüne sahip silikon bazlı işlemcilere sahiptir. Kullanılan işlemci boyutu ve elde edilen performans dikkate alındığında erişilebilecek optimal seviyelere yaklaşıldığını söylemekte bir sakınca yoktur. Süper bilgisayar da bu işlemcilerin kullanımından

oluşturulduğu için silikon temelli işlemcilerle ulaşılabilecek hesaplama gücünün eşiklerine geldiğimiz söylenebilir. Eskiden olduğu gibi günümüzde de sahip olunan hesaplama gücü ihtiyacı, temelde kriptolojik ihtiyaçların giderilmesinde kullanılmaktadır. Genellikle hesaplama gücü ile şifrelenmiş bu dosyaların kaba kuvvet kullanarak anahtar tahmini yapılmaya ya da farklı kriptanaliz teknikleri kullanılarak korunan veriye ulaşılmaya çalışılmaktadır. Bu noktada hesaplama gücü büyük bir önem taşımaktadır. Günümüzde sahip olunan ve ilerleyen süreçte erişimi çok daha kolay bir hal alacak olan kuantum hesaplama gücü bu türde kriptanaliz yöntemlerinin başarılı olmasında büyük kolaylıklar sağlayacaktır (Boakye-boateng ve Lashkari, 2019).

Hesaplama gücünün her geçen gün arttığı bir ortamda veri güvenliğinin sağlanabilmesi için şifreleme algoritması seçerken yapılması gereken bazı işlemler bulunmaktadır. Bunlar; güvenilir algoritma seçimi, uygun anahtar uzunluğu seçimi ve anahtar paylaşımının güvence altına alınmasıdır. Seçilecek olan şifreleme algoritmasının algoritmik seviyede sahip olduğu karmaşıklığın yeterli seviyede olması gerekmektedir. Örnek vermek gerekirse AES ya da OTP gibi oldukça uzun bir süredir kullanılan şifreleme algoritmalarının sahip oldukları karmaşıklık seviyesi, kuantum sonrası dönem diye adlandırılan ve algoritmaların güvenilirliğinin çok ciddi bir şekilde test edileceği süreçte işler halde kalabileceği öngörülmektedir. Kuantum sonrası süreç için geliştirilen birçok şifreleme yöntemi bulunmaktadır. Bunları; kod tabanlı (code-based), özütlü tabanlı (hash-based), kafes tabanlı (lattice-based), çok değişkenli (multivariate) ve izojen tabanlı (isogeny-based) olarak sınıflandırabiliriz. Ayrıca seçilen anahtar boyutunun uzunluğu da bir diğer önemli faktördür. AES algoritması için 256 ya da geliştirilecek daha uzunluğa sahip bitlik anahtar uzunluklarının kullanılması halinde AES algoritmasının sahip olduğu algoritmik karmaşıklığın kuantum sonrası (Armanuzzaman vd., 2017) gerçekleştirilecek siber saldırılara karşı dayanıklı olacağı düşünülmektedir. Bir diğer önemli husus ise anahtar paylaşımının güvenli yapılmasıdır. Geliştirilen olağanüstü şifreleme algoritmaları, oluşturulan ve şifrelemede kullanılan yeterli uzunluktaki anahtarların varlığına rağmen en önemli faktörlerden biri güvenli anahtar paylaşım algoritmalarıdır. Kullanılan anahtarın güvenliğinin sağlanması için günümüzde birçok anahtar paylaşım algoritması kullanılmaktadır. Diffie-

Şifreleme yöntemleri iki alt başlıkta incelenmektedir. Bunlar simetrik ve asimetrik anahtarlı şifreleme yöntemleridir. Simetrik anahtarlı şifreleme algoritmaları günümüzde çok daha fazla tercih edilen, şifreleme ve şifreyi çözme sürecinde kullanılan anahtarın aynı olması mantığıyla çalışan algoritmalarlardır. Simetrik şifrelemelerde anahtar güvenliği tek anahtar kullanıldığı için bir nebze daha fazla önem taşımaktadır. Simetrik şifreleme algoritmaları oldukça hızlı çalışan algoritmalarlardır. Bu sebeple daha çok tercih edilmektedirler. En bilinen simetrik anahtarlı şifreleme algoritmaları Blowfish, AES, DES, 3DES, OTP gibi algoritmalar ancak çok sayıda simetrik anahtar şifreleme mantığıyla geliştirilmiş algoritma bulunmaktadır (Peechara ve Sucharita, 2021). Simetrik şifreleme çalışma prensibi Şekil 18’de paylaşılmıştır.



53

olduğu yenilik sayesinde birçok simetrik algoritmanın anahtar paylaşımında bu algoritmadan destek alınmaktadır (Shankar ve Akshaya, 2014).

#### **A. İleri Şifreleme Standardı (Advanced Encryption Standard, AES)**

Simetrik şifreleme algoritmalarından DES algoritması uzun bir süre boyunca güvenilir görülmüş ve kullanılmıştır. Simetrik yapıdadır ancak DES algoritmasının kırıldığıının ispatlanması sonrasında yeni bir şifreleme algoritmasına ihtiyaç duyulmuştur. AES şifreleme algoritması adında da geçtiği üzere bir şifreleme standardı olup DES şifreleme algoritmasının zayıf yönlerinin geliştirilmiş halidir. Ayrıca AES algoritması Rijndael algoritmasının geliştirilmiş halidir. Rijndael algoritmasında yer değiştirme ve permutasyon mantığı kullanılmaktadır. Kullanılan bu algoritmanın karmaşıklığı uygun büyüklükte blok ve anahtar kullanılması durumunda oldukça kuvvetlidir. AES algoritması blok şifreleme mantığını kullanır ve anahtar olarak şu an için 128, 192 ve 256 bitlik boyutlardaki anahtarları kullanmaktadır. AES algoritması geliştirilmiş olduğu DES algoritmasına göre çok daha güvenli ve hızlı bir algoritmadır. Bu sebeple günümüzde çokça kullanılan popüler şifreleme algoritmalarından biridir. AES simetrik şifreleme algoritmasının anahtar boyutu ve blok büyüklüğü sebebiyle yüksek hesaplama gücüne sahip saldırılara karşı dayanıklı olduğu kabul edilmektedir (Liang vd., 2021).

#### **B. Vernam Şifreleme Algoritması**

Vernam şifreleme algoritması One-Time-Pad (OTP) algoritması için kullanılan bir diğer isimdir. Gilbert Sandford Vernam tarafından geliştirilen ve kendi soy ismi ile anılan Vernam şifreleme algoritması, simetrik anahtarlı ve yüksek algoritmik karmaşıklığa sahip bir şifreleme algoritmasıdır. Çalışma mantığında XOR işlemi yatmaktadır. Gizlenecek verinin dosya boyutu kadar rastgele anahtar üreterek ve bunları XOR işlemine tabi tutarak gerçekleştirilen bir şifreleme algoritmasıdır. OTP algoritmasında en önemli koşul kullanılan anahtarın gerçek rastgele olarak seçilmesidir. Bunun sağlanabilmesi için günümüzde ufak bellekler boyutunda OTP anahtar üreteçleri satılmaktadır. Çünkü gerçek bir rastgelelik için bir doğa olayının (şimşek, yıldırım vs.) taklit edilmesi gerekmektedir. Ancak bu durumda gerçek bir rastgelelikten bahsetmek

mümkün olmaktadır. Kullanılan bu donanımlar gerçek rastgeleliğe en yakın sonucu veren anahtar üreten donanımlardır. Yazılımsal olarak da rastgele anahtar üretimi mümkündür. Ancak örnek vermek gerekirse Java kütüphanesinde bulunan rastgele anahtar üretme algoritmasının üretmiş olduğu anahtarların gerçek rastgeleliğe yakınlığı çok yüksek değildir. Bu sebeple güçlü bir bilgisayarın (süper ya da kuantum bilgisayarları) sahip olduğu hesaplama gücü ile Java rastgele anahtar üretiminde kullanılan fonksiyonun üretmiş olduğu anahtarlarda desen tespit edilebilir ve bu durum üretilen anahtarların tahmin edilmesinde kolaylık sağlayabilir (Sharma ve Somwanshi, 2018).

OTP algoritmasına çok basit bir örnek vermek gerekirse; 3 harfli CAY kelimesinin ASK kelimesi anahtar olarak kullanılarak XOR'lanması sonucunda CSI sonucu elde edilmektedir. CSI kelimesinin şifreli bir metin olduğu bilindiği farz edilerek çözülmeye çalışıldığında elde edilecek ve anlamlı olduğu düşünülen birçok dil de dikkate alınarak limitsiz sonuçlar elde edilebilir. Ancak elde edilen sonuçlardan hangisinin gönderilen orijinal metin olduğundan emin olmak anahtara sahip olmadan mümkün değildir. Çünkü üç harfli ve anlam içeren birçok kelime bulunmaktadır. Bu sebeple OTP algoritması anahtar paylaşımı güvenli yapıldığı durumlarda kuantum sonrası dönem de dahil olmak üzere güvenli kabul edilen algoritmalar arasındadır. Tezimizde de bu algoritmanın steganografiden faydalanılarak geliştirilmiş hali önerilmiştir. Anahtar rastgeleliği üzerine de çalışma yapılmış ve anahtar paylaşımına farklı bir çözüm getirilmiştir (Menon, 2018).

### **C. Üçlü Veri Şifreleme Standardı (Triple Data Encryption Standard, TDES)**

Triple DES algoritması DES algoritmasının 3 kez uygulanması sonucunda elde edilmektedir. DES algoritmasının kırılabilir bir yapıda olması sebebiyle aynı sürecin 3 defa üst üste uygulanması neticesinde daha güvenilir bir sistem elde edileceği düşünülmüştür. Anahtar uzunluğu 3DES algoritmasında arttığı için günümüzde birçok alanda örneğin bankacılık sistemlerinde olduğu gibi bu algoritmanın kullanımına devam edilmektedir. Anlaşılacağı üzere 3DES algoritması DES'e göre 3 kat daha yavaştır. Ayrıca AES algoritmasına göre ise 6 kat daha yavaş bir algoritmadır. Veri şifreleme standardı olarak Amerikan Ulusal Standartlar Bürosunun şifreleme üzerine standart geliştirilmesi için bir

talepte bulunması üzerine birçok Amerikan kuruluđu bu duyuruya algoritma önerileri iletmiştir. IBM'in önermiş olduđu şifreleme algoritması Amerikan Ulusal Güvenlik Ajansı tarafından üç yıllık bir çalışma neticesinde geliştirilerek DES algoritması önerilmiştir. Bir veri şifreleme standardı olan DES algoritması simetrik bir şifreleme algoritmasıdır. Blok şifreleme ve döngüler kullanılan bu algoritmada her döngüde kullanılan anahtar farklı olmaktadır. Ancak 2000'li yıllarda sahip olunan bilgisayar hesaplama gücü bu algoritmanın kaba kuvvet kullanılarak çözülmesine imkân tanımıştır. Bu sebeple AES algoritması yeni standart olarak kabul edilmiş ancak 3DES algoritması önerilerek halen kullanılmaya devam etmektedir (Wang ve Li, 2021).

#### **D. Önerilen Algoritma**

Tezimizde güvenli veri iletiminin sağlanması için planlanan ikinci modül verinin şifrelenmesi, anahtar üretimi ve anahtar paylaşımının sağlanmasıdır. Bu aşamada seçilen şifreleme algoritması OTP (Vernam) olmuştur. OTP algoritması şifreleme ve şifre çözme süreçlerinde aynı anahtarı kullanan simetrik bir şifreleme algoritmasıdır. Ayrıca Vernam şifreleme algoritmasının sahip olduđu yapısal karmaşıklık ilerleyen süreçte karşılaşılabilecek saldırılara karşı doğal bir koruma sağlamaktadır. Bunu şifrelenecek dosya boyutu kadar rastgele anahtar boyutu kullanması ve XOR işlemini gerçekleştirmesi sayesinde elde etmektedir. Anlaşılabileceği üzere uygulanması basit ancak kırılabilmesi teorik olarak imkânsız kabul edilen bir algoritmadır. OTP algoritmasının iki geliştirilmeye açık çalışma konusu bulunmaktadır. Bunlardan ilki yazılımsal olarak gerçek rastgele anahtar üretimidir. Anahtar üretiminde gerçek bir rastgelelik ihtiyacı fiziksel donanımların yardımıyla sağlanmaktadır. Yazılımsal olarak gerçek bir rastgelelikten bahsetmek pek mümkün değildir. Bu sebeple çalışmamızda donanım desteği olmadan, yazılımsal olarak elde edilen anahtarların rastgeleliğini artırıcı bir yöntem önerilmiştir. Önerilen algoritma test edilmiş ve elde edilen sonuçlar tez çalışmamızın ilerleyen bölümlerinde paylaşılmıştır.

İkinci çalışmaya açık konu ise diğer tüm şifreleme algoritmalarında da benzer bir ihtiyaç görülen anahtar paylaşımı sürecidir. Anahtar paylaşımı hususunda kullanılan birçok mekanizma olmasına rağmen bu işlemi

steganografi biliminden yararlanarak, tezimizde önermiş olduğumuz şekilde yapan otonom bir sistem literatürde görülmemektedir. Bu sebeple tezimizde anahtar paylaşımının gerçekleştirilmesi için anahtar paylaşımı yapılmadan bu ihtiyacı karşılayan bir algoritma geliştirilmiştir. Steganografi bölümünde bu işlemin nasıl gerçekleştirildiği ifade edilmiştir.

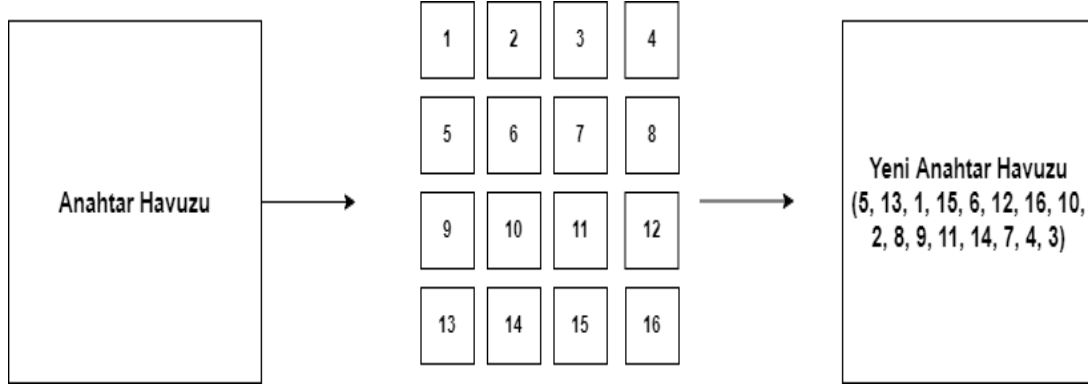
Çalışmamızda önerilen yöntemlerin uygulanmasında Java programlama dili kullanılmıştır. OTP algoritmasını Java dilinde programlamanın en büyük dezavantajı, gerçek rastgele bir sayı elde etmektir. Java rastgele anahtar üretim fonksiyonu belirlenen aralıkta sayılar üretmektedir. Ancak gerçek rastgelelik tartışmaya açıktır çünkü böyle bir şey gerçekten var olamaz ve varsa geleneksel yöntemlerle elde etmek çok zordur. En iyi yöntemle bile, yeterince rastgele bit oluşturursanız, bir model belirmeye başlayacaktır; bu herhangi bir anahtar oluşturma sistemi için zayıflık işaretidir. Bu nedenle önerilen algoritmamız anahtar rastgeleliği sorunuyla başa çıkmak için birtakım çözümler getirmektedir.

Önermiş olduğumuz yöntemde yapılması gereken işlemler sırasıyla gönderici tarafından şu şekilde yapılmaktadır:

- Gönderici ve alıcı tarafında önceden belirlenmiş aynı anahtar havuzu bulunur.
- Her iki tarafta da bulunan havuz 16 eşit alt parçaya bölünür.
- Rastgele olarak anahtar havuzu alt parçaları (16 adet) birleştirilerek yeni havuz elde edilir.
- Yeni havuzun oluşturulma sırası kaydedilir.
- İhtiyaç duyulan anahtar uzunluğu kadar oluşturulan havuzdan rastgele anahtar seçimi yapılır.
- Seçilen anahtarın havuzda hangi konumdan alındığı bilgisi kaydedilir.
- Seçilen anahtar kullanılarak OTP şifreleme algoritması uygulanır.
- Şifrelenmiş dosyaya alt segmentler rastgele seçilerek oluşturulan anahtar havuzu seçim sırası bilgisi ve anahtarın seçim yeri bilgisi steganografi mantığından faydalanılarak gizlenir.

- Gerekli tüm bilgileri taşıyan dosya alıcıya gönderilir.

Taraflarda bulunan anahtar havuzunun parçalara bölünüp rastgele olarak yeniden oluşturulması Şekil 19’da gösterilmiştir.

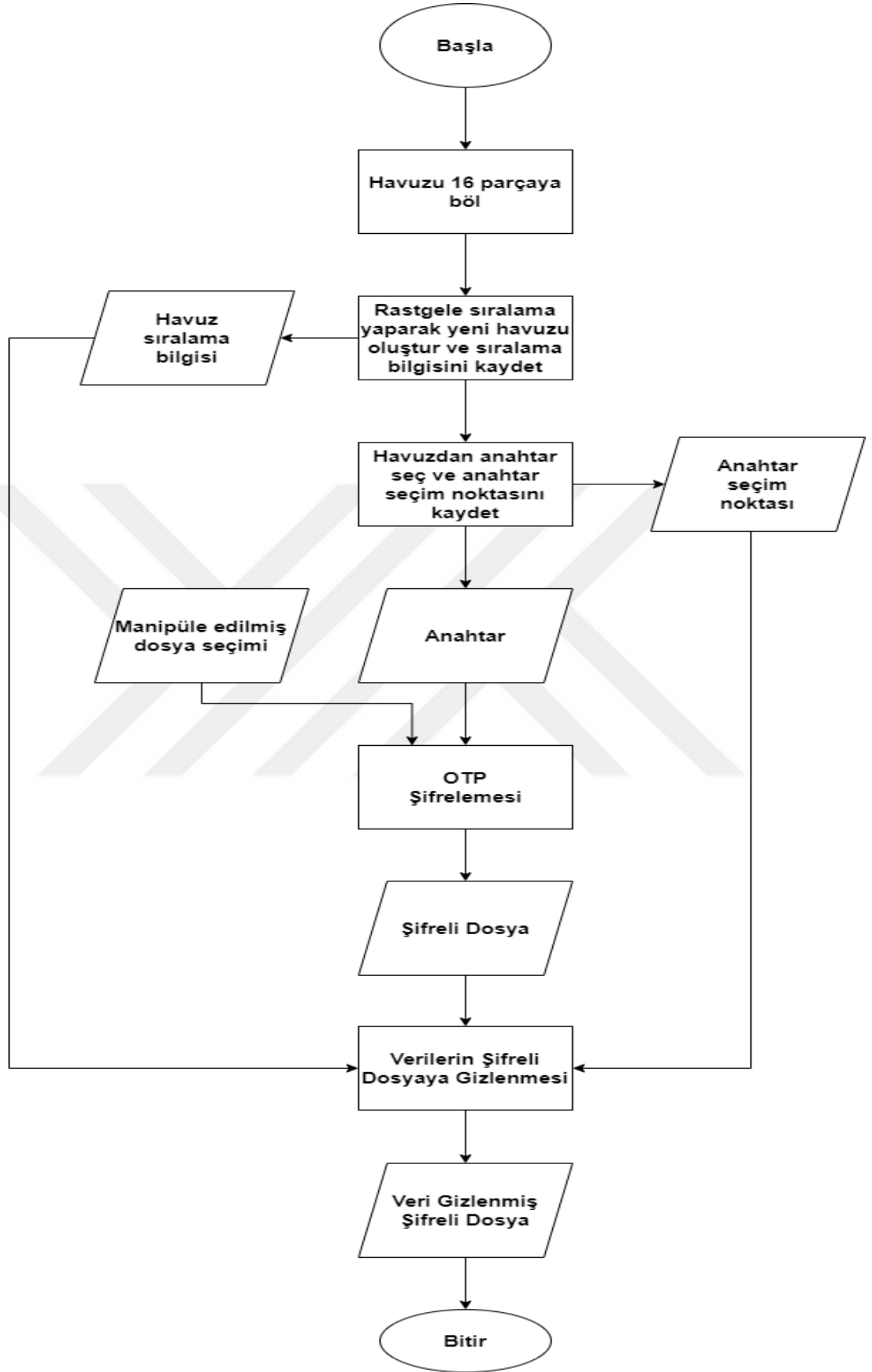


Şekil 19 Yeni anahtar havuzu elde edilme yöntemi

Dosya, şifrelenmesi ve gerekli bilgilerin gizlenmesi sürecinden sonra alıcı tarafına ulaşır. Alıcı tarafında şifrelenmiş veriden orijinal verinin manipüle edilmiş halinin elde edilebilmesi için aşağıda belirtilen adımlar uygulamaktadır:

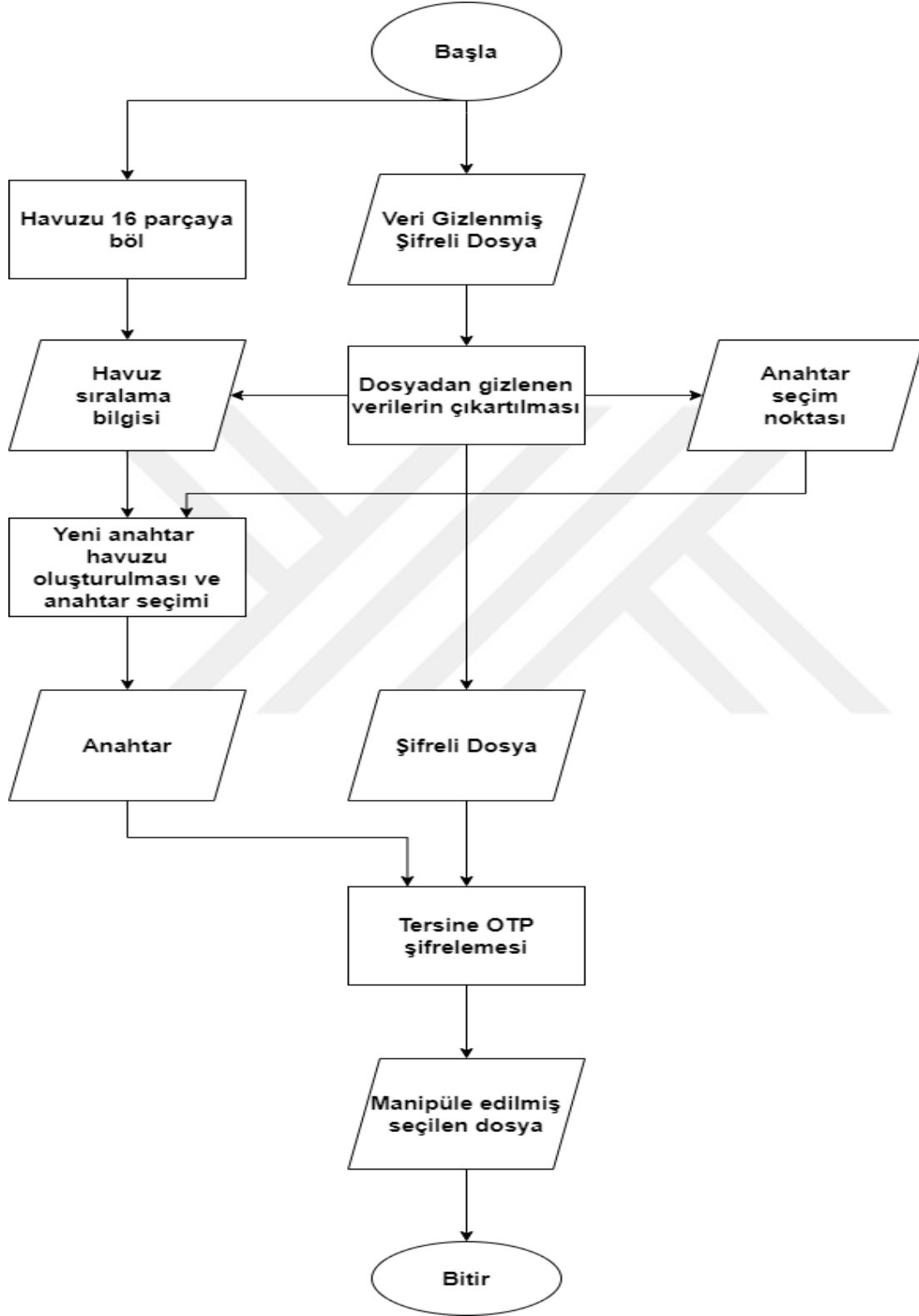
- Şifreli dosyadan gizlenen bilgiler (rastgele havuz oluşum sırası, anahtar seçim noktası) çıkartılır.
- Önceden paylaşımı yapılmış anahtar havuzu 16 alt parçaya bölünür.
- Şifreli dosyadan elde edilen rastgele havuz oluşturulma sırası bilgisi kullanılarak oluşturulan yeni havuz alıcı tarafında da oluşturulur.
- Yeni elde edilen havuzdan anahtar seçim yeri bilgisi kullanılarak dosya boyutu kadar okuma yapılır ve kullanılmış anahtar elde edilir.
- Anahtar kullanılarak şifrelenmiş dosya tersine OTP adımları izlenerek açılır ve dosyanın manipüle edilmiş haline ulaşılır.

Önerilen algoritmanın gönderici tarafında nasıl gerçekleştirildiğini gösteren blok diyagramı aşağıdaki Şekil 20’de paylaşılmıştır.



Şekil 20 Önerilen algoritma gönderici tarafı blok diyagramı

Önerilen algoritmanın alıcı tarafında nasıl gerçekleştirildiğini gösteren blok diyagramı aşağıdaki Şekil 21’de paylaşılmıştır.



Şekil 21 Önerilen algoritma alıcı tarafı blok diyagramı

## E. Test ve Analiz

Önerilen algoritmada anahtar seçiminde rastgeleliği arttırıcı ve anahtar paylaşımında steganografiden faydalanılan bir yöntem önerilmiştir. Tezimizin dosya manipülasyonu aşamasında önermiş olduğu manipülasyon yönteminden elde edilen manipüle edilmiş dosyalar test amaçlı kullanılmıştır. Seçilen manipüle edilmiş dosya OTP şifreleme algoritması ile şifrelenmiştir. Anahtar seçiminde rastgeleliğin arttırılması için şöyle bir yöntem izlenmiştir: Her iki tarafta da aynı anahtar havuzu bulunmaktadır. Bu havuzlar 16 parçaya bölünmüştür. Rastgele olacak şekilde 16 alt parça birleştirilmiş ve yeni bir havuz elde edilmiştir. Havuzun birleştirilme sırası kaydedilmiş ve steganografi bölümünde paylaşıldığı üzere bu bilgi gizlenmiştir. OTP algoritması dosya boyutu kadar anahtar kullanımı öngördüğü için oluşturulan havuzdan dosya boyutu kadar rastgele bir noktadan anahtar seçimi yapılmıştır. Bu seçimin yapıldığı yer bilgisi de steganografi ile gizlenmek üzere kaydedilmiştir. Anahtar elde edildikten sonra OTP algoritması uygulanmış ve manipüle edilmiş dosya şifrelenmiştir. Daha sonrasında havuz ve anahtar bilgisi dosya üzerine gizlenmiştir.

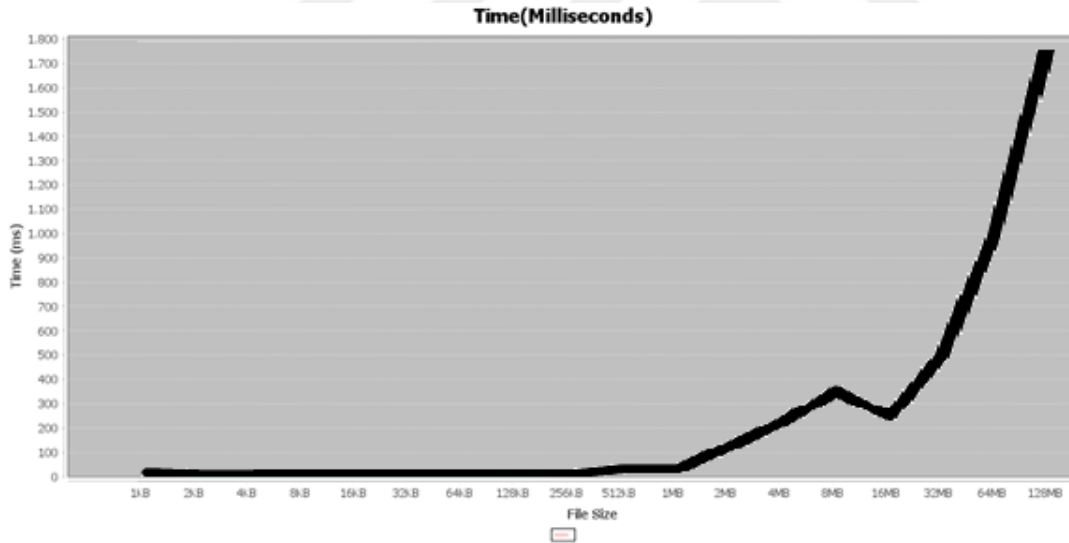
Şifrelenmiş dosya blokzincir kısmında paylaşılan şekilde alıcı tarafına iletilmektedir. Alıcı tarafı şifrelenmiş dosyayı elde ettiğinde öncelikli olarak yeni havuzu elde edebilmek için gizlenen verileri dosyadan elde eder. Havuz oluşturma bilgisi ve anahtar seçim noktası bilgisini dosyadan çıkartır. Geriye OTP ile şifrelenmiş dosya kalır. Ardından yeni havuz oluşumunu gerçekleştirebilmek için anahtar havuzunu 16 alt parçaya böler ve elinde bulunan sıralamayı takip ederek yeni havuzu oluşturur. Bu havuzdan anahtar seçim noktası bilgisi kullanılarak dosya boyutu kadar anahtar okunur ve tersine OTP algoritmasında kullanılarak tersine şifreleme süreci tamamlanır. Elde edilen dosya, dosyanın manipüle edilmiş halidir. Orijinal veriye ulaşmak için tersine manipülasyon işleminin yapılması gerekmektedir.

Önermiş olduğumuz şifreleme ve şifre çözme algoritmaları 1 kilobayt ile 128 megabayt boyutları arasında Çizelge 1’de paylaşıldığı üzere test edilmiştir. Elde edilen sonuçlar şifreleme ve şifre çözmek için mili saniye cinsinden hesaplanmış olup paylaşılmıştır.

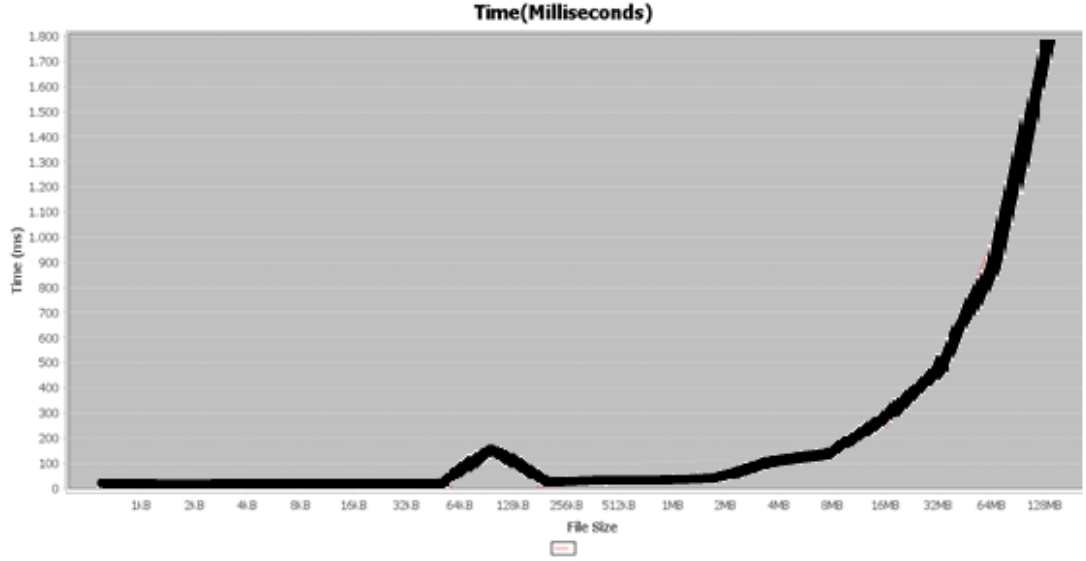
Çizelge 1 Şifreleme ve Şifre Çözme Süreleri (ms)

| Dosya Boyutu | Şifreleme | Şifre Çözme |
|--------------|-----------|-------------|
| 1 KB         | 6         | 5           |
| 2 KB         | 7         | 8           |
| 4 KB         | 7         | 6           |
| 8 KB         | 7         | 7           |
| 16 KB        | 7         | 8           |
| 32 KB        | 7         | 8           |
| 64 KB        | 7         | 7           |
| 128 KB       | 5         | 146         |
| 256 KB       | 10        | 18          |
| 512 KB       | 28        | 27          |
| 1 MB         | 31        | 27          |
| 2 MB         | 119       | 35          |
| 4 MB         | 212       | 98          |
| 8 MB         | 346       | 124         |
| 16 MB        | 242       | 271         |
| 32 MB        | 488       | 471         |
| 64 MB        | 974       | 871         |
| 128 MB       | 1727      | 1772        |

Çizelge 1'de paylaşılan test sonuçları Şekil 22 ve Şekil 23'ün oluşturulmasında kullanılmaktadır.



Şekil 22 Önerilen algoritma şifreleme sonuçları grafiği



Şekil 23 Önerilen Algoritma Şifre Çözme Sonuçları Grafiği

Şekil 22 ve Şekil 23’de paylaşılan grafikler incelendiğinde beklendiği gibi işlem süresinin doğrudan dosya boyutuna bağlı olduğu görülmektedir. Ayrıca aşağıda paylaşılan Çizelge 2’de AES ve 3DES algoritmalarının seçilen veri boyutlarındaki dosyalarda 10’ar kez uygulanması ve ortalamasının alınması sonucunda elde edilen sonuçları paylaşılmıştır.

Çizelge 2 AES, 3DES ve önerilen yöntem şifreleme ve şifre çözme sonuçları

| Şifreleme Algoritması  | Dosya Boyutu | Şifreleme (ms) | Şifre Çözme (ms) |
|------------------------|--------------|----------------|------------------|
| 3DES (168 Bit)         | 1 KB         | 488,2          | 487,3            |
| AES (128 Bit)          | 1 KB         | 81,2           | 82,0             |
| <b>Önerilen Yöntem</b> | <b>1 KB</b>  | <b>6</b>       | <b>6</b>         |
| 3DES (168 Bit)         | 16 KB        | 521,5          | 519,2            |
| AES (128 Bit)          | 16 KB        | 86,6           | 83,4             |
| <b>Önerilen Yöntem</b> | <b>16 KB</b> | <b>7</b>       | <b>8</b>         |
| 3DES (168 Bit)         | 32 KB        | 504,1          | 502,8            |
| AES (128 Bit)          | 32 KB        | 84             | 86,3             |
| <b>Önerilen Yöntem</b> | <b>32 KB</b> | <b>7</b>       | <b>8</b>         |

Çizelge 2 Önerilen Algoritma Şifre Çözme Sonuçları Grafiği Devam

|                        |              |              |             |
|------------------------|--------------|--------------|-------------|
| 3DES (168 Bit)         | 1 MB         | 513,5        | 506         |
| AES (128 Bit)          | 1 MB         | 85,5         | 83,4        |
| <b>Önerilen Yöntem</b> | <b>1 MB</b>  | <b>31</b>    | <b>27</b>   |
| 3DES (168 Bit)         | 16 MB        | 1002,2       | 998,6       |
| <b>AES (128 Bit)</b>   | <b>16 MB</b> | <b>165,9</b> | <b>83,3</b> |
| Önerilen Yöntem        | 16 MB        | 242          | 271         |
| 3DES (168 Bit)         | 32 MB        | 1428         | 1350        |
| <b>AES (128 Bit)</b>   | <b>32 MB</b> | <b>239,8</b> | <b>79,6</b> |
| Önerilen Yöntem        | 32 MB        | 488          | 471         |

Tablo 2’de paylaşılan elde edilen sonuçlar incelendiğinde OTP algoritmamızla şifrelenen dosyaların emsal şifreleme algoritmalarına nazaran küçük boyutlu dosyalarda çok daha az sürede gerçekleştirildiği görülmektedir. Dosya boyutu arttığında AES algoritması daha iyi sonuçlar vermeye başlamaktadır. Bu durumun sebebi OTP algoritmasının dosya boyutu kadar anahtar kullanarak tüm dosyayı şifrelemesidir. AES algoritmasında ise daha önceki bölümlerde ifade edildiği üzere 128 bitlik anahtar ile tüm dosyanın şifrlenmesinde blok mantığı kullanılarak gerçekleştirilmektedir.

Ayrıca elde edilen anahtarların rastgeleliğinin ölçülebilmesi için Amerikan Ulusal Standartlar ve Teknoloji Enstitüsünün yayınlamış olduğu Kriptografik Uygulamalar için Rastgele ve Sahte Sayı Üreticileri için İstatistiksel Test Paketi raporunda paylaşılan sıklık testi tezimizde uygulanmıştır. Bu teste göre elde edilen anahtarın rastgele olarak kabul edilebilmesi için gerekli olan sonuç 0.01’den büyük olmalıdır. Tezimizde geliştirilen rastgele anahtar seçim yönteminin üretmiş olduğu anahtarların rastgeleliği 0.1095 çıkmıştır. Yani üretilen anahtarlar rastgeledir.

## F. Sonuç

Tez çalışmamızın şifreleme modülünde önerilen algoritma ile anahtar rastgeleliği üst seviyede sağlanmaya çalışılmış ve anahtar paylaşımına yenilikçi bir çözüm getirilmeye çalışılmıştır. Anahtar rastgeleliğinin arttırılmasında alıcı ve gönderici arasında önceden paylaşılmış anahtar havuzlarının alt segmentlere ayrılması ve sonrasında her işlem gerçekleştirildiğinde rastgele olarak havuz dizilimini rastgele olarak gerçekleştirip, bu yeni havuz üzerinden anahtar seçimi yapılarak gerçekleştirilmektedir. 5 GB'lık bir anahtar havuzunun iki tarafta da olduğu düşünüldüğünde, bu havuzun 16 alt parçaya bölünerek rastgele olarak yeniden oluşturulması ve her anahtar seçimi işleminde bu sürecin tekrar etmesi rastgeleliği arttırıcı bir özelliktir.

Elde edilen yeni havuzdan anahtar seçimi yapılırken rastgele bir nokta belirlenmekte ve bu noktadan itibaren şifrelenecek dosya boyutu kadar anahtar okunarak anahtar seçimi süreci gerçekleştirilmektedir. Seçilen anahtarın havuzdaki başlangıç noktasının adresi tutularak steganografi aşamasında kullanılmak üzere saklanır.

Anahtar havuzunun rastgele oluşturulma sırası ve anahtar seçim noktasının bilgisi steganografi modülünde gizlenmektedir. Bu bilginin tespit edilmesi durumu düşünüldüğünde yani gizlenen bilginin stego-dosya'dan çıkartıldığı ve şifreli metnin elde edildiği durumda anahtar havuzu bilgisi saldırgan tarafından bilinmediği için yıkıcı bir risk teşkil edemeyecektir. Yine Kirchhof'un kanununa uygun olarak geliştirilen algoritma, herkes tarafından biliniyor olsa da sistem tüm olumsuzluklara rağmen güvenli bir yapıya sahiptir.

Tezimizde önerilen şifreleme modülü ile OTP şifreleme algoritmasının anahtar seçimi ve anahtar paylaşımı geliştirilmiştir. Önerilen algoritmamız, geleneksel OTP algoritmasının XoR operatörünü kullanması sayesinde, OTP algoritmasının sahip olduğu algoritmik karmaşıklığa bire bir sahiptir. Geliştirilen anahtar havuzu ve anahtar seçimi eklentileri şifrelemeye hiçbir extra karmaşıklık katmamış aksine rastgelelik açısından ve anahtar paylaşımına yenilikçi çözümler getirmiştir. Bu modülün başarı ile tamamlanması sayesinde diğer bir güvenlik modülü olan steganografi modülünün uygulanabilirliği mümkün hale gelmiştir.

Geliştirilmiş OTP algoritmamız sayesinde tezimizde geliştirmiş olduğumuz sistemimiz, kuantum sonrası dönem için güvenilir bir hale gelmiştir. Simetrik anahtarlı şifreleme algoritmalarında en büyük sorun olarak kabul edilen anahtar paylaşımı hususunda çözüm olarak önerilen yeni yöntemiz ile anahtar güvenliği üst seviyede sağlanmaktadır.



#### IV. STEGANOGRAFI

Steganografi bilimi verinin gizlenmesi üzerine odaklanan bir çalışma alanıdır. Gizlenen verinin fark edilmemesi için tarih boyunca birçok yöntem denenmiştir. Çoğunlukla askeri amaçlarla kullanılan steganografi yöntemleri verinin dijitalleşmesi ile birlikte dijital forma geçmiş ve birçok kişi tarafından çeşitli amaçlarla (askeri, istihbarat, illegal amaçlar vb.) kullanılabilir bir hal almıştır. Ancak yapılan dijital steganografinin elde ettiği sonuçlar yüzyıllar önce görülen örnekleriyle aynıdır. Daha önce insanlar tarafından fark edilmemesi için çalışılan steganografik çalışmalar günümüzde insanları geliştirdiği bilgisayarların fark edememesi için yapılmaktadır (Shehab ve Alhaddad, 2022).

Verinin dijitalleşmesi neticesinde steganografi teknikleri tümüyle değişmiştir; resim, yazı, ses ve video gibi kullanılan dosya türlerinde uygulanmakta ve veri gizlemesi yapılmaktadır (Adee ve Mouratidis, 2022). Gizlenen veriler çoğunlukla yazı formunda olup resim, ses veya video gibi veriler de gizlenebilmektedir. Günümüzde steganografi teknikleri protokol ve uzaysal tabanlı olmak üzere iki ana başlıkta incelenmektedir. Protokol steganografi tekniklerine Ayırık Fourier Dönüşümü (Discrete Fourier Transform), Ayırık Kosinüs Dönüşümü (Discrete Cosine Transform) ve Ayırık Dalgacık Dönüşümü (Discrete Wavelet Transform) teknikleri örnek verilebilir (Hammad vd., 2022). Uzaysal tabanlı tekniklere ise En az Önemli Bit (Least Significant Bit), Piksel Değeri Farkı (Pixel Value Differencing), Köşe Temelli Veri Gizleme (Edge-Based Data Embedding Method) ve Optimal Piksel Düzeltme Prosedürü (Optimum Pixel Adjustment Procedure) gibi teknikler örnek gösterilebilir (Xie vd., 2021).

Tez çalışmamızdan üretilen ve şu anda hakem incelemesinde olan makale çalışmamızda steganografide çokça kullanılan DWT algoritması ve OPAP algoritması birlikte kullanılarak resim içerisine metin gizlenmesi yapılmıştır. Önerilen yöntem ile kapak-resim olarak kullanılan dosya ayırık dalgacık dönüşümü kullanılarak Yüksek-Yüksek (YY), Yüksek-Düşük (YD), Düşük-Yüksek (DY) ve Düşük-Düşük (DD) olmak üzere alt bantlara bölünmüştür. Üzerinde veri gizleme

işleme LSB tekniği kullanılarak yapılmış ve ne düşük fark edilebilen bant olan DD bandında veri gizleme işlemi gerçekleştirilmiştir. Daha sonrasında tersine DWT algoritması kullanarak resim tekrar oluşturulmuştur. Elde edilen stego-resim kullanmış olduğumuz DWT algoritmasının kayıplara neden olması ve eklenen gizlenmiş verilerin oluşturmuş olduğu farklılık sebebiyle steganaliz yöntemlerince fark edilebilir yapıdadır. Bunun engellenmesi için OPAP algoritması kullanılmış ve elde edilen iyileştirmeler incelenmiştir. 1, 2 ve 3 bitlik veri gizleme işlemleri sonucunda OPAP algoritmasının 1 bitlik değişimlerde yani 1 bitlik LSB kullanılarak veri gizlenmesinde bir katkısı olmadığı görülmüştür. 2 ve 3 bitlik veri gizlemelerinde ise elde edilen PSNR değeri incelendiğinde 2 bit veri gizlemede OPAP kullanımının neredeyse 1 bitlik veri gizlenmiş gibi bir PSNR değeri elde edilmesine, 3 bitlikte ise 2 bitlik PSNR değeri elde edilmesine katkı sağladığı görülmüştür. Ayrıca OPAP sonrası elde edilen stego-resimden gizlenen verinin geri elde edilmesinde hiçbir kayıp olmamış ve gizlenen veriye erişim saplanmıştır. Önerilen bu makale çalışmasındaki algoritma sayesinde steganaliz yöntemlerinin daha zor fark etmesini sağlayacak bir iyileştirme elde edilmiştir.

Yine tezimizden üretilen Blokzincir Steganografisi çalışmasında steganografinin 2009 yılında hayatımıza giren Bitcoin kripto parasının ana gücü olan blokzincir teknolojisinin 2014 yılında bu isimle anılması ve uygulanabilirlik imkanlarının test edilmesi sonucunda günümüzde birçok alanda denenebilir bir çalışma konusu haline gelmesi neticesinde tezimizde denenmiştir. Blokzincir teknolojisinin bir sonraki bölümde anlatıldığı üzere sahip olduğu yapısal farklılık ve sistemlere katmış olduğu güvenlik ve gizlilik özellikleri sayesinde günümüzde kullanılan tüm steganaliz yöntemlerine karşı başarılı ve tespit edilmesi teorik olarak imkânsız olan, blokzincir sistemini bir nevi kapak-resim gibi kullanan algoritmamız tanıtılmıştır (Takaoğlu vd., 2021).

Ayrıca daha önce tez çalışmamızda yazıcı steganografisi üzerine yürütmüş olduğumuz araştırmalar neticesinde günümüzde de halen yapılmakta olan yazıcı steganografisi hakkındaki görüşlerimiz paylaşılmıştır. Kâğıt para sahteciliğinde renkli yazıcıların yaygınlaşması neticesinde görülen artış bir önlem alınması ihtiyacı ortaya koymuştur. Bu sebeple bastırılan yazıcı çıktılarında gözle görülemeyen ve tam olarak hangi bilgilerin gizlendiği paylaşılmayan bir veri gizlemesi yapılmaktadır. Konunun daha iyi anlaşılabilmesi için şu örneğin paylaşılmasında fayda vardır.

Yakın zamanda basına sızdırılan Amerikan askeri operasyonları ve bu operasyonlarda görülen olumsuz ve gizli bilgi niteliğinde saklanan uygulamalarının bir gazeteci tarafından basınla paylaşılması neticesinde bu bilgi sızdırılmasının kim tarafından yapıldığı bastırılan yazıcı çıktılarının incelenmesi sonucunda tespit edilmiştir. Çıktının alındığı yazıcı steganografi sayesinde tespit edilmiş ve haberi paylaşan kişiye kadar gerekli olan tüm bilgiler çorap söküğü gibi ortaya çıkmıştır. Çalışmamızda bu durum kamuoyu ile paylaşılmış ve konunun etik durumu üzerine görüşlerimiz paylaşılmıştır (Takaoğlu ve Takaoğlu, 2019).

Anahtar havuzu üretimi ve anahtar paylaşımı üzerine getirmiş olduğumuz algoritma önerilerinden tezimizde kullanılmaya karar verilen algoritmada steganografi yapılmasına karar verilmiştir. Günümüzde kullanılan dijital steganografi algoritmalarından bağımsız olarak, verinin gizlenmesini esas alan, yani steganografinin anlamı olan gizli yazı mantığından hareket ederek yeni bir veri gizleme yöntemi uygulanmıştır.

Tez çalışmamızın modüllerden oluştuğu ve tümünün birlikte çalışması neticesinde önermiş olduğumuz algoritmanın üst seviyede güvenlik sağlayacağını belirtmek gerekir. Çünkü dosya manipülasyonu aşamasında manipüle edilerek yeni bir dosya yapısına dönüştürülen dosyalar steganografi aşamasında yapacağımız veri gizlemesine imkân tanıyan çalışmadır. Manipüle edilmiş ve anlamlandırılabilen hiçbir yapısı olmayan dosyanın şifrelenmesi neticesinde elde edilen şifreli dosya üzerine gizlemek istediğimiz anahtar uzunluğu bilgisi, anahtar havuzu oluşturulma sırası, anahtarın havuzda başladığı yerin bilgisi gibi veriler gizlenmektedir.

#### **A. Önerilen Steganografi Algoritması**

Çalışmamızda dosya manipülasyonu işlemi gerçekleştikten sonra elde edilen haliyle üzerinde çalışılan dosya şifreleme aşamasına geçer. Şifreleme işlemi OTP algoritması kullanılarak gerçekleştirilir. Ancak anahtar havuzu üretiminde ve rastgele anahtar üretiminde geliştirmiş olduğumuz algoritma sayesinde rastgelelik arttırılmaktadır. Anahtar paylaşımında ise steganografi biliminin çalışma mantığından hareket ederek gizleme işlemi yapılmaktadır. Seçilen rastgele anahtar yeri bilgisi ve havuz oluşturma sırası bilgisi aşağıdaki sözde kodda görüleceği üzere belirlenmiş olan sayıda parçalara bölünüp yine algoritmada belirlenen ve değişkenlik gösteren lokasyonlara gizlenir. Tezimizde

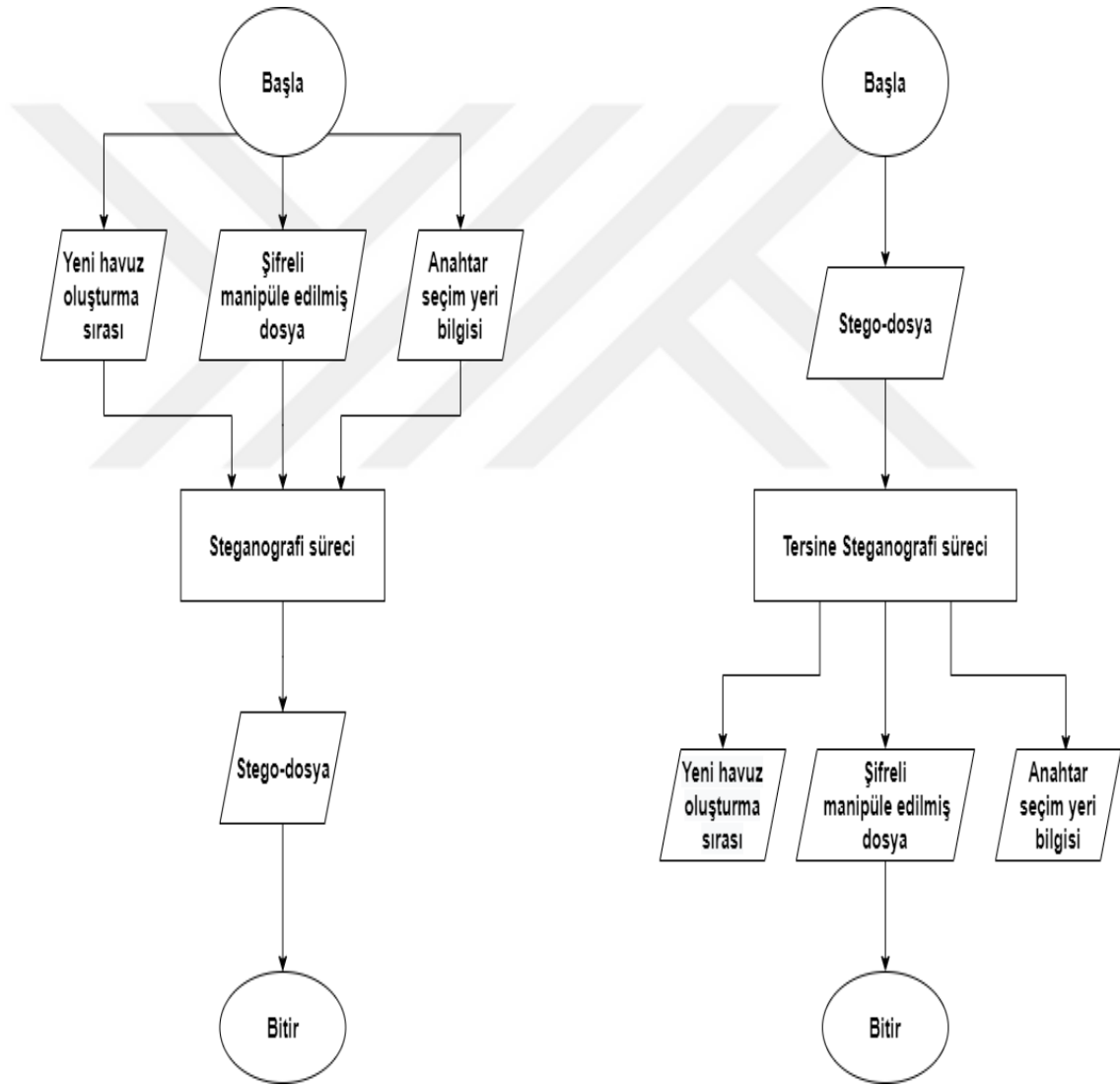
geliştirilen tüm modüller nihai bir son ürüne çevrilmek amaçlı geliştirildiği için steganografi bölümünde de görüleceği üzere geliştirilen tüm mekanizmalar en ince ayrıntısına kadar verilmemiş olup ne yapıldığı ifade edilerek ilerlenilmiştir.

- Başla
- Manipüle edilmiş dosyayı OKU
- Anahtar havuzunu 16 parçaya BÖL
- 16 parçayı rastgele sıralayarak yeni anahtar havuzunu OLUŞTUR
- Havuzdan dosya boyutunda bir rastgele anahtar SEÇ
- Anahtar seçim yeri bilgisini KAYDET
- OTP şifreleme algoritmasını seçilen anahtar ile UYGULA
- Gizlenecek havuz oluşturma sırası ve anahtar seçim yeri bilgilerini BELİRLE
- Bilgileri parçalara böl ve belirlenen yerlere EKLE
- Bitir

Aşağıdaki sözde kodda görüleceği üzere tersize steganografi yöntemi izlenerek gizlenen verilere ulaşılabilir ve sonrasında orijinal dosyaya erişilebilir.

- Başla
- Şifreli manipüle edilmiş dosyayı OKU
- Gizlenmiş havuz ve anahtar bilgilerini ÇIKART
- Havuzu 16 parçaya BÖL
- Yeni havuz oluşumunu elde edilen sıralama bilgisini kullanarak OLUŞTUR
- Oluşturulan havuzdan elde edilen anahtar seçim yeri bilgisini kullanarak anahtarı OKU
- Tersine OTP şifreleme algoritmasını anahtar ile UYGULA
- Bitir

Algoritma, anahtar havuzunun rastgele oluşturulması bilgisini ve anahtar seçim yeri bilgisini parçalara böler ve şifrelenmiş dosyanın önceden belirlenen yerlerine kaydeder. Tüm bu sistem sayesinde anahtar paylaşımı dosya ile birlikte gönderim esnasında gerçekleştirilir ve ayrıca ek bir anahtar paylaşım mekanizmasına gerek görülmez. Blokzincir eklentisi aşamasında paylaşılacak bilgiler incelendiğinde daha iyi anlaşılacağı üzere dosya bütünlüğü ve kurcalanamazlık blokzincir sayesinde sağlandığı için güvenlik üst düzeyde gerçekleşmiş olur. Aşağıdaki Şekil 24’de steganografi ve tersine steganografi algoritmalarının blok diyagramı paylaşılmıştır.



Şekil 24 Steganografi ve tersine steganografi diyagramları

## B. Sonuç

Steganografi süreci çalışmamızda alışlageldik yöntemler kullanılarak gerçekleştirilmemiştir. Çünkü geleneksel metin steganografisinde uygulanan yöntemler bizim gizlemek istediğimiz verilerin saklanması uygun değildir. Bu sebeple çalışmamızda bilginin saklanması için öncelikle gizleneceği dosyanın içinde farkedilmemesi sağlanmıştır. Bu farkedilmeme süreci manipülayon aşamasında dosya türlerinin ayırt edilemez tek bir dosya türüne dönüştürülmesi sayesinde olmuştur. Havuz sıralama bilgisi ve anahtar seçim yeri bilgisi manipüle edilmiş ve sonrasında şifrelenmiş dosya üzerine gizlenmiştir. Gizleme işlemi yapılırken gizlenecek bilgiler parçalara bölünmüş ve önceden belirlenen ve değişkenlik gösteren yerlere eklenerek dosya içerisinde fark edilmemesi sağlanmıştır. Bu sayede steganaliz yöntemleri manipüle edilen dosyaya gizlenen bu bilgilerin fark edilmesinde işlevsiz kalmaktadır. Çünkü steganaliz yöntemlerinin aramış oldukları veri gizleme tekniklerine çalışmamızda yer verilmemiştir. Steganografi algoritmamız, steganografi mantığından yola çıkarak yeni bir dosya türü için yeni bir gizleme yöntemi önermiştir. Bu sayede daha önce de belirtildiği üzere hem steganaliz yöntemlerine karşı başarılı bir algoritma elde edilmiş hem de anahtar paylaşımı süreci alışlageldik yöntemlerin aksine herhangi bir kanal kullanılmadan bir başka deyişle anahtar paylaşımı yapmadan alıcıya iletilmiştir.

## V. BLOKZİNCİR TEKNOLOJİSİ

Blokzincir teknolojisi, 2009 yılında Satoshi Nakamoto takma isimli bir kişi ya da grup insan tarafından önerilen Bitcoin kripto parasının başarılı olması sonucunda dikkatleri üzerine çekmiştir. Gerçek anlamda blokzincir teknolojisi kavramının ortaya çıkması ve ardının doldurulması 2014 yılına denk gelmektedir. Blokzincir 1.0 diye adlandırılan ve Bitcoin gibi finansal ürünlerin çalışıldığı bu dönemde birçok kripto para ve kripto para geliştirme platformları ve programlama dilleri geliştirilmiştir. Bitcoin sonrası benzeri ilgi çeken Ethereum kripto parası aynı Bitcoin'in yaptığı gibi kendi platformunu geliştirmiş ve yeni kripto paraların geliştirilmesinde bir hizmet olarak bu platformu sunmuştur. Günümüzde geliştirilen kripto paraların çok ciddi bir kısmı Bitcoin veya Ethereum blokzincir geliştirme platformundan faydalanılarak geliştirilmektedir. Solana ve benzeri birçok platform da günümüzde alternatif ve bu sistemlerde görülen eksikliklerin giderilmesi gibi katkılar sunan platformlardır. Blokzincir sistemlerinin geliştirilebilmesi için birçok programlama dilinden faydalanılabilmektedir. Java, JavaScript, C, C++, Solidity vb birçok programlama dili kullanılarak ihtiyaç duyulan blokzincir sistemleri geliştirilebilmektedir (Gatabazi vd., 2022).

Blokzincir teknolojinin finansal alanlar dışında kullanımına imkân tanıyan ve akıllı sözleşme diye tabir edilen, spesifik bir durum için önceden kodlandığı şekilde, aynı durum her oluştuğunda, aynı işlemi yapacak şekilde hareket eden kod parçaları sayesinde blokzincir sistemleri statik bir halden daha dinamik bir yapıya dönüşmüştür. Blokzincir teknolojinin akıllı sözleşmelerle buluşmasına Blokzincir 2.0 denilmektedir. Ethereum platformu akıllı sözleşmelerin kolaylıkla blokzincir sistemlerine eklenebilmesi için gerekli altyapıyı sunan ilk blokzincir geliştirme platformu olmuştur (Hsueh ve Chin, 2022).

Blokzincir teknolojinin finans dışındaki alanlarda uygulanabilirliğinin test edildiği ve hali hazırdaki sistemlere bir katman olarak da eklenebilecek

yapıda çalışmaların görüldüğü döneme Blokzincir 3.0 denilmektedir. Günümüzde blokzincir teknolojisinin neredeyse her alanda uygulanması üzerine çalışmalar yürütülmektedir. Sağlık, kamu hizmetleri, askeriye, havacılık, taşımacılık, endüstri, akıllı şehirler, finans, eğitim gibi konular başta olmak üzere şifreleme, anahtar dağıtımı, veri gizleme, kuantum anahtar dağıtımı gibi daha spesifik ve teknik konularda blokzincir teknolojisinin katabileceği artılar üzerine çalışmalar yürütülmektedir (Muduli vd., 2022).

Blokzincir teknolojisi özünde yeni çıkmış bir çalışma disiplini değildir. Blokzincir teknolojisi hali hazırda bulunan teknolojilerin spesifik bir ihtiyacın giderilmesinde uygun bir sıralama ile birleştirilmesi neticesinde elde edilmiştir. Zaman damgası algoritması, Merkle ağacı algoritması, özüt algoritmaları ve bilgisayar bilimi teorik bilgileri doğru bir şekilde uygulanarak öncelikle Bitcoin sonrasında da bir terim olarak anılan blokzincir teknolojisi elde edilmiştir. İlk üretilen dijital ve kripto para Bitcoin değildir. Birçok benzeri çalışmalar denenmiş ancak Bitcoin kadar tutulmamışlardır. Dünyanın blokzincir teknolojisine hazır olması da belki bu denli bir kabullenişin hızlanmasını sağlamıştır. İnsan psikolojisi de düşünüldüğünde, bir teknolojik yeniliğin finansal bir kazanç olarak insanlara yansması da bu kabullenişin hızlanmasında bir katkı sunmuş olabilir. Neticede blokzincir teknolojisi 2009 yılından günümüze gelen süreçte farklı dönüm noktalarından geçmiş ve gelişimini halen sürdürmektedir (Sanda vd., 2022).

Blokzincir teknolojisi yukarıda paylaşılan gelişim süreciyle paralel olarak özünde bloklardan oluşan oldukça güvenli ve şeffaf bir çalışma konusudur (Wang vd., 2022). Blokzincir sistemleri bloklardan oluşmaktadır. İlk oluşturulan blok yaratılış bloku olarak isimlendirilir. Bu blokta daha önceden oluşturulan ve blokun bağlandığı bir özüt değeri bulunmamaktadır. Ancak kendisinden sonra oluşturulan tüm bloklar özüt algoritmaları kullanılarak birbirlerine bağlanırlar. Özüt algoritmaları tek yönlü çalışan, özütlenen değerde meydana gelebilecek en ufak değişiklikte farklılık gösteren SHA256 özütleme algoritması örnek verilirse 256 bitlik bir değer üreten algoritmalarlardır. Bu algoritmalar sayesinde blokzincir sistemlerinin güvenlik ihtiyacı büyük ölçüde sağlanmaktadır. Zaman damgası algoritması ise bir blokzincirinde oluşturulan ve blokzincir sistemi tarafından doğrulandığı anın bilgisini tutan zaman

serileridir. Ülkemizde gerekli sertifikalara uygun halde zaman damgası hizmetini sadece TÜBİTAK Kamu Sertifikasyon Merkezi sağlamaktadır (Takaoğlu vd., 2019). Ancak zaman damgaları her programlama dilinde kodlanabilecek yapıdadırlar. Zaman damgalarında ifade edilen ve blokzincir sistemi tarafından doğrulanan şekilde ifade edilen yapı konsensüs algoritmaları tarafından gerçekleştirilmektedir. Bitcoin blokzincirinde kullanılan konsensüs algoritması PoW, yani işin ispatı algoritmasıdır. Bu algoritmanın çalışma mantığında çözülmesi gereken bir matematiksel bilmece, madenci diye isimlendirilen ve donanımları sayesinde işlem gücü oluşturan düğümlerce çözülmeye çalışılır. En hızlı bu bilmeceyi çözen madenci blok oluşturulması hakkını elde eder. Blok yazma hakkı kazanılınca yanında belirlenen miktarda bir ödül verilir. Bu ödülün maddi değeri madencinin yatırım ve masraflarını aşması durumunda o blokzincir sistemine duyulan madenci ilgisi artar. Neticesinde artan ilgi artan hesaplama gücünü doğurur. Bu sebeple bilmece zorluğu hesaplama gücü arttıkça zorlaştırılır. Bu sistemde gerekli olan hesaplama gücü günümüzde kripto madencilik için geliştirilen ekran kartlarınca yapılmaktadır (Takaoğlu vd., 2021). PoW algoritması neden olduğu elektrik tüketimi sebebiyle çevre dostu bir konsensüs algoritması değildir. Hissenin ispatı, PoS algoritmasında ise benzer yazma hakkı ve ödül dağıtma sistemi düğümlerin cüzdanlarında bulunan hisse yani kripto para ile doğru orantılı olarak gerçekleşmektedir. Örneğin PoS algoritması ile geliştirilmiş bir X coin projesinde cüzdanında en çok X coin taşıyan düğüm blok oluşturulurken yazma hakkını kazanma oranı en yüksek düğümdür. Bu sistemde karşılaşılan ve sürekli aynı düğümlerin ödül alması ile sonuçlanan adaletsiz durum yenilenen ve sürekli aynı düğümlerin ödül almasını engelleyen yeni PoS algoritmalarıyla giderilmektedir. Bu bağlamda PoS algoritması PoW algoritmasına nazaran daha çevreci bir konsensüs algoritmasıdır. Günümüzde birçok bilinen konsensüs algoritması olduğu gibi spesifik durumlarda sistemin ihtiyaçlarına uygun olarak konsensüs algoritması geliştirmek mümkündür (Varavallo vd., 2022).

Blokzincir sistemleri için dağıtık veri tabanı ya da dağıtık defter teknolojisi tabiri yapılmaktadır. Çünkü sistemi oluşturan tüm düğümlerde aynı veri tabanının bilgisi bulunmaktadır. Bir işlemin bloklara yazılabilmesi için sistemi oluşturan düğümlerin %51'inin onayı gerekmektedir. Gerekli

çoğunluğun sağlandığı ve işlem bilgisinin bloklara kaydedildiği durumlarda bu veri kaydı kesinlikle değiştirilemez ve yapılan işlem geri alınamaz bir yapıya kavuşmaktadır. Blokzincir sisteminde aktif olmayan düğümler doğal olarak ellerinde bulunan veri tabanı bilgisi eski olduğu için sistem için olumsuz bir duruma sebebiyet vermezler. Bitcoin örneğinde düğümün uzun bir süre sonra sisteme bağlanması durumunda öncelikli olarak güncel veri tabanının yüklenmesi işlemi gerçekleşmektedir. Bu sayede düğümün elinde sisteme bağlandığında veri tabanının son hali bulunmaktadır (Amjad vd., 2022).

Kripto paralar düşünüldüğünde düğümlerin cüzdanlarında gerçek bir para tutumu söz konusu değildir. Kripto cüzdanlarda bir kripto paranın aidiyet bilgisi tutulmaktadır. Herhangi bir cüzdanda bulunan x miktardaki bir kripto paranın o cüzdana ait olma bilgisi Merkle ağaçları sayesinde sağlanmaktadır. Yine Merkle ağaçları sayesinde blokların baş bölgelerinin bilgilerinin saklanması sayesinde oluşabilecek muazzam büyüklükleri veri tabanı boyutlarından kurtulmuş olunur. 2009 yılından bu yana gelen Bitcoin işlemlerinin bilgilerinin ulaşmış oldukları büyüklük her cüzdanda en ince ayrıntılarına kadar tutulmuş olduğu düşünüldüğünde elde edilen sistemin sürdürülebilirliği mümkün olamayacak bir hale gelmektedir. Merkle ağaçları sayesinde blokzincir sistemlerinin dağıtık bir veritabanı/defter olması sağlanabilmektedir (Damisa ve Nwulu, 2022).

Blokzincir sistemleri daha önce de ifade edildiği üzere bloklardan oluşur ve her bir blok aynı bir defter yaprağı gibi dolduğunda blokzincir sistemi tarafından onaylanıp zincire eklenir. Her yeni blok kendisinden bir önceki blokun özüt değerini kendi yapısında tutar. Kendisinden sonra oluşan blok da aynı şekilde sisteme eklenen blokun üretmiş olduğu özüt değerini işaretleyerek sisteme dahil olur. Her bir blok, oluşmasına vesile olan işlemlerin özütlenmesi neticesinde tek bir özüt değerine sahip olur. Bu blok içerisinde gerçekleşebilecek herhangi bir saldırı ya da düşünülmemiş bir açık sebebiyle değişikliğin yapılabilmesi durumunda özüt değeri sayesinde bu değişiklik fark edilebilmekte ve o blok, yapılan değişiklik geri alınıp eski haline dönünceye kadar sistemden çıkarılmaktadır. Bu özüt değerlerinin sağlamış olduğu özellik sayesinde blokzincir sistemleri kurcalanamaz bir yapıya kavuşmaktadır. Bilinenin aksine blokzincir sistemlerinde şifreleme algoritmalarından ziyade

özütleme algoritmaları ve dijital imzalar sayesinde güvenlik sağlanmaktadır (Batool ve Byun, 2022).

Açık blokzincirlerde düğümlerin bilgileri anonimdir. Bu sayede kullanıcı gizliliği en üst seviyede sağlanmış olur. Kişilerin cüzdan aidiyetlerini isteyerek açıklamaları ya da yapılan işlemlerin incelenebilir yapıda olması sebebiyle sistemin şeffaf olması ve etkileşim halinde olunan kripto cüzdanların analiz edilmesinden kime ait olduğu ile ilgili fikir üretilebilerek cüzdanın kime ait olduğu anlaşılabilir. Ancak cüzdan sahibinin açıklaması dışında yapılan tüm bu analizler kesin bir sonuç vermeyebilir (Çeşitli uygulamalar ve offshore hesaplar kullanılarak). Gerçekleşen işlemler bloklara kaydedildiği için ve özüt algoritmaları ile bloklar birbirlerine bağlandıkları için gerçekleşen işlemler değiştirilemez yahut geri alınamaz. Anlaşılabilirliği üzere halka açık blokzincirler oldukça güvenli, şeffaf ve anonim yapıdadırlar. Özel blokzincirler ise açık blokzincirlerden farklı olarak sisteme erişim izninin seçilen düğümlere verildiği ve diğer tüm özellikleri aynı olduğu sistemlerdir. Bu sistemlerin erişim izni olmayan kişilerce incelenmesi mümkün değildir. Özel şirketlerin kendi sistemlerinde bu tür blokzincir entegrasyonlarını düşünmeleri doğaldır (Meidute-Kavaliauskiene vd., 2022).

Blokzincir sistemleri daha önce de ifade edildiği üzere bir katman olarak hali hazırdaki sistemlere eklenebilir. Ekleneceği sistemdeki ihtiyaca göre sistemin tamamının ya da belirli bir kısmının blokzincire çekilmesi, kaydedilmesi durumu düşünülebilir. Onchain ve offchain diye isimlendirilen bu yöntemler sayesinde blokzincir teknolojisinin sahip olduğu özelliklerin hali hazırda kullanılan sistemlere kazandırılması sağlanmaktadır.

Tez çalışması sürecinde doktora öğrencisi Mustafa Takaoğlu'nun İstanbul Aydın Üniversitesi Blokzincir Uygulama ve Araştırma Merkezinde Yönetim Kurulu Üyesi ve Merkez Müdür Yardımcısı olarak görevlendirilmesi neticesinde blokzincir teknolojisi çok daha ayrıntılı olarak incelenmiş, ulusal ve uluslararası birçok konuşmacı ile online seminerler gerçekleştirilmiştir. Bu seminerlerde blokzincir teknolojisinin farklı uygulama alanlarında çalışmalar yürüten özellikle Avrupa Birliği, Birleşmiş Milletler gibi kurumlarda da aktif olarak görev alan kişilerin bilgileri Türk kamuoyu ile paylaşılmıştır. Bu bilgi birikimleri neticesinde blokzincir teknolojisinin farklı alanlarda uygulanması

üzerine bu tez çalışmasında Milli Bağış Zinciri, Avichain Havacılık Veritabanı Entegrasyonu, Blokzincir Steganografisi başta olmak üzere blokzincir teknolojisinin uygulanabilecek farklı alanlardaki denemeleri üzerinde durulmuştur. Tezimizin içinde kullanılan blokzincir eklentisi ise özütleme algoritmaları ile alakalı olmuştur. Bu sebeple tez isminde Blokzincir Teknolojisine Dayalı ibaresi bulunmaktadır. İlerleyen bölümlerde ifade edildiği üzere tezimize eklenen blokzincir modülü sayesinde karmaşıklık arttırılmadan, sisteme ağır bir yük eklenmeden sistem güvenliği üst düzeye çıkartılmıştır.

#### A. Önerilen Blokzincir Algoritması

Tezimizde geliştirilen modüllerden dördüncü ve son modül olan blokzincir modülü esasen özütleme algoritması kullanımına dayanmaktadır. Tezimizde geliştirmiş olduğumuz sistem esasen tüm dosya türlerinde kurcalanmaya karşı koruma sağlayan bir katmandır. İmage-chain isimli makale çalışmasında görülen ve makale olarak yazmayı düşündüğümüz daha geniş kapsamlı bir uygulamanın sadece resim üzerine geliştirildiği güzel bir fikirdir. Bu çalışmada tüm resimlerin bir nevi blok gibi düşünüldüğü ve birbirlerine özüt değerleri üzerinden bağlandığı bir öneri getirilmiştir. Bu çalışmadan bağımsız olarak tezimizde bizim önermiş olduğumuz blokzincir eklentisinde manipüle edilmiş, şifrelenmiş ve anahtar paylaşımının steganografiden faydalanılarak gerçekleştirildiği bu sistemde veri iletiminin koruma altına alınması ve kurcalanmalara karşı korunması amaçlanmıştır. Bu amaçla gönderilen dosya SHA256 algoritması ile özütlenmektedir. SHA256 algoritması tek yönlü olarak çalışan ve çıktı olarak 256 bitlik bir değer veren bir özütleme algoritmasıdır. Aşağıdaki Şekil 25’de bu süreçle ilgili bir görsel paylaşılmıştır.



Şekil 25 SHA256 algoritması ile şifrelenmiş dosya özütlenmesi

Elde edilen özüt değeri dosya alıcıya iletdikten sonra alıcıdan bir onay beklenmektedir. Bu amaçla alıcı eline geçen dosyanın özüt değerini hesaplayıp göndericiye bu değeri göndermektedir. Göndericinin elindeki özüt değeri ile

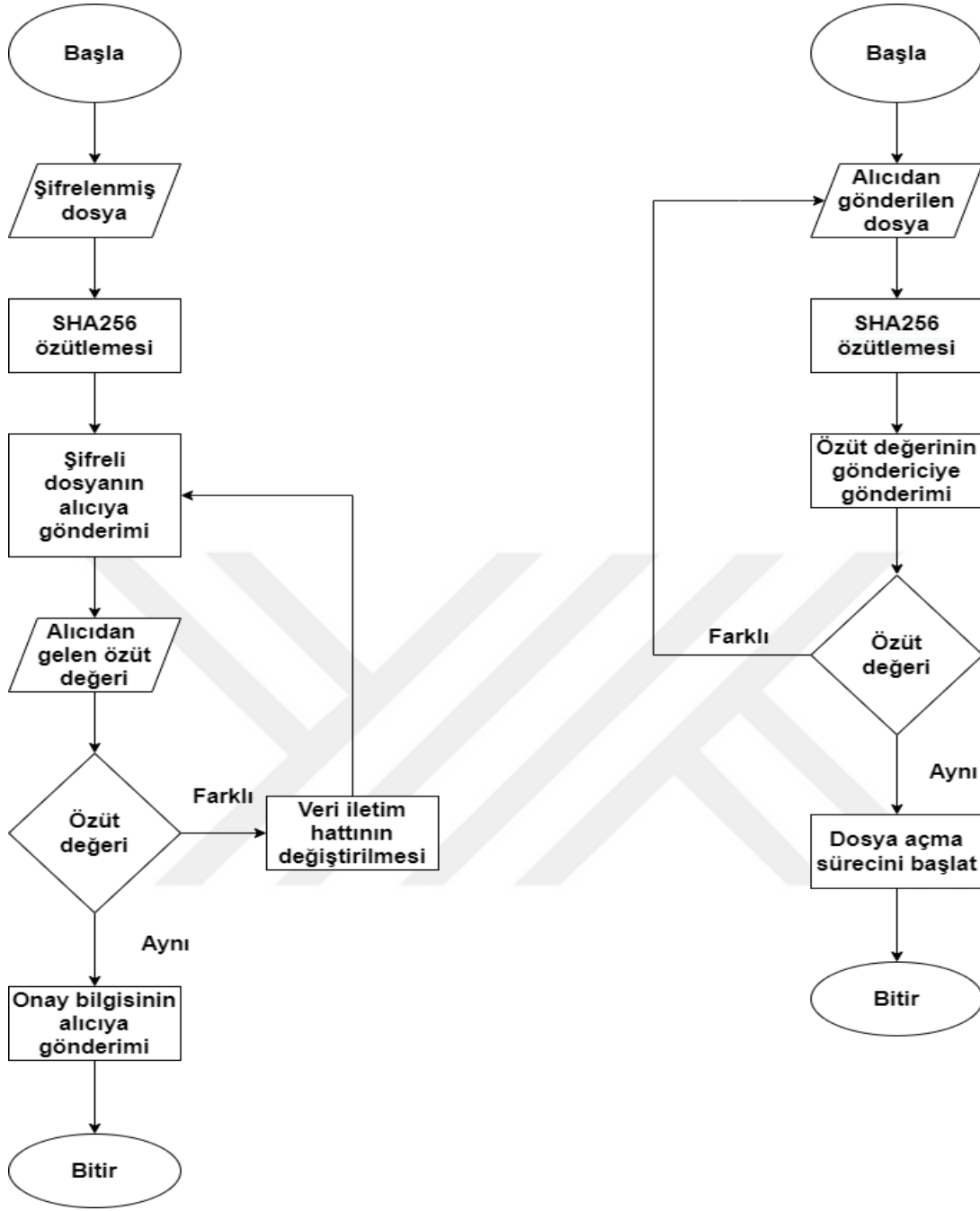
alıcıdan gelen özet değerinin eşleşmesi durumunda algoritma veriyi çıkarmaya başlamaktadır. Özet değerlerinin uyuşmaması durumunda sistemde bir dinleyici ya da saldırgan olduğu düşünüldüğü için yeni bir hat oluşturup veri iletiminin bu ağ üzerinden yapılması sağlanmaktadır. Bu sayede gönderilen verinin kurcalanmasına engel olunmuştur ve steganaliz ya da kriptanaliz yöntemlerine karşı bir koruma katmanı eklenmektedir. Aşağıdaki sözde kodda bu sürecin nasıl gerçekleştirildiği paylaşılmıştır.

- Başla
- Gönderilmek istenen dosyayı OKU
- Dosyanın özet değerini SHA256 ile HESAPLA
- Dosyayı alıcıya GÖNDER
- Alıcıdan gelen özet değerini hesapladığın değerle KARŞILAŞTIR
- Uyum sağlanmışsa alıcıya onay bilgisi GÖNDER
- Uyum sağlanmamışsa alıcıya hata bilgisi GÖNDER ve hattı DEĞİŞTİR
- Bitir

Alıcı tarafında yapılacakların sözde kodu aşağıda paylaşılmıştır.

- Başla
- Gelen dosyayı OKU
- Dosyanın özet değerini SHA256 ile HESAPLA
- Elde edilen özet değerini göndericiye GÖNDER
- Alıcıdan gelen onay bilgisi ise dosyayı açma işlemlerini BAŞLAT
- Alıcıdan gelen bilgi hata veriyorsa süreci yeniden BAŞLAT
- Bitir

Geliştirilen blokzincir algoritmasının alıcı ve gönderici tarafları için süreçlerinin gösterildiği akış diyagramı Şekil 26'da paylaşılmıştır.



Şekil 26 Blokzincir eklentisi alıcı ve gönderici için akış diyagramı

## B. Sonuç

Geliştirilen blokzincir modülünde elde edilmek istenen katkı sistemin güvenliğinin artırılmasıdır. Manipülasyon süreci, şifreleme ve şifrenin steganografik bir şekilde gizlenmesinin sonrasında elde edilen tüm bu güvenlik katmanlarının da kurcalanamaz yani gerçekleştirilecek herhangi bir saldırı ya da iletim ağında gerçekleşebilecek veri kayıpları oluşması durumunda veri iletimini iptal eden ve yeni bir hattan gönderim sağlayan güvenliğin üst düzey

olduđu bir sistem elde edilmiřtir. SHA256  z tleme algoritmaları  ok hızlı  alıřan ve benzer sonu lar  retmeyen g venilir  z tleme algoritmalarıdır. Alıcı ve verici arasında bu  z t algoritmalarının paylařılması ve dođrulama s recinin ger ekleřmesi sayesinde katman katman geliřtirilen ve g venliđi arttıran veri iletim sistemimizin kurcalama giriřimlerine karřı g venilir bir hale gelmesi sađlanmıřtır.

Benzer bir mantık kuantum anahtar paylařımında da g r lebilir. Fizik kurallarının da katkısıyla veri iletim ađının dinlenmesi veya dosyadan bir kısım par aların okunmaya  alıřılması durumunda bu kuantum fiziđinin sađlamıř olduđu kalıtsal katkılar sayesinde anında tespit edilebilmekte, ađda ger ekleřtirilen iletim iptal edilmekte ve yeni bir hat ile g nderim tekrar sađlanmaktadır.  nermiř olduđumuz blokzincir algoritmasında benzer bir g venlik sađlanmaya  alıřılmıř, dosyaya bir kurcalama giriřiminin tespit edilmesi durumunda veri iletimi iptal edilip yeni bir hatta ge ilerek tekrar g nderimi yapılmaktadır.

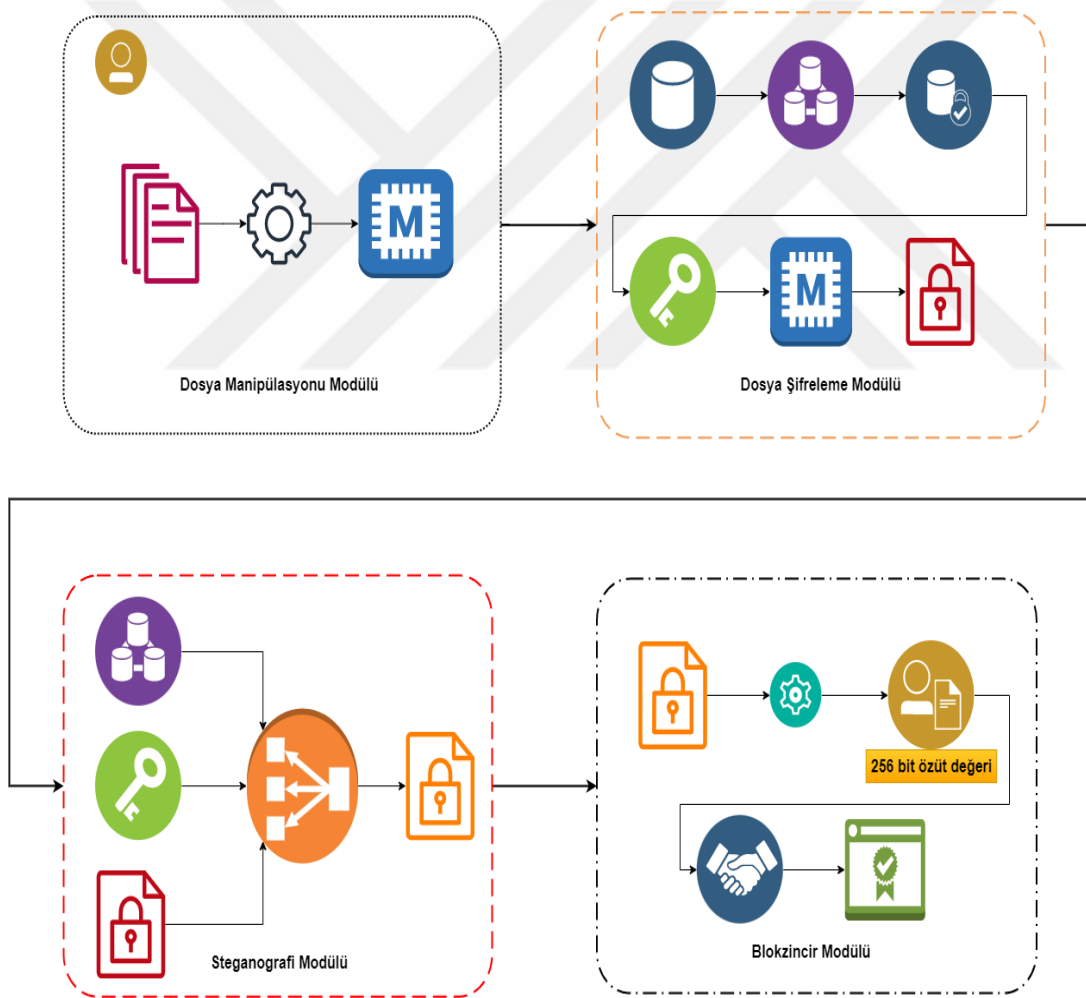


## VI. ANALİZ VE TARTIŞMA

Tez çalışmamızda önerilen algoritma dört ana modülden oluşmaktadır. Her bir modül sistemin sürdürülebilirliği için hayati öneme sahip olup özel olarak geliştirilmiştir. Tezimizde bilime katkı sağlamak amacıyla modüler yapının kazandırmış olduğu imkanlar kullanılarak gerek steganografide metin steganografisi için gerekse de şifrelemede anahtar rastgeleliği ve anahtar dağıtımı için yenilikçi fikirler geliştirilmiştir. Bu iki fikrin akademik yayın yapılması için tez süreci yeterli olmamış, doktora sürecinden sonra gerçekleştirilen bu çalışmaların akademik yayınları hızla çıkartılacaktır. Blokzincir teknolojisinde ise tezimizden üretilen ve doktora mezuniyeti yayın şartını sağladığımız, literatür taraması kısmında bahsi geçen OTA blokzincir steganografisi algoritmasında önerilen yöntem ile yine bilime katkı sağlanmış, alanında ilk olma özelliği taşıyan bir algoritma literatüre kazandırılmıştır. Ayrıca yine blokzincir modülünde geliştirilen özüt algoritmalarının kullanımıyla gerçekleşen modül sayesinde elde edilen sistemin sadece resim için geliştirilen ufak bir çalışması MDPI Applied Science dergisinde başkalarınca yayımlanmıştır. Tezimizde geliştirmiş olduğumuz bu modülün de akademik bir çalışmaya dönüştürülmesi ve indeksli bir dergide file-chain ismiyle yayımlanması için gerekli akademik çalışmalar sürdürülmektedir. Tezimizde geliştirilen her bir modül akademik bir yayın değeri statüsü taşımaktadır.

Aşağıdaki Şekil 27’de algoritmamızın modüllerini gösteren paylaşımda tüm sistem genel olarak görselleştirilmiştir. İlk modül olan dosya manipülasyonu modülünde tüm işletim sistemlerinde kullanılan dosya türlerini kapsayacak şekilde çalışabilen ve dosyaların hiçbir şekilde okunamamasını sağlayan algoritmamız yeni bir dosya türü üretmektedir. Üretilen bu manipüle edilmiş dosya türü veri güvenliğine birçok katkı sağlamaktadır. Öncelikle manipüle edilmiş dosyanın orijinal hali hakkında fikir sahibi olunabilmesi mümkün değildir. Bu saldırganların özellikle aradıkları bir dosya türüyle ilgili yürüttükleri analiz yöntemlerinin boşa çıkmasını sağlamaktadır. Ayrıca hattın

başarı ile saldırganlar tarafından dinlenmesi durumunda, elde edilen veri parçacıklarının anlamsız bir yapıda olması sağlanmaktadır. Bu durum genellikle saldırganların dosyaya duydukları ilginin kaybolmasına sebebiyet vermektedir. Bir diğer katkı ise şifreleme sisteminin bir şekilde (havuz kaybı ve steganografiyle gizlenen bilgilerin elde edilmesi) çözülebilmesi durumunda, elde edilen dosyanın açılabilir halde olması bir güvenlik katmanını eklemektedir. Son olarak manipüle edilmiş dosya metin steganografisinin uygulanabilmesine imkân tanımaktadır. Bu bağlamda önerilmiş olan yöntem, metin steganografisi için yeni bir yöntemdir. Bu sebeple önerilen yöntemin akademik yayın çalışması yapılmalı ve steganaliz yöntemlerine karşı dayanıklılığı gözler önüne serilmelidir.



Şekil 27 Önerilen algoritma modülleri

Şekil 27’de paylaşılan ikinci modül, dosya şifreleme modülü manipüle edilmiş dosya ile çalışmaktadır. Geliştirmiş olduğumuz algoritma sayesinde anahtar rastgeleliği üst seviyeye çıkartılmış ve anahtar paylaşımında yenilikçi

bir çözüm getirilmiştir. Anahtar havuzunun her iki tarafta önceden belirlenmiş olma durumu ve bu havuzun alt segmentlere bölünmesi, tezimizde 16 parça olmasına karar verilmiştir ve tekrardan rastgele olacak şekilde bu alt segmentlerin birleştirilmesi neticesinde elde edilen yeni havuz anahtar seçiminde kullanılmaktadır. Her anahtar seçimi gerçekleştirilirken yeniden havuz karıştırılmakta ve karmaşıklık her seferinde arttırılmaktadır. Ayrıca seçilen anahtarlar da bu havuzlardan rastgele olacak şekilde seçilmektedir. Hem yeni havuz oluşturma sırası bilgisi hem de bu yeni oluşturulan havuz üzerinde rastgele seçilen anahtar noktası kayıt altına alınmakta ve dosya üzerine gizlenerek gönderimi yapılmaktadır. Görüleceği üzere anahtar hiçbir şekilde paylaşılmamaktadır. Anahtarın nasıl elde edileceği bilgisi alıcı tarafı ile paylaşılmaktadır. Bu bağlamda tezimizde geliştirmiş olduğumuz şifreleme modülünde anahtar paylaşımı anahtar paylaşımı yapılmadan gerçekleştirilmektedir. Önerilen bu sistemin akademik yayın çalışması en kısa sürede tamamlanıp literatüre kazandırılacaktır.

Şekil 27’de paylaşımı yapılan steganografi modülünde kendisinden önceki iki modülün katkıları sayesinde veri gizleme işlemi gerçekleştirilebilmektedir. Steganografi bilindiği üzere veri gizleme bilimidir. Günümüzde de dijital steganografinin gerçekleştirilebilmesi için geleneksel yöntemler kullanılmaktadır. Metin steganografisi gerçekleştirilmesi oldukça zor ve kolaylıkla steganaliz yöntemleriyle tespit edilebilen çalışmalardır. Tezimizde geliştirilen steganografi modülünde ilk modül olan manipülasyon modülünün sağlamış olduğu okunamaz dosya yapısı sayesinde gizlenmek istenen ve ikinci modülden gelen bilgiler manipüle edilmiş ve şifrelenmiş dosyanın üzerine çeşitlilik gösteren parçalara bölünerek gizlenmektedir. Dosyanın saldırganlar tarafından incelenmesi durumunda gizlenmiş bilgilerin anlaşılabilmesi bu sayede mümkün olmayan bir hale gelmektedir. Önerilen bu yöntem sayesinde yeni bir metin steganografisi yöntemi elde edilmiş olup akademik yayın çalışması en kısa sürede yapılacaktır.

Şekil 27’de paylaşılan son modül olan blokzincir modülünde geliştirilen sistem, algoritmamıza yönelebilecek saldırılara karşı bir koruma sağlamaktadır. Önceki modüllerde gerçekleştirilen işlemler neticesinde üretilen şifreli belgenin SHA256 özüt algoritması kullanılarak elde edilen özüt değeri ile

alıcı tarafına dosyanın iletimi sonrasında hesaplanan özüt değeriyle karşılaştırma yapılması sonucunda dosyaya bir saldırı yapıp yapılmadığı anlaşılmaktadır. Saldırı dışında veri iletimi esnasında gerçekleşebilecek çevresel etkiler sebebiyle dosyanın farklılaşması durumları tespit edilecektir. Her iki durumda da dosyanın bozulması sebebiyle orijinal veriye ulaşılması imkânsız olacağı için dosya etkilenmemiş bir şekilde alıcıya iletilene kadar yeni hattan gönderim süreci devam edecektir. Bu durum alıcı tarafında gereksiz enerji kaybı yaşanmamasına ve aynı kuantum anahtar dağıtımı mekaniğinde olduğu gibi hareket edilmektedir. Literatürde tezimizde geliştirilen bu sisteme yakın ancak çok ufak bir kısmı kullanılarak önerilmiş akademik yayınlar tespit edilmiştir. Doktora tezi sürecinde çok yoğun çalışılması ve akademik yayınların sınırlı sürede yetiştirilememesi sebebiyle bu tarz fikirlerimizin başkaları tarafından yayınlanması durumu maalesef olmuştur. Ancak blokzincir modülünde geliştirilen sistemin akademik yayın haline getirilmesi ve literatüre kazandırılması yapılacak çalışmalarımız arasında yer almaktadır. Son olarak blokzincir modülü olarak isimlendirilen sistemde tam teşekküllü bir blokzincir sistemi kurulmamıştır. Tezimizin isminde de geçtiği üzere, blokzincir teknolojisine dayalı yani blokzincir teknolojisinin olmazsa olmaz parçalarından biri olan özüt algoritmalarından faydalanılarak geliştirilmiş bu sistem sayesinde algoritmamız aynı blokzincir sistemlerinde olduğu gibi kurcalamalara karşı dayanıklı bir hale gelmiştir.

Geliştirmiş olduğumuz algoritmamızın doktora süreci sonrasında ürünleştirilmeye başlanacaktır. Test ve analiz aşamalarında tespit edilemeyen kusurların kullanıcı geri bildirimleriyle tespiti ve gelişen teknolojinin sağladığı imkanlar da değerlendirilerek yeni versiyonların geliştirilmesi ve insanların kullanımına açılması planlanmaktadır. Önerilen algoritmanın patentinin alınması için araştırmalar yapılmıştır. Ancak Amerika hariç dünyada yazılımlara patent alınmasının pek mümkün olmadığı görülmüştür. Bu sebeple tez çalışmamızda önerilen fikirlerin haklarının korunması için akademik yayın yapılmalarına karar verilmiştir.

## VII. SONUÇ VE ÖNERİLER

Blokzincir teknolojisine dayalı, şifreleme ve steganografi teknikleri kullanılan, yüksek güvenli li bilgi deęişim algoritması isimli tez  alışmamızda geliştirilmesi düşün len tüm mod ller başarı ile geliştirilmiştir. Bilginin\verinin güvenilir bir şekilde paylaşılması için geliştirilen mod ller sayesinde maksimum güvenilirlik sağlanmıştır. OTP şifreleme algoritması kuantum hesaplama gücünün yaygınlaştığı ve kuantum sonrası dönem diye adlandırılan süreçte dahi güvenilir kabul edilen bir simetrik anahtarlı şifreleme algoritmasıdır. Tezimizde OTP şifreleme algoritması seçilmiş ve literatürde sorun olarak gösterilen anahtar rastgeleliği ve anahtar paylaşımı hususunda yenilikçi ve etkili çözümler getirilmiştir.

Veri iletim ağıının dinlenmesi durumuna önlem olması amacıyla dosya türlerinin tamamı manip le edilerek erişilemez ve anlamlı bir bilginin  ıkmayacağı bir dosya türüne dönüşümü sağlanmıştır. Ayrıca bu mod l metin steganografisi yapılmasına da imkân tanımıştır.

Şifreleme algoritmasında anahtar paylaşımı ve anahtar rastgeleliğinin arttırılması süreçlerinde steganografiden yararlanılmıştır. Manip le edilen ve şifrelenen dosyanın içine; anahtar havuzunun rastgeleliğini arttıran bilgi ve yeni elde edilecek havuzdan nasıl anahtar seçileceğı bilgisi gizlenmiştir. Bu sayede hem yeni bir steganografi yöntemi geliştirilmiştir hem de anahtar paylaşımının anahtar paylaşımı yapılmadan gerçekleştirilmesi sağlanmıştır.

Sonuç olarak tez  alışmamızda önerilen “Blokzincir teknolojisine dayalı, şifreleme ve steganografi teknikleri kullanılan, yüksek güvenli li bilgi deęişim algoritması” isimli  alışmamız başarı ile tamamlanmış ve tüm mod lleriyle sorunsuz  alışır bir hale kavuşmuştur.

İlerleyen süreçte bu alanda  alışmalar yür tmek isteyen araştırmacıların manip lasyon sürecinde daha dinamik sistemler geliştirilmesi üzerine  alışmaları önerilebilir. Ayrıca anahtar havuzunun önceden alıcı ve gönderici

taraflarında paylaşıldığı tezimizdeki fikir geliştirilerek daha farklı havuz paylaşımı/üretimi teknikleri üzerine odaklanılabilir. Anahtar havuzlarının rastgeleliğinin arttırılması için yeni fikirler geliştirilebilir. Steganografi aşamasında ise gizlenmek istenen bilgilerin tezimizde yapıldığı gibi direkt şifreli dosyaya gizlenmesi yerine daha farklı çözümler üzerinde düşünülebilir. Yine tez çalışmamızda seçilen OTP algoritması yerine başka şifreleme algoritmaları seçilebilir. OTP algoritmasında görülen dosya boyutuyla aynı uzunluktaki anahtar uzunluğu ve rastgelelik durumu farklı algoritmalar denenerek üstesinden gelinebilir ancak anahtar paylaşımı noktasında tezimizde önerilen yöntem esas alınarak yeni çalışmalar denenebilir.

Tez çalışmamızın 6 yıl sürmesine sebebiyet veren ve eski tez konusu olan blokzincir teknolojisinin çalışılmaması şart koşulan özel durumumuz sebebiyle bu çalışmada tam teşekküllü bir blokzincir mimarisi önerilememiştir. Daha önce de ifade edildiği üzere blokzincir temelli bir çözüm geliştirilmiştir. Bu sebeple algoritmamızın blokzincir modülü tekrardan ele alınıp gizli bir blokzincir sistemi geliştirilerek uyumluluğu test edilebilir. Bu bağlamda blokzincir sistemlerinin açık kanal olarak değerlendirilmesi üzerine de çalışmalar gerçekleştirilebilir. Anahtar paylaşımında blokzincir sistemlerinden yararlanılabilir.

Sonuç olarak tez çalışmamız bilime net katkılar sağlamış, getirmiş olduğu yenilikler sayesinde birçok yeni araştırmanın yapılabilmesine kapı açmıştır. Bu vesileyle tez çalışmasında emeği geçen herkese çok teşekkür ediyor, tez çalışmamızın insanlığa fayda sağlamasını ümit ediyoruz.

## VIII. KAYNAKÇA

### KİTAPLAR

MATZUTT, R., HİLLER, J., HENZE, M., ZİEGELDORF, J. H., MÜLLMANN, D., HOHLFELD, O. ve WEHRLE, K. (2018). **A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin**, In **Financial Cryptography and Data Security**, Berlin, Springer Yayınevi, 1. Baskı.

XU, X., PAUTASSO, C., ZHU, L., LU, Q. ve WEBER, I. (2018). **A pattern collection for blockchain-based applications**, Irsee, ACM Yayınevi 1. Baskı.

### MAKALELER

ADEE, R. ve MOURATİDİS H. A. (2022). “Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography”, **Sensors**, cilt 22, sayı 1109.

AJLOUNİ, N. M. M., ÖZYAVAŞ, A. ve TAKAOĞLU, M. (2021). “A Survey of Artificial Intelligence Driven Blockchain Technology: Blockchain Intelligence”, **Manchester Journal of Artificial Intelligence and Applied Sciences**, cilt 2, sayı 1.

ALİEV, H., KİM, H. ve CHOİ, S. (2020). “A Scalable and Secure Group Key Management Method for Secure V2V Communication”, **Sensors**, cilt 20, sayı 6137.

ALVAREZ, R., CABALLERO-GİL, C., SANTONJA, J. ve ZAMORA, A. (2017). “Algorithms for Lightweight Key Exchange”, **Sensors**, cilt 17, sayı 1517.

AMJAD, S., ABBAS, S., ABUBAKER, Z., ALSHARİF, M. H., JAHİD, A. ve JAVAİD, N. (2022). “Blockchain Based Authentication and Cluster Head Selection Using DDR-LEACH in Internet of Sensor Things”, **Sensors**, cilt 22, sayı 1972.

ARMANUZZAMAN, M., ALAM, K. M. R., HASSAN, M. M. ve MORİMOTO Y. (2017). “A secure and efficient data transmission technique using quantum

- key distribution”, **Proc. 2017 Int. Conf. Networking, Syst. Secur. NSysS**, sayı 2018-Janua, ss. 1–5.
- BASUKİ, A. I. ve ROSİYADİ, D. (2019). “Joint Transaction-Image Steganography for High Capacity Covert Communication”, **International Conference on Computer, Control, Informatics and its Applications: Emerging Trends in Big Data and Artificial Intelligence, IC3INA**, ss. 41–46.
- BATOO, A. ve BYUN, Y. (2022). “Reduction of Online Fraudulent Activities in Freelancing Sites Using Blockchain and Biometric”, **Electronics**, cilt 11, sayı 789.
- BELGHAZİ, Z., BENAMAR, N., ADDAİM, A. ve KERRACHE, C. A. (2019). “Secure WiFi-Direct Using Key Exchange for IoT Device-to-Device Communications in a Smart Environment”, **Future Internet**, cilt 11, sayı 251.
- BELKHOUBA, T., DU, X., MOHAMED, A., AL-ALİ, A. K. ve GUİZANİ M. (2018). “Symmetric Encryption Relying on Chaotic Henon System for Secure Hardware-Friendly Wireless Communication of Implantable Medical Systems”, **J. Sens. Actuator Netw.**, cilt 7, sayı 21.
- BOAKYE-BOATENG, K., KUADA, E., ANTWI-BOASIAKO, E. ve DJABA, E. (2019). “Encryption Protocol for Resource-Constrained Devices in Fog-Based IoT Using One-Time Pads”, **IEEE Internet of Things Journal**, cilt 6, sayı 2, ss. 3925-3933.
- BOAKYE-BOATENG, K. ve LASHKARİ, A. H. (2019). “Securing GOOSE : The Return of One-Time Pads”, **International Carnahan Conference on Security Technology (ICCST)**, ss. 1-8.
- CHEN, D., LU, W., XING, W. ve WANG, N. (2019). “An Untraceable Data Sharing Scheme in Wireless Sensor Networks”, **Sensors**, cilt 19, sayı 114.
- CHOUDHARY, K., GABA, G. S., BUTUN, I. ve KUMAR, P. (2020). “MAKE-IT—A Lightweight Mutual Authentication and Key Exchange Protocol for Industrial Internet of Things”, **Sensors**, cilt 20, sayı 5166.
- CHUANG, Y.-H. ve TSENG, Y.-M. (2021). “CAKE: Compatible Authentication and Key Exchange Protocol for a Smart City in 5G Networks”, **Symmetry**, cilt 13, sayı 698.
- DAMİSA, U. ve NWULU, N. I. (2022). “Blockchain-Based Auctioning for Energy Storage Sharing in a Smart Community”, **Energies**, cilt 15, sayı 1954.

- EJAZ, A., SHOUKAT, I. A., IQBAL, U., RAUF, A. ve KANWAL, A. (2021). “A secure key dependent dynamic substitution method for symmetric cryptosystems”, **PeerJ Computer Science**, cilt 7:e587.
- ESCRIBANO PABLOS, J. I., GONZÁLEZ VASCO, M. I., MARRIAGA, M. E. ve PÉREZ DEL POZO, Á. L. (2020). “Compiled Constructions towards Post-Quantum Group Key Exchange: A Design from Kyber”, **Mathematics**, cilt 8, sayı 1853.
- FURTAK, J. (2020). “Cryptographic Keys Generating and Renewing System for IoT Network Nodes—A Concept”, **Sensors**, cilt 20, sayı 5012.
- GATABAZI, P., KABERA, G., MBA, J. C., PINDZA, E. ve MELESSE, S. F. (2022). “Cryptocurrencies and Tokens Lifetime Analysis from 2009 to 2021”, **Economies**, cilt 10, sayı 60.
- GEBREMİCHAEL, T., JENNEHAG, U. ve GİDLUND, M. (2018). “Lightweight IoT Group Key Establishment Scheme Using One-way Accumulator”, **International Symposium on Networks, Computers and Communications (ISNCC)**, ss. 1-7.
- GEORGİEVA-TSANEVA, G., BOGDANOVA, G. ve GOSPODİNOVA, E. (2022). “Mathematically Based Assessment of the Accuracy of Protection of Cardiac Data Realized with the Help of Cryptography and Steganography”, **Mathematics**, cilt 10, sayı 390.
- GIRON, A. A., MARTİNA, J. E. ve CUSTÓDİO, R. (2021). “Steganographic Analysis of Blockchains”, **Sensors**, cilt 21, sayı 4078.
- GOUMİDİ, H., HAROUS, S., ALİOUAT, Z. ve GUEROUİ A. M. (2021). “Lightweight Secure Authentication and Key Distribution Scheme for Vehicular Cloud Computing”, **Symmetry**, cilt 13, sayı 484.
- HAMİD, H. R. M. H. ve ABDULLAH, N. Y. (2015). “Physical Authentication Using Random Number Generated (RNG) Keypad Based on One Time Pad (OTP) Concept”, **Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec)**, ss. 135-139.
- HAMMAD, B. T., AHMED, I. T. ve JAMİL, N. A. (2022). “Steganalysis Classification Algorithm Based on Distinctive Texture Features”, **Symmetry**, cilt 14, sayı 236.

- HORNG, J. H. (2021). "Blockchain-Based Reversible Data Hiding for Securing Medical Images", **Journal of Healthcare Engineering**, cilt 2021, sayı 9943402.
- HSUEH, C. -W. ve CHİN, C, -T. (2022). "Toward Blockchain Realization", **FinTech**, cilt 2022, sayı 1, ss. 81-99.
- HUSSEİN, A. F., ALZUBAİDİ, A. K., HABASH, Q. A. ve JABER, M. M. (2019). "An Adaptive Biomedical Data Managing Scheme Based on the Blockchain Technique", **Appl. Sci.**, cilt 9, sayı 2494.
- JAVED, M. U., REHMAN, M., JAVAİD, N., ALDEGHEİSHEM, A., ALRAJEH, N. ve TAHİR, M. (2020). "Blockchain-Based Secure Data Storage for Distributed Vehicular Networks", **Appl. Sci.**, cilt 10, sayı 2011.
- İŞLER, B., TAKAOĞLU, M. ve KÜÇÜKALİ, U. F. (2019). "Blokzincir ve Kripto Paraların İnsanlığa Etkileri", **e-Journal of New Media**, cilt 3, sayı 2, ss. 71-83.
- ONUMA, K. ve MİYATA, S. A. (2021). "Proposal for Correlation-Based Steganography Using Shamir's Secret Sharing Scheme and DCT Domain", **In Proceedings of the 2021 International Conference on Information Networking (ICOIN)**, pp. 255–260.
- KİM, M., MOON, J., WON, D. ve PARK, N. (2020). "Revisit of Password-Authenticated Key Exchange Protocol for Healthcare Support Wireless Communication", **Electronics**, cilt 9, sayı 733.
- LEE, D.-H. ve LEE, I.-Y. (2018). "Dynamic Group Authentication and Key Exchange Scheme Based on Threshold Secret Sharing for IoT Smart Metering Environments", **Sensors**, cilt 18, sayı 3534.
- Lİ, C., Jİ, S., ZHANG, X., WANG, H., Lİ, D. ve LİU, H. (2018). "An Effective and Secure Key Management Protocol for Message Delivery in Autonomous Vehicular Clouds", **Sensors**, cilt 18, sayı 2896.
- Lİ, G., ZHANG, Z., ZHANG, J. ve HU, A. (2021). "Encrypting Wireless Communications on the Fly Using One-Time Pad and Key Generation", **IEEE Internet of Things Journal**, cilt 8, sayı 1, ss. 357-369.
- LİANG, H., ZHANG, G., HOU, W., HUANG, P., LİU, B. ve Lİ, S. (2021). "A novel asymmetric hyperchaotic image encryption scheme based on elliptic curve cryptography", **Appl. Sci.**, cilt 11, sayı 12.

- LİN, C.-H., HU, G.-H., CHAN, C.-Y. ve YAN, J.-J. (2021). “Chaos-Based Synchronized Dynamic Keys and Their Application to Image Encryption with an Improved AES Algorithm”, **Appl. Sci.**, cilt 11, sayı 1329.
- LİN, H.-Y. (2019). “A Novel Dual Authenticated Encryption Scheme Suitable for Social Networking Services”, **Appl. Sci.**, cilt 9, sayı 1452.
- LİU, L., WANG, Y., ZHANG, J. ve YANG, Q. A. (2019). “Secure and Efficient Group Key Agreement Scheme for VANET”, **Sensors**, cilt 19, sayı 482.
- MANUCOM, E. M. M., GERARDO, B. D. ve MEDİNA, R. P. (2019). “Analysis of Key Randomness in Improved One-Time Pad Cryptography”, **IEEE 13th International Conference on Anti-counterfeiting, Security, and Identification (ASID)**, ss. 11-16.
- MARJAİ, P., LEHOTAY-KÉRY, P. ve KİSS, A. A. (2022). “Novel Dictionary-Based Method to Compress Log Files with Different Message Frequency Distributions”, **Appl. Sci.**, cilt 12, sayı 2044.
- MAWLOOD HUSSEİN, S., LÓPEZ RAMOS, J. A. ve ÁLVAREZ BERMEJO, J. A. (2020). “Distributed Key Management to Secure IoT Wireless Sensor Networks in Smart-Agro”, **Sensors**, cilt 20, sayı 2242.
- MEİDUTE-KAVALIAUSKIENE, I., YAZDİ, A. K. ve MEHDİABADİ, A. (2022). “Integration of Blockchain Technology and Prioritization of Deployment Barriers in the Blood Supply Chain”, **Logistics**, cilt 6, sayı 21.
- MENG, Y. ve Lİ, J. (2021). “Data Sharing Mechanism of Sensors and Actuators of Industrial IoT Based on Blockchain-Assisted Identity-Based Cryptography”, **Sensors**, cilt 21, sayı 6084.
- MENON, N. (2018). “Triple Layer Data Hiding Mechanism using Cryptography and Steganography”, **3rd IEEE Int. Conf. Recent Trends Electron. Inf. Commun. Technol.**, ss. 407–410.
- MİHALKOVİCH, A., SAKALASKAS, E. ve LUKSYS, K. (2020). “Key Exchange Protocol Defined over a Non-Commuting Group Based on an NP-Complete Decisional Problem”, **Symmetry**, cilt 12, sayı 1389.
- MOHSİN, A. H. (2021). “PSO–Blockchain-Based Image Steganography: Towards a New Method to Secure Updating and Sharing COVID-19 Data in Decentralised Hospitals Intelligence Architecture”, **Multimedia Tools and Applications**, cilt 80, sayı 9, ss. 14137–61.

- MOORE, G. E. (1965). "Cramming more components onto integrated circuits", **Electronics**, cilt 38, sayı 8.
- MUDULİ, K., RAUT, R., NARKHEDE, B. E., SHEE, H. (2022). "Blockchain Technology for Enhancing Supply Chain Performance and Reducing the Threats Arising from the COVID-19 Pandemic", **Sustainability**, cilt 14, sayı 3290.
- KASAPBASİ, M. C. (2019). "A New Chaotic Image Steganography Technique Based on Huffman Compression of Turkish Texts and Fractal Encryption with Post-Quantum Security", **IEEE Access**, cilt 2019, sayı 7, ss. 148495–148510.
- KUMAR, T. M., REDDY, K. S., RİNALDİ, S., PARAMESHACHARİ, B. D. ve ARUNACHALAM, K. (2021). "A Low Area High Speed FPGA Implementation of AES Architecture for Cryptography Application", **Electronics**, cilt10, sayı 2023.
- PARK, Y. -H., KİM, Y., LEE, S. -O. ve KO, K. (2021). "Secure Outsourced Blockchain-Based Medical Data Sharing System Using Proxy Re-Encryption", **Appl. Sci.**, cilt 11, sayı 9422.
- PARTALA, J. (2018). "Provably Secure Covert Communication on Blockchain", **Cryptography**, cilt 2, sayı 3, ss. 1–18.
- PEECHARA, R. R. ve SUCHARİTA, V. (2021). "A chaos theory inspired, asynchronous two-way encryption mechanism for cloud computing", **PeerJ Comput. Sci.**, cilt 7, sayı 2011, ss. e628.
- PRANTO, T. H., NOMAN, A. A., MAHMUD, A. ve HAQUE, A. B. (2021). "Blockchain and smart contract for IoT enabled smart agriculture", **PeerJ Computer Science**, , ss.7:e407.
- RAJ, A. A., BENO, A. ve JAİSAKTHİ, R. (2020). "Security Enhancement of Information using Multilayered Cryptographic Algorithm", **4th International Conference on Trends in Electronics and Informatics (ICOEI)**, ss. 348-353.
- RİVERO-GARCÍA, A., SANTOS-GONZÁLEZ, I., HERNÁNDEZ-GOYA, C., CABALLERO-GİL, P. ve YUNG, M. (2017). "Patients' Data Management System Protected by Identity-Based Authentication and Key Exchange", **Sensors**, cilt 17, sayı 733.

- RODRÍGUEZ-GARCÍA, M., SÍCİLÍA, M. ve DODERO, J. M. (2021). “A privacy-preserving design for sharing demand-driven patient datasets over permissioned blockchains and P2P secure transfer”, **PeerJ Computer Science**, cilt 7, sayı 2012, ss. 7:e568.
- ROY, S. ve KHATWANI, C. (2017). “Cryptanalysis and Improvement of ECC Based Authentication and Key Exchanging Protocols”, **Cryptography**, cilt 1, sayı 9.
- SAAD, A. H. S., MOHAMED, M. S. ve HAFEZ, E. H. (2021). “Coverless Image Steganography Based on Optical Mark Recognition and Machine Learning”, **IEEE Access**, cilt 2021, sayı 9, ss. 16522–16531.
- SANDA, O., PAVLIDIS, M. ve POLATIDIS, N. (2022). “A Regulatory Readiness Assessment Framework for Blockchain Adoption in Healthcare”, **Digital**, cilt 2022, sayı 2, ss.65-87.
- SARKAR, P., SUDIPTA, K. G. ve SARKAR, M. (2020). “Stego-Chain: A Framework to Mine Encoded Stego-Block in a Decentralized Network”, **Journal of King Saud University- Computer and Information Sciences**, cilt 6, sayı 2.
- SETİADİ, D. R. I. M., RACHMAWANTO, E. H. ve SARI, C. A. (2017). “Secure Image Steganography Algorithm Based on DCT with OTP Encryption”, **J. Appl. Intell. Syst.**, cilt 2017, sayı 2, ss. 1–11.
- SHANKAR, M. ve AKSHAYA, A. (2014). “Hybrid Cryptographic Technique Using RSA”, **Int. J. Netw. Secur. Its Appl.**, cilt 6, sayı 6, ss. 39–48.
- SHARMA, M. K. ve SOMWANSHI, D. (2018). “Improvement in Homomorphic Encryption Algorithm with Elliptic Curve Cryptography and OTP Technique”, **3rd Int. Conf. Work. Recent Adv. Innov. Eng. ICRAIE**, cilt 2018, ss. 22–25.
- SHEHAB, D. A. ve ALHADDAD, M. J. (2022). “Comprehensive Survey of Multimedia Steganalysis: Techniques, Evaluations, and Trends in Future Research”, **Symmetry**, cilt 14, sayı 117.
- STULMAN, A. ve STULMAN, A. (2019). “Secured by Fluctuating Topology Using the Fluctuating Topology of MANETs to Secure Key Exchange”, **Electronics**, cilt 8, sayı 1172.

- SUBRAMANIAN, N., ELHARROUSS, O., AL-MAADEED, S. ve BOURIDANE, A. (2021). "Image Steganography: A Review of the Recent Advances", **IEEE Access**, cilt 2021, sayı 9, ss. 23409–23423.
- SUDHAKAR, K., SRİKANTH, S. ve SETHURAMAN, M. (2015). "Secured mutual authentication between two entities", **Proc. IEEE 9th Int. Conf. Intell. Syst. Control. ISCO**.
- ŞAHİN, F., ÇEVİK, T. ve TAKAOĞLU, M. (2021). "Review of the Literature on the Steganography Concept", **International Journal of Computer Applications (IJCA)**, cilt 183, sayı 2, ss. 38-46.
- TABARES-SOTO, R., ARTEAGA-ARTEAGA, H.B., MORA-RUBİO, A., BRAVO-ORTÍZ, M.A., ARIAS-GARZÓN, D., GRİSALES, J.A.A., JACOME, A.B., OROZCO-ARIAS, S., ISAZA, G. ve POLLAN, R.R. (2021). "Strategy to Improve the Accuracy of Convolutional Neural Network Architectures Applied to Digital Image Steganalysis in the Spatial Domain", **PeerJ Comput. Sci.**, cilt 2021, sayı 7, ss. 1–21.
- TAKAOĞLU, M., AJLOUNİ, N. M. M., ÖZYAVAŞ, A. ve HAMEED, A. A. (2021). "Blokzincir Temelli Milli Bağış Zinciri Projesi", **Uluslararası Bilimsel Araştırmalar ve Yenilikçi Çalışmalar Sempozyumu**, 344-369.
- TAKAOĞLU, M., ÖZYAVAŞ, A. ve AJLOUNİ, N. M. M. (2021). "AviChainDB: Blockchain Integration on Aviation Databases", **OSTIV Meteorological Panel**.
- TAKAOĞLU, F. ve TAKAOĞLU, M. (2020). "Yazıcı Steganografisi ve Sarı Nokta Analizinin Günümüzde Geçerliliği", **Yeni Medya Elektronik Dergisi**, cilt 4, sayı 3, ss. 186-194.
- TAKAOĞLU, F. ve TAKAOĞLU, M. (2019). "Yazıcı Steganografisi ve Sarı Nokta Analizi - Bir Mini Derleme", **ArtGRID - Journal of Architecture Engineering and Fine Arts**, cilt 1, sayı 1, ss. 25-35.
- TAKAOĞLU, M., ÖZYAVAŞ, A., AJLOUNİ, N. M. M., ALSHAHRANİ, A. ve ALKASESBEH, B. (2021). "A Novel and Robust Hybrid Blockchain and Steganography Scheme", **Applied Sciences-Basel**, cilt 11, sayı 22, pp.1-19.
- TAKAOĞLU, M., ÖZER, Ç. ve PARLAK, E. (2019). "Blokzinciri Teknolojisi ve Türkiye'deki Muhtemel Uygulanma Alanları", **Uluslararası Doğu Anadolu Fen Mühendislik ve Tasarım Dergisi**, cilt 1, sayı 2, ss. 260-295.

- TAKAOĞLU, M. ve GÜNEŞ, A. (2019). “Yükseköğretimde Blokzincir Teknolojisi”, **5th International Congress on Education, Distance Education and Educational Technology- ICDET**.
- VARAVALLO, G., CARAGNANO, G., BERTONE, F., VERNETTİ-PROT, L. ve TERZO, O. (2022). “Traceability Platform Based on Green Blockchain: An Application Case Study in Dairy Supply Chain”, **Sustainability**, cilt 14, sayı 3321.
- WAHAB, O. F. A., KHALAF, A. A. M., HUSSEİN, A. I. ve HAMED, H. F. A. (2021). “Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques”, **IEEE Access**, cilt 2021, sayı 9, ss. 31805–31815.
- WANG, B. ve Lİ, Z. (2021). “Healthchain: A Privacy Protection System for Medical Data Based on Blockchain”, **Future Internet**, cilt 13, sayı 247.
- WANG, L., HE, Y. ve WU, Z. (2022). “Design of a Blockchain-Enabled Traceability System Framework for Food Supply Chains”, **Foods**, cilt 11, sayı 744.
- WANG, P. ve Lİ, X. (2021). “Tedl: A text encryption method based on deep learning”, **Appl. Sci.**, cilt 11, sayı 4, ss. 1–30.
- XİE, G., REN, J., MARSHALL, S., ZHAO, H. ve Lİ, H. (2021). “A New Cost Function for Spatial Image Steganography Based on 2D-SSA and WMF”, **IEEE Access**, cilt 2021, sayı 9, ss. 30604-30614.
- YEOM, S., CHOİ, S., CHİ, J. ve PARK, S. (2021). “Blockchain-Based Employment Contract System Architecture Allowing Encrypted Keyword Searches”, **Electronics**, cilt 10, sayı 1086.
- YOON, H., MOON, S., KİM, Y., HAHN, C., LEE, W. ve HUR, J. (2020). “SPEKS: Forward Private SGX-Based Public Key Encryption with Keyword Search”, **Appl. Sci.**, cilt 10, sayı 7842.
- YU, B., Lİ, X. ve ZHAO, H. (2020). “PoW-BC: A PoW Consensus Protocol Based on Block Compression”, **KSII Transactions on Internet and Information Systems (TIIS)**, cilt 15, sayı 4, ss.1389-1408,
- YUAN, E., WANG, L., CHENG, S., AO, N. ve GUO, Q. (2020). “A Key Management Scheme Based on Pairing-Free Identity Based Digital Signature Algorithm for Heterogeneous Wireless Sensor Networks”, **Sensors**, cilt 20, sayı 1543.



## **EKLER**

**EK-1:** PDF dosyalarının bayt tekniğiyle manipülasyon sonuçları

**EK-2:** PDF dosyasının ara belleğe alınarak manipüle edilmesinin sonuçları

**EK-3:** PDF dosyası tersine bayt manipülasyonu verileri

**EK-4:** PDF dosyası tersine ara bellek manipülasyonu verileri

**EK-5:** JPG bayt tekniğiyle manipülasyon verileri

**EK-6:** JPG ara bellek tekniğiyle manipülasyon verileri

**EK-7:** JPG bayt tekniği tersine manipülasyon verileri

**EK-8:** JPG ara bellek tekniği tersine manipülasyon verileri

**EK-9:** DOC bayt tekniğiyle manipülasyon verileri

**EK-10:** DOC ara bellek tekniğiyle manipülasyon verileri

**EK-11:** DOC bayt tekniği tersine manipülasyon verileri

**EK-12:** DOC ara bellek tekniği tersine manipülasyon verileri

**EK-13:** XLSX bayt tekniğiyle manipülasyon verileri

**EK-14:** XLSX ara bellek tekniğiyle manipülasyon verileri

**EK-15:** XLSX bayt tekniği tersine manipülasyon verileri

**EK-16:** XLSX ara bellek tekniği tersine manipülasyon verileri



**EK-1: PDF dosyalarının bayt tekniğiyle manipülasyon sonuçları**

|                 |                 |                 |                 |
|-----------------|-----------------|-----------------|-----------------|
| 1546029:16170   | 257163:2163     | 3287306:24824   | 6784288:51469   |
| 173550:1477     | 187138:1499     | 706450:5591     | 290191:2432     |
| 670011:5399     | 393586:3161     | 3180489:23762   | 1168711:9134    |
| 4613810:36175   | 1136769:9100    | 381762:3297     | 620408:5059     |
| 1750269:14008   | 281517:2392     | 247829:1923     | 717773:5745     |
| 328240:2939     | 665820:5210     | 3449156:25894   | 216512:1771     |
| 69493:563       | 4671295:37423   | 363519:3031     | 2133567:16461   |
| 1310107:10566   | 428220:3590     | 177733:1352     | 466077:3767     |
| 10132373:85337  | 675559:5338     | 12684942:94331  | 157282:1232     |
| 933988:7851     | 1004244:7939    | 4476386:34401   | 5389128:41039   |
| 348687:3001     | 837807:7002     | 359654:2991     | 2490744:19450   |
| 150242:1274     | 1013681:8111    | 576565:4317     | 4197673:31833   |
| 302417:2569     | 410810:3311     | 2208215:16266   | 1210226:9561    |
| 547528:4871     | 544191:4563     | 921295:6902     | 933898:7607     |
| 574422:4881     | 289167:2262     | 885410:6910     | 4284458:32484   |
| 224965:1850     | 201379:1555     | 11561719:85739  | 79602:703       |
| 582769:4830     | 246482:1914     | 1487044:12020   | 2225778:17099   |
| 491647:4410     | 252033:1952     | 947158:7175     | 158793:1333     |
| 1094645:9309    | 874414:6780     | 825184:6210     | 763343:5953     |
| 5830119:48737   | 626171:5043     | 169801:1314     | 8741311:66066   |
| 86602:659       | 992653:7863     | 3285518:24397   | 5910124:45509   |
| 1531979:13382   | 645484:5116     | 3291278:24764   | 158111:1346     |
| 184292:1671     | 254971:1965     | 1647554:12153   | 556004:4638     |
| 123220:1047     | 3706141:29487   | 438179:3408     | 104293:840      |
| 118719:1020     | 784428:6272     | 2607028:19466   | 659059:5123     |
| 640243:5516     | 484849:3726     | 8525241:62631   | 2058197:16075   |
| 1442836:12031   | 76008:595       | 605723:5116     | 1690454:13069   |
| 507008:4093     | 611023:4687     | 397208:3177     | 17297558:130371 |
| 142183:1136     | 788600:6166     | 927601:6876     | 770223:6576     |
| 3523011:29785   | 468255:3653     | 234926:1868     | 504971:4256     |
| 1923708:16684   | 452901:3521     | 329196:2429     | 1233838:9679    |
| 4724302:38647   | 455182:3388     | 933746:6872     | 871131:6698     |
| 7918949:64817   | 2182784:16112   | 7240453:53770   | 2610266:19369   |
| 4583670:37785   | 348332:2946     | 618386:5055     | 1708346:13529   |
| 18292388:168545 | 24431469:183428 | 1114234:8269    | 282125:2292     |
| 4051567:34572   | 618386:5038     | 852419:6496     | 10528814:79365  |
| 6294838:55010   | 8063940:62338   | 348332:2760     | 377680:3124     |
| 218559:1795     | 1037871:8492    | 518098:3875     | 1625741:12631   |
| 408957:3514     | 284287:2275     | 1102474:8162    | 3310141:24718   |
| 102741:906      | 1045126:7694    | 954413:7169     | 196218:1727     |
| 616573:5283     | 328008:2515     | 83830:696       | 1200114:9537    |
| 621721:5404     | 888938:6478     | 1853700:13821   | 3074467:22851   |
| 321280:2635     | 193101:1611     | 22101840:166194 | 866328:6759     |
| 727412:6105     | 489591:3724     | 13818080:105206 | 218319:1683     |
| 549065:4581     | 1361587:9885    | 208671:1741     | 266606:2051     |
| 44437253:335947 | 414306:3155     | 291027:2407     | 1237621:9407    |
| 20600274:159788 | 365601:2709     | 35695403:267773 | 1145762:8678    |

|                 |               |                 |                 |
|-----------------|---------------|-----------------|-----------------|
| 3140980:25735   | 661096:4869   | 93991771:711218 | 465022:3674     |
| 770642:6208     | 947377:6902   | 3620243:30080   | 3592810:27346   |
| 5389128:41117   | 663751:4978   | 625441:5192     | 1565817:12017   |
| 123319:1042     | 260170:1976   | 212961:1854     | 185051:1541     |
| 2091773:16431   | 5439611:40548 | 1891798:16000   | 654712:5046     |
| 197976:1749     | 55814:465     | 451792:4021     | 354141:2746     |
| 1893498:14591   | 709177:5665   | 1092926:9145    | 602333:4678     |
| 773144:6049     | 1896813:13808 | 1805004:15117   | 211865:1626     |
| 22291542:168609 | 252033:2024   | 724497:5638     | 10424657:78462  |
| 1879723:15980   | 640537:4770   | 345271:2701     | 429221:3938     |
| 155498:1302     | 477066:3584   | 282516:2224     | 453508:3778     |
| 111461:943      | 249922:2000   | 2865213:21792   | 398137:3231     |
| 1282675:10134   | 194820:1523   | 1012398:7950    | 684281:5346     |
| 8249672:62644   | 4866445:36530 | 3417760:25889   | 783393:6056     |
| 2054085:16016   | 534101:4266   | 5150294:38814   | 4147580:31142   |
| 8081299:61311   | 276774:2146   | 1343518:10798   | 15372790:115751 |
| 380514:3192     | 622367:4614   | 1280390:9705    | 835265:7037     |
| 217676:1807     | 365686:2779   | 184292:1522     | 528123:4414     |
| 3821139:29183   | 535109:4040   | 452901:3493     | 1579322:12207   |
| 580982:4871     | 663869:4953   | 5267853:39484   | 415431:3366     |
| 9436883:70997   | 533372:4081   | 354071:3038     | 172826:1544     |
| 582769:4835     | 760475:5929   | 160226:1382     | 1448152:11567   |
| 1086414:8530    | 486299:3696   | 660790:5054     | 690095:5450     |
| 3219011:24720   | 1594043:11742 | 1662772:12375   | 5389128:40699   |
| 106708:898      | 307419:2521   | 2840429:21473   | 3727761:28591   |
| 176702:1459     | 296032:2296   | 475071:3819     | 1076330:8343    |
| 161556:1293     | 331375:2515   | 225646:1802     | 536973:4215     |
| 121645:976      | 533501:3899   | 202069:1625     | 1509466:11437   |
| 166762:1332     | 1375851:10118 | 1344099:10338   | 3742653:28635   |
| 120629:957      | 305250:2422   | 1974448:15289   | 89810:790       |
| 180053:1435     | 442707:3272   | 230062:1894     | 293040:2428     |
| 2344283:18852   | 152697:1149   | 2972688:22397   | 24336341:183016 |
| 2344283:18654   | 1873696:13725 | 295422:2455     | 9731948:75561   |
| 1933808:15129   | 1719434:13181 | 3148097:23889   | 2454838:19198   |
| 1195798:9399    | 644475:4910   | 2319343:18136   | 1368982:10421   |
| 43757900:333055 | 392748:2984   | 663900:5193     | 18131979:136168 |
| 276739:2337     | 1035030:7914  | 975554:7435     | 11682541:89407  |
| 1533162:12805   | 1621355:12174 | 426470:3376     | 91667:769       |
| 885357:7610     | 316670:2496   | 1586645:11959   | 428220:3776     |
| 1325042:11134   | 657549:4906   | 1002586:7686    | 1496611:12251   |
| 137497:1177     | 1418263:10575 | 283359:2386     | 1086235:8401    |
| 96088:832       | 540922:4166   | 1630109:12356   | 9555950:72441   |
| 1341232:10516   | 276457:2105   | 862426:7008     | 2188914:16908   |
| 1571242:12626   | 346886:2621   | 375922:3001     | 521809:4142     |
| 2105335:16183   | 1164027:8995  | 299542:2372     | 7309547:54722   |
| 1325017:10316   | 3303401:24921 | 319747:2474     | 115584:963      |
| 397395:3248     | 2302154:17422 | 13723267:102931 | 164322:1372     |
| 2709360:20370   | 1269882:9550  | 588633:5010     | 84537:705       |
| 561380:4576     | 373561:2904   | 3019685:23748   | 4286956:33347   |
| 986213:7920     | 1204149:9203  | 9520200:72079   | 55720385:422896 |

|                 |                 |                 |                 |
|-----------------|-----------------|-----------------|-----------------|
| 550860:4306     | 1189999:8901    | 111272:929      | 3159294:26239   |
| 1303021:10023   | 23459147:177588 | 265734:2218     | 921:12          |
| 583720:4578     | 1841876:15752   | 3738018:28484   | 918:11          |
| 269033:2131     | 12090522:90808  | 3698414:28627   | 918:12          |
| 3288606:25323   | 455735:3633     | 1295570:10048   | 885483:7633     |
| 5406254:40859   | 257719:2101     | 1689960:12828   | 919546:7625     |
| 586209:4857     | 400340:3314     | 462878:3745     | 580982:5125     |
| 2095885:16180   | 1414455:10652   | 189983:1485     | 261193:2067     |
| 1004452:7814    | 965487:7319     | 125808:1013     | 2101173:16364   |
| 1060809:8220    | 154709:1244     | 784428:6048     | 430168:3463     |
| 4685676:35110   | 500297:4026     | 637791:4993     | 195422:1551     |
| 1088404:8821    | 350405:2698     | 637791:5150     | 28234475:214749 |
| 597826:4649     | 728206:5490     | 3706141:28247   | 3441603:28783   |
| 668755:5181     | 205249:1619     | 3706141:28185   | 1000144:7941    |
| 389918:3043     | 5988480:50140   | 2139662:16663   | 782721:6165     |
| 763870:5932     | 241485:2007     | 99434:888       | 45638932:345018 |
| 183439:1442     | 2038247:15925   | 254971:2188     | 814419:6823     |
| 310627:2556     | 3974778:30708   | 888938:6918     | 1588710:13604   |
| 819257:6478     | 595626:4781     | 355285:2821     | 616573:5131     |
| 216000:1703     | 968216:7672     | 626171:4783     | 727412:6063     |
| 561764:4323     | 119889:976      | 201379:1586     | 549065:4760     |
| 28761678:217469 | 285672:2208     | 710439:5520     | 606365:4971     |
| 669942:5662     | 309585:2419     | 1656387:12664   | 679352:5384     |
| 538656:4767     | 247437:1965     | 26358:222       | 1124304:9114    |
| 2015704:16335   | 468147:3674     | 18451481:140111 | 368277:2921     |
| 104355:892      | 733510:5748     | 1118315:9480    | 1206937:9425    |
| 5238234:39894   | 1531979:12158   | 478702:4026     | 1737635:13650   |
| 1550213:12428   | 2223062:18010   | 402058:3308     | 100091:846      |
| 699222:5543     | 178387:1467     | 287066:2280     | 40023454:301396 |
| 756303:5950     | 18652791:141993 | 12548990:94575  | 393612:3318     |
| 584006:4589     | 246508:2069     | 1743532:14325   | 456129:3775     |
| 216765:1788     | 3368876:26547   | 368807:2982     | 609895:5021     |
| 571005:4667     | 4727116:36552   | 4053739:30966   | 271298:2245     |
| 701262:5556     | 6587782:50847   | 1269354:9918    | 348812:2850     |
| 2807029:21770   | 694740:5743     | 115778:1000     | 7777195:60902   |
| 1913187:14957   | 226406:1824     | 1852050:14120   | 4912572:37472   |
| 372429:3017     | 311948:2499     | 3067890:23275   | 5904829:44893   |
| 226741:1785     | 504499:3983     | 2915068:23218   | 7024183:53536   |
| 1318224:10286   | 2316192:18296   | 2723149:22190   | 1886719:15042   |
| 412991:3313     | 919546:7357     | 384967:3133     | 172270:1468     |
| 1138748:9169    | 623885:4965     | 200608:1599     | 83494:673       |
| 357079:2862     | 123380:1004     | 2685260:21275   | 83904:665       |
| 3328749:25585   | 989256:7900     | 3308843:26142   | 302417:2415     |
| 873841:7287     | 250379:2112     | 183419:1532     | 1526433:12039   |
| 247115:2028     | 119714:967      | 3036902:24592   | 419790:3369     |
| 1485058:11684   | 378934:3196     | 26704458:203946 |                 |
| 1000138:7970    | 289661:2436     | 1074982:8854    |                 |
| 1123316:8940    | 99364:825       | 152697:1319     |                 |
| 252345:2014     | 8225319:64545   | 237158:1971     |                 |
| 562427:4450     | 22527691:170877 | 780130:6165     |                 |

|                                                                                                                                                                                  |                                                                                                                |                                                                         |  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|--|
| 182059:1453<br>782783:6145<br>523974:4108<br>196236063:1484217<br>5051327:42035<br>4106683:34728<br>3756167:31205<br>1180311:9760<br>256769:2130<br>1245510:10105<br>121419:1047 | 2301915:19105<br>1035050:8644<br>4859301:36342<br>620216:5048<br>161949:1291<br>6579089:50435<br>3106669:24023 | 205798:1653<br>308692:2458<br>155553:1233<br>892803:7062<br>352449:2812 |  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|--|



**EK-2: PDF dosyasının ara belleğe alınarak manipüle edilmesinin sonuçları**

|              |               |               |
|--------------|---------------|---------------|
| 1546029:111  | 83830:3       | 261193:6      |
| 1750269:56   | 1853700:45    | 2101173:44    |
| 328240:8     | 22101840:463  | 430168:9      |
| 69493:3      | 13818080:579  | 195422:4      |
| 1310107:46   | 208671:6      | 28234475:1316 |
| 10132373:265 | 291027:7      | 3441603:159   |
| 933988:20    | 35695403:1309 | 1000144:20    |
| 348687:8     | 93991771:9217 | 782721:16     |
| 150242:3     | 3620243:115   | 45638932:1672 |
| 302417:7     | 625441:20     | 814419:16     |
| 547528:11    | 212961:12     | 1588710:36    |
| 574422:12    | 1891798:54    | 616573:12     |
| 224965:4     | 451792:23     | 727412:16     |
| 582769:11    | 1092926:34    | 549065:12     |
| 491647:11    | 1805004:97    | 606365:12     |
| 1094645:24   | 724497:21     | 679352:13     |
| 5830119:142  | 345271:13     | 44437253:4121 |
| 86602:3      | 282516:7      | 20600274:551  |
| 1531979:36   | 2865213:95    | 3140980:85    |
| 184292:7     | 1012398:29    | 770642:34     |
| 123220:5     | 3417760:109   | 5389128:122   |
| 118719:4     | 5150294:149   | 123319:5      |
| 507008:15    | 1343518:55    | 2091773:47    |
| 142183:5     | 1280390:37    | 197976:6      |
| 3523011:75   | 184292:5      | 1893498:39    |
| 1923708:42   | 452901:18     | 773144:22     |
| 4724302:101  | 5267853:196   | 22291542:524  |
| 7918949:164  | 354071:13     | 1879723:49    |
| 4583670:114  | 160226:6      | 155498:7      |
| 18292388:390 | 660790:17     | 111461:16     |
| 4051567:82   | 1662772:46    | 1282675:99    |
| 6294838:131  | 2840429:82    | 8249672:218   |
| 218559:5     | 475071:13     | 2054085:75    |
| 408957:7     | 225646:10     | 8081299:247   |
| 102741:2     | 202069:7      | 380514:15     |
| 616573:13    | 1344099:36    | 217676:7      |
| 621721:12    | 1974448:47    | 3821139:110   |
| 321280:6     | 230062:5      | 580982:19     |
| 727412:13    | 2972688:60    | 9436883:276   |
| 549065:11    | 295422:6      | 582769:14     |
| 257163:5     | 3148097:62    | 1086414:29    |
| 187138:4     | 2319343:45    | 3219011:82    |
| 393586:7     | 663900:13     | 106708:6      |
| 1136769:21   | 975554:22     | 176702:14     |
| 4671295:99   | 426470:15     | 161556:12     |
| 428220:8     | 1586645:50    | 121645:4      |
| 675559:13    | 1002586:39    | 166762:11     |

|              |               |               |
|--------------|---------------|---------------|
| 1004244:20   | 283359:13     | 120629:4      |
| 837807:18    | 1630109:64    | 180053:8      |
| 1013681:19   | 862426:25     | 2344283:73    |
| 410810:8     | 375922:15     | 2344283:67    |
| 544191:10    | 299542:13     | 1933808:48    |
| 289167:6     | 319747:11     | 1195798:33    |
| 201379:4     | 13723267:392  | 43757900:1252 |
| 874414:17    | 588633:14     | 276739:23     |
| 626171:13    | 3019685:92    | 1533162:62    |
| 992653:19    | 9520200:561   | 885357:33     |
| 645484:14    | 111272:4      | 1325042:52    |
| 254971:5     | 265734:6      | 137497:14     |
| 3706141:83   | 3738018:931   | 96088:12      |
| 784428:16    | 3698414:804   | 1341232:41    |
| 484849:11    | 1295570:261   | 1571242:49    |
| 76008:3      | 1689960:306   | 2105335:110   |
| 611023:13    | 462878:10     | 1325017:49    |
| 468255:10    | 189983:4      | 397395:17     |
| 452901:10    | 125808:3      | 2709360:101   |
| 455182:9     | 784428:17     | 561380:16     |
| 2182784:47   | 637791:15     | 986213:31     |
| 348332:8     | 637791:15     | 550860:19     |
| 24431469:534 | 3706141:745   | 1303021:2756  |
| 618386:15    | 3706141:77    | 583720:2530   |
| 8063940:180  | 2139662:47    | 269033:2911   |
| 1037871:20   | 99434:3       | 3288606:1036  |
| 284287:6     | 254971:5      | 5406254:151   |
| 1045126:20   | 888938:18     | 586209:24     |
| 193101:4     | 355285:8      | 2095885:78    |
| 489591:11    | 626171:13     | 1004452:32    |
| 1361587:26   | 201379:5      | 1060809:34    |
| 414306:11    | 710439:14     | 4685676:143   |
| 365601:8     | 1656387:35    | 1088404:33    |
| 661096:13    | 26358:1       | 597826:19     |
| 947377:18    | 18451481:394  | 668755:27     |
| 663751:13    | 1118315:26    | 389918:16     |
| 260170:6     | 478702:11     | 763870:27     |
| 5439611:286  | 402058:8      | 183439:11     |
| 55814:2      | 287066:6      | 310627:13     |
| 709177:14    | 12548990:1193 | 819257:23     |
| 1896813:40   | 1743532:125   | 216000:9      |
| 252033:6     | 368807:9      | 561764:21     |
| 640537:16    | 4053739:177   | 28761678:1191 |
| 477066:11    | 1269354:32    | 669942:20     |
| 249922:6     | 115778:2      | 538656:16     |
| 194820:4     | 1852050:46    | 2015704:55    |
| 4866445:103  | 3067890:149   | 104355:7      |
| 534101:10    | 6784288:230   | 5238234:156   |
| 276774:5     | 290191:6      | 1550213:119   |
| 622367:13    | 1168711:31    | 699222:18     |

|              |               |                 |
|--------------|---------------|-----------------|
| 365686:7     | 620408:19     | 756303:21       |
| 535109:11    | 717773:18     | 584006:18       |
| 663869:13    | 216512:5      | 216765:8        |
| 533372:12    | 2133567:115   | 571005:49       |
| 760475:15    | 466077:10     | 701262:23       |
| 486299:10    | 157282:4      | 2807029:163     |
| 1594043:30   | 5389128:132   | 1913187:43      |
| 307419:6     | 2490744:143   | 372429:12       |
| 296032:6     | 4197673:106   | 226741:13       |
| 331375:7     | 1210226:36    | 1318224:37      |
| 533501:10    | 933898:23     | 412991:11       |
| 1375851:28   | 4284458:89    | 1138748:27      |
| 305250:7     | 79602:3       | 357079:10       |
| 442707:9     | 2225778:47    | 3328749:156     |
| 152697:4     | 158793:3      | 873841:30       |
| 1873696:39   | 763343:17     | 247115:15       |
| 1719434:34   | 8741311:265   | 1485058:59      |
| 644475:13    | 5910124:277   | 1000138:43      |
| 392748:9     | 158111:4      | 1123316:52      |
| 1035030:20   | 556004:12     | 252345:17       |
| 1621355:31   | 104293:3      | 562427:102      |
| 316670:7     | 659059:14     | 182059:11       |
| 657549:13    | 2058197:49    | 782783:32       |
| 1418263:32   | 1690454:38    | 523974:20       |
| 540922:11    | 17297558:590  | 196236063:29134 |
| 276457:7     | 770223:19     | 5051327:98      |
| 346886:9     | 504971:14     | 4106683:84      |
| 1164027:27   | 1233838:43    | 3756167:75      |
| 3303401:73   | 871131:29     | 1180311:38      |
| 2302154:49   | 2610266:301   | 5988480:226     |
| 1269882:29   | 1708346:429   | 241485:8        |
| 373561:7     | 282125:8      | 2038247:51      |
| 1204149:23   | 10528814:3166 | 3974778:170     |
| 1189999:23   | 377680:10     | 595626:15       |
| 23459147:872 | 1625741:252   | 968216:22       |
| 1841876:34   | 3310141:68    | 119889:5        |
| 12090522:242 | 196218:4      | 285672:11       |
| 455735:10    | 1200114:27    | 309585:10       |
| 257719:6     | 3074467:79    | 247437:7        |
| 400340:8     | 866328:22     | 468147:12       |
| 1414455:32   | 218319:6      | 733510:17       |
| 965487:21    | 266606:8      | 1531979:33      |
| 154709:3     | 1237621:34    | 2223062:128     |
| 500297:11    | 1145762:37    | 178387:7        |
| 350405:8     | 465022:13     | 18652791:448    |
| 728206:15    | 3592810:106   | 246508:7        |
| 205249:4     | 1565817:48    | 3368876:62      |
| 3287306:70   | 185051:5      | 4727116:87      |
| 706450:14    | 654712:23     | 6587782:1057    |
| 3180489:63   | 354141:8      | 694740:18       |

|              |               |                |
|--------------|---------------|----------------|
| 381762:9     | 602333:19     | 226406:11      |
| 247829:5     | 211865:10     | 311948:10      |
| 3449156:72   | 10424657:322  | 504499:196     |
| 363519:7     | 429221:14     | 2316192:150    |
| 177733:4     | 453508:16     | 919546:133     |
| 12684942:360 | 398137:12     | 623885:129     |
| 4476386:93   | 684281:18     | 123380:98      |
| 359654:8     | 783393:18     | 989256:164     |
| 576565:14    | 4147580:171   | 250379:123     |
| 2208215:50   | 15372790:537  | 119714:17      |
| 921295:20    | 835265:23     | 378934:137     |
| 885410:19    | 528123:14     | 289661:125     |
| 11561719:318 | 1579322:47    | 99364:13       |
| 1487044:33   | 415431:9      | 8225319:874    |
| 947158:18    | 172826:5      | 22527691:433   |
| 825184:16    | 1448152:35    | 2301915:47     |
| 169801:4     | 690095:18     | 1035050:22     |
| 3285518:74   | 5389128:357   | 4859301:90     |
| 3291278:77   | 3727761:91    | 620216:17      |
| 1647554:36   | 1076330:30    | 161949:7       |
| 438179:8     | 536973:14     | 6579089:132    |
| 2607028:51   | 1509466:122   | 3106669:60     |
| 8525241:170  | 3742653:89    | 256769:8       |
| 605723:13    | 89810:2       | 1245510:27     |
| 397208:10    | 293040:8      | 1124304:24     |
| 927601:19    | 24336341:2104 | 368277:9       |
| 234926:5     | 9731948:9212  | 1206937:28     |
| 329196:7     | 2454838:362   | 1737635:37     |
| 933746:19    | 1368982:29    | 100091:4       |
| 7240453:437  | 18131979:365  | 40023454:10572 |
| 618386:16    | 11682541:235  | 393612:10      |
| 1114234:176  | 91667:2       | 456129:11      |
| 852419:29    | 428220:8      | 609895:14      |
| 348332:11    | 1496611:32    | 271298:7       |
| 518098:13    | 1086235:27    | 348812:8       |
| 1102474:72   | 9555950:517   | 7777195:144    |
| 954413:21    | 2188914:45    | 4912572:90     |
| 155553:5     | 521809:9      | 5904829:108    |
| 892803:21    | 7309547:214   | 7024183:140    |
| 352449:10    | 115584:2      | 1886719:39     |
| 2915068:57   | 164322:3      | 172270:5       |
| 2723149:55   | 84537:2       | 83494:4        |
| 384967:11    | 4286956:82    | 83904:3        |
| 200608:7     | 55720385:3937 | 302417:9       |
| 2685260:58   | 3159294:63    | 1526433:32     |
| 3308843:74   | 921:0         | 419790:10      |
| 183419:7     | 918:1         | 1074982:24     |
| 3036902:70   | 918:0         | 152697:5       |
| 121419:5     | 885483:17     | 237158:7       |
| 205798:7     | 919546:18     | 780130:24      |

|           |           |  |
|-----------|-----------|--|
| 308692:10 | 580982:11 |  |
|-----------|-----------|--|





**EK-3: PDF dosyası tersine bayt manipölasyonu verileri**

|                 |                  |                  |
|-----------------|------------------|------------------|
| 3092062:13091   | 14480910:52566   | 830866:3240      |
| 347104:1421     | 1236776:4602     | 345656:1474      |
| 1340026:5512    | 2228472:8175     | 2896308:11602    |
| 3500542:14434   | 1704842:6287     | 1380194:6131     |
| 656484:2745     | 696668:2641      | 10778260:44896   |
| 138990:608      | 1036200:3752     | 7455526:29494    |
| 2620218:10623   | 2204952:7978     | 2152664:8402     |
| 20264750:82281  | 1908830:6931     | 1073950:4444     |
| 1867980:7608    | 167664:602       | 3018936:11114    |
| 697378:2769     | 3707404:13387    | 7485310:28401    |
| 300488:1190     | 44203684:165538  | 179624:706       |
| 604838:2466     | 27636164:100207  | 586084:2265      |
| 1095060:4314    | 417346:1617      | 48672686:191504  |
| 1148848:4690    | 582058:2222      | 19463900:76852   |
| 449934:1855     | 71390810:264217  | 4909680:19755    |
| 1165542:4604    | 187983546:705216 | 2737968:10006    |
| 983298:3924     | 7240490:27773    | 36263962:133389  |
| 11660242:47182  | 1250886:4728     | 23365086:94948   |
| 2189294:8423    | 425926:1623      | 183338:716       |
| 173208:630      | 3783600:14665    | 856444:3410      |
| 3063962:12011   | 903588:3323      | 2993226:12688    |
| 368588:1381     | 2185856:8188     | 2172474:9391     |
| 246444:974      | 3610012:13316    | 19111904:78574   |
| 237442:873      | 1448998:5435     | 4377832:17268    |
| 9227624:37005   | 690546:2543      | 1043622:4132     |
| 1280490:5162    | 565036:2068      | 14619098:58890   |
| 284370:1126     | 5730430:21360    | 231172:923       |
| 7046026:28426   | 2024800:7725     | 328648:1296      |
| 3847420:15119   | 6835524:26916    | 169078:716       |
| 9448608:39341   | 10300592:45895   | 8573916:34081    |
| 15837902:64900  | 2687040:11645    | 111440774:471039 |
| 9167344:37157   | 2560784:11165    | 6318592:28360    |
| 36584780:152605 | 368588:1528      | 1846:13          |
| 8103138:34109   | 905806:3421      | 1840:15          |
| 12589680:51164  | 10535710:39558   | 1840:16          |
| 437122:1850     | 708146:2701      | 1770970:8336     |
| 1014020:4132    | 320456:1192      | 1839096:8276     |
| 817918:3257     | 1321584:4974     | 1161968:5214     |
| 205486:824      | 3325548:12382    | 522390:2136      |
| 1233150:5288    | 5680862:20915    | 4202350:18249    |
| 1243446:5165    | 950146:3411      | 860340:3855      |
| 642564:2474     | 451296:1739      | 390848:2046      |
| 1454828:6283    | 404142:1584      | 56468954:254327  |
| 1098134:4385    | 2688202:10529    | 6883210:33948    |
| 374280:1549     | 3948900:14516    | 2000292:9835     |
| 514330:2184     | 460128:1774      | 1565446:7186     |
| 787176:3448     | 5945380:23161    | 91277868:427232  |

|                 |                 |                 |
|-----------------|-----------------|-----------------|
| 2273542:9537    | 590848:2285     | 1628842:7639    |
| 2885676:11701   | 6296198:24708   | 3177424:15116   |
| 563038:2197     | 4638690:17796   | 1233150:5879    |
| 9342594:37093   | 1327804:5049    | 1454828:7023    |
| 856444:3234     | 1951112:7249    | 1098134:5135    |
| 1351122:5328    | 852944:3077     | 1212734:5277    |
| 2008492:8310    | 3173294:11863   | 1358708:5929    |
| 1675618:6509    | 2005176:7628    | 88874510:411641 |
| 2027366:7969    | 566722:2320     | 41200552:192782 |
| 821624:3183     | 3260222:12939   | 6281964:29366   |
| 1088386:4201    | 1724856:6601    | 1541288:6904    |
| 578338:2211     | 751848:2821     | 10778260:51029  |
| 402762:1594     | 599088:2223     | 246642:1207     |
| 1331644:5181    | 639498:2414     | 4183550:19663   |
| 492968:1911     | 27446538:115221 | 395956:1735     |
| 1748832:7342    | 1177270:5333    | 3787000:16868   |
| 1252346:5471    | 6039374:22976   | 1546292:7308    |
| 1985310:8162    | 19040404:72475  | 44583088:206831 |
| 1290972:5341    | 222548:840      | 3759450:20621   |
| 509946:2105     | 531472:1955     | 311000:1823     |
| 7412286:31025   | 7476040:28364   | 222926:1201     |
| 1568860:6371    | 7396832:28581   | 2565354:12877   |
| 969702:4030     | 2591144:9620    | 16499348:76946  |
| 152020:647      | 3379924:12440   | 4108174:18872   |
| 1222050:5266    | 925760:3377     | 16162602:64836  |
| 504070:2002     | 379970:1385     | 761032:3269     |
| 936514:3838     | 251620:976      | 435356:1829     |
| 905806:3688     | 1568860:6188    | 7642282:31186   |
| 910368:3643     | 1275586:4658    | 1161968:4903    |
| 4365572:20784   | 1275586:4716    | 18873770:79594  |
| 696668:3085     | 7412286:26756   | 1165542:5125    |
| 48862942:215514 | 7412286:27507   | 2172832:8889    |
| 1236776:5298    | 4279328:15996   | 6438026:26232   |
| 16127884:70958  | 198872:797      | 213420:937      |
| 2075746:8759    | 509946:1926     | 353408:1501     |
| 568578:2285     | 1777880:6559    | 323116:1481     |
| 2090256:8718    | 710574:2628     | 243294:1137     |
| 1577204:6829    | 1252346:4571    | 333528:1464     |
| 656020:2725     | 402762:1509     | 241262:1013     |
| 386206:1547     | 1420882:5222    | 360110:1627     |
| 979186:3763     | 3312778:12198   | 4688570:19956   |
| 2723178:11227   | 52720:216       | 4688570:17888   |
| 828616:3529     | 36902966:146688 | 3867620:15751   |
| 731206:2945     | 2236634:9073    | 2391600:9250    |
| 1322196:5533    | 957408:3850     | 87515804:363517 |
| 1894758:8364    | 804120:3206     | 553482:2580     |
| 1327506:5904    | 574136:2275     | 3066328:13879   |
| 520344:2023     | 25097984:100356 | 1770718:8027    |
| 10879226:48553  | 3487068:15356   | 2650088:11357   |
| 1777880:9170    | 737618:3159     | 274998:1212     |

|                 |                 |                 |
|-----------------|-----------------|-----------------|
| 111632:499      | 8107482:32020   | 192180:826      |
| 3793630:17052   | 2538712:10245   | 2682468:11495   |
| 504070:2194     | 231560:943      | 3142488:12974   |
| 1281078:5770    | 3704104:14761   | 4210674:15893   |
| 954136:4330     | 6135784:24761   | 2650038:10340   |
| 499848:2196     | 13568580:54389  | 794794:3207     |
| 389644:1652     | 580386:2321     | 5418724:22719   |
| 9732894:46795   | 2337426:9254    | 1122764:4186    |
| 1068206:4632    | 1240820:4951    | 1972430:7614    |
| 553552:2294     | 1435550:5719    | 1101724:4107    |
| 1244738:5508    | 433028:1778     | 2606046:9847    |
| 1418358:6223    | 4267138:17128   | 1167444:4921    |
| 731376:3033     | 932158:3881     | 538070:2313     |
| 1070222:4575    | 314568:1266     | 6577216:26449   |
| 1327742:5662    | 10778260:43710  | 10812512:42989  |
| 1066748:4499    | 4981492:19762   | 1172422:4910    |
| 1520954:6477    | 8395350:34135   | 4191774:16992   |
| 972602:4219     | 2420456:9701    | 2008908:8472    |
| 3188090:15931   | 1867800:7418    | 2121622:8681    |
| 614842:2561     | 8568920:34831   | 9371356:37901   |
| 592068:2467     | 159208:647      | 2176812:9341    |
| 662754:2792     | 4451560:17583   | 1195656:5211    |
| 1067006:4564    | 317590:1312     | 1337514:5493    |
| 2751706:12282   | 1526690:6066    | 779840:3417     |
| 610504:2881     | 17482626:68680  | 1527744:6772    |
| 885418:3503     | 11820252:44041  | 366882:1591     |
| 3747396:16128   | 316226:1181     | 621258:2645     |
| 3438872:15266   | 1112012:4110    | 1638518:7260    |
| 1288954:5553    | 208590:782      | 432004:1889     |
| 785500:3308     | 1318122:4794    | 1123532:4521    |
| 2070064:8918    | 4116398:14947   | 57523360:234718 |
| 3242714:13970   | 3380912:12480   | 1339888:5478    |
| 633344:2672     | 34595120:127842 | 1077316:4609    |
| 305398:1310     | 1540450:6093    | 4031412:16569   |
| 1315102:5789    | 1009946:4121    | 208714:879      |
| 2836530:12360   | 2467680:10299   | 10476472:43059  |
| 1081848:4768    | 1742266:7046    | 3100430:13197   |
| 552918:2319     | 5220536:20744   | 1398448:6041    |
| 693776:2894     | 3416696:13511   | 1512610:6368    |
| 2328058:10055   | 564254:2215     | 1168016:4631    |
| 6606806:28847   | 21057632:80528  | 433534:1701     |
| 4604312:20268   | 755364:2959     | 1142014:4872    |
| 2539768:11082   | 3251486:12509   | 1402528:6032    |
| 747126:3215     | 6620286:25599   | 5614062:22056   |
| 2408302:10251   | 392440:1540     | 3826378:14596   |
| 2380002:10491   | 2400232:9075    | 744862:3151     |
| 46918298:205504 | 6148938:23384   | 453486:1920     |
| 3683756:14431   | 1732660:6743    | 2636452:10680   |
| 24181048:105737 | 436642:1662     | 825986:3187     |
| 911474:3815     | 533216:2020     | 2277500:8526    |

|                 |                 |                   |
|-----------------|-----------------|-------------------|
| 515442:2158     | 2475246:9154    | 714162:2651       |
| 800684:3410     | 2291528:8391    | 6657502:24958     |
| 2828914:11623   | 930048:3582     | 1747686:7373      |
| 1930978:8202    | 7185624:27186   | 494234:2035       |
| 309422:1282     | 3131638:11798   | 2970120:12030     |
| 1000598:4072    | 370106:1451     | 2000280:8211      |
| 700814:2813     | 1309428:4813    | 2246636:9266      |
| 1456416:5950    | 708286:2665     | 504694:2044       |
| 410502:1626     | 1204670:4605    | 1124858:4751      |
| 6574616:27075   | 423734:1692     | 364122:1515       |
| 1412904:5814    | 20849318:79811  | 1565570:6270      |
| 6360982:26213   | 858446:3201     | 1047952:4401      |
| 763528:3025     | 907020:3414     | 392472130:1500682 |
| 495662:1951     | 796278:3086     | 10102658:37059    |
| 6898316:28189   | 1368566:5213    | 8213370:30322     |
| 727042:2852     | 1566790:5935    | 7512338:27684     |
| 355470:1431     | 8295164:31408   | 2360626:9052      |
| 25369888:103484 | 30745584:119719 | 11976964:44287    |
| 8952776:36642   | 1670534:6433    | 482974:1810       |
| 719312:2721     | 1056250:3959    | 4076498:15263     |
| 1153134:4494    | 3158648:11963   | 7949560:29519     |
| 4416434:18233   | 2413878:10694   | 1191256:4316      |
| 1842594:7416    | 3475274:14079   | 1936436:6941      |
| 1770824:7188    | 200186:803      | 239782:931        |
| 23123442:92588  | 80046912:313268 | 571348:2116       |
| 2974092:11235   | 787228:3087     | 619174:2242       |
| 1894320:7056    | 912262:3446     | 494878:1790       |
| 1650372:7833    | 1219794:4753    | 936298:3423       |
| 339606:1647     | 542600:2245     | 1467024:5332      |
| 6571040:25417   | 697628:2863     | 3063962:11475     |
| 6582560:24481   | 15554394:62057  | 4446128:16330     |
| 3295112:11922   | 9825148:38731   | 356778:1350       |
| 876362:3111     | 11809662:46553  | 37305586:137235   |
| 5214060:18811   | 14048370:54562  | 493020:1922       |
| 17050486:62230  | 3773442:14333   | 6737756:24591     |
| 1211450:4433    | 344544:1402     | 9454236:34927     |
| 794420:2841     | 167812:716      | 13175568:47964    |
| 1855206:6994    | 166992:647      | 1389484:5166      |
| 469856:1657     | 604838:2557     | 452816:1741       |
| 658396:2354     | 3052870:11475   | 623900:2434       |
| 1867496:6733    | 1839096:7100    | 1009002:3697      |
| 839584:3107     | 1247774:4547    | 4632388:16772     |
| 2149968:8112    | 246764:897      | 736558:3527       |
| 305398:1092     | 1978516:7213    |                   |
| 474320:1697     | 500762:1906     |                   |
| 1560264:5550    | 239432:890      |                   |
| 411600:1494     | 757872:2791     |                   |
| 617388:2193     | 579326:2162     |                   |
| 311110:1106     | 198732:724      |                   |
| 1785610:6610    | 16450642:60546  |                   |

|                 |                 |  |
|-----------------|-----------------|--|
| 704902:2655     | 45055386:165574 |  |
| 5830140:22975   | 4603834:16892   |  |
| 5446302:22249   | 2070104:7608    |  |
| 769938:2813     | 9718606:36126   |  |
| 401220:1678     | 1240436:4561    |  |
| 5370524:26104   | 323902:1236     |  |
| 6617690:27803   | 13158182:54315  |  |
| 366842:1684     | 6213342:23036   |  |
| 6073808:27273   | 513542:1961     |  |
| 53408920:220372 | 2491024:9554    |  |
| 242842:966      | 2248612:8544    |  |





**EK-4: PDF dosyası tersine ara bellek manipölasyonu verileri**

|              |                |               |
|--------------|----------------|---------------|
| 3092062:126  | 2228472:23     | 860340:6      |
| 347104:15    | 1704842:20     | 390848:3      |
| 1340026:93   | 696668:5       | 56468954:1246 |
| 3500542:29   | 1036200:6      | 6883210:104   |
| 656484:11    | 2204952:22     | 2000292:28    |
| 138990:3     | 1908830:19     | 1565446:23    |
| 2620218:31   | 167664:2       | 91277868:9714 |
| 20264750:139 | 3707404:35     | 1628842:19    |
| 1867980:14   | 44203684:414   | 3177424:33    |
| 697378:5     | 27636164:253   | 1233150:20    |
| 300488:6     | 417346:3       | 1454828:25    |
| 604838:5     | 582058:4       | 1098134:17    |
| 1095060:8    | 71390810:1026  | 1212734:22    |
| 1148848:8    | 187983546:1992 | 1358708:21    |
| 449934:4     | 7240490:107    | 88874510:1149 |
| 1165542:8    | 1250886:21     | 41200552:761  |
| 983298:8     | 425926:3       | 6281964:78    |
| 11660242:126 | 3783600:64     | 1541288:19    |
| 2189294:22   | 903588:6       | 10778260:242  |
| 173208:3     | 2185856:32     | 246642:2      |
| 3063962:40   | 3610012:45     | 4183550:139   |
| 368588:5     | 1448998:21     | 395956:3      |
| 246444:5     | 690546:4       | 3787000:56    |
| 237442:4     | 565036:4       | 1546292:26    |
| 9227624:61   | 5730430:70     | 44583088:575  |
| 1280490:8    | 2024800:30     | 3759450:55    |
| 284370:2     | 6835524:114    | 311000:3      |
| 7046026:66   | 10300592:150   | 222926:2      |
| 3847420:44   | 2687040:41     | 2565354:38    |
| 9448608:128  | 2560784:35     | 16499348:394  |
| 15837902:229 | 368588:3       | 4108174:62    |
| 9167344:132  | 905806:6       | 16162602:281  |
| 36584780:478 | 10535710:151   | 761032:10     |
| 8103138:119  | 708146:4       | 435356:10     |
| 12589680:183 | 320456:3       | 7642282:101   |
| 437122:3     | 1321584:23     | 1161968:16    |
| 1014020:7    | 3325548:51     | 18873770:493  |
| 817918:7     | 5680862:63     | 1165542:19    |
| 205486:2     | 950146:8       | 2172832:37    |
| 1233150:19   | 451296:4       | 6438026:181   |
| 1243446:20   | 404142:4       | 213420:5      |
| 642564:4     | 2688202:60     | 353408:91     |
| 1454828:23   | 3948900:186    | 323116:6      |
| 1098134:17   | 460128:3       | 243294:6      |
| 374280:3     | 5945380:85     | 333528:5      |
| 514330:3     | 590848:4       | 241262:6      |
| 787176:6     | 6296198:84     | 360110:7      |
| 2273542:29   | 4638690:59     | 4688570:72    |

|               |              |               |
|---------------|--------------|---------------|
| 2885676:40    | 1327804:16   | 4688570:69    |
| 563038:3      | 1951112:32   | 3867620:59    |
| 9342594:150   | 852944:6     | 2391600:36    |
| 856444:7      | 3173294:44   | 87515804:1202 |
| 1351122:20    | 2005176:32   | 553482:10     |
| 2008492:33    | 566722:4     | 3066328:40    |
| 1675618:25    | 3260222:46   | 1770718:112   |
| 2027366:30    | 1724856:26   | 2650088:40    |
| 821624:6      | 751848:4     | 274998:5      |
| 1088386:16    | 599088:5     | 192180:5      |
| 578338:4      | 639498:4     | 2682468:40    |
| 402762:3      | 27446538:373 | 3142488:45    |
| 1331644:20    | 1177270:21   | 4210674:61    |
| 492968:4      | 6039374:92   | 2650038:34    |
| 1748832:23    | 19040404:178 | 794794:10     |
| 1252346:17    | 222548:1     | 5418724:69    |
| 1985310:28    | 531472:3     | 1122764:19    |
| 1290972:15    | 7476040:9259 | 1972430:28    |
| 509946:3      | 7396832:181  | 1101724:17    |
| 7412286:94    | 2591144:31   | 2606046:34    |
| 1568860:23    | 3379924:44   | 1167444:15    |
| 969702:6      | 925760:6     | 538070:8      |
| 152020:1      | 379970:3     | 6577216:214   |
| 1222050:21    | 251620:2     | 10812512:330  |
| 504070:3      | 1568860:25   | 1172422:18    |
| 936514:6      | 1275586:20   | 4191774:148   |
| 905806:5      | 1275586:103  | 2008908:29    |
| 910368:5      | 7412286:108  | 2121622:28    |
| 4365572:61    | 7412286:97   | 9371356:114   |
| 696668:5      | 4279328:140  | 2176812:30    |
| 48862942:670  | 198872:2     | 1195656:18    |
| 1236776:17    | 509946:4     | 1337514:19    |
| 16127884:7497 | 1777880:27   | 779840:9      |
| 2075746:363   | 710574:5     | 1527744:17    |
| 568578:4      | 1252346:19   | 366882:5      |
| 2090256:352   | 402762:3     | 621258:8      |
| 1577204:642   | 1420882:19   | 1638518:17    |
| 656020:5      | 3312778:132  | 432004:6      |
| 386206:5      | 52720:1      | 1123532:14    |
| 979186:8      | 36902966:604 | 57523360:1133 |
| 2723178:43    | 2236634:33   | 1339888:19    |
| 828616:5      | 957408:6     | 1077316:16    |
| 731206:6      | 804120:5     | 4031412:53    |
| 1322196:18    | 574136:4     | 208714:4      |
| 1894758:23    | 25097984:472 | 10476472:139  |
| 1327506:16    | 3487068:54   | 3100430:38    |
| 520344:3      | 737618:5     | 1398448:19    |
| 10879226:133  | 8107482:218  | 1512610:16    |
| 1777880:22    | 2538712:37   | 1168016:14    |
| 111632:2      | 231560:1     | 433534:6      |

|              |              |                 |
|--------------|--------------|-----------------|
| 3793630:42   | 3704104:49   | 1142014:13      |
| 504070:4     | 6135784:167  | 1402528:20      |
| 1281078:8    | 13568580:173 | 5614062:73      |
| 954136:6     | 580386:4     | 3826378:44      |
| 499848:4     | 2337426:33   | 744862:9        |
| 389644:3     | 1240820:16   | 453486:7        |
| 9732894:102  | 1435550:21   | 2636452:37      |
| 1068206:7    | 433028:3     | 825986:15       |
| 553552:5     | 4267138:144  | 2277500:28      |
| 1244738:8    | 932158:6     | 714162:12       |
| 1418358:18   | 314568:2     | 6657502:415     |
| 731376:5     | 10778260:156 | 1747686:129     |
| 1070222:15   | 4981492:208  | 494234:7        |
| 1327742:9    | 8395350:118  | 2970120:126     |
| 1066748:7    | 2420456:45   | 2000280:25      |
| 1520954:17   | 1867800:25   | 2246636:30      |
| 972602:6     | 8568920:113  | 504694:8        |
| 3188090:33   | 159208:1     | 1124858:16      |
| 614842:4     | 4451560:62   | 364122:6        |
| 592068:4     | 317590:2     | 1565570:21      |
| 662754:4     | 1526690:22   | 1047952:15      |
| 1067006:12   | 17482626:236 | 392472130:13497 |
| 2751706:32   | 11820252:297 | 10102658:227    |
| 610504:5     | 316226:3     | 8213370:125     |
| 885418:6     | 1112012:16   | 7512338:99      |
| 3747396:41   | 208590:2     | 2360626:33      |
| 3438872:38   | 1318122:18   | 11976964:175    |
| 1288954:22   | 4116398:54   | 482974:7        |
| 785500:6     | 3380912:41   | 4076498:59      |
| 2070064:75   | 34595120:479 | 7949560:118     |
| 3242714:46   | 1540450:24   | 1191256:18      |
| 633344:4     | 1009946:6    | 1936436:34      |
| 305398:3     | 2467680:37   | 239782:5        |
| 1315102:16   | 1742266:29   | 571348:10       |
| 2836530:32   | 5220536:65   | 619174:12       |
| 1081848:12   | 3416696:47   | 494878:8        |
| 552918:4     | 564254:4     | 936298:13       |
| 693776:6     | 21057632:282 | 1467024:23      |
| 2328058:28   | 755364:4     | 3063962:38      |
| 6606806:69   | 3251486:48   | 4446128:45      |
| 4604312:55   | 6620286:239  | 356778:5        |
| 2539768:27   | 392440:3     | 37305586:448    |
| 747126:5     | 2400232:29   | 493020:9        |
| 2408302:25   | 6148938:89   | 6737756:88      |
| 2380002:39   | 1732660:27   | 9454236:129     |
| 46918298:573 | 436642:2     | 13175568:186    |
| 3683756:50   | 533216:3     | 1389484:21      |
| 24181048:378 | 2475246:38   | 452816:8        |
| 911474:6     | 2291528:34   | 623900:11       |
| 515442:4     | 930048:5     | 1009002:16      |

|              |                |               |
|--------------|----------------|---------------|
| 800684:5     | 7185624:95     | 4632388:64    |
| 2828914:45   | 3131638:42     | 1839096:27    |
| 1930978:25   | 370106:3       | 1247774:17    |
| 309422:2     | 1309428:20     | 246764:4      |
| 1000598:7    | 708286:4       | 1978516:27    |
| 700814:6     | 1204670:21     | 500762:8      |
| 1456416:20   | 423734:2       | 239432:5      |
| 410502:3     | 20849318:289   | 757872:8      |
| 6574616:68   | 858446:5       | 579326:7      |
| 1412904:15   | 907020:6       | 198732:4      |
| 6360982:63   | 796278:4       | 16450642:213  |
| 763528:5     | 1368566:22     | 45055386:638  |
| 495662:4     | 1566790:23     | 4603834:61    |
| 6898316:71   | 8295164:114    | 2070104:29    |
| 727042:4     | 30745584:9813  | 9718606:140   |
| 355470:2     | 1670534:24     | 1240436:19    |
| 25369888:254 | 1056250:15     | 323902:7      |
| 8952776:77   | 3158648:50     | 13158182:178  |
| 719312:5     | 830866:5       | 6213342:82    |
| 1153134:10   | 345656:3       | 513542:8      |
| 4416434:37   | 2896308:43     | 2491024:36    |
| 1842594:18   | 1380194:23     | 2248612:31    |
| 1770824:20   | 10778260:157   | 736558:11     |
| 23123442:239 | 7455526:185    | 2413878:33    |
| 2974092:32   | 2152664:27     | 3475274:48    |
| 1894320:19   | 1073950:13     | 200186:5      |
| 1650372:19   | 3018936:38     | 80046912:9625 |
| 339606:3     | 7485310:98     | 787228:12     |
| 6571040:62   | 179624:2       | 912262:14     |
| 6582560:62   | 586084:4       | 1219794:21    |
| 3295112:31   | 48672686:596   | 542600:8      |
| 876362:5     | 19463900:267   | 697628:12     |
| 5214060:97   | 4909680:61     | 15554394:201  |
| 17050486:230 | 2737968:39     | 9825148:143   |
| 1211450:16   | 36263962:545   | 11809662:167  |
| 794420:5     | 23365086:324   | 14048370:202  |
| 1855206:21   | 183338:2       | 3773442:51    |
| 469856:3     | 856444:5       | 344544:6      |
| 658396:4     | 2993226:44     | 167812:3      |
| 1867496:24   | 2172474:31     | 166992:14     |
| 14480910:140 | 19111904:240   | 604838:11     |
| 1236776:12   | 4377832:55     | 3052870:46    |
| 2149968:28   | 1043622:6      | 839584:13     |
| 305398:5     | 14619098:231   | 6073808:86    |
| 474320:7     | 231172:4       | 53408920:777  |
| 1560264:24   | 328648:3       | 242842:5      |
| 411600:7     | 169078:2       | 4202350:60    |
| 617388:12    | 8573916:494    | 366842:5      |
| 311110:6     | 111440774:1755 | 1840:1        |
| 1785610:25   | 6318592:90     | 1770970:21    |

|                         |                  |                          |
|-------------------------|------------------|--------------------------|
| 704902:10<br>5830140:88 | 1846:1<br>1840:0 | 1839096:21<br>1161968:16 |
|-------------------------|------------------|--------------------------|





**EK-5: JPG bayt tekniğiyle manipölasyon verileri**

|           |           |                |
|-----------|-----------|----------------|
| 11870:137 | 25765:275 | 3512640:26594  |
| 39851:338 | 30075:241 | 3574624:27080  |
| 24434:210 | 34927:316 | 2374696:18094  |
| 21038:184 | 36957:321 | 6672065:50486  |
| 41094:389 | 15897:195 | 6681621:50777  |
| 13788:124 | 18522:165 | 8518303:64889  |
| 11871:113 | 19352:163 | 9886250:74942  |
| 17933:154 | 18685:156 | 10608348:79822 |
| 38256:336 | 16454:136 | 10118733:76480 |
| 37141:316 | 16264:136 | 7928293:60577  |
| 30802:270 | 16133:143 | 8027241:61298  |
| 36411:307 | 34138:358 | 8233762:62631  |
| 30925:525 | 36941:302 | 8285917:63661  |
| 30775:242 | 18754:165 | 8303651:63062  |
| 31399:304 | 35878:309 | 8561182:64823  |
| 32900:765 | 28559:241 | 8472914:64359  |
| 32141:300 | 27768:211 | 8536550:65182  |
| 32601:308 | 27010:209 | 8344773:63434  |
| 24029:242 | 25750:210 | 8171774:62021  |
| 22780:325 | 18119:149 | 7316898:55822  |
| 22769:205 | 18530:152 | 6911501:52093  |
| 21635:175 | 19754:183 | 7674013:58345  |
| 23719:207 | 18631:163 | 7158315:54454  |
| 9437:320  | 22660:181 | 6191705:47154  |
| 32647:324 | 20769:171 | 6351528:48294  |
| 23652:193 | 19968:168 | 6167024:46644  |
| 34109:290 | 19829:180 | 6021296:45380  |
| 13606:119 | 18924:172 | 6211207:47170  |
| 12636:112 | 15668:130 | 6182690:47025  |
| 12156:114 | 33168:276 | 7587826:57549  |
| 28660:274 | 16737:138 | 7421364:55984  |
| 26669:206 | 18271:155 | 7627543:57445  |
| 27423:238 | 23212:193 | 7617402:56871  |
| 24634:208 | 23139:179 | 7640179:57205  |
| 27618:246 | 24312:196 | 7505200:57169  |
| 26939:222 | 23784:199 | 7375715:55728  |
| 26585:223 | 23296:190 | 7342319:55939  |
| 25976:211 | 27020:215 | 7249229:55128  |
| 26396:221 | 27330:222 | 6214522:47441  |
| 26099:212 | 36581:275 | 7037324:53747  |
| 27053:206 | 26440:198 | 1521751:11282  |
| 21219:192 | 36301:275 | 7399581:55929  |
| 21044:180 | 14748:111 | 7426147:56490  |
| 21333:186 | 22833:175 | 7118498:54202  |
| 22026:189 | 23090:183 | 7154857:53995  |
| 20145:155 | 21221:205 | 7217965:55150  |
| 20410:160 | 41885:340 | 5934738:44991  |
| 20317:175 | 21546:203 | 7398157:55500  |

|           |           |               |
|-----------|-----------|---------------|
| 21488:186 | 18737:155 | 7458398:55916 |
| 27400:257 | 18354:152 | 7192952:54646 |
| 27306:233 | 42875:340 | 6971640:52928 |
| 27263:247 | 56085:423 | 3487236:26675 |
| 28189:264 | 9405:77   | 3404895:27597 |
| 29501:274 | 55756:445 | 3366423:25100 |
| 28142:238 | 13467:116 | 3377868:25676 |
| 29994:258 | 16253:124 | 3434285:25431 |
| 28467:254 | 23741:191 | 3388339:25769 |
| 31490:298 | 16342:132 | 740292:5718   |
| 30580:256 | 17898:139 | 4346537:32821 |
| 30209:268 | 15603:120 | 4581491:34920 |
| 31804:290 | 16763:127 | 4407679:33251 |
| 29898:291 | 22962:176 | 3679182:28175 |
| 31500:261 | 23278:177 | 4369253:33979 |
| 31078:275 | 9365:73   | 4788722:38098 |
| 14155:138 | 8646:67   | 5260002:39780 |
| 16086:152 | 14929:115 | 5170436:39362 |
| 13856:115 | 25682:209 | 5787226:43864 |
| 44373:379 | 37073:328 | 5584165:42669 |
| 44730:409 | 37201:287 | 2057821:15533 |
| 41604:347 | 37628:334 | 2213201:17201 |
| 38303:310 | 37659:310 | 2268515:18137 |
| 38583:332 | 25671:220 | 2857051:21512 |
| 38109:309 | 25774:208 | 3190508:24994 |
| 38051:298 | 25259:203 | 3092439:23504 |
| 38267:351 | 25559:200 | 2012347:15796 |
| 39217:346 | 27071:214 | 1956484:14891 |
| 38354:296 | 27051:217 | 1759502:13785 |
| 37511:326 | 23966:200 | 1810770:13669 |
| 37563:326 | 20705:164 | 1812679:13731 |
| 38953:303 | 41825:331 | 1389856:10424 |
| 38912:346 | 41667:327 | 2562718:19446 |
| 39094:326 | 41430:332 | 6307876:49103 |
| 38785:343 | 31687:250 | 6193727:47837 |
| 38859:317 | 23884:196 | 6178972:48277 |
| 39548:342 | 14350:111 | 5460070:40996 |
| 39670:314 | 26989:204 | 5147369:39015 |
| 39800:345 | 22758:193 | 4812794:37214 |
| 38035:329 | 24091:226 | 2633108:20786 |
| 37872:313 | 23329:195 | 2716872:20950 |
| 37992:317 | 21019:166 | 5432866:42259 |
| 38149:325 | 18733:157 | 5469932:42534 |
| 38072:292 | 38547:322 | 5633128:43363 |
| 42810:337 | 34210:268 | 5667180:43315 |
| 56595:529 | 39158:314 | 6834136:51447 |
| 57019:455 | 21615:170 | 5416789:41937 |
| 56847:505 | 24144:195 | 5139115:40143 |
| 57044:468 | 41026:339 | 6694547:52174 |
| 57160:486 | 16640:132 | 6814632:51999 |

|               |               |               |
|---------------|---------------|---------------|
| 55991:451     | 27189:207     | 2032071:15588 |
| 25654:220     | 33425:250     | 2239423:17189 |
| 25819:222     | 38692:305     | 1991721:14996 |
| 25841:217     | 44985:362     | 2138857:16197 |
| 24359:185     | 39339:338     | 2275537:17544 |
| 22953:174     | 2702983:21106 | 2207758:17496 |
| 38746:324     | 5170732:46988 | 2347284:17999 |
| 40241:329     | 3275260:28160 | 5734561:44809 |
| 37755:324     | 5594925:47158 | 2235905:17273 |
| 21858:187     | 4431264:37104 | 2702525:20975 |
| 24066:217     | 3777977:30897 | 5067088:39936 |
| 24226:209     | 3757391:28562 | 5245301:41108 |
| 24411:200     | 3360223:25519 | 5262374:41265 |
| 24457:193     | 3717218:29318 | 5143972:39764 |
| 24495:210     | 4478902:34925 | 5004325:37947 |
| 24574:233     | 3753793:28714 | 5756942:44568 |
| 27999:243     | 3494227:26697 | 4857261:38226 |
| 27599:212     | 3746057:28247 | 5135777:39497 |
| 27286:223     | 3791503:29597 | 5098548:39121 |
| 24280:207     | 3727005:28128 | 5108451:38472 |
| 24381:210     | 3297405:25910 | 7702962:66091 |
| 24577:200     | 3497370:26604 | 6771477:59752 |
| 26111:195     | 4831960:36760 | 6404666:60644 |
| 26160:203     | 3628427:27526 | 4273691:43011 |
| 12197:107     | 3400380:25719 | 2935115:25980 |
| 15990:136     | 3273966:24906 | 4255913:39096 |
| 14374:121     | 3485995:26456 | 4011917:37679 |
| 12921:109     | 3501872:26666 | 6584872:63719 |
| 13188:115     | 3481965:28219 | 5479761:48088 |
| 15892:155     | 3506703:27990 | 2333255:19730 |
| 15169:125     | 2481793:18487 | 2362487:20650 |
| 16381:131     | 2040567:15609 | 4004829:35994 |
| 30515:305     | 2057904:15533 | 3978579:34428 |
| 28789:251     | 1984935:15160 | 4686460:38899 |
| 15772:130     | 2151420:16438 | 6908788:57967 |
| 17506:195     | 2744332:21029 | 7444396:64494 |
| 17679:149     | 2754876:20669 | 7983776:69036 |
| 39703:342     | 2726159:20421 | 7854404:67072 |
| 33646:289     | 3362788:25220 | 7771865:63787 |
| 35937:293     | 3357898:25406 | 3258867:26622 |
| 6539:84       | 3337696:25681 | 3261017:26823 |
| 28690:254     | 3367735:25962 | 3144680:28003 |
| 23398:202     | 3513685:26878 | 3161811:27464 |
| 16617:145     | 3510579:26716 | 5449952:49342 |
| 33635:265     | 138375:1155   | 105510:811    |
| 16081:127     | 139523:1159   | 306129:2391   |
| 7880270:66342 | 112405:1000   | 258666:2026   |
| 9225209:78148 | 128088:1154   | 159502:1302   |
| 9343705:76485 | 110264:954    | 225165:1834   |
| 2745028:23770 | 270649:2310   | 307315:2684   |

|               |             |             |
|---------------|-------------|-------------|
| 2785678:23471 | 115726:941  | 112237:989  |
| 2931397:24199 | 127738:1007 | 161148:1382 |
| 2566658:20733 | 139162:1093 | 191944:1616 |
| 5729901:45389 | 249496:1952 | 199557:1636 |
| 6425519:54970 | 262893:2033 | 181120:1458 |
| 6048163:50243 | 162386:1255 | 68097:556   |
| 6703175:54429 | 221564:1695 | 448438:3812 |
| 6067661:47818 | 100277:768  | 398539:3417 |
| 2037533:16043 | 99538:801   | 147616:1247 |
| 1777491:13756 | 189295:1453 | 117583:1006 |
| 6095961:50127 | 122267:982  | 139785:1268 |
| 5502309:45720 | 93115:725   | 73750:662   |
| 3165239:26260 | 165330:1289 | 64334:538   |
| 3409341:27540 | 190586:1517 | 56119:486   |
| 3362486:26873 | 128878:1017 | 122066:1139 |
| 3084053:25284 | 97720:826   | 92960:797   |
| 3121944:25778 | 131115:1086 | 83837:698   |
| 3096026:25853 | 112237:928  | 86130:706   |
| 1487365:11768 | 113222:921  | 72500:595   |
| 3886900:31815 | 251641:1944 | 102824:838  |
| 3936247:32897 | 240090:1858 | 76092:673   |
| 2460449:20487 | 239463:1886 | 150733:1238 |
| 4543521:37990 | 254753:2055 | 106703:865  |
| 98822:839     | 325624:2806 | 84182:713   |
| 113837:924    | 403171:3313 | 124145:1003 |
| 103476:862    | 410119:3323 | 80061:644   |
| 51808:462     | 368099:2900 | 190163:1619 |
| 164190:1328   | 281468:2302 | 244448:2197 |
| 89956:704     | 292513:2300 | 143406:1215 |
| 238515:1949   | 188153:1527 | 162400:1297 |
| 185166:1542   | 288437:2384 | 244621:2186 |
| 166146:1339   | 281365:2339 | 225707:1962 |
| 74784:604     | 164377:1305 | 243703:2292 |
| 181174:1405   | 182033:1459 | 214272:1776 |
| 151257:1211   | 195993:1560 | 217352:1717 |
| 270506:2279   | 108062:835  | 223054:1734 |
| 164652:1379   | 86158:688   | 220187:1702 |
| 159528:1324   | 87396:725   | 219526:1701 |
| 160863:1355   | 111453:897  | 248777:1989 |
| 384549:2992   | 118002:992  | 315075:2551 |
| 371952:2907   | 209300:1924 | 141095:1121 |
| 354927:2845   | 127844:1064 | 249105:2115 |
| 191823:1504   | 212768:1781 | 148987:1240 |
| 164854:1303   | 210862:1732 | 185949:1481 |
| 356865:2804   | 120922:947  | 238862:2055 |
| 192507:1488   | 268640:2315 | 244637:2064 |
| 313375:2536   | 120410:1007 | 164026:1321 |
| 183593:1591   | 231007:1854 | 245083:2274 |
| 126141:1015   | 253950:2006 |             |
| 240088:2011   | 128564:1034 |             |

|             |             |  |
|-------------|-------------|--|
| 254646:2115 | 259875:2079 |  |
|-------------|-------------|--|





**EK-6: JPG ara bellek tekniğiyle manipölasyon verileri**

|         |         |              |
|---------|---------|--------------|
| 11870:5 | 26440:1 | 6694547:125  |
| 39851:8 | 36301:2 | 6814632:130  |
| 24434:4 | 14748:0 | 2032071:40   |
| 21038:3 | 22833:0 | 2239423:40   |
| 41094:5 | 23090:1 | 1991721:39   |
| 13788:3 | 21221:1 | 2138857:52   |
| 11871:2 | 41885:2 | 2275537:63   |
| 17933:3 | 21546:1 | 2207758:56   |
| 38256:3 | 18737:1 | 2347284:48   |
| 37141:3 | 18354:1 | 5734561:114  |
| 30802:3 | 42875:1 | 2235905:42   |
| 36411:4 | 56085:1 | 2702525:51   |
| 30925:3 | 9405:0  | 5067088:104  |
| 30775:3 | 55756:2 | 5245301:100  |
| 31399:3 | 13467:3 | 5262374:106  |
| 32900:3 | 16253:1 | 5143972:138  |
| 32141:3 | 23741:1 | 5004325:100  |
| 32601:2 | 16342:1 | 5756942:114  |
| 24029:2 | 17898:1 | 4857261:96   |
| 22780:1 | 15603:0 | 5135777:105  |
| 22769:2 | 16763:0 | 5098548:101  |
| 21635:1 | 22962:1 | 5108451:103  |
| 23719:2 | 23278:1 | 7702962:149  |
| 9437:1  | 9365:0  | 6771477:149  |
| 32647:2 | 8646:1  | 6404666:138  |
| 23652:1 | 14929:0 | 4273691:90   |
| 34109:2 | 25682:1 | 2935115:59   |
| 13606:1 | 37073:2 | 4255913:91   |
| 12636:1 | 37201:1 | 4011917:78   |
| 12156:1 | 37628:1 | 6584872:122  |
| 28660:2 | 37659:1 | 5479761:99   |
| 26669:1 | 25671:1 | 2333255:41   |
| 27423:1 | 25774:1 | 2362487:43   |
| 24634:4 | 25259:1 | 4004829:71   |
| 27618:1 | 25559:1 | 3978579:73   |
| 26939:1 | 27071:1 | 4686460:85   |
| 26585:1 | 27051:1 | 6908788:126  |
| 25976:1 | 23966:0 | 7444396:133  |
| 26396:1 | 20705:0 | 7983776:1151 |
| 26099:0 | 41825:1 | 7854404:3634 |
| 27053:1 | 41667:1 | 7771865:1869 |
| 21219:1 | 41430:1 | 3258867:420  |
| 21044:1 | 31687:0 | 3261017:472  |
| 21333:1 | 23884:0 | 3144680:387  |
| 22026:1 | 14350:1 | 3161811:338  |
| 20145:1 | 26989:1 | 5449952:161  |
| 20410:1 | 22758:0 | 7880270:172  |
| 20317:1 | 24091:0 | 9225209:514  |

|         |             |             |
|---------|-------------|-------------|
| 21488:1 | 23329:1     | 9343705:287 |
| 27400:2 | 21019:1     | 2745028:113 |
| 27306:1 | 18733:0     | 2785678:109 |
| 27263:1 | 38547:2     | 2931397:108 |
| 28189:1 | 34210:1     | 2566658:52  |
| 29501:1 | 39158:2     | 5729901:226 |
| 28142:1 | 21615:0     | 6425519:179 |
| 29994:2 | 24144:0     | 6048163:287 |
| 28467:1 | 41026:1     | 6703175:202 |
| 31490:1 | 16640:0     | 6067661:234 |
| 30580:2 | 27189:1     | 2037533:39  |
| 30209:1 | 33425:1     | 1777491:97  |
| 31804:2 | 38692:1     | 6095961:232 |
| 29898:2 | 44985:2     | 5502309:171 |
| 31500:2 | 39339:1     | 3165239:129 |
| 31078:1 | 2702983:53  | 3409341:140 |
| 14155:1 | 5170732:110 | 3362486:124 |
| 16086:1 | 3275260:63  | 3084053:70  |
| 13856:1 | 5594925:108 | 3121944:110 |
| 44373:2 | 4431264:91  | 3096026:181 |
| 44730:1 | 3777977:89  | 1487365:31  |
| 41604:1 | 3757391:78  | 3886900:143 |
| 38303:2 | 3360223:75  | 3936247:123 |
| 38583:3 | 3717218:92  | 2460449:102 |
| 38109:2 | 4478902:118 | 4543521:134 |
| 38051:2 | 3753793:100 | 98822:3     |
| 38267:1 | 3494227:72  | 113837:4    |
| 39217:1 | 3746057:81  | 103476:2    |
| 38354:2 | 3791503:74  | 51808:1     |
| 37511:1 | 3727005:75  | 164190:4    |
| 37563:1 | 3297405:65  | 89956:2     |
| 38953:2 | 3497370:95  | 238515:4    |
| 38912:1 | 4831960:90  | 185166:3    |
| 39094:2 | 3628427:65  | 166146:4    |
| 38785:1 | 3400380:61  | 74784:1     |
| 38859:3 | 3273966:58  | 181174:3    |
| 39548:2 | 3485995:63  | 151257:3    |
| 39670:1 | 3501872:62  | 270506:6    |
| 39800:1 | 3481965:68  | 164652:3    |
| 38035:2 | 3506703:67  | 159528:3    |
| 37872:1 | 2481793:49  | 160863:3    |
| 37992:1 | 2040567:41  | 384549:7    |
| 38149:1 | 2057904:41  | 371952:7    |
| 38072:0 | 1984935:37  | 354927:57   |
| 42810:1 | 2151420:40  | 191823:5    |
| 56595:1 | 2744332:48  | 164854:4    |
| 57019:2 | 2754876:50  | 356865:9    |
| 56847:1 | 2726159:53  | 192507:4    |
| 57044:2 | 3362788:60  | 313375:8    |
| 57160:1 | 3357898:61  | 183593:3    |

|         |              |           |
|---------|--------------|-----------|
| 55991:1 | 3337696:59   | 126141:2  |
| 25654:1 | 3367735:61   | 240088:5  |
| 25819:1 | 3513685:70   | 254646:5  |
| 25841:1 | 3510579:68   | 138375:3  |
| 24359:1 | 3512640:64   | 139523:3  |
| 22953:0 | 3574624:66   | 112405:3  |
| 38746:2 | 2374696:42   | 128088:65 |
| 40241:1 | 6672065:124  | 110264:4  |
| 37755:1 | 6681621:124  | 270649:7  |
| 21858:1 | 8518303:162  | 115726:3  |
| 24066:0 | 9886250:190  | 127738:3  |
| 24226:0 | 10608348:197 | 139162:4  |
| 24411:1 | 10118733:183 | 249496:6  |
| 24457:1 | 7928293:145  | 262893:6  |
| 24495:1 | 8027241:153  | 162386:4  |
| 24574:1 | 8233762:165  | 221564:4  |
| 27999:1 | 8285917:164  | 100277:2  |
| 27599:0 | 8303651:170  | 99538:2   |
| 27286:1 | 8561182:165  | 189295:5  |
| 24280:1 | 8472914:159  | 122267:2  |
| 24381:2 | 8536550:169  | 93115:2   |
| 24577:1 | 8344773:162  | 165330:4  |
| 26111:1 | 8171774:158  | 190586:3  |
| 26160:1 | 7316898:143  | 128878:2  |
| 12197:1 | 6911501:135  | 97720:3   |
| 15990:1 | 7674013:155  | 131115:3  |
| 14374:1 | 7158315:141  | 112237:3  |
| 12921:1 | 6191705:121  | 113222:2  |
| 13188:1 | 6351528:123  | 251641:5  |
| 15892:2 | 6167024:116  | 240090:5  |
| 15169:1 | 6021296:113  | 239463:6  |
| 16381:1 | 6211207:119  | 254753:5  |
| 30515:1 | 6182690:117  | 325624:8  |
| 28789:1 | 7587826:148  | 403171:32 |
| 15772:1 | 7421364:140  | 410119:12 |
| 17506:1 | 7627543:171  | 368099:10 |
| 17679:1 | 7617402:156  | 281468:7  |
| 39703:1 | 7640179:158  | 292513:6  |
| 33646:1 | 7505200:157  | 188153:4  |
| 35937:1 | 7375715:142  | 288437:7  |
| 6539:1  | 7342319:148  | 281365:5  |
| 28690:1 | 7249229:149  | 164377:3  |
| 23398:1 | 6214522:121  | 182033:4  |
| 16617:1 | 7037324:146  | 195993:4  |
| 33635:1 | 1521751:29   | 108062:64 |
| 16081:1 | 7399581:170  | 86158:2   |
| 25765:1 | 7426147:148  | 87396:2   |
| 30075:1 | 7118498:141  | 111453:3  |
| 34927:2 | 7154857:150  | 118002:3  |
| 36957:1 | 7217965:146  | 209300:5  |

|          |             |           |
|----------|-------------|-----------|
| 15897:0  | 5934738:121 | 127844:3  |
| 18522:0  | 7398157:157 | 212768:5  |
| 19352:1  | 7458398:190 | 210862:6  |
| 18685:1  | 7192952:140 | 120922:3  |
| 16454:1  | 6971640:149 | 268640:6  |
| 16264:1  | 3487236:70  | 120410:4  |
| 16133:1  | 3404895:73  | 231007:6  |
| 34138:1  | 3366423:71  | 253950:7  |
| 36941:2  | 3377868:70  | 128564:3  |
| 18754:1  | 3434285:70  | 259875:7  |
| 35878:1  | 3388339:70  | 315075:6  |
| 28559:1  | 740292:15   | 141095:3  |
| 27768:2  | 4346537:88  | 249105:5  |
| 27010:1  | 4581491:95  | 148987:3  |
| 25750:1  | 4407679:102 | 185949:73 |
| 18119:1  | 3679182:99  | 238862:7  |
| 18530:1  | 4369253:98  | 244637:6  |
| 19754:1  | 4788722:98  | 164026:4  |
| 18631:1  | 5260002:104 | 245083:5  |
| 22660:1  | 5170436:101 | 190163:5  |
| 20769:2  | 5787226:128 | 244448:6  |
| 19968:1  | 5584165:114 | 143406:3  |
| 19829:1  | 2057821:38  | 162400:4  |
| 18924:1  | 2213201:40  | 244621:5  |
| 15668:1  | 2268515:41  | 225707:6  |
| 33168:2  | 2857051:53  | 243703:5  |
| 16737:1  | 3190508:61  | 214272:5  |
| 18271:1  | 3092439:60  | 217352:6  |
| 23212:1  | 2012347:37  | 223054:6  |
| 23139:1  | 1956484:34  | 220187:4  |
| 24312:1  | 1759502:32  | 219526:4  |
| 23784:1  | 1810770:59  | 248777:99 |
| 23296:2  | 1812679:44  | 105510:3  |
| 27020:1  | 1389856:37  | 306129:7  |
| 27330:1  | 2562718:60  | 258666:5  |
| 36581:1  | 6307876:138 | 159502:4  |
| 86130:2  | 6193727:133 | 225165:5  |
| 72500:4  | 6178972:121 | 307315:7  |
| 102824:3 | 5460070:110 | 112237:3  |
| 76092:3  | 5147369:100 | 161148:4  |
| 150733:4 | 4812794:91  | 191944:4  |
| 106703:3 | 2633108:55  | 199557:5  |
| 84182:2  | 2716872:54  | 181120:4  |
| 124145:4 | 5432866:108 | 68097:2   |
| 80061:2  | 5469932:125 | 448438:10 |
| 64334:1  | 5633128:214 | 398539:85 |
| 56119:1  | 5667180:115 | 147616:5  |
| 122066:4 | 6834136:189 | 117583:3  |
| 92960:2  | 5416789:101 | 139785:4  |

**EK-7: JPG bayt tekniği tersine manipölasyon verileri**

|           |                |               |
|-----------|----------------|---------------|
| 23744:307 | 43234:212      | 6168110:22183 |
| 79706:382 | 48292:192      | 6243892:22830 |
| 48872:192 | 82056:326      | 6192056:22603 |
| 42080:174 | 33284:141      | 2974734:10757 |
| 82192:315 | 54382:255      | 7773804:28490 |
| 27580:114 | 66854:270      | 7872498:28025 |
| 23746:89  | 77388:350      | 4920902:17487 |
| 35870:137 | 89974:370      | 9087046:33128 |
| 76516:311 | 78682:319      | 197648:729    |
| 74286:291 | 5405970:21128  | 227678:884    |
| 61608:237 | 10341468:41124 | 206956:747    |
| 72826:274 | 6550524:25327  | 103620:438    |
| 61854:240 | 11189854:44516 | 328384:1246   |
| 61554:241 | 8862532:35325  | 179916:667    |
| 62802:246 | 7555958:30359  | 477034:1826   |
| 65804:251 | 7514786:28921  | 370336:1338   |
| 64286:257 | 6720450:25917  | 332296:1199   |
| 65206:274 | 7434440:28941  | 149572:539    |
| 48062:195 | 8957808:34811  | 362352:1307   |
| 45564:178 | 7507590:29845  | 302518:1089   |
| 45542:183 | 6988458:26838  | 541016:1952   |
| 43274:178 | 7492118:29556  | 329308:1187   |
| 47442:178 | 7583010:29667  | 319060:1153   |
| 18878:74  | 7454014:29228  | 321730:1175   |
| 65298:253 | 6594814:25929  | 769102:2767   |
| 47308:213 | 6994744:27579  | 743908:2682   |
| 68222:309 | 9663924:38505  | 709858:2564   |
| 27216:133 | 7256858:27287  | 383650:1382   |
| 25276:111 | 6800764:27493  | 329712:1211   |
| 24316:104 | 6547936:24484  | 713734:2596   |
| 57324:236 | 6971994:25965  | 385018:1391   |
| 53342:209 | 7003748:26635  | 626754:2320   |
| 54850:228 | 6963934:25085  | 367190:1363   |
| 49272:194 | 7013410:28465  | 252286:975    |
| 55240:223 | 4963590:17800  | 480180:1810   |
| 53882:212 | 4081138:14144  | 509296:1835   |
| 53174:215 | 4115812:14236  | 276754:1030   |
| 51956:206 | 3969874:13995  | 279050:1004   |
| 52796:200 | 4302844:15219  | 224814:820    |
| 52202:205 | 5488668:21004  | 256180:937    |
| 54110:205 | 5509756:20235  | 220532:795    |
| 42442:176 | 5452322:19589  | 541302:1946   |
| 42092:187 | 6725580:25239  | 231456:822    |
| 42670:168 | 6715800:25997  | 255480:928    |
| 44056:166 | 6675396:25002  | 278328:1021   |
| 40294:165 | 6735474:26299  | 498996:1783   |
| 40824:163 | 7027374:29147  | 525790:1910   |
| 40638:154 | 7021162:28917  | 324776:1161   |

|            |                |             |
|------------|----------------|-------------|
| 42980:167  | 7025284:25801  | 443132:1595 |
| 54804:210  | 7149252:28251  | 200558:717  |
| 54616:209  | 4749396:18240  | 199080:720  |
| 54530:209  | 13344134:51709 | 378594:1361 |
| 56382:214  | 13363246:53010 | 244538:872  |
| 59006:230  | 17036610:65821 | 186234:677  |
| 56288:217  | 19772504:81216 | 330664:1189 |
| 59992:235  | 21216700:85932 | 381176:1361 |
| 56938:217  | 20237470:84902 | 257760:925  |
| 62984:251  | 15856590:59331 | 195444:706  |
| 61164:253  | 16054486:56762 | 262234:934  |
| 60422:246  | 16467528:58874 | 224478:817  |
| 63612:258  | 16571838:58788 | 226448:811  |
| 59800:233  | 16607306:59314 | 503286:1899 |
| 63004:233  | 17122368:65260 | 480184:1808 |
| 62160:239  | 16945832:63305 | 478930:1859 |
| 28314:115  | 17073104:71918 | 509510:1830 |
| 32176:132  | 16689550:66926 | 651252:2340 |
| 27716:114  | 16343552:58624 | 806346:2891 |
| 88750:343  | 14633800:51552 | 820242:2954 |
| 89464:350  | 13823006:48518 | 736202:2650 |
| 83212:309  | 15348030:54497 | 562940:2048 |
| 76610:313  | 14316634:52530 | 585030:2099 |
| 77170:285  | 12383414:44028 | 376310:1360 |
| 76222:322  | 12703060:44333 | 576878:2109 |
| 76106:364  | 12334052:43470 | 562734:2025 |
| 76538:319  | 12042596:42868 | 328758:1171 |
| 78438:324  | 12422418:43856 | 364070:1325 |
| 76712:325  | 12365384:44248 | 391990:1416 |
| 75026:281  | 15175656:56965 | 216128:839  |
| 75130:355  | 14842732:55462 | 172320:681  |
| 77910:304  | 15255090:55256 | 174796:680  |
| 77828:350  | 15234808:55182 | 222910:840  |
| 78192:300  | 15280362:55355 | 236008:898  |
| 77574:312  | 15010404:52645 | 418604:1555 |
| 77722:337  | 14751434:55206 | 255692:917  |
| 79100:308  | 14684642:60151 | 425540:1542 |
| 79344:333  | 14498462:56902 | 421728:1522 |
| 79604:334  | 12429048:46054 | 241848:872  |
| 76074:297  | 14074652:50342 | 537284:1940 |
| 75748:283  | 3043506:10736  | 240824:851  |
| 75988:301  | 14799166:52625 | 462018:1700 |
| 76302:321  | 14852298:54294 | 507904:1823 |
| 76148:322  | 14237000:51692 | 257132:921  |
| 85624:389  | 14309718:57475 | 519754:1874 |
| 113194:773 | 14435934:59977 | 630154:2260 |
| 114042:460 | 11869480:48869 | 282194:1098 |
| 113698:467 | 14796318:53436 | 498214:2064 |
| 114092:438 | 14916800:53914 | 297978:1317 |
| 114324:455 | 14385908:52287 | 371902:1467 |

|            |                |             |
|------------|----------------|-------------|
| 111986:450 | 13943284:50480 | 477728:1963 |
| 51312:206  | 6974476:25533  | 489278:2071 |
| 51642:221  | 6809794:26153  | 328056:1246 |
| 51686:207  | 6732850:24253  | 490170:1781 |
| 48722:186  | 6755740:24943  | 380330:1408 |
| 45910:171  | 6868574:24874  | 488900:1881 |
| 77496:307  | 6776682:24996  | 286816:1111 |
| 80486:301  | 1480588:5390   | 324804:1214 |
| 75514:311  | 8693078:31556  | 489246:1796 |
| 43720:172  | 9162986:33648  | 451418:1625 |
| 48136:189  | 8815362:31823  | 487410:1764 |
| 48456:178  | 7358368:27776  | 428548:1571 |
| 48826:191  | 8738510:34521  | 434708:1563 |
| 48918:244  | 9577448:38578  | 446112:1640 |
| 48994:184  | 10520008:38463 | 440378:1592 |
| 49152:191  | 10340876:38853 | 439056:1578 |
| 56002:210  | 11574456:44594 | 497558:1763 |
| 55202:222  | 11168334:42997 | 211024:734  |
| 54576:218  | 4115646:14631  | 612262:2150 |
| 48564:187  | 4426406:16432  | 517336:1894 |
| 48766:197  | 4537034:16137  | 319008:1139 |
| 49158:186  | 5714106:20378  | 450334:1570 |
| 52226:198  | 6381020:23490  | 614634:2152 |
| 52324:206  | 6184882:23291  | 224478:776  |
| 24398:109  | 4024698:14910  | 322300:1209 |
| 31984:138  | 3912972:14638  | 383892:1450 |
| 28752:130  | 3519008:13368  | 399118:1502 |
| 25846:101  | 3621544:14074  | 362244:1381 |
| 26380:112  | 3625362:13764  | 136198:496  |
| 31788:123  | 2779716:12356  | 896880:3264 |
| 30342:152  | 5125440:21257  | 797082:2898 |
| 32766:125  | 12615756:49616 | 295236:1085 |
| 61034:233  | 12387458:46904 | 235170:845  |
| 57582:226  | 12357948:44434 | 279574:1002 |
| 31548:125  | 10920144:38914 | 147504:537  |
| 35016:134  | 10294742:37083 | 128672:469  |
| 35362:147  | 9625592:34828  | 112242:427  |
| 79410:309  | 5266220:19873  | 244136:894  |
| 67296:258  | 5433748:19519  | 185924:669  |
| 71878:269  | 10865736:39178 | 167678:600  |
| 13082:50   | 10939868:40113 | 172264:620  |
| 57384:212  | 11266260:40982 | 145004:534  |
| 46800:178  | 11334364:40981 | 205652:725  |
| 33238:132  | 13668276:49877 | 152188:550  |
| 67274:268  | 10833582:39171 | 301470:1103 |
| 32166:123  | 10278234:36420 | 213410:763  |
| 51534:206  | 13389098:50154 | 168368:636  |
| 60154:226  | 13629268:49502 | 248294:906  |
| 69858:256  | 4064146:14348  | 160126:597  |
| 32270:126  | 4478850:15978  | 46560:178   |

|            |                |               |
|------------|----------------|---------------|
| 68280:268  | 3983446:14427  | 18734:74      |
| 73886:264  | 4277718:15813  | 17296:67      |
| 37512:137  | 4471814:16133  | 75260:325     |
| 71760:284  | 5405054:19761  | 75322:303     |
| 57122:218  | 10134180:36691 | 51346:192     |
| 55540:220  | 10490606:38299 | 51552:196     |
| 54024:200  | 10524752:38315 | 50522:211     |
| 51504:199  | 10287948:37691 | 51122:250     |
| 36242:138  | 10008654:36275 | 54146:221     |
| 37064:140  | 11513888:42041 | 54106:207     |
| 39512:144  | 9714526:35450  | 47936:178     |
| 37266:141  | 10271558:37386 | 41414:156     |
| 45324:179  | 10197100:37069 | 83654:319     |
| 41542:153  | 10216906:36062 | 83338:374     |
| 39940:155  | 15405928:55263 | 82864:312     |
| 39662:156  | 13542958:48942 | 63378:259     |
| 37852:142  | 12809336:46517 | 47772:191     |
| 31340:121  | 8547386:30798  | 28704:124     |
| 66340:252  | 5870234:20999  | 53982:207     |
| 33478:126  | 8511830:31266  | 45520:176     |
| 36546:137  | 8023838:28703  | 48186:187     |
| 46428:169  | 13169748:48183 | 46662:187     |
| 46282:171  | 10959526:39731 | 42042:181     |
| 48628:180  | 4666514:17184  | 37470:160     |
| 47572:178  | 4724978:17029  | 77098:307     |
| 46596:173  | 8009662:29035  | 68424:267     |
| 54044:201  | 7957162:28457  | 78320:327     |
| 54664:201  | 9372924:34047  | 6330482:22950 |
| 73166:274  | 13817580:50104 | 6818686:25041 |
| 52884:235  | 14888796:54173 | 6724976:24560 |
| 72606:310  | 15967556:58274 | 29862:185     |
| 29500:121  | 15708812:57290 | 51368:236     |
| 45670:177  | 15543734:56510 | 74150:298     |
| 46184:180  | 6517738:23801  | 74406:282     |
| 42446:172  | 6522038:23737  | 4551078:16510 |
| 83774:347  | 6289364:22773  | 4415520:15909 |
| 43096:181  | 6323626:22859  | 4694572:16968 |
| 37478:139  | 10899908:39719 | 73918:276     |
| 36712:147  | 15760544:57620 | 31798:115     |
| 85754:313  | 18450422:66074 | 37048:144     |
| 112174:421 | 18687414:68229 | 38708:193     |
| 18814:85   | 5490060:20223  | 37374:167     |
| 111516:429 | 5571360:20105  | 32912:136     |
| 26938:97   | 5862798:21448  | 32532:134     |
| 32510:128  | 5133320:18529  |               |
| 47486:220  | 11459806:41753 |               |
| 32688:135  | 12851042:46512 |               |
| 35800:138  | 12096330:43959 |               |
| 31210:120  | 13406354:47791 |               |
| 33530:125  | 12135326:43818 |               |

|                |                |  |
|----------------|----------------|--|
| 45928:166      | 4075070:14992  |  |
| 11004622:40373 | 3554986:12899  |  |
| 11469126:41926 | 12191926:44271 |  |





**EK-8: JPG ara bellek tekniği tersine manipölasyon verileri**

|          |          |              |
|----------|----------|--------------|
| 23744:61 | 31340:1  | 4115646:46   |
| 79706:5  | 66340:1  | 4426406:55   |
| 48872:4  | 33478:1  | 4537034:54   |
| 42080:2  | 36546:1  | 5714106:68   |
| 82192:3  | 46428:1  | 6381020:78   |
| 27580:1  | 46282:2  | 6184882:70   |
| 23746:1  | 48628:1  | 4024698:46   |
| 35870:2  | 47572:2  | 3912972:45   |
| 76516:4  | 46596:1  | 3519008:41   |
| 74286:2  | 54044:1  | 3621544:44   |
| 61608:2  | 54664:2  | 3625362:43   |
| 72826:2  | 73166:2  | 2779716:28   |
| 61854:2  | 52884:1  | 5125440:163  |
| 61554:2  | 72606:1  | 12615756:166 |
| 62802:3  | 29500:1  | 12387458:135 |
| 65804:2  | 45670:2  | 12357948:137 |
| 64286:2  | 46184:1  | 10920144:123 |
| 65206:2  | 42446:1  | 10294742:116 |
| 48062:2  | 83774:1  | 9625592:110  |
| 45564:1  | 43096:3  | 5266220:63   |
| 45542:1  | 37478:2  | 5433748:62   |
| 43274:2  | 36712:1  | 10865736:122 |
| 47442:1  | 85754:1  | 10939868:124 |
| 18878:3  | 112174:6 | 11266260:226 |
| 65298:1  | 18814:0  | 11334364:197 |
| 47308:1  | 111516:1 | 13668276:178 |
| 68222:2  | 26938:1  | 10833582:147 |
| 27216:1  | 32510:1  | 10278234:140 |
| 25276:1  | 47486:1  | 13389098:174 |
| 24316:1  | 32688:1  | 13629268:151 |
| 57324:1  | 35800:0  | 4064146:37   |
| 53342:2  | 31210:1  | 4478850:50   |
| 54850:2  | 33530:1  | 3983446:38   |
| 49272:5  | 45928:1  | 4277718:49   |
| 55240:1  | 46560:1  | 4551078:51   |
| 53882:2  | 18734:1  | 4415520:7636 |
| 53174:1  | 17296:0  | 4694572:1090 |
| 51956:1  | 29862:1  | 11469126:135 |
| 52796:1  | 51368:1  | 4471814:55   |
| 52202:2  | 74150:1  | 5405054:56   |
| 54110:1  | 74406:1  | 10134180:114 |
| 42442:1  | 75260:2  | 10490606:233 |
| 42092:2  | 75322:1  | 10524752:140 |
| 42670:1  | 51346:1  | 10287948:145 |
| 44056:2  | 51552:1  | 10008654:144 |
| 40294:1  | 50522:2  | 11513888:149 |
| 40824:1  | 51122:1  | 9714526:115  |
| 40638:1  | 54146:1  | 10271558:114 |

|          |              |              |
|----------|--------------|--------------|
| 42980:1  | 54106:1      | 10197100:107 |
| 54804:1  | 47936:1      | 10216906:114 |
| 54616:1  | 41414:1      | 15405928:298 |
| 54530:1  | 83654:2      | 13542958:233 |
| 56382:1  | 83338:1      | 12809336:184 |
| 59006:1  | 82864:1      | 8547386:108  |
| 56288:1  | 63378:1      | 5870234:70   |
| 59992:1  | 47772:1      | 8511830:106  |
| 56938:1  | 28704:0      | 8023838:94   |
| 62984:1  | 53982:1      | 13169748:163 |
| 61164:1  | 45520:1      | 10959526:128 |
| 60422:1  | 48186:2      | 4666514:54   |
| 63612:1  | 46662:1      | 4724978:55   |
| 59800:0  | 42042:1      | 8009662:205  |
| 63004:1  | 37470:2      | 7957162:93   |
| 62160:2  | 77098:1      | 9372924:105  |
| 28314:1  | 68424:2      | 13817580:151 |
| 32176:1  | 78320:1      | 14888796:278 |
| 27716:1  | 43234:1      | 15967556:288 |
| 88750:1  | 48292:2      | 15708812:188 |
| 89464:2  | 82056:1      | 15543734:334 |
| 83212:1  | 33284:1      | 6517738:67   |
| 76610:2  | 54382:1      | 6522038:75   |
| 77170:3  | 66854:1      | 6289364:70   |
| 76222:2  | 77388:1      | 6323626:77   |
| 76106:2  | 89974:1      | 10899908:131 |
| 76538:2  | 78682:1      | 15760544:192 |
| 78438:3  | 5405970:60   | 18450422:231 |
| 76712:2  | 10341468:123 | 18687414:229 |
| 75026:1  | 6550524:66   | 5490060:150  |
| 75130:1  | 11189854:112 | 5571360:7296 |
| 77910:2  | 8862532:93   | 5862798:445  |
| 77828:2  | 7555958:79   | 5133320:57   |
| 78192:2  | 7514786:92   | 11459806:138 |
| 77574:5  | 6720450:84   | 12851042:145 |
| 77722:1  | 7434440:85   | 12096330:111 |
| 79100:1  | 8957808:98   | 13406354:151 |
| 79344:1  | 7507590:85   | 12135326:140 |
| 79604:1  | 6988458:73   | 4075070:45   |
| 76074:1  | 7492118:78   | 3554986:42   |
| 75748:1  | 7583010:89   | 12191926:147 |
| 75988:1  | 7454014:87   | 11004622:556 |
| 76302:1  | 6594814:84   | 6330482:81   |
| 76148:2  | 6994744:104  | 6818686:83   |
| 85624:1  | 9663924:130  | 6724976:85   |
| 113194:1 | 7256858:94   | 6168110:72   |
| 114042:2 | 6800764:84   | 6243892:72   |
| 113698:2 | 6547936:74   | 6192056:73   |
| 114092:1 | 6971994:80   | 2974734:30   |
| 114324:2 | 7003748:80   | 7773804:95   |

|          |              |            |
|----------|--------------|------------|
| 111986:1 | 6963934:79   | 7872498:92 |
| 51312:1  | 7013410:74   | 4920902:57 |
| 51642:1  | 4963590:53   | 9087046:94 |
| 51686:1  | 4081138:45   | 197648:1   |
| 48722:1  | 4115812:43   | 227678:2   |
| 45910:1  | 3969874:41   | 206956:2   |
| 77496:1  | 4302844:49   | 103620:1   |
| 80486:1  | 5488668:67   | 328384:2   |
| 75514:1  | 5509756:64   | 179916:1   |
| 43720:2  | 5452322:72   | 477034:4   |
| 48136:1  | 6725580:88   | 370336:3   |
| 48456:1  | 6715800:5888 | 332296:2   |
| 48826:1  | 6675396:440  | 149572:1   |
| 48918:1  | 6735474:862  | 362352:3   |
| 48994:0  | 7027374:69   | 302518:2   |
| 49152:1  | 7021162:67   | 541016:3   |
| 56002:1  | 7025284:65   | 329308:2   |
| 55202:1  | 7149252:64   | 319060:2   |
| 54576:1  | 4749396:45   | 321730:2   |
| 48564:1  | 13344134:119 | 769102:6   |
| 48766:1  | 13363246:168 | 743908:5   |
| 49158:1  | 17036610:193 | 709858:5   |
| 52226:1  | 19772504:192 | 383650:4   |
| 52324:1  | 21216700:282 | 329712:2   |
| 24398:1  | 20237470:260 | 713734:5   |
| 31984:1  | 15856590:191 | 385018:5   |
| 28752:1  | 16054486:292 | 626754:5   |
| 25846:0  | 16467528:160 | 367190:2   |
| 26380:0  | 16571838:205 | 252286:2   |
| 31788:1  | 16607306:238 | 480180:80  |
| 30342:0  | 17122368:217 | 509296:4   |
| 32766:1  | 16945832:203 | 276754:2   |
| 61034:1  | 17073104:177 | 279050:2   |
| 57582:1  | 16689550:318 | 224814:2   |
| 31548:1  | 16343552:196 | 256180:2   |
| 35016:1  | 14633800:167 | 220532:1   |
| 35362:1  | 13823006:145 | 541302:3   |
| 79410:2  | 15348030:181 | 231456:3   |
| 67296:1  | 14316634:144 | 255480:2   |
| 71878:2  | 12383414:111 | 278328:3   |
| 13082:0  | 12703060:272 | 498996:4   |
| 57384:3  | 12334052:155 | 525790:4   |
| 46800:1  | 12042596:137 | 324776:2   |
| 33238:0  | 12422418:118 | 443132:3   |
| 67274:1  | 12365384:130 | 200558:2   |
| 32166:1  | 15175656:173 | 199080:2   |
| 51534:1  | 14842732:172 | 378594:2   |
| 60154:1  | 15255090:152 | 244538:2   |
| 69858:1  | 15234808:159 | 186234:2   |
| 73918:1  | 15280362:278 | 330664:87  |

|          |               |           |
|----------|---------------|-----------|
| 31798:2  | 15010404:139  | 381176:3  |
| 37048:1  | 14751434:151  | 257760:2  |
| 38708:1  | 14684642:151  | 195444:2  |
| 37374:2  | 14498462:137  | 262234:3  |
| 32912:1  | 12429048:136  | 224478:1  |
| 32532:1  | 14074652:154  | 226448:2  |
| 32270:1  | 3043506:33    | 503286:4  |
| 68280:2  | 14799166:141  | 480184:4  |
| 73886:2  | 14852298:248  | 478930:6  |
| 37512:1  | 14237000:172  | 509510:4  |
| 71760:2  | 14309718:162  | 651252:6  |
| 57122:1  | 14435934:107  | 806346:7  |
| 55540:2  | 11869480:125  | 820242:7  |
| 54024:1  | 14796318:187  | 736202:7  |
| 51504:2  | 14916800:176  | 562940:4  |
| 36242:1  | 14385908:157  | 585030:91 |
| 37064:1  | 13943284:369  | 376310:3  |
| 39512:1  | 6974476:83    | 576878:4  |
| 37266:1  | 6809794:78    | 562734:4  |
| 45324:1  | 6732850:72    | 328758:4  |
| 41542:2  | 6755740:70    | 364070:5  |
| 39940:1  | 6868574:70    | 391990:3  |
| 39662:1  | 6776682:72    | 216128:2  |
| 37852:2  | 1480588:17    | 172320:2  |
| 255692:2 | 8693078:92    | 174796:1  |
| 425540:3 | 9162986:99    | 222910:2  |
| 421728:3 | 8815362:91    | 236008:2  |
| 241848:2 | 7358368:74    | 418604:3  |
| 537284:3 | 8738510:102   | 147504:1  |
| 240824:2 | 9577448:113   | 128672:1  |
| 462018:3 | 10520008:8835 | 112242:1  |
| 507904:3 | 10340876:126  | 244136:1  |
| 257132:2 | 11574456:142  | 185924:2  |
| 519754:3 | 11168334:131  | 167678:3  |
| 630154:4 | 497558:5      | 172264:2  |
| 282194:2 | 211024:2      | 145004:1  |
| 498214:4 | 612262:3      | 205652:2  |
| 297978:2 | 517336:3      | 152188:1  |
| 371902:2 | 319008:2      | 301470:2  |
| 477728:4 | 450334:3      | 213410:1  |
| 489278:3 | 614634:3      | 168368:2  |
| 328056:2 | 224478:2      | 248294:2  |
| 490170:5 | 322300:3      | 160126:1  |
| 380330:2 | 383892:2      | 446112:3  |
| 488900:3 | 399118:3      | 440378:3  |
| 286816:1 | 362244:2      | 439056:3  |
| 324804:2 | 136198:2      |           |
| 489246:3 | 896880:5      |           |
| 451418:2 | 797082:5      |           |
| 487410:3 | 295236:2      |           |

|          |          |  |
|----------|----------|--|
| 428548:3 | 235170:2 |  |
| 434708:3 | 279574:2 |  |





**EK-9: DOC bayt tekniğiyle manipölasyon verileri**

|             |               |               |
|-------------|---------------|---------------|
| 133009:1211 | 17632:166     | 93945:980     |
| 12781:123   | 14891:129     | 277269:2523   |
| 15091:172   | 16856:148     | 304890:2629   |
| 15207:141   | 16983:151     | 3500090:30972 |
| 14762:130   | 15363:141     | 4787734:42763 |
| 14909:135   | 18102:156     | 20084:180     |
| 11022:110   | 61896:555     | 118411:1047   |
| 12623:115   | 41394:363     | 22077:195     |
| 19308:170   | 14991:135     | 118434:1026   |
| 118138:1035 | 15523:137     | 24663:221     |
| 21984:187   | 642160:5625   | 20036:186     |
| 117861:1013 | 17023:157     | 118426:1075   |
| 19174:198   | 16733:152     | 23340:220     |
| 27224:284   | 17805:198     | 19590:175     |
| 18901:177   | 17805:177     | 118461:1051   |
| 118285:1099 | 742368:6813   | 23456:212     |
| 25021:201   | 742102:6472   | 13332:122     |
| 117540:1027 | 2364650:20326 | 16098:146     |
| 18127:183   | 18125:155     | 20096:181     |
| 26715:229   | 12045:102     | 3717823:33254 |
| 19009:152   | 12681:112     | 2804969:24934 |
| 117953:1025 | 47414:392     | 13028:120     |
| 24212:219   | 45933:388     | 2011583:17521 |
| 19248:166   | 14597:132     | 14626:129     |
| 118088:1022 | 16180:135     | 13621:123     |
| 24137:220   | 17343:152     | 19016:169     |
| 117971:1036 | 56359:512     | 12940:116     |
| 19859:175   | 55739:485     | 351694:3138   |
| 25183:211   | 47207:413     | 412548:3837   |
| 20041:166   | 1319017:11671 | 18251:166     |
| 118389:1015 | 17241:155     | 15194:136     |
| 23673:186   | 48533:424     | 13179:123     |
| 19379:156   | 33710:304     | 13282:115     |
| 117939:999  | 305269:2592   | 141179:1284   |
| 23720:212   | 152602:1273   | 254888:2323   |
| 26813:244   | 14793:134     | 14164:128     |
| 17824:156   | 15640:143     | 75758:735     |
| 118107:1022 | 240672:2159   | 15573:154     |
| 19695:185   | 40073:350     | 26250:239     |
| 24566:215   | 14915:130     | 63679:586     |
| 19067:182   | 35283:306     | 16320:150     |
| 118127:1020 | 35824:312     | 47592:434     |
| 23514:199   | 13594:131     | 152615:1340   |
| 19388:169   | 751994:6445   | 11277:106     |
| 117948:1017 | 16544:145     | 112686:1010   |
| 24542:222   | 14583:124     | 12311:119     |
| 118393:1033 | 1443838:12486 | 66083:629     |
| 24614:233   | 27380:228     | 14042:126     |

|               |               |               |
|---------------|---------------|---------------|
| 20037:189     | 536738:4361   | 121309:1063   |
| 23573:208     | 253860:2023   | 14903:137     |
| 118372:1021   | 19891:166     | 14194:131     |
| 19297:166     | 1584958:12907 | 550396:4916   |
| 118184:1012   | 1583672:13666 | 18478:165     |
| 24072:211     | 23321:196     | 16217:149     |
| 20084:178     | 13502:113     | 18181:166     |
| 118411:1018   | 12554:104     | 19342:172     |
| 24607:217     | 316129:2742   | 19416:169     |
| 29344:257     | 310381:2718   | 52209:444     |
| 13187:114     | 51127:462     | 51466:453     |
| 25148:216     | 54545:517     | 59119:524     |
| 12816:114     | 35218:302     | 13301:118     |
| 125572:1073   | 35255:279     | 16683:152     |
| 460344:3976   | 419815:3591   | 12677:113     |
| 23693:210     | 4905:44       | 12856:117     |
| 13151:115     | 17857:150     | 12717:113     |
| 14082:125     | 16563:140     | 12792:124     |
| 12124:130     | 106376:930    | 12505:116     |
| 13257:137     | 15799:145     | 1846520:16790 |
| 96387:805     | 26868:255     | 22818:202     |
| 14071:129     | 56524:505     | 149730:1290   |
| 13201:171     | 228131:2018   | 149365:1318   |
| 13269:116     | 243673:2157   | 204837:1860   |
| 13291:116     | 37217:312     | 45935:405     |
| 21507:204     | 170387:1513   | 268460:2367   |
| 13237:116     | 58825:544     | 573740:5145   |
| 14459:125     | 71403:634     | 41322:370     |
| 12553:110     | 12471:109     | 22932:208     |
| 33340:329     | 13344:107     | 22913:204     |
| 65695:573     | 18881:155     | 16297:151     |
| 1263744:12220 | 22090:194     | 403096:3551   |
| 11352:104     | 22090:209     | 13537:124     |
| 12211:107     | 211643:1822   | 12685:116     |
| 15507:138     | 35280:325     | 34865:306     |
| 12369:112     | 14411:164     | 15148:136     |
| 13005:119     | 23519:206     | 12505:118     |
| 11550:108     | 121458:1160   | 11681:104     |
| 12037:109     | 17914:156     | 37867:338     |
| 2425617:21623 | 260650:2377   | 35622:341     |
| 192087:1723   | 11991:128     | 12103:106     |
| 14623:136     | 814367:7080   | 61902:528     |
| 14325:111     | 227879:1949   | 19651:170     |
| 17229:146     | 258896:2161   | 14176:130     |
| 15375:162     | 20245:179     | 19439:171     |
| 14134:135     | 117642:1008   | 94739:784     |
| 14294:129     | 47979:417     | 13377:118     |
| 16194:148     | 137954:1141   | 16451:143     |
| 20021:211     | 12271:99      | 9497643:86044 |
| 274402:2546   | 12343:98      | 15552:143     |

|               |                 |             |
|---------------|-----------------|-------------|
| 573922:5008   | 12475:99        | 12834:118   |
| 192620:1656   | 12381:98        | 14012:133   |
| 37222:304     | 612090:5104     | 13078:117   |
| 14135:126     | 3727206:32638   | 44053:436   |
| 276727:2377   | 35319:305       | 34794:304   |
| 54296:471     | 35220:305       | 33967:306   |
| 87088:756     | 30351:265       | 463846:4220 |
| 444800:3849   | 30373:274       | 33920:304   |
| 20425:182     | 30327:264       | 201265:1974 |
| 11995:109     | 13422:125       | 16378:146   |
| 14477:131     | 19572:168       | 31024:285   |
| 23149:206     | 31298:273       | 13103:120   |
| 25159:244     | 3101530:29035   | 27243:264   |
| 192087:1674   | 13768:131       | 274861:2680 |
| 15168:133     | 49368:492       | 13754:136   |
| 2801086:24824 | 12664:139       | 40458:360   |
| 1281827:11164 | 211435:2132     | 13237:128   |
| 17091:149     | 12005:113       | 17153:159   |
| 35234:304     | 142555:1183     | 15943:143   |
| 35224:310     | 12323:96        | 17541:268   |
| 13021:122     | 14123:112       | 17437:332   |
| 13849:127     | 13126:118       | 224011:2108 |
| 14719:140     | 35227:291       | 74399:649   |
| 13656:121     | 35715:315       | 268136:2515 |
| 14562:129     | 31817:274       | 39831:370   |
| 11917:107     | 12183:116       | 58198:525   |
| 12980:127     | 35831:310       | 130766:1160 |
| 25514:225     | 12601:112       | 16131:205   |
| 12810:113     | 229063:1962     | 210186:1949 |
| 2475907:22225 | 5696496:49004   | 276785:2597 |
| 25762:224     | 14014:124       | 966718:8528 |
| 15270:132     | 14729454:135808 | 594458:5133 |
| 118138:1022   | 23314655:215296 | 4508:43     |
| 18385:169     | 23311589:216256 | 14601:131   |
| 118331:1052   | 64544:583       | 209272:1815 |
| 23060:216     | 31747:289       | 476303:4362 |
| 21762:208     | 35600:348       | 182259:1603 |
| 117127:1034   | 12739:129       | 16193:146   |
| 18625:170     | 26385:255       | 16184:145   |
| 16222:152     | 12310:131       | 301789:2830 |
| 286869:2588   | 12319:134       | 75602:744   |
| 27224:239     | 54567:538       | 15921:160   |
| 117176:1045   | 11890:123       | 117546:1024 |
| 18348:284     | 15712:149       | 24072:211   |
| 18302:169     | 83543:819       | 15331:138   |
| 117578:1112   | 35269:356       | 13792:130   |
| 117057:1118   | 13999:158       | 17572:171   |
| 17918:165     | 93677:944       | 879606:7792 |
| 18520:218     | 12463:128       | 192755:1748 |
| 117584:1200   | 118616:1397     | 13279:122   |

|             |               |               |
|-------------|---------------|---------------|
| 117600:1201 | 118616:1236   | 33742:307     |
| 19268:167   | 268839:2677   | 683075:6018   |
| 18796:183   | 70951:631     | 958057:8920   |
| 117564:1156 | 2562792:22553 | 1492842:13557 |
| 17821:198   | 1148247:9619  | 24012:212     |
| 117585:1184 | 23820:207     | 23573:203     |
| 18025:193   | 23514:213     | 118220:1037   |
| 117941:1185 | 19718:175     | 18406:166     |
| 23372:208   | 117962:1095   | 118346:1073   |
| 18803:191   | 24127:214     | 23329:240     |
| 117529:1139 | 117609:1036   | 18692:175     |
| 24566:251   | 18502:164     | 19491:172     |
| 18455:189   | 117610:1033   |               |
| 117559:1115 | 118276:1069   |               |



**EK-10:** DOC ara bellek tekniğiyle manipölasyon verileri

|           |            |              |
|-----------|------------|--------------|
| 133009:22 | 18302:1    | 30327:1      |
| 12781:3   | 117578:2   | 13422:1      |
| 15091:2   | 117057:3   | 19572:1      |
| 15207:1   | 17918:1    | 31298:1      |
| 14762:2   | 18520:1    | 3101530:66   |
| 14909:2   | 117584:2   | 13768:1      |
| 11022:1   | 117600:4   | 49368:1      |
| 12623:2   | 19268:1    | 12664:1      |
| 19308:2   | 18796:1    | 211435:5     |
| 118138:5  | 117564:3   | 12005:1      |
| 21984:1   | 17821:1    | 142555:3     |
| 117861:5  | 117585:4   | 12323:1      |
| 19174:2   | 18025:1    | 14123:1      |
| 27224:3   | 117941:4   | 13126:1      |
| 18901:2   | 23372:1    | 35227:1      |
| 118285:5  | 18803:1    | 35715:1      |
| 25021:1   | 117529:3   | 31817:2      |
| 117540:5  | 24566:2    | 12183:5      |
| 18127:1   | 18455:1    | 35831:1      |
| 26715:5   | 117559:4   | 12601:0      |
| 19009:2   | 23514:1    | 229063:8     |
| 117953:4  | 19718:1    | 5696496:138  |
| 24212:1   | 117962:3   | 14014:1      |
| 19248:1   | 24127:1    | 14729454:297 |
| 118088:4  | 117609:4   | 23314655:637 |
| 24137:1   | 18502:1    | 23311589:460 |
| 117971:4  | 117610:3   | 64544:1      |
| 19859:2   | 118276:5   | 31747:2      |
| 25183:2   | 19491:1    | 35600:1      |
| 20041:1   | 23573:2    | 12739:1      |
| 118389:5  | 118220:3   | 26385:1      |
| 23673:2   | 18406:1    | 12310:1      |
| 19379:3   | 118346:4   | 12319:0      |
| 117939:4  | 23329:2    | 54567:1      |
| 23720:2   | 18692:1    | 11890:1      |
| 26813:3   | 117546:3   | 15712:1      |
| 17824:2   | 24072:2    | 83543:2      |
| 118107:4  | 15331:1    | 35269:1      |
| 19695:2   | 13792:1    | 13999:1      |
| 24566:2   | 17572:1    | 93677:2      |
| 19067:3   | 879606:20  | 12463:1      |
| 118127:8  | 192755:5   | 118616:3     |
| 23514:2   | 13279:1    | 118616:2     |
| 19388:2   | 33742:1    | 268839:5     |
| 117948:7  | 683075:15  | 70951:2      |
| 24542:2   | 958057:20  | 2562792:51   |
| 118393:5  | 1492842:33 | 1148247:22   |
| 24614:2   | 24012:1    | 23820:1      |

|            |            |             |
|------------|------------|-------------|
| 20037:4    | 17632:1    | 12103:1     |
| 23573:2    | 14891:1    | 61902:2     |
| 118372:3   | 16856:1    | 19651:1     |
| 19297:1    | 16983:1    | 14176:1     |
| 118184:3   | 15363:0    | 19439:1     |
| 24072:2    | 18102:1    | 94739:3     |
| 20084:2    | 61896:2    | 13377:1     |
| 118411:2   | 41394:2    | 16451:1     |
| 24607:1    | 14991:1    | 9497643:190 |
| 29344:1    | 15523:1    | 15552:2     |
| 13187:1    | 642160:14  | 12834:2     |
| 25148:2    | 17023:1    | 14012:1     |
| 12816:0    | 16733:1    | 13078:2     |
| 125572:4   | 17805:0    | 44053:2     |
| 460344:10  | 17805:0    | 34794:2     |
| 23693:1    | 742368:15  | 33967:2     |
| 13151:1    | 742102:16  | 463846:13   |
| 14082:1    | 2364650:70 | 33920:2     |
| 12124:1    | 18125:1    | 201265:7    |
| 13257:1    | 12045:1    | 16378:1     |
| 96387:2    | 12681:1    | 31024:1     |
| 14071:1    | 47414:2    | 13103:2     |
| 13201:1    | 45933:1    | 27243:2     |
| 13269:1    | 14597:1    | 274861:7    |
| 13291:1    | 16180:1    | 13754:3     |
| 21507:1    | 17343:1    | 40458:2     |
| 13237:0    | 56359:2    | 13237:1     |
| 14459:1    | 55739:2    | 17153:2     |
| 12553:1    | 47207:1    | 15943:1     |
| 33340:3    | 1319017:27 | 17541:2     |
| 65695:2    | 17241:1    | 17437:1     |
| 1263744:41 | 48533:2    | 224011:7    |
| 11352:1    | 33710:1    | 74399:3     |
| 12211:1    | 305269:8   | 268136:7    |
| 15507:2    | 152602:4   | 39831:2     |
| 12369:1    | 14793:1    | 58198:2     |
| 13005:1    | 15640:1    | 130766:4    |
| 11550:1    | 240672:5   | 16131:2     |
| 12037:2    | 40073:1    | 210186:7    |
| 2425617:59 | 14915:1    | 276785:8    |
| 192087:5   | 35283:1    | 966718:22   |
| 14623:2    | 35824:2    | 594458:16   |
| 14325:1    | 13594:1    | 4508:1      |
| 17229:2    | 751994:17  | 14601:1     |
| 15375:2    | 16544:1    | 209272:8    |
| 14134:1    | 14583:1    | 476303:12   |
| 14294:1    | 1443838:30 | 182259:6    |
| 16194:1    | 27380:2    | 16193:2     |
| 20021:1    | 536738:11  | 16184:1     |
| 274402:6   | 253860:5   | 301789:7    |

|            |            |             |
|------------|------------|-------------|
| 573922:14  | 19891:0    | 75602:3     |
| 192620:4   | 1584958:32 | 15921:1     |
| 37222:1    | 1583672:34 | 93945:3     |
| 14135:1    | 23321:1    | 277269:8    |
| 276727:6   | 13502:1    | 304890:8    |
| 54296:2    | 12554:1    | 3500090:83  |
| 87088:3    | 316129:6   | 4787734:141 |
| 444800:9   | 310381:7   | 20084:3     |
| 20425:2    | 51127:2    | 118411:7    |
| 11995:2    | 54545:1    | 22077:3     |
| 14477:1    | 35218:1    | 118434:19   |
| 23149:1    | 35255:1    | 24663:4     |
| 25159:1    | 419815:8   | 20036:3     |
| 192087:4   | 4905:1     | 118426:6    |
| 15168:1    | 17857:1    | 23340:2     |
| 2801086:71 | 16563:1    | 19590:1     |
| 1281827:29 | 106376:3   | 118461:5    |
| 17091:1    | 15799:1    | 23456:1     |
| 35234:1    | 26868:1    | 13332:1     |
| 35224:1    | 56524:2    | 16098:2     |
| 13021:1    | 228131:5   | 20096:6     |
| 13849:1    | 243673:6   | 3717823:74  |
| 14719:1    | 37217:2    | 2804969:57  |
| 13656:1    | 170387:5   | 13028:1     |
| 14562:1    | 58825:3    | 2011583:42  |
| 11917:1    | 71403:3    | 14626:2     |
| 12980:1    | 12471:1    | 13621:1     |
| 25514:1    | 13344:0    | 19016:1     |
| 12810:1    | 18881:1    | 12940:1     |
| 2475907:55 | 22090:1    | 351694:8    |
| 25762:2    | 22090:1    | 412548:11   |
| 15270:1    | 211643:6   | 18251:1     |
| 118138:3   | 35280:1    | 15194:1     |
| 18385:1    | 14411:1    | 13179:2     |
| 118331:3   | 23519:1    | 13282:1     |
| 23060:1    | 121458:4   | 141179:5    |
| 21762:2    | 17914:1    | 254888:7    |
| 117127:2   | 260650:6   | 14164:2     |
| 18625:0    | 11991:1    | 75758:3     |
| 16222:1    | 814367:20  | 15573:1     |
| 286869:6   | 227879:7   | 26250:1     |
| 27224:1    | 258896:6   | 63679:2     |
| 117176:3   | 20245:0    | 16320:1     |
| 18348:2    | 117642:3   | 47592:2     |
| 11277:1    | 47979:2    | 152615:5    |
| 112686:3   | 137954:3   | 12856:1     |
| 12311:1    | 12271:1    | 12717:1     |
| 66083:3    | 12343:0    | 12792:2     |
| 14042:1    | 12475:1    | 12505:1     |
| 121309:4   | 12381:1    | 1846520:40  |

|           |            |          |
|-----------|------------|----------|
| 14903:1   | 612090:14  | 22818:2  |
| 14194:1   | 3727206:82 | 149730:6 |
| 550396:14 | 35319:2    | 149365:6 |
| 18478:1   | 35220:1    | 204837:7 |
| 16217:1   | 30351:1    | 45935:2  |
| 18181:1   | 30373:1    | 268460:8 |
| 19342:1   | 573740:15  | 13537:1  |
| 19416:2   | 41322:1    | 12685:0  |
| 52209:2   | 22932:2    | 34865:2  |
| 51466:3   | 22913:1    | 15148:0  |
| 59119:3   | 16297:2    | 12505:0  |
| 13301:1   | 403096:11  | 35622:2  |
| 16683:1   | 11681:1    |          |
| 12677:2   | 37867:2    |          |



**EK-11: DOC bayt tekniđi tersine manipölasyon verileri**

|             |               |                |
|-------------|---------------|----------------|
| 266022:1234 | 48028:178     | 39306:164      |
| 25566:108   | 35268:132     | 28356:114      |
| 30186:126   | 29786:112     | 38882:172      |
| 30418:120   | 33716:124     | 189482:717     |
| 29528:118   | 33970:143     | 26758:112      |
| 29822:132   | 30730:129     | 32906:125      |
| 25250:115   | 36208:191     | 18995290:71822 |
| 38620:160   | 123796:489    | 31108:120      |
| 236280:972  | 82792:335     | 25672:104      |
| 43972:186   | 29986:113     | 28028:112      |
| 235726:950  | 31050:126     | 26160:109      |
| 38352:168   | 1284324:4921  | 88110:338      |
| 54452:239   | 34050:174     | 69592:295      |
| 37806:179   | 33470:198     | 67938:276      |
| 236574:984  | 35614:154     | 927696:3515    |
| 50046:196   | 35614:146     | 67844:258      |
| 235084:1017 | 1484740:6104  | 402534:1509    |
| 36258:144   | 1484208:5848  | 32760:126      |
| 53434:253   | 4729304:21151 | 62052:240      |
| 38022:191   | 36254:144     | 26210:104      |
| 235910:1084 | 24094:101     | 54490:209      |
| 48428:192   | 25366:99      | 549726:2063    |
| 38500:164   | 94832:372     | 27512:111      |
| 236180:1056 | 91870:373     | 80920:317      |
| 48278:240   | 29198:151     | 26478:112      |
| 235946:1032 | 32364:140     | 34310:137      |
| 39722:180   | 34690:170     | 31890:121      |
| 50370:211   | 112722:452    | 35086:137      |
| 40086:166   | 111482:517    | 34878:144      |
| 236782:926  | 94418:413     | 448026:1768    |
| 47350:183   | 2638038:11163 | 148802:598     |
| 38762:147   | 34486:145     | 536276:2043    |
| 235882:920  | 97070:392     | 79666:319      |
| 47444:176   | 67424:266     | 116400:447     |
| 53630:217   | 610542:2547   | 261536:1048    |
| 35652:158   | 305208:1392   | 32266:125      |
| 236218:922  | 29590:135     | 420376:1612    |
| 39394:161   | 31284:135     | 553574:2236    |
| 49136:203   | 481348:2133   | 1933440:7178   |
| 38138:145   | 80150:366     | 1188920:4535   |
| 236258:925  | 29834:205     | 9020:40        |
| 47032:178   | 70570:294     | 29206:109      |
| 38780:153   | 71652:316     | 418548:1545    |
| 235900:924  | 27192:278     | 952610:3703    |
| 49088:182   | 1503992:6356  | 364522:1426    |
| 236790:913  | 33092:143     | 32390:127      |
| 49232:276   | 29170:138     | 32372:122      |
| 40078:157   | 2887680:12523 | 603582:2338    |

|               |               |               |
|---------------|---------------|---------------|
| 47150:209     | 54764:321     | 151208:574    |
| 236748:908    | 1073480:6086  | 31846:126     |
| 38598:169     | 507724:2483   | 187894:701    |
| 236372:902    | 39786:158     | 554542:2139   |
| 48148:195     | 3169920:13835 | 609784:2269   |
| 22048:87      | 3167348:14009 | 7000184:26165 |
| 40172:152     | 46646:256     | 9575472:36448 |
| 236826:929    | 27008:135     | 40172:157     |
| 49218:197     | 25112:148     | 236826:876    |
| 58692:217     | 632262:2663   | 44158:173     |
| 26378:105     | 620766:2457   | 236872:874    |
| 25636:103     | 102258:400    | 49330:198     |
| 251148:967    | 109094:457    | 40076:147     |
| 920692:3586   | 70440:341     | 236856:895    |
| 47390:175     | 70514:289     | 46684:170     |
| 50300:184     | 839634:3224   | 39184:142     |
| 26306:99      | 9814:56       | 236926:891    |
| 24252:115     | 35718:139     | 46916:170     |
| 28168:127     | 33130:119     | 26668:100     |
| 26518:124     | 212756:783    | 32200:122     |
| 192778:750    | 31602:116     | 40196:163     |
| 26406:117     | 53740:195     | 7435650:27456 |
| 28146:123     | 113052:408    | 5609942:20819 |
| 26542:102     | 456266:1746   | 26060:114     |
| 26586:100     | 487350:1910   | 4023170:15067 |
| 43018:157     | 74438:282     | 29256:116     |
| 26478:106     | 340778:1318   | 27246:106     |
| 28922:123     | 117654:486    | 38036:149     |
| 25110:99      | 142810:529    | 25884:97      |
| 66684:279     | 24946:100     | 703392:2640   |
| 131394:500    | 26692:96      | 825100:3042   |
| 2527492:10446 | 37766:136     | 36506:143     |
| 22708:214     | 44184:186     | 30392:113     |
| 24426:100     | 44184:161     | 26362:100     |
| 31018:134     | 423290:1571   | 26568:102     |
| 24742:97      | 70564:257     | 282362:1066   |
| 26014:115     | 28826:108     | 509780:1894   |
| 23104:97      | 47042:170     | 28332:113     |
| 24078:96      | 242920:889    | 151520:555    |
| 4851238:18776 | 35832:134     | 31150:121     |
| 384178:1459   | 521304:1853   | 52504:197     |
| 29250:116     | 23986:97      | 127362:493    |
| 28654:109     | 1628738:5817  | 32644:122     |
| 34462:133     | 455762:1640   | 95188:353     |
| 30754:119     | 517796:1886   | 305234:1146   |
| 28272:117     | 40494:152     | 22558:90      |
| 28592:119     | 235288:859    | 225376:843    |
| 32392:124     | 95962:349     | 24626:99      |
| 40046:153     | 275912:1030   | 132170:492    |
| 548808:2098   | 24546:91      | 28088:111     |

|               |                 |               |
|---------------|-----------------|---------------|
| 1147848:4322  | 24690:93        | 242622:922    |
| 385244:1457   | 24954:91        | 29810:112     |
| 74448:284     | 24766:91        | 28392:110     |
| 28274:109     | 1224184:4550    | 1100796:4051  |
| 553458:2215   | 7454416:28023   | 36960:147     |
| 108596:470    | 70642:270       | 32438:121     |
| 174180:670    | 70444:251       | 36366:134     |
| 889604:3474   | 60706:218       | 38688:144     |
| 40854:164     | 60750:219       | 38836:148     |
| 23994:91      | 60658:254       | 104422:407    |
| 28958:110     | 26848:101       | 102936:394    |
| 46302:173     | 39148:150       | 118242:448    |
| 50322:190     | 62600:231       | 26606:107     |
| 384178:1452   | 6203064:23608   | 33370:124     |
| 30340:117     | 27540:117       | 25358:99      |
| 5602176:24242 | 98740:366       | 25716:97      |
| 2563658:14081 | 25332:111       | 25438:95      |
| 34186:160     | 422874:1570     | 25588:96      |
| 70472:302     | 24014:94        | 25014:94      |
| 70452:305     | 285114:1059     | 3693044:13894 |
| 26046:125     | 24650:95        | 45640:172     |
| 27702:114     | 28250:107       | 299464:1157   |
| 29442:148     | 26256:101       | 298734:1174   |
| 27316:119     | 70458:267       | 409678:1569   |
| 29128:122     | 71434:267       | 91874:412     |
| 23838:103     | 63638:268       | 536924:2019   |
| 25964:107     | 24370:94        | 1147484:4182  |
| 51032:215     | 71666:271       | 82648:316     |
| 25624:108     | 25206:95        | 45868:171     |
| 4951818:24672 | 458130:1701     | 45830:170     |
| 51528:218     | 11392996:43229  | 32598:135     |
| 30544:117     | 28032:128       | 806196:3039   |
| 236280:933    | 29458912:113558 | 27078:109     |
| 36774:150     | 46629314:178634 | 25374:102     |
| 236666:978    | 46623182:180385 | 69734:263     |
| 46124:191     | 129092:511      | 30300:115     |
| 43528:171     | 63498:243       | 25014:97      |
| 234258:889    | 71204:281       | 23366:89      |
| 37254:141     | 25482:105       | 75738:293     |
| 32448:127     | 52774:203       | 71248:280     |
| 573742:2149   | 24624:97        | 235224:889    |
| 54452:205     | 24642:100       | 236556:981    |
| 234356:883    | 109138:412      | 38986:164     |
| 36700:138     | 23784:120       | 47150:178     |
| 36608:136     | 31428:129       | 236444:1006   |
| 235160:896    | 167090:632      | 36816:153     |
| 234118:902    | 70542:285       | 236696:1074   |
| 35840:138     | 28002:109       | 46662:222     |
| 37044:142     | 187358:714      | 37388:165     |
| 235172:901    | 24930:106       | 235096:935    |

|             |               |               |
|-------------|---------------|---------------|
| 235204:907  | 237236:898    | 48148:187     |
| 38540:159   | 237236:924    | 30666:130     |
| 37596:153   | 537682:1997   | 27588:111     |
| 235132:893  | 141906:529    | 35148:137     |
| 35646:148   | 5125588:19481 | 1759216:6829  |
| 235174:899  | 2296498:8876  | 385514:1462   |
| 36054:145   | 47644:188     | 26562:103     |
| 235886:906  | 24210:97      | 67488:254     |
| 46748:191   | 123808:484    | 1366154:5283  |
| 37610:144   | 39440:163     | 1916118:7206  |
| 235062:1066 | 235928:957    | 2985688:11816 |
| 49136:196   | 48258:190     | 47032:180     |
| 36914:145   | 235222:902    |               |
| 235122:957  | 37008:143     |               |



**EK-12:** DOC ara bellek tekniđi tersine manipölasyon verileri

|           |            |            |
|-----------|------------|------------|
| 266022:84 | 48028:1    | 151208:1   |
| 25566:2   | 35268:2    | 31846:1    |
| 30186:3   | 29786:1    | 187894:1   |
| 30418:1   | 33716:1    | 554542:4   |
| 29528:2   | 33970:2    | 609784:5   |
| 29822:4   | 30730:1    | 7000184:54 |
| 25250:3   | 36208:1    | 9575472:88 |
| 38620:4   | 123796:2   | 40172:1    |
| 236280:12 | 82792:2    | 236826:1   |
| 43972:3   | 29986:1    | 44158:1    |
| 235726:12 | 31050:1    | 236872:3   |
| 38352:3   | 1284324:12 | 49330:1    |
| 54452:4   | 34050:1    | 40076:1    |
| 37806:2   | 33470:1    | 236856:2   |
| 236574:11 | 35614:1    | 46684:1    |
| 50046:4   | 35614:1    | 39184:1    |
| 235084:11 | 1484740:12 | 236926:2   |
| 36258:2   | 1484208:12 | 46916:1    |
| 53434:7   | 4729304:68 | 26668:1    |
| 38022:2   | 36254:1    | 32200:0    |
| 235910:10 | 24094:1    | 40196:1    |
| 48428:2   | 25366:1    | 7435650:69 |
| 38500:1   | 94832:1    | 5609942:60 |
| 236180:3  | 91870:1    | 26060:0    |
| 48278:1   | 29198:1    | 4023170:41 |
| 235946:3  | 32364:2    | 29256:1    |
| 39722:1   | 34690:2    | 27246:1    |
| 50370:2   | 112722:1   | 38036:1    |
| 40086:1   | 111482:2   | 25884:0    |
| 236782:2  | 94418:1    | 703392:5   |
| 47350:1   | 2638038:30 | 825100:5   |
| 38762:1   | 34486:1    | 36506:1    |
| 235882:2  | 97070:2    | 30392:0    |
| 47444:2   | 67424:1    | 26362:1    |
| 53630:1   | 610542:4   | 26568:1    |
| 35652:1   | 305208:3   | 282362:2   |
| 236218:3  | 29590:1    | 509780:4   |
| 39394:2   | 31284:3    | 28332:0    |
| 49136:1   | 481348:3   | 151520:2   |
| 38138:2   | 80150:2    | 31150:1    |
| 236258:4  | 29834:0    | 52504:1    |
| 47032:1   | 70570:1    | 127362:2   |
| 38780:2   | 71652:2    | 32644:0    |
| 235900:4  | 27192:0    | 95188:1    |
| 49088:1   | 1503992:14 | 305234:3   |
| 236790:4  | 33092:1    | 22558:0    |
| 49232:3   | 29170:1    | 225376:2   |
| 40078:2   | 2887680:30 | 24626:1    |

|            |            |            |
|------------|------------|------------|
| 47150:1    | 54764:1    | 132170:2   |
| 236748:2   | 1073480:8  | 28088:1    |
| 38598:1    | 507724:5   | 242622:2   |
| 236372:3   | 39786:0    | 29810:1    |
| 48148:1    | 3169920:41 | 28392:0    |
| 22048:1    | 3167348:36 | 1100796:9  |
| 40172:1    | 46646:1    | 36960:1    |
| 236826:2   | 27008:0    | 32438:1    |
| 49218:1    | 25112:0    | 36366:1    |
| 58692:1    | 632262:8   | 38688:1    |
| 26378:1    | 620766:5   | 38836:1    |
| 25636:0    | 102258:2   | 104422:1   |
| 251148:2   | 109094:2   | 102936:1   |
| 920692:7   | 70440:1    | 118242:1   |
| 47390:1    | 70514:1    | 26606:1    |
| 50300:2    | 839634:6   | 33370:0    |
| 26306:1    | 9814:1     | 25358:1    |
| 24252:1    | 35718:1    | 25716:0    |
| 28168:1    | 33130:2    | 25438:0    |
| 26518:0    | 212756:3   | 25588:1    |
| 192778:2   | 31602:1    | 25014:1    |
| 26406:1    | 53740:1    | 3693044:33 |
| 28146:1    | 113052:2   | 45640:1    |
| 26542:0    | 456266:5   | 299464:3   |
| 26586:2    | 487350:5   | 298734:3   |
| 43018:0    | 74438:1    | 409678:3   |
| 26478:0    | 340778:3   | 91874:2    |
| 28922:1    | 117654:1   | 536924:4   |
| 25110:0    | 142810:3   | 1147484:8  |
| 66684:2    | 24946:1    | 82648:1    |
| 131394:1   | 26692:1    | 45868:1    |
| 2527492:33 | 37766:1    | 45830:1    |
| 22708:1    | 44184:0    | 32598:1    |
| 24426:1    | 44184:1    | 806196:6   |
| 31018:1    | 423290:3   | 27078:1    |
| 24742:1    | 70564:1    | 25374:0    |
| 26014:1    | 28826:0    | 69734:2    |
| 23104:1    | 47042:1    | 30300:1    |
| 24078:1    | 242920:3   | 25014:1    |
| 4851238:50 | 35832:1    | 23366:1    |
| 384178:3   | 521304:4   | 75738:1    |
| 29250:0    | 23986:0    | 71248:1    |
| 28654:0    | 1628738:13 | 36054:1    |
| 34462:0    | 455762:4   | 235886:4   |
| 30754:1    | 517796:4   | 46748:1    |
| 28272:1    | 40494:0    | 37610:1    |
| 28592:1    | 235288:2   | 235062:4   |
| 32392:1    | 95962:1    | 49136:1    |
| 40046:0    | 275912:2   | 36914:1    |
| 548808:4   | 24546:1    | 235122:3   |

|            |              |            |
|------------|--------------|------------|
| 1147848:9  | 24690:1      | 47032:2    |
| 385244:3   | 24954:1      | 39440:1    |
| 74448:1    | 24766:1      | 235928:3   |
| 28274:1    | 1224184:8    | 48258:1    |
| 553458:3   | 7454416:88   | 235222:2   |
| 108596:1   | 70642:2      | 37008:0    |
| 174180:2   | 70444:1      | 235224:2   |
| 889604:5   | 60706:2      | 236556:5   |
| 40854:1    | 60750:1      | 38986:1    |
| 23994:1    | 60658:1      | 47150:1    |
| 28958:1    | 26848:1      | 236444:2   |
| 46302:1    | 39148:1      | 36816:0    |
| 50322:1    | 62600:1      | 236696:2   |
| 384178:3   | 6203064:62   | 46662:1    |
| 30340:1    | 27540:0      | 37388:1    |
| 5602176:63 | 98740:1      | 235096:2   |
| 2563658:25 | 25332:1      | 48148:1    |
| 34186:1    | 422874:4     | 30666:1    |
| 70472:1    | 24014:1      | 27588:0    |
| 70452:1    | 285114:2     | 35148:1    |
| 26046:1    | 24650:0      | 1759216:11 |
| 27702:1    | 28250:1      | 385514:3   |
| 29442:0    | 26256:1      | 26562:1    |
| 27316:1    | 70458:1      | 67488:1    |
| 29128:0    | 71434:1      | 1366154:9  |
| 23838:1    | 63638:1      | 1916118:13 |
| 25964:1    | 24370:1      | 2985688:44 |
| 51032:1    | 71666:1      | 80920:1    |
| 25624:1    | 25206:1      | 26478:0    |
| 4951818:50 | 458130:4     | 34310:1    |
| 51528:1    | 11392996:119 | 31890:0    |
| 30544:0    | 28032:1      | 35086:1    |
| 236280:2   | 29458912:315 | 34878:0    |
| 36774:0    | 46629314:391 | 448026:4   |
| 236666:1   | 46623182:470 | 148802:1   |
| 46124:0    | 129092:1     | 536276:4   |
| 43528:1    | 63498:1      | 79666:1    |
| 234258:1   | 71204:0      | 116400:1   |
| 37254:0    | 25482:1      | 261536:2   |
| 32448:1    | 52774:1      | 32266:1    |
| 573742:4   | 24624:1      | 420376:2   |
| 54452:1    | 24642:0      | 553574:3   |
| 234356:2   | 109138:2     | 1933440:13 |
| 36700:1    | 23784:0      | 1188920:8  |
| 36608:1    | 31428:1      | 9020:1     |
| 235160:2   | 167090:2     | 29206:0    |
| 234118:3   | 70542:1      | 418548:3   |
| 35840:1    | 28002:0      | 952610:6   |
| 37044:1    | 187358:2     | 364522:4   |
| 235172:2   | 24930:1      | 32390:0    |

|              |            |          |
|--------------|------------|----------|
| 235204:2     | 237236:1   | 32372:0  |
| 38540:2      | 237236:3   | 603582:5 |
| 37596:1      | 537682:3   | 67938:1  |
| 235132:2     | 141906:2   | 927696:6 |
| 35646:1      | 5125588:56 | 67844:0  |
| 235174:2     | 2296498:27 | 402534:4 |
| 26758:0      | 47644:0    | 32760:1  |
| 32906:1      | 24210:1    | 62052:0  |
| 18995290:165 | 123808:2   | 26210:1  |
| 31108:1      | 39306:0    | 54490:1  |
| 25672:1      | 28356:1    | 549726:4 |
| 28028:0      | 38882:1    | 27512:1  |
| 26160:1      | 189482:1   |          |
| 88110:1      | 69592:1    |          |



**EK-13: XLSX bayt tekniğiyle manipölasyon verileri**

|              |                 |           |
|--------------|-----------------|-----------|
| 19396:230    | 17635:140       | 5147:40   |
| 30694:324    | 15683:138       | 4891:39   |
| 5109:65      | 17497:144       | 4665:38   |
| 4982:50      | 16853:142       | 5167:48   |
| 5318:45      | 17246:141       | 9088:82   |
| 8401:85      | 18408:154       | 5203:44   |
| 10294:98     | 29997:246       | 4983:46   |
| 11566:98     | 16527:139       | 5326:47   |
| 591329:5110  | 16068:146       | 33662:272 |
| 61707:521    | 16489:142       | 5369:42   |
| 10744:115    | 17018:142       | 11043:85  |
| 11520:96     | 247915:2011     | 5091:39   |
| 13554:109    | 339434:2805     | 14125:106 |
| 83826:684    | 14224424:118457 | 17648:141 |
| 266312:2128  | 15687197:135584 | 4920:39   |
| 12313:105    | 9759:89         | 5297:41   |
| 1210884:9388 | 62569:561       | 21831:191 |
| 4900:43      | 15063:133       | 9487:85   |
| 90259:706    | 68939:608       | 24853:213 |
| 17942:164    | 4999:44         | 5146:42   |
| 17998:151    | 4676:42         | 4860:44   |
| 16440:143    | 4916:44         | 19224:148 |
| 16745:138    | 4945:47         | 17358:128 |
| 19979:159    | 4809:40         | 16240:121 |
| 16652:142    | 5839:54         | 15911:122 |
| 17056:132    | 117344:1261     | 21303:182 |
| 19206:153    | 298541:2912     | 4791:55   |
| 17630:154    | 10802:86        | 5489:57   |
| 18046:158    | 1086702:8485    | 4944:44   |
| 17019:134    | 14637:120       | 4876:41   |
| 16640:129    | 5120:181        | 5124:40   |
| 16937:142    | 19998:156       | 5253:45   |
| 17250:138    | 16269:123       | 5196:41   |
| 16744:136    | 5214:42         | 4834:38   |
| 17798:146    | 5092:40         | 27572:229 |
| 21303:185    | 8728:65         | 5287:45   |
| 19521:153    | 8733:66         | 4925:41   |
| 17044:136    | 8542:66         | 4830:42   |
| 16532:139    | 17592:129       | 7179:62   |
| 16860:136    | 4933:43         | 11269:104 |
| 16916:139    | 21281:178       | 9687:74   |
| 16472:139    | 4781:48         | 10093:77  |
| 17120:139    | 4867:50         | 17867:154 |
| 19956:166    | 4837:40         | 5033:42   |
| 18176:150    | 5099:41         | 5123:40   |
|              |                 | 5159:40   |



**EK-14: XLSX ara bellek tekniğiyle manipölasyon verileri**

|            |              |         |
|------------|--------------|---------|
| 19396:10   | 16853:1      | 17497:2 |
| 30694:4    | 17246:2      | 5147:0  |
| 5109:2     | 18408:1      | 4891:1  |
| 4982:2     | 29997:2      | 4665:0  |
| 5318:1     | 16527:1      | 5167:1  |
| 8401:3     | 16068:1      | 9088:0  |
| 10294:2    | 16489:1      | 5203:1  |
| 11566:2    | 17018:1      | 4983:0  |
| 591329:34  | 247915:5     | 5326:1  |
| 61707:3    | 339434:8     | 33662:1 |
| 10744:1    | 14224424:300 | 5369:0  |
| 11520:1    | 15687197:347 | 11043:1 |
| 13554:1    | 9759:1       | 5091:0  |
| 83826:4    | 62569:2      | 14125:0 |
| 266312:9   | 15063:1      | 17648:1 |
| 12313:1    | 68939:2      | 4920:0  |
| 1210884:29 | 4999:1       | 5297:0  |
| 4900:1     | 4676:0       | 21831:1 |
| 90259:5    | 4916:1       | 9487:0  |
| 17942:1    | 4945:0       | 24853:1 |
| 17998:2    | 4809:0       | 5146:1  |
| 16440:1    | 5839:0       | 4860:0  |
| 16745:1    | 117344:2     | 19224:1 |
| 19979:1    | 298541:7     | 17358:1 |
| 16652:1    | 10802:1      | 16240:1 |
| 17056:1    | 1086702:28   | 15911:0 |
| 19206:1    | 14637:1      | 21303:0 |
| 17630:1    | 5120:0       | 4791:1  |
| 18046:1    | 19998:0      | 5489:1  |
| 17019:1    | 16269:1      | 4944:0  |
| 16640:1    | 5214:1       | 4876:1  |
| 16937:1    | 5092:1       | 5124:0  |
| 17250:1    | 8728:1       | 5253:2  |
| 16744:1    | 8733:0       | 5196:1  |
| 17798:1    | 8542:1       | 4834:0  |
| 21303:1    | 17592:1      | 27572:1 |
| 19521:1    | 4933:0       | 5287:1  |
| 17044:0    | 21281:1      | 4925:1  |
| 16532:1    | 4781:0       | 4830:0  |
| 16860:0    | 4867:1       | 7179:0  |
| 16916:0    | 4837:1       | 11269:1 |
| 16472:0    | 5099:1       | 5159:0  |
| 17120:0    | 9687:0       |         |
| 19956:1    | 10093:1      |         |
| 18176:1    | 17867:1      |         |
| 17635:0    | 5033:1       |         |
| 15683:1    | 5123:1       |         |



**EK-15: XLSX bayt tekniği tersine manipölasyon verileri**

|              |                 |           |
|--------------|-----------------|-----------|
| 38796:299    | 31370:127       | 10322:44  |
| 61392:617    | 34998:136       | 10298:49  |
| 10222:67     | 33710:127       | 9786:42   |
| 9968:89      | 34496:139       | 9334:40   |
| 10640:69     | 36820:151       | 10338:43  |
| 16806:113    | 59998:255       | 18180:77  |
| 20592:109    | 33058:143       | 10410:42  |
| 23136:102    | 32140:123       | 9970:41   |
| 1182662:4701 | 32982:127       | 10656:46  |
| 123418:504   | 34040:135       | 67328:258 |
| 21492:91     | 495834:1973     | 10742:50  |
| 23044:193    | 678872:2490     | 22090:87  |
| 27112:112    | 28448852:109097 | 10186:42  |
| 167656:682   | 31374398:120174 | 28254:117 |
| 532628:2173  | 19522:84        | 35300:139 |
| 24630:164    | 125142:496      | 9844:42   |
| 2421772:9902 | 30130:144       | 10598:46  |
| 9804:52      | 137882:542      | 43666:175 |
| 180522:728   | 10002:41        | 18978:77  |
| 35888:149    | 9356:39         | 49710:195 |
| 36000:147    | 9836:41         | 10296:43  |
| 32884:133    | 9894:49         | 9724:42   |
| 33494:138    | 9622:40         | 38452:158 |
| 39962:170    | 11682:50        | 34720:139 |
| 33308:137    | 234692:906      | 32484:137 |
| 34116:134    | 597086:2282     | 31826:126 |
| 38416:142    | 21608:88        | 42610:175 |
| 35264:133    | 2173408:8247    | 9586:41   |
| 36096:139    | 29278:114       | 10982:45  |
| 34042:134    | 10244:43        | 9892:43   |
| 33284:133    | 40000:154       | 9756:40   |
| 33878:151    | 32542:135       | 10252:40  |
| 34504:139    | 10432:44        | 10510:44  |
| 33492:152    | 10188:44        | 10396:43  |
| 35600:147    | 17460:72        | 9672:44   |
| 42610:168    | 17470:72        | 55148:229 |
| 39046:155    | 17088:71        | 10578:45  |
| 34092:138    | 35188:138       | 9854:46   |
| 33068:139    | 9870:41         | 9664:39   |
| 33724:134    | 42566:177       | 14362:59  |
| 33836:133    | 9566:38         | 22542:86  |
| 32948:128    | 9738:41         | 35738:142 |
| 34244:142    | 9678:40         | 10070:41  |
| 39916:177    | 10202:44        | 10250:43  |
| 36356:143    | 19378:75        |           |
| 35274:146    | 20190:87        |           |



**EK-16:** XLSX ara bellek tekniđi tersine manipölasyon verileri

|            |              |         |
|------------|--------------|---------|
| 38796:73   | 36820:1      | 9786:1  |
| 61392:4    | 59998:1      | 9334:1  |
| 10222:1    | 33058:2      | 10338:0 |
| 9968:2     | 32140:1      | 18180:1 |
| 10640:1    | 32982:1      | 10410:1 |
| 16806:3    | 34040:1      | 9970:1  |
| 20592:2    | 495834:3     | 10656:1 |
| 23136:1    | 678872:6     | 67328:1 |
| 1182662:21 | 28448852:226 | 10742:3 |
| 123418:4   | 31374398:207 | 22090:4 |
| 21492:3    | 19522:1      | 10186:1 |
| 23044:2    | 125142:1     | 28254:1 |
| 27112:2    | 30130:1      | 35300:1 |
| 167656:3   | 137882:1     | 9844:2  |
| 532628:8   | 10002:1      | 10598:2 |
| 24630:2    | 9356:1       | 43666:2 |
| 2421772:21 | 9836:0       | 18978:1 |
| 9804:2     | 9894:1       | 49710:0 |
| 180522:5   | 9622:1       | 10296:1 |
| 35888:1    | 11682:1      | 9724:1  |
| 36000:2    | 234692:17    | 38452:1 |
| 32884:1    | 597086:4     | 34720:1 |
| 33494:1    | 21608:1      | 32484:0 |
| 39962:1    | 2173408:12   | 31826:1 |
| 33308:1    | 29278:0      | 42610:1 |
| 34116:1    | 10244:1      | 9586:1  |
| 38416:1    | 40000:0      | 10982:0 |
| 35264:1    | 32542:0      | 9892:0  |
| 36096:1    | 10432:1      | 9756:4  |
| 34042:2    | 10188:1      | 10252:1 |
| 33284:1    | 17460:0      | 10510:1 |
| 33878:1    | 17470:1      | 10396:1 |
| 34504:1    | 17088:0      | 9672:1  |
| 33492:1    | 35188:2      | 55148:1 |
| 35600:1    | 9870:0       | 10578:0 |
| 42610:1    | 42566:0      | 9854:1  |
| 39046:1    | 9566:1       | 9664:1  |
| 34092:1    | 9738:1       | 14362:1 |
| 33068:1    | 9678:0       | 22542:1 |
| 33724:1    | 10202:1      | 35274:1 |
| 33836:1    | 19378:1      | 31370:1 |
| 32948:0    | 20190:0      | 34998:1 |
| 34244:1    | 35738:1      | 33710:1 |
| 39916:0    | 10070:1      | 34496:1 |
| 36356:1    | 10250:1      | 10322:1 |
|            |              | 10298:1 |



## ÖZGEÇMİŞ

**Ad-Soyad** : Mustafa TAKAOĞLU

### ÖĞRENİM DURUMU

- **Lisans** : İstanbul Aydın Üniversitesi  
Mimarlık-Mühendislik Fakültesi  
Bilgisayar Mühendisliği (İngilizce)
- **Yüksek Lisans** : İstanbul Aydın Üniversitesi  
Fen Bilimleri Enstitüsü  
Bilgisayar Mühendisliği

### MESLEKİ DENEYİM

#### 01.2019- Devam Ediyor İstanbul Aydın Üniversitesi

Araştırma görevlisi olarak İstanbul Aydın Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği (İngilizce) Bölümünde göreve başlamıştır. Geçen süreç içerisinde 17 akademik yayın çalışmasında bulunmuştur. 400’den fazla bilgisayar mühendisliği öğrencilerine akademik danışmanlık yapmıştır. Bilgisayar Mühendisliği MÜDEK Sertifikasyon süreçlerinde gerekli çalışmaları yürütmüştür. İstanbul Aydın Üniversitesi Blokzincir Uygulama ve Araştırma Merkezinin kuruluş süreçlerinde görev almış ve merkezin müdür yardımcılığı görevini sürecin başlangıcından bu yana sürdürmektedir.

#### Yabancı Diller

İngilizce

### TEZDEN TÜRETİLEN YAYINLAR, SUNUMLAR VE PATENTLER

- Takaoğlu M., Özyavaş A., Ajlouni N. M. M., Alshahrani A., Alkasesbeh B., (2021), A Novel and Robust Hybrid Blockchain and Steganography Scheme, Applied Sciences-Basel, 11(22), 1-19., DOI: 10.3390/app112210698. (Doktora yayın şartının sağlanması amacıyla Lisansüstü Enstitüsünce tezimizden türetilen yayın olarak kayda alınmıştır.)

- Takaoğlu M., Ajlouni N. M. M., Özyavaş A., Hameed A. A., (2021), Blokzincir Temelli Milli Bağış Zinciri Projesi, Uluslararası Bilimsel Araştırmalar ve Yenilikçi Çalışmalar Sempozyumu, 344-369.
- Takaoğlu M., Özyavaş A., Ajlouni N. M. M., (2021), AviChainDB: Blockchain Integration on Aviation Databases, OSTIV Meteorological Panel 2021.
- Takaoğlu F., Takaoğlu M., (2020), Yazıcı Steganografisi ve Sarı Nokta Analizinin Günümüzde Geçerliliği, Yeni Medya Elektronik Dergisi, 4(3), 186-194., DOI:10.17932/IAU.EJNM.25480200.2020/ejnm\_v4i3004.
- Takaoğlu F., Takaoğlu M., (2019), Yazıcı Steganografisi ve Sarı Nokta Analizi - Bir Mini Derleme, ArtGRID - Journal of Architecture Engineering and Fine Arts, 1(1), 25-35.
- Takaoğlu M., Özer Ç., Parlak E., (2019), Blokzinciri Teknolojisi ve Türkiye'deki Muhtemel Uygulanma Alanları, Uluslararası Doğu Anadolu Fen Mühendislik ve Tasarım Dergisi, 1(2), 260-295.
- Takaoğlu M., Güneş A., (2019), Yükseköğretimde Blokzincir Teknolojisi, 5th International Congress on Education, Distance Education and Educational Technology- ICDET.
- Şahin F., Çevik T., Takaoğlu M., (2021), Review of the Literature on the Steganography Concept, International Journal of Computer Applications (IJCA), 183(2), 38-46.
- İşler B., Takaoğlu M., Küçükali U. F., (2019), Blokzincir ve Kripto Paraların İnsanlığa Etkileri, e-Journal of New Media, 3(2), 71-83., DOI:10.17932/IAU.EJNM.25480200.2019.3/2.71-83.
- Ajlouni N. M. M., Özyavaş A., Takaoğlu M., (2021), A Survey of Artificial Intelligence Driven Blockchain Technology: Blockchain Intelligence, Manchester Journal of Artificial Intelligence and Applied Sciences, 2(1).

