
GAZİ ÜNİVERSİTESİ
Gazi
1926

ELİPTİK EĞRİ KRİPTOGRAFİSİ İLE DİJİTAL GÖRÜNTÜ ŞİFRELEME

Muhammed HABEK

YÜKSEK LİSANS TEZİ
ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MART 2024

ETİK BEYAN

Gazi Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Muhammed HABEK

22/03/2024

ELİPTİK EĞRİ KRİPTOGRAFİSİ İLE DİJİTAL GÖRÜNTÜ ŞİFRELEME

(Yüksek Lisans Tezi)

Muhammed HABEK

GAZİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

Mart 2024

ÖZET

Günümüzde bilgi alışverişi hiç olmadığı kadar fazla yapılmaktadır. Bu durumun sonucunda bilgi hırsızlığı da aynı oranda artmıştır. Özellikle görüntü gibi bilgi değeri yüksek olan verilerde saldırganlık oranı daha fazla olmaktadır. Bu durumda, bilgileri saldırganlara karşı korumak için önlem alınması bir zorunluluk haline gelmiştir. Görüntülerin güvenliğini sağlamak için birçok yöntem geliştirilmiştir. Bunlar arasında şifreleme, sıkıştırma, filigran ekleme gibi uygulamalar yer almaktadır. Bunlar arasında en güvenli olan yöntem görüntünün şifrelenmesidir. Önerilen tez çalışmasında dijital görüntü şifrelemeye yönelik yeni bir yöntem geliştirilmiştir. Bu yöntemde görüntü şifrelemek için eliptik eğri kriptografisi kullanılmıştır. Görüntü şifrelemede kullanılan anahtarın paylaşımı Diffie-Hellman anahtar değişim protokolü ile gerçekleştirilmiştir. Görüntü şifreleme uygulaması sırasında orijinal görüntüde herhangi bir piksel kaybı olmamaktadır. Sonuç olarak literatürdeki benzer çalışmalardan daha hızlı, daha güvenilir ve kayıpsız yeni bir yöntem geliştirilmiştir.

Bilim Kodu	:	90521
Anahtar Kelimeler	:	Dijital görüntü şifreleme, eliptik eğri kriptografisi, Diffie-Hellman anahtar değişimi
Sayfa Adedi	:	73
Danışman	:	Prof. Dr. Erkan AFACAN

DIGITAL IMAGE ENCRYPTION USING ELLIPTIC CURVE CRYPTOGRAPHY

(M. Sc. Thesis)

Muhammed HABEK

GAZİ UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

March 2024

ABSTRACT

Nowadays, information has been exchanged more than ever before. As a result of this situation, information theft has also increased at the same rate. The rate of aggression is higher, especially in areas with high information value, such as images. This has made it a necessity to take measures so as to protect information against attackers. Many methods have been developed to protect images. These include applications such as encryption, compression and watermarking. The safest method among these is the encryption of the image. In the proposed study, a novel method for digital image encryption has been developed. In this method, elliptic curve cryptography has been used to encrypt the image. The key used in image encryption has been shared using the Diffie-Hellman key exchange protocol. There is no pixel loss from the original image during image encryption. As a result, a new method has been developed that is faster, more reliable and lossless than similar studies in the literature.

Science Code : 90521
Key Words : Digital image encryption, elliptic curve cryptography, Diffie-Hellman key exchange
Page Number : 73
Supervisor : Prof. Dr. Erkan AFACAN

TEŞEKKÜR

Bu zorlu yüksek lisans çalışma süresince bana her türlü desteği sağlayan, kendisindeki bilgi ve tecrübeleri her fırsatta aktaran değerli tez danışmanım Sayın Prof. Dr. Erkan AFACAN hocama saygılarımı sunuyorum.

Yüksek lisans tezi ve bildiri yayını sürecinde bana her türlü desteğini sağlayan, bana bu yolda ikinci bir danışmanım gibi çalışmalarıma destek olan Sayın Dr. Yasin GENÇ hocama şükran ve saygılarımı iletiyorum.

Ayrıca bu zorlu çalışma süresince bana manevi bir şekilde destek olan, bu süreç boyunca beni sürekli çalışmaya teşvik eden başta annem, babam, eşim ve kızım olmak üzere tüm aileme teşekkür ediyorum.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	**Açıklamalar**
dB	Desibel
s	Saniye

Kısaltmalar	**Açıklamalar**
AES	Advanced Encryption Standard (Gelişmiş Şifreleme Standardı)
BCR	Bit Correct Ratio (Bit Doğruluk Oranı)
ECC	Elliptic Curve Cryptography (Eliptik Eğri Kriptografisi)
ECDH	Elliptic Curve Diffie Hellman (Eliptik Eğri Diffie Hellman)
LTM	Logistic Tent Maps (Lojistik Çadır Haritaları)
MSE	Mean Squared Error (Ortalama Kare Hatası)
NPCR	Number of Pixel Change Rate (Piksel Sayısı Değişim Oranı)
PSNR	Peak Signal to Noise Ratio (Tepe Sinyal Gürültü Oranı)
PWLCM	Piece Wise Linear Chaotic Map (Parçalı Doğrusal Kaotik Harita)
RMSE	Root Mean Squared Error (Kök Ortalama Kare Hatası)
RSA	Rivest-Shamir-Adleman
SDR	Signal to Distortion Ratio (Sinyal Bozulma Oran)
SNR	Signal to Noise Ratio (Sinyal Gürültü Oranı)

Kısaltmalar	Açıklamalar
SSIM	Structural Similarity Index (Yapısal Benzerlik İndeksi)
TSM	Tent-Sinusoidal Map (Çadır Sinüzoidal Haritası)

1. GİRİŞ

Bilgi alışverişi, tarih boyunca insanların ihtiyaç duyduğu temel bir unsur olmuştur. Bilgisayar ve internetin keşfiyle birlikte bu ihtiyaç daha da artmıştır. Özellikle bilgi ve iletişim teknolojilerindeki hızlı gelişmeler, bilgi alışverişini büyük ölçüde artırmıştır. Bu artış, bilgilerin güvenliği konusundaki ihtiyacı ortaya çıkarmıştır. Değerli ve hassas bilgilerin güvenli bir şekilde paylaşılması, özellikle görüntülerin kullanıldığı askeri, tıbbi, nesnelerin interneti ve sosyal medya gibi çeşitli alanlarda büyük bir gereklilik haline gelmiştir.

Görüntüler, güvenliğin sağlanması gereken önemli bilgi türlerinden biridir. Çünkü görüntüler, çeşitli alanlarda veri ve bilgi aktarımında önemli bir rol oynamaktadır. Özellikle askeri alanda kullanılan görüntüler, ulusal güvenliği tehdit edebilecek bilgiler içerebilirken, tıbbi görüntüler hastaların kişisel verilerini içerebilir. Bu bilgilerin yetkisiz kişilerin eline geçmesi olumsuz sonuçlara yol açabilir.

Görüntülerin güvenliğini sağlamak için çeşitli kriptografik teknikler ve algoritmalar kullanılabilir. Görüntülerin şifrelenmesi, verilerin yetkisiz kişilerin erişiminden korunması için etkili bir yöntemdir. Güçlü şifreleme algoritmaları kullanılarak görüntülerin şifrelenmesi, yetkisiz kişilerin görüntüleri elde etmesi durumunda, görüntüden herhangi bir bilgi elde edilmesini engelleyecektir.

Görüntülerin güvenliği günümüzde; şifreli kanallarda taşıma, şifreli bir şekilde iletim, depolamanın şifreli yapılması gibi yöntemlerle sağlanmaktadır. Fakat taşıma yapılan kanalların veya depolama yerlerinin güvenliği her zaman yeterince sağlanamadığı için görüntülerin şifrelenmiş bir şekilde iletilmesi ve depolanması güvenlik açısından daha sağlıklı bir yöntemdir. Bu sayede veri iletimi yapılan kanala veya depolama alanlarına yetkisiz kişiler tarafından saldırılması halinde saldırganın eline geçen görüntü, bir bilgi değeri taşımayacaktır. Saldırı sonucunda bilgi hırsızlığı yapılsa bile görüntü içeriği korunmuş olur.

Görüntü şifrelemenin, gizli anahtarın ortak olduğu simetrik şifreleme yöntemleriyle yapılması; gizli anahtarın korunması zorluğu ve yüksek maliyet gibi sistemi negatif

etkileyen faktörleri beraberinde getirmektedir. Bu sebeple görüntü şifrelemenin gizli anahtarın farklı olduğu asimetrik şifrelemeyle yapılması bu negatif faktörleri en aza indirgeyecektir.

Bu bölümün geri kalanında eliptik eğrilerle ve görüntü şifreleme ile ilgili literatür taraması verilmiştir.

Ye, çift görüntü şifreleme yöntemini önermiştir. Bu çalışmada iki orijinal görüntü, kesikli dalga dönüşümü kullanılarak sıkıştırılmış bir kuantizasyon matrisine dönüştürülür. Matrisler ECC (Eliptik Eğri Kriptografisi; Elliptic Curve Cryptography) ile şifrelenir. Görüntüler, kaos tabanlı algoritma kullanılarak şifrelenir [1].

Dawahdeh, eliptik eğri kriptografisini Hill şifreleme ile birleştiren bir görüntü şifreleme algoritması önermiştir. Bu çalışmada Hill şifreleme simetrik şifreleme olarak değil, asimetrik şifreleme olarak kullanılmaktadır. Önerilen şifreleme yönteminde, ters matrise sahip olan bir 4x4 matris gizli anahtar olarak kullanılır. Bu nedenle, şifre çözme işleminde ters matrisi hesaplamak gerekli olmayacaktır [2].

Nagaraj, görüntüleri şifrelemek için ECC kullanan bir algoritma önermiştir. Önerilen şifreleme yönteminde, ters matrise sahip olan bir 4x4 sihirli matris gizli anahtar olarak kullanılır. Görüntüler 8x8 veri matrislerine dönüştürülür ve ECC kullanılarak şifrelenir [3].

El-Latif, kaotik bir sistemi ve ECC'yi birleştiren geliştirilmiş bir görüntü şifreleme yöntemi önermiştir. Bu yöntemde, kaotik sistem kullanılarak yeni bir anahtar akışı oluşturulur ve döngüsel eliptik eğri noktaları ile oluşturulan sözde rasgele bit dizisiyle karıştırılır. Daha sonra görüntü 8 bit veriye ayrılır ve XOR operasyonu ile şifrelenir [4].

Singh, ECC kullanarak görüntü şifreleyen bir yöntem sunmuştur. Önerilen algoritmanın hızını artırmak için görüntü pikselleri ECC sistemine göre gruplandırılır ve FromDigits algoritması kullanılarak büyük tamsayılara dönüştürülür. Şifreli görüntüyü oluşturmak için büyük tamsayılar IntegerDigits algoritması kullanılarak 0-255 aralığına indirgenir [5].

Reyad, kaos destekli eliptik eğri sözde rasgele sayı üreteci kullanarak anahtar dizileri ile görüntü şifreleyen bir yöntem sunmuştur. Bu çalışmada sözde rasgele dizilerden

oluşturulan anahtar dizileri, kaotik harita ile eliptik eğri nokta operasyonlarına bağlanır [6].

Liu, kaotik haritalar ve ECC temel alınarak geliştirilmiş bir görüntü şifreleme yöntemi önermiştir. Anahtarlar Menezes-Vanstone ECC kullanılarak oluşturulmuştur. Bu yöntemde şifreleme, kesikli kaotik harita ile kesirli iki boyutlu üçgen fonksiyonu kullanılarak uygulanır [7].

Obaid, ECC ile Hilbert matrislerini kullanarak bir görüntü şifreleme yöntemi sunmuştur. Bu çalışmada, ters matrislere sahip olan 2x2 ve 4x4 matrisler gizli anahtar olarak kullanılır. Bu nedenle şifre çözme işleminde ters matrisi hesaplamak gerekli olmayacaktır [8].

Chen, büyük görüntüler için yeni bir şifreleme yöntemi önermiştir. Büyük görüntüler, 256x256 büyüklüğünde alt görüntülere bölünür. Ardından, anahtar matrisi oluşturma algoritması kullanılarak alt görüntüler 256x256 büyüklüğünde anahtar matrise dönüştürülür. Son olarak görüntü, anahtar matrisleri kullanılarak şifrelenir [9].

Luo; ECC, ElGamal şifreleme tekniği ve kaotik sistemleri kullanarak bir görüntü şifreleme yöntemi önermiştir. Önerilen algoritmada gizli anahtar, SHA-512 kullanılarak orijinal görüntüden elde edilir. Daha sonra, LTM (Lojistik Çadır Haritaları; Logistic Tent Maps) ve TSM (Çadır Sinüzoidal Haritası; Tent Sinusoidal Map) olan kaotik harita denklemlerini kullanarak dört kaotik dizi oluşturulur. Permutasyon ve ECC-ElGamal şifreleme işleminden sonra, difüzyon işlemi uygulandığında görüntü şifrelenmiş olur [10].

Bashir, ECC ve kaotik sistem kullanarak geliştirilmiş bir şifreleme yöntemi önermiştir. Yöntemin düz metin ve şifreli metin saldırılarına karşı direncini artırmak için her düz metin için Hash-256 kodları kullanılmıştır. Bu kodlar, ECC'nin başlangıç noktasını kayıp olmadan kullanıcılar arasında paylaşmaya olanak tanır [11].

Zhang, ECC'yi temel alarak bir dijital görüntü şifreleme tekniği önermiştir. Bir eliptik eğri, açık ve gizli anahtarların hesaplanması için seçilir. PWLCM (Parçalı Doğrusal Kaotik Harita; Piecewise Linear Chaotic Map) adımına kadar iterasyonlar uygulandıktan sonra, kaotik bir dizi elde edilir. Bir kaotik görüntü, bu kaotik diziden elde edilir. Kaotik görüntüden pikseller gruplandırılarak büyük tamsayılar oluşturulur. Büyük tamsayılar, ECC kullanılarak şifrelenir [12].

Ibrahim; Henon haritası, dinamik S-kutuları (S-Boxes) ve ECC kullanarak bir görüntü şifreleme yöntemi önermiştir. Güvenli dinamik S-kutuları oluşturmak için Henon haritasına dayanan bir algoritma önerilmiştir. Dinamik S-kutuları, bazı güvenlik algoritmalarının karışımı nedeniyle seçilmiş düz metin saldırılarına karşı dirençli bir görüntü şifreleme yöntemi oluşturmak için kullanılır. Algoritmada güvenlik ataklarına karşı dirençli olmak adına gizli anahtar, ECC kullanılarak oluşturulur [13].

Hafsa, AES (Gelişmiş Şifreleme Standardı; Advanced Encryption Standard) ile ECC'yi birleştiren bir şifreleme yöntemi önermiştir. Bu nedenle, hızlı şifreleme avantajına sahip ve oturum anahtarını güvenli bir şekilde değiştirmenin avantajına sahip bir asimetrik şifreleme önerilmiştir. Bu çalışmada, yeni bir ECC donanım mimarisi ve yeni bir AES algoritması sunulmaktadır [14].

Parida, ECC ve kaotik haritaları kullanarak bir görüntü şifreleme yöntemi önermiştir. Sunulan şema, ECDH (Eliptik Eğri Diffie Hellman; Elliptic Curve Diffie Hellman) anahtar değişimi; şifreleme, şifre çözme ve şifreli verilerin imzalanması olmak üzere üç aşamaya ayrılmıştır. Şifreleme, tek pikseller yerine piksel bloklarında gerçekleştirilir. Şifreleme verimliliğini ve hızını artırmak için genişletilmiş ElGamal şifreleme kodu kullanır. Anahtar değişimi, ECDH anahtarları ve bunların gizli ve açık anahtar çiftleri hesaplanarak gerçekleştirilir [15].

Laiphrakpam, ECC ile geliştirilmiş bir ElGamal şifreleme yöntemi temelinde, tıbbi görüntüler için yeni bir şifreleme yöntemi önermiştir. Bu yöntem, orijinal bir görüntüyü şifrelemek için Koblitz kodlama tekniği yerine bir eliptik eğri koordinatına kodlamak amacıyla geliştirilmiş bir ElGamal tekniği kullanır. Bu nedenle, kodlama süreci hızlı gerçekleştirilir [16].

Azam, Mordell eliptik eğrilerini kullanan yeni bir görüntü şifreleme yöntemi önermiştir. Bu çalışmada, gönderici ve alıcı taraf bir eliptik eğri seçer. Daha sonra, sözde rasgele sayılar ve eliptik eğriler üzerinde dinamik bir S-kutusu kullanılarak pikseller maskelenip karıştırılır [17].

Jasra, görüntüleri eliptik eğriler üzerine eşlemeye yardımcı olan birkaç yöntem sunmuştur. Bu çalışmada, bir eşleme tekniğinin etkinliğini etkileyen parametreler incelenmiştir.

Bunlar arasında eşlemenin tamamlanma durumu, tersine çevrilebilirlik, bant genişliği/kullanılan bit sayısı, zaman ve maliyet etkinliği bulunmaktadır. Başlangıç noktasına dayalı eşleme, piksel sayısına oranla noktaların haritalandırılması, Koblitz yöntemi ve piksel gruplandırılması bu yöntemlerden bazılarıdır. Bu yöntemlerin avantajları ve dezavantajları söz konusu çalışmada sunulmuştur [18].

Gupta, görüntü şifrelemek için ECC kullanarak performans analizi ve diğer algoritmalarla karşılaştırma yaptığı bir çalışma sunmuştur. Bu makalede, anahtar değişimi olarak Diffie-Hellman anahtar değişim protokolü uygulanmıştır. Farklı boyutlardaki görüntüler, ECC kullanılarak şifrelenmiştir. Farklı boyuttaki görüntüler için, şifreleme süresi, şifre çözme süresi, güç tüketimi ve şifrelemeden sonra görüntü boyutu gibi analizler de makalede sunulmuştur [19].

Wu, simetrik bir görüntü şifreleme algoritması önermiştir. ECC ve kaotik sistem temelli olan bu algoritma, renkli görüntülerin şifrelenmesi için kullanılabilmektedir [20].

Bu tez kapsamında eliptik eğri kriptografisi kullanılarak dijital görüntü şifreleme algoritmasına yönelik yeni bir yöntem geliştirilmiştir. Literatürdeki çalışmalar ayrıntılı olarak incelenip avantajları ve dezavantajları ortaya çıkarılmıştır. Geliştirilen algoritmada, literatürdeki çalışmalara alternatif bir şifreleme yöntemi sunulmuştur. Sunulan yöntem, literatürdeki benzer algoritmalardan daha hızlı, daha güvenilir, daha doğru sonuçlar veren bir algoritmaya sahiptir.

Önerilen algoritmada renkli dijital görüntüyü şifrelemek için eliptik eğri kriptografisi kullanılmıştır. Anahtar değişimi için Diffie-Hellman anahtar değişim protokolü kullanılmıştır. Önerilen algoritmada görüntü şifreleme ve şifreli görüntüyü çözme işleminin çok zaman almaması için eliptik eğri nokta çarpım işlemleri diğer algoritmalara göre daha az kullanılmıştır. Şifreleme ve şifre çözme işleminin büyük bir kısmı XOR operasyonuyla yapıldığı için önerilen algoritma, literatürdeki diğer çalışmalara göre daha hızlı çalışmaktadır.

2. TEMEL KAVRAMLAR

Bu bölümde kriptografi ile ilgili temel kavramlar sunulmuştur. Yapılan çalışmada önerilen uygulamanın daha iyi anlaşılabilmesi için gerekli terimler açıklanmıştır. Açıklanan konular arasında kriptoloji, kriptoanaliz, kriptografi, simetrik şifreleme, asimetrik şifreleme, Diffie-Hellman anahtar değişimi, XOR operasyonu ve sözde rasgele sayı üreteçleri yer almaktadır.

2.1. Kriptoloji

Kriptoloji, mesajların şifrelenmesi ve şifreli mesajların çözülmesi amacıyla matematiksel yöntemlerin kullanıldığı bir bilim dalıdır. Kriptoloji, genellikle kriptografi ve kriptoanaliz olmak üzere iki ana alt bölümde incelenir [21].

Kriptoloji, matematik biliminin önemli konularını içeren bir disiplindir. Sayılar teorisi, asal sayılar, gruplar, halkalar, cisimler, çarpanlara ayırma, matrisler ve modüler aritmetik gibi matematiksel kavramlar, kriptolojinin temel altyapısını oluşturur.

Kriptografi, mesajların gizliliğini sağlamak amacıyla matematiksel yöntemlerin tasarımı ve analizi ile ilgilenen bir alandır. Bu, kriptograflar tarafından gerçekleştirilir ve iletilen bilgilerin güvenli bir şekilde iletilmesini sağlar.

Diğer yandan, kriptoanaliz, şifrelenmiş mesajın anahtar bilinmeksizin şifreyi çözme teknikleriyle ilgilenen bir bilim dalıdır. Kriptoanalistler, şifreleme yöntemlerini kırma ve şifreli bilgilere erişim sağlama konusunda çalışırlar.

2.1.1. Kriptografi

Güvensiz bir iletişim kanalı üzerinden güvenli bir şekilde iletişim sağlamak için, kullanıcılar arasında iletilen mesajlar şifrelenir [21].

Temel bir kriptografi sisteminde aşağıda belirtilen unsurlar bulunur:

1. Şifrelenmemiş düz metin (plaintext) M

2. Şifreleme işlemi sonucunda elde edilen şifreli metin (ciphertext) *C*
3. Anahtar (key) *k*
4. Şifreleme yapan taraf *A*
5. Şifre çözme işlemi yapan taraf *B*
6. Düz metne ulaşmaya çalışan yetkisiz taraf *E*
7. Güvenli kanal
8. Güvenli olmayan kanal

A tarafından şifrelenen mesajın *B* tarafında çözülmesi, her iki kullanıcının da aynı *k* anahtarına sahip olmasını gerektirir. Bu *k* anahtarının güvenli bir kanal aracılığıyla *A*'dan *B*'ye iletilmesi gerekir.

A, şifrelenmiş mesajı şifreleyerek güvenli olmayan bir iletişim kanalı üzerinden *B*'ye gönderir. *B*, şifreli metni çözmek için gerekli olan *k* anahtarına sahipse, şifre çözme yöntemiyle şifreli metni çözerek *M* düz metnini elde eder. Kötü niyetli saldırgan *E*, iki taraf arasındaki iletişimi dinlemek ve bilgilere erişmek için çeşitli yöntemler kullanır. *E*, şifreli metni çözmek için *k* anahtarına sahip olmalıdır. Ancak *k* anahtarı güvenli bir iletişim kanalı üzerinden iletilir, bu nedenle *E*'nin bunu ele geçirmesi zordur.

Anahtar dağıtımı, kriptografi sistemlerinde son derece kritik bir konudur. *A* ve *B* gibi iki taraf, gizli bir şekilde anahtarlarını paylaşabilir veya matematiksel yöntemlerle uygun bir anahtar seçebilirler. Bu nedenle anahtar dağıtım algoritması, kriptografi sisteminin temel bir bileşeni olarak büyük bir öneme sahiptir [22].

Kriptografi sistemlerinde dikkate değer başka bir husus, şifreleme ve şifre çözme algoritmalarının herkes tarafından bilinmesidir (Kerckhoff kanunu). Algoritmaların gizliliğinin, kriptografi sisteminin güvenliğini artıracağı açıktır, ancak gizli algoritmaların test edilmediği bir duruma işaret eder. Bir kriptografi sisteminin dayanıklılığını değerlendirmenin yollarından biri, algoritmanın herkese açık hale getirilip diğer kriptograflar ve kriptoanalistler tarafından analiz edilmesidir.

Kötü niyetli *E*'nin anahtarı ele geçirmesi durumunda, algoritmanın herkes tarafından bilinmesi nedeniyle şifreli mesajı kolayca çözebileceğine dikkat çekilmektedir. Ancak bu senaryoda gizlilik problemine odaklanılsa da, güvenli bir kriptografi sistemi tasarımının

daha fazla unsuru vardır. Bu unsurlar arasında, mesajın eksiksiz bir şekilde iletilmesini engellemek (mesaj bütünlüğü), bir mesajın gerçekten belirli bir kaynaktan geldiğini doğrulamak (kimlik doğrulaması) ve gönderen tarafından gönderilen bir mesajın inkar edilemeyeceğini sağlamak gibi özellikler bulunmaktadır.

Yukarıda özetlenen senaryolar, *A* ve *B* arasında güvenli bir iletişim kurmak için kriptografi sistemlerinin tasarımında dikkate alınması gereken temel unsurları belirtir. Bu unsurlar aynı zamanda kriptografi sistemlerinin temel amaçlarıdır. Bu amaçlar aşağıda açıklanmıştır:

1. Gizlilik (Privacy/Confidentiality): Gizlilik, gönderilen şifrelenmiş mesajın sadece yetkili kişiler tarafından okunabilmesini sağlar. Örneğin, *A* tarafından gönderilen mesajın kötü niyetli üçüncü bir kişi olan *E* tarafından okunamaması gizlilik sayesinde sağlanır.
2. Bütünlük (Integrity): Bu, gönderilen mesajın yetkisiz kişiler tarafından değiştirilemeyeceğini garanti eder. *A*'nın gönderdiği mesajın *E* tarafından değiştirilip değiştirilmediğini *B* tespit edebilir.
3. Kimlik denetimi (Authentication/Identification): Kimlik denetimi, *B*'nin alınan mesajın gerçekten doğru bir kaynaktan geldiğini doğrulamasını sağlar. *B*, *A* tarafından gönderildiği iddia edilen şifrelenmiş mesajın gerçekten *A* tarafından gönderildiğini doğrulayabilmelidir.
4. İnkar edilemezlik (Non-repudiation): Bu, gönderilen şifreli mesajın gönderen tarafından inkar edilemeyeceği anlamına gelir. *A*'dan gelen bir mesajın, *B* tarafından alındığı ve gerekirse tarafsız bir üçüncü kişinin de ikna edilebildiği durumlar da dahil olmak üzere inkar edilememesi önemli bir husustur.

Bu unsurlar, kriptografi sistemlerinin tasarımında büyük önem taşırlar ve güvenli iletişimi sağlamanın temel taşlarıdır.

2.1.2. Kriptoanaliz

Kriptoanaliz, kriptografi sistemlerinin şifresini çözme bilimidir ve genellikle istihbarat faaliyetlerinde veya yüksek güvenlik gerektiren iletişimlerde kullanılır. Ayrıca, kriptografi sistemlerinin güvenilirliğini değerlendirmek için kritik bir öneme sahiptir. Kötü niyetli saldırganlar, kriptografi sistemlerini çözmek amacıyla çeşitli kriptoanaliz yöntemleri

kullanırlar. Eğer bir kriptografi sistemi bu tür saldırılara karşı başarılı bir şekilde dayanabilirse, güvenilir bir kriptografi sistemi olarak kabul edilir [23].

Kriptoanaliz farklı yöntemlerle gerçekleştirilebilir ve genellikle dört ana kategoriye ayrılır:

Klasik kriptoanaliz: Bu, şifrelenmiş metinden açık metni veya şifreleme için kullanılan gizli anahtarı elde etme bilimidir.

Analitik saldırılar: Kriptografi sisteminin matematiksel yapısını inceleyen ve bu bilgiye dayalı olarak saldırılar gerçekleştiren yöntemlerdir. Bu tez kapsamında, klasik kriptoanaliz uygulamaları, konuyla yakından ilgili olduğu için dördüncü bölümde ayrıntılı olarak anlatılmıştır.

Uygulama saldırıları: Bu tür saldırılar genellikle fiziksel sistemlere odaklanır. Örneğin, yan kanal analizi ile bir işlemcinin elektriksel güç tüketimi ölçülerek gizli anahtar elde edilebilir. Ayrıca, elektromanyetik radyasyon veya algoritmaların çalışma zamanındaki davranışı gibi fiziksel özellikler kullanılarak da gizli anahtar hakkında bilgi elde edilebilir.

Sosyal mühendislik saldırıları: Günümüzde oldukça yaygın kullanılan bir kriptoanaliz yöntemidir. Bu tür saldırılarda, kullanıcıların dikkatsizlik, dalgınlık veya bilgi eksikliği gibi zayıf noktaları kullanılarak kriptografi sisteminin gizli anahtarı elde edilebilir.

Bu kriptoanaliz yöntemleri, kriptografi sistemlerinin güvenliğini test etmek ve olası zayıf noktaları belirlemek için kullanılır.

2.2. Simetrik Şifreleme

Simetrik şifreleme, aynı anahtarın hem şifreleme hem de şifre çözme işlemlerinde kullanıldığı bir şifreleme yöntemidir. Bu, bilgiyi güvenli bir şekilde iletmek veya depolamak için kullanılan anahtarın, gönderen ve alıcı arasında paylaşıldığı anlamına gelir. Bu yöntemde şifreleme ve şifre çözme için kullanılan anahtar gizli anahtardır. Anahtar üçüncü bir tarafla paylaşılmaz.

Simetrik şifreleme, işlemleri hızlı bir şekilde gerçekleştirebilir. Bu, büyük veri setleriyle çalışırken performans avantajı sağlar. Doğru şekilde uygulandığında, simetrik şifreleme yüksek düzeyde güvenlik sağlar. Anahtarın gizli kalması durumunda, şifreli verinin çözülmesi zordur.

2.3. Asimetrik Şifreleme

Asimetrik şifreleme, farklı anahtarların kullanıldığı bir şifreleme yöntemidir. Açık anahtar (public key) ve özel anahtar (private key) olmak üzere iki anahtar bulunur. Açık anahtar, veriyi şifrelemek için kullanılırken, özel anahtar şifreyi çözmek için kullanılır. Bu yöntemde taraflardan biri açık anahtarını açık bir şekilde paylaşır, ancak özel anahtar sadece sahibi tarafından bilinir. Gönderen, alıcının açık anahtarını kullanarak veriyi şifreler ve sadece alıcı, şifreli veriyi özel anahtarıyla çözebilir.

Asimetrik şifrelemede açık anahtarlar açıkça paylaşılır ve bu durum, anahtar yönetimini kolaylaştırır. İki taraf arasında güvenli bir şekilde anahtar değişimi yapılabilir ve bu sayede açık anahtarlar kullanılarak asimetrik şifreleme yapılmış olur. Ayrıca asimetrik şifreleme, dijital imza oluşturmak için de kullanılabilir.

2.4. Diffie-Hellman Anahtar Değişimi

Diffie-Hellman anahtar değişimi, iki taraf arasında güvenli bir şekilde anahtar paylaşma protokolüdür. Bu protokol, iki tarafın açıkça paylaşılan bir ortamda, her birinin gizli anahtarını kullanarak ortak bir gizli anahtar oluşturmasına olanak tanır. Bu ortak anahtar, daha sonra şifreleme anahtarı olarak veya diğer güvenlik amaçları için kullanılabilir. Bu protokol, 1976 yılında Whitfield Diffie ve Martin Hellman tarafından icat edilmiştir ve modern kriptografinin temel yapı taşlarından biridir [21].

Bu yöntem, iki tarafın, güvenli bir iletişim kanalı olmayan açık bir ağ üzerinden birbirleriyle gizli bir anahtar paylaşmalarına olanak tanır. Bu, sonraki iletişimde simetrik şifreleme algoritmasında kullanılmak üzere ortak bir gizli anahtarın oluşturulmasını sağlar.

Diffie-Hellman anahtar değişimi protokolü aşağıdaki şekilde gerçekleştirilir:

1. p büyük bir asal sayı ve $\alpha \in \mathbb{Z}_p^*$ bir ilkel kök olsun. Bu parametreler kamuya açık bir şekilde paylaşılabilir.
2. A, $0 \leq a \leq p$-2 şartını sağlayan rasgele gizli bir a değeri seçer. Daha sonra $\alpha^a \pmod p$ değerini hesaplayarak B'ye gönderir.
3. B, $0 \leq b \leq p$-2 şartını sağlayan rasgele gizli bir b değeri seçer. Daha sonra $\alpha^b \pmod p$ değerini hesaplayarak A'ya gönderir.
4. A, B tarafından gönderilen α^b değerini kullanarak ortak anahtar $K=(\alpha^b)^a$ değerini hesaplar.
5. Benzer şekilde B, A tarafından gönderilen α^a değerini kullanarak ortak anahtar $K=(\alpha^a)^b$ değerini hesaplar.
6. Böylece her iki taraf da ortak anahtar $K=(\alpha^b)^a=(\alpha^a)^b$ değerini elde etmiş olur.

Bu adımlar sonucunda, her iki taraf aynı ortak gizli anahtara sahip olur. Diffie-Hellman anahtar değişim protokolünde herhangi bir mesaj şifrelenmez, sadece taraflar ortak bir gizli anahtar üzerinde anlaşma sağlamış olur.

2.5. XOR Operasyonu

Şifreleme süreçlerinde XOR operasyonu, temel ve etkili bir matematiksel operatördür ve birkaç önemli özellik sunar. Bu özellikler, XOR operasyonunun şifreleme alanında neden tercih edildiğini anlamamıza yardımcı olur:

Basit ve hızlı işlem: XOR operasyonu, işlemcinin bellek üzerindeki iki bit dizisini hızlı ve basit bir şekilde karşılaştırmasını sağlar. Bu özellik, XOR operasyonunun donanım seviyesinde hızlı bir şekilde uygulanabilmesine izin verir.

Geri çevrilebilirlik: XOR operasyonu, aynı anahtarla geri çevrilebilir bir işlemdir. Yani, aynı XOR işlemi ve aynı anahtar kullanılarak orijinal veriye geri dönmek mümkündür. Bu özellik, şifreleme ve şifre çözme işlemlerinde kullanılan matematiksel işlemlerde önemli bir avantaj sağlar.

Anahtar bağımlılığı: XOR operasyonu, hassas anahtar bağımlılığı yoluyla güvenlik ekler. Anahtarın küçük bir miktarda değiştirilmesi, XOR operasyonunun sonucunu çok büyük ölçüde değiştirir. Bu da güvenlik açısından avantaj sağlar.

Doğrusal olmaması: XOR operasyonu, doğrusal olmayan bir matematiksel işlemdir. Bu, şifreleme algoritmalarında daha karmaşık yapılar oluşturmak için kullanılabilir ve kriptoanaliz saldırılarına karşı direnç ekler.

2.6. Sözde Rasgele Sayı Üreteçleri

Sözde rasgele sayı üreteçleri, tamamen rasgele veya önceden belirlenmiş bir dağılıma sahip sayıları üretebilen matematiksel modellerdir. Bilgisayar biliminde, bu sayılar genellikle sözde rasgele sayılar (pseudorandom) olarak adlandırılır. Çünkü gerçekten tamamen rasgele olmamalarına rağmen, pratikte rasgele gibi davranırlar. Sözde rasgele sayı üreteçleri, şifreleme süreçlerinde kullanılan anahtarlar, oturum anahtarları ve diğer kriptografik unsurları oluşturmak için yaygın olarak kullanılır [24].

Sözde rasgele sayı üreteçlerinin kriptografideki rollerinden bazıları şunlardır:

Anahtar üretimi: Şifreleme algoritmaları, iletilen verilerin güvenliği için anahtarlar kullanır. Sözde rasgele sayı üreteçleri, bu anahtarları oluşturmak için kullanılır. Güçlü bir anahtar, tahmin edilemez ve kuvvetli bir sözde rasgele sayı üreteci, bu gereksinimleri karşılamak için ideal bir araçtır.

Saat dalgası saldırılarına karşı koruma: Zayıf sözde rasgele sayı üreteçleri, saldırganların şifreleme sistemine müdahale etmelerine olanak tanır. Saat dalgası saldırıları gibi zamanla yapılan saldırıları önlemek için, sözde rasgele sayı üreteçleri, her seferinde farklı ve öngörülemeyen değerler üretmelidir.

Önemli sayıların oluşturulması: Kriptografik işlemler sırasında kullanılan rasgele sayılar, özellikle büyük asal sayılar gibi önemli matematiksel yapıların oluşturulmasında kullanılır. Bu sayılar, şifreleme algoritmalarının dayandığı matematiksel karmaşıklığı artırarak güvenlik seviyelerini yükseltir.

Sözde rasgele sayı üreteçleri, şifreleme dünyasında güvenliği artırmakta ve siber tehditlere karşı koruma sağlamakta kritik bir rol oynamaktadır. Bu üreteçlerin doğru bir şekilde tasarlanması ve uygulanması, şifreleme sistemlerinin güvenliğini arttırabilir ve hassas

bilgilerin korunmasına katkıda bulunabilir. Bu nedenle sözde rasgele sayı üreteçleri dikkatlice seçilmeli ve uygulanmalıdır.

3. ELİPTİK EĞRİ KRİPTOGRAFİSİ VE GÜVENLİK ATAKLARI

Bu bölümde, eliptik eğri kriptografisi ile ilgili kavramlar ve kriptoanaliz yöntemleri olan güvenlik atakları anlatılmıştır.

3.1. Temel Cebir İfadeleri

Bu bölümde eliptik eğrilerin kriptografi işlemlerinde kullanılmasını daha anlaşılır bir şekilde açıklamak için ikili işlem, grup, cisim, halka, sonlu cisim, asal cisim gibi soyut cebir kavramlarını içeren temel matematiksel ifadeler sunulmuştur.

3.1.1. Tanım

A boş olmayan bir küme olsun. AxA'dan A'ya bir * fonksiyonuna A'da bir ikili işlem ve (A,*) ikilisine de bir cebirsel yapı denir [21, 25].

i) $\forall a,b \in A$ için A'da bir $a*b$ elemanı vardır. Bu özelliğe kapalılık özelliği denir.
ii) Bu eleman tek türlü olarak belirlidir. Bu özellik ise iyi tanımlılık olarak adlandırılır.

3.1.2. Tanım

G boş olmayan bir küme ve *, G kümesi üzerinde tanımlı bir ikili işlem olsun. (G,*) cebirsel yapısı aşağıdaki özellikleri sağlıyorsa grup olarak ifade edilir [21, 25].

i) *, G'de bir ikili işlemdir.
ii) * işleminin G'de birleşme özelliği vardır. $\forall a,b,c \in G$ için, $a*(b*c)=(a*b)*c$ eşitliği sağlanır.
iii) * işleminin, G'de birim elemanı vardır. $\forall a \in G$ için, $a*e=e*a=a$ eşitliğini sağlayacak $\exists e \in G$ tanımlıdır.
iv) * işlemine göre, G'deki her elemanın tersi vardır. $a \in G$ için, $a*a^{-1}=a^{-1}*a=e$ eşitliğini sağlayacak $\exists a^{-1} \in G$ bulunabilir.

3.1.3. Tanım

(G,*) bir grup olmak üzere, $\forall a,b \in G$ için $a*b=b*a$ değişme özelliğini sağlayan gruba, değişmeli grup veya Abel grup denir. Değişmeli gruplarda işlem + ise toplamsal grup denir. Eğer grubun işlemi · ise çarpımsal grup olarak ifade edilir [21, 25].

3.1.4. Tanım

G sonlu bir küme ise, yani G'nin eleman sayısı sonlu ise, (G,*) grubuna bir sonlu grup denir. Bu sonlu grubun eleman sayısına da grubun mertebesi denir [21, 25].

3.1.5. Tanım

R boş olmayan bir küme ve bu küme üzerinde tanımlı iki ikili işlem + ve · olsun. (R, +, ·) ikili işlemli cebirsel yapısı aşağıdaki özellikleri sağlıyorsa halka olarak ifade edilir [21, 25].

i) (R,+) bir değişmeli gruptur.
ii) · işleminin R'de birleşme özelliği vardır.
iii) · işleminin + işlemi üzerinde sağdan ve soldan dağılma özelliğine sahiptir. Böylece, $\forall a,b,c \in R$ için, $a.(b+c)=a.b+a.c$ ve $(a+b).c=a.c+b.c$ eşitlikleri sağlanır.

R halkasının + işlemine göre etkisiz elemanına halkanın sıfır elemanı denir ve 0_R ile gösterilir. Halkanın · işlemine göre etkisiz elemanı olmayabilir. Eğer varsa bu halkaya birimli halka denir ve birim eleman 1_R ile gösterilir. Bununla birlikte halka, · işlemine göre değişme özelliğine sahipse değişmeli halka olarak ifade edilir [21, 25].

3.1.6. Tanım

R, birimli ve değişmeli bir halka olsun. $R^*=R-\{0_R\}$ ikinci işlem olan · işlemine göre bir grup ise R bir cisim olarak tanımlanır. Bir cismin sıfırdan farklı her elemanının çarpımsal tersi vardır ve tektir. Bir cisim halkanın özel bir hali olup birimli, değişmeli ve sıfırdan farklı her elemanının tersi olan bir halkadır [21, 25].

3.1.7. Tanım

Sonlu sayıda elemanı bulunan cisimler sonlu cisim olarak ifade edilir. Sonlu cisim F ile gösterilir. Bu sonlu cisim üzerinde + ve · ikili işlemlerini barındırır ve aşağıdaki özellikleri sağlar [21, 25].

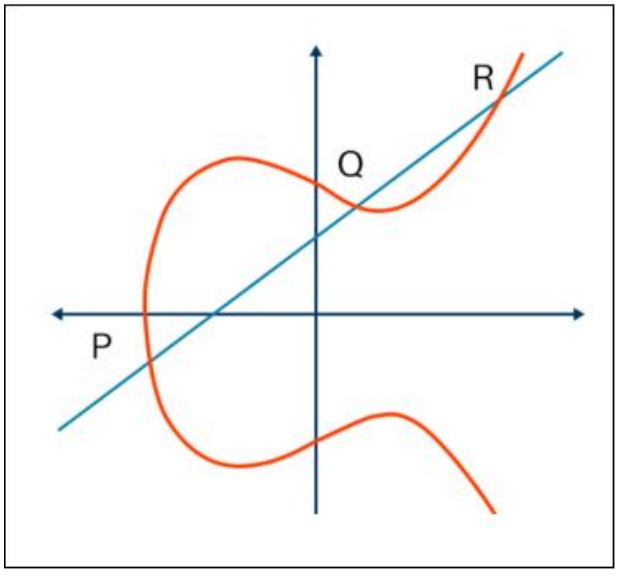
i) $(F,+)$ bir değişmeli gruptur.
ii) · işlemi, + işlemi üzerinde sağdan ve soldan dağılma özelliğine sahiptir. Böylece, $\forall a,b,c \in R$ için, $a.(b+c)=a.b+a.c$ ve $(a+b).c=a.c+b.c$ eşitlikleri sağlanır.
iii) $(F-\{0\},\cdot)$ bir değişmeli gruptur.

3.1.8. Tanım

p asal bir sayı olsun. $\{0,1,2,3,....,p-1\}$ tamsayı kümesi modüler (mod p) + ve · işlemlerine göre cisim özelliğini sağlar. Bu cisme sonlu asal cisim denir ve F_p ile ifade edilir [21, 25].

3.2. Eliptik Eğri

Eliptik eğri, matematikte kullanılan bir kavramdır. Bir eliptik eğri, iki boyutlu bir eşitlikle tanımlanır ve genellikle $y = f(x)$ şeklinde gösterilir [21]. Şekil 3.1'de örnek bir eliptik eğri bulunmaktadır.



Şekil 3.1. Eliptik Eğri

Eliptik eğri nokta toplamı

Bir $y^2 \equiv x^3+ax+b \pmod{p}$ E eliptik eğrisi üzerinde $P(x_1,y_1)$ ve $Q(x_2,y_2)$ iki nokta olsun. İki noktanın toplamında $P(x_1,y_1)+Q(x_2,y_2)=R(x_3,y_3)$ işlemi ile elde edilen üçüncü bir nokta $R(x_3,y_3)$ olsun. Eğer $P \neq Q$ ise $R(x_3,y_3)$ noktasındaki x_3 ve y_3 Eş. 3.1 ve Eş. 3.2'deki gibi hesaplanır. Eğer $P=Q$ ise $R(x_3,y_3)$ noktasındaki x_3 ve y_3 Eş. 3.3 ve Eş. 3.4'teki gibi hesaplanır [21].

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \tag{3.1}$$

$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1 \tag{3.2}$$

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \tag{3.3}$$

$$y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1 \tag{3.4}$$

Burada a, E eliptik eğrisindeki a parametresidir.

3.3. Eliptik Eğri Kriptografisi

Eliptik eğriler, kriptografi alanında oldukça fazla kullanılır. Özellikle, asimetrik kriptografi algoritmaları ve simetrik kriptografi algoritmalarının bir kısmı eliptik eğriler üzerinde çalışır. Bu algoritmalar, verileri şifrelemek ve şifreyi çözmek için güçlü bir güvenlik sağlar [21].

Eliptik eğri kriptografisi, kriptografi alanında son yıllarda oldukça popüler hale gelen bir yöntemdir. Eliptik eğri kriptografisi, genelde açık anahtar kriptografisi yöntemi olarak kullanılır. Bu yöntem, verileri şifrelemek ve şifreyi çözmek için iki farklı anahtar kullanır. Bunlardan birisi şifreleme için kullanılan açık anahtar, diğeri ise şifreyi çözmek için kullanılan özel anahtardır.

ECC, RSA (Rivest-Shamir-Adleman) gibi algoritmalardan farklı olarak, verileri şifrelemek için eliptik eğriler üzerinde çalışır. ECC sistemi RSA sistemine göre daha kısa anahtar uzunluğuyla aynı korumayı sağlayabilmektedir. ECC, RSA algoritmasına kıyasla daha az bit gerektirir ve dolayısıyla daha az işlem gücüne ihtiyaç duyar. Bu nedenle, ECC, mobil cihazlar ve nesnelerin interneti (IoT; Internet of Things) cihazlar gibi düşük güçlü cihazlarda daha iyi sonuçlar verebilir. Ayrıca ECC, RSA algoritmasına göre daha az yer kaplar ve dolayısıyla daha az bellek gerektirir.

Eliptik eğri kriptografisi, 1985 yılında Neal Koblitz ve Victor Miller tarafından keşfedilmiştir [26, 27]. Bu iki matematikçi, eliptik eğrilerin kriptografik uygulamalarda kullanılabileceğini ilk kez ortaya koymuşlardır. Eliptik eğriler, 1980'lerin başında bilim adamları tarafından araştırılmış olsa da, kriptografik uygulamalar için kullanılması konusunda ilk öneri Koblitz ve Miller tarafından yapılmıştır. 1990'lı yıllarda, eliptik eğri kriptografisi, özellikle dijital imza ve anahtar değişim gibi uygulamalar için kullanılmaya başlanmıştır. 2000'li yılların başında ise eliptik eğri kriptografisi, internet güvenliği ve mobil cihazlar gibi alanlarda da sıklıkla kullanılmaya başlanmıştır. Son yıllarda, eliptik eğri kriptografisi ile ilgili yapılan araştırmalar ve geliştirmeler, bu yöntemin daha da güvenli hale getirilmesine ve daha geniş bir kullanım alanına sahip olmasına olanak sağlamıştır.

Eliptik eğri kriptografisinin yukarıda sayılan avantajlarının olmasının yanı sıra bazı sınırlamaları vardır. Örneğin, ECC algoritmaları, çok büyük verileri şifrelemek için uygun değildir ve ayrıca, ECC algoritmalarının güvenliği, kullanılan eğrinin seçimiyle ilgilidir. Bu nedenle, ECC algoritmalarının kullanımı, uygun bir eğri seçimine bağlı olarak güvenli olabilir.

3.4. Eliptik Eğrilerle Dijital Görüntü Şifreleme

Eliptik eğri kriptografisi, dijital görüntü şifreleme için de kullanılabilen bir yöntemdir. Bu yöntem, görüntü verilerini eliptik eğri üzerinde şifrelemek suretiyle güvenli bir şekilde saklar.

Görüntü şifrelemede, görüntü verileri eliptik eğri üzerinde bir dizi noktaya dönüştürülür. Bu noktalar, şifreleme işlemi sırasında kullanılan anahtar değerine göre seçilir. Şifrelenmiş

veriler, sadece anahtarı bilen kişiler tarafından çözülebilir. Bu yöntem, görüntülerin güvenli bir şekilde saklanmasını ve güvenli bir şekilde iletilebilmesini sağlar.

3.5. Güvenlik Atakları

Bu bölümde güvenlik ataklarıyla ilgili bilgilere yer verilmiştir.

3.5.1. Bilinen düz metin saldırısı (Known plain text attack)

Bilinen düz metin saldırısında, saldırgan şifreleme anahtarını bulmak için açık metin ve şifreli metin arasındaki ilişkiyi kullanır [28, 29].

Bilinen düz metin saldırısı gerçekleştirmek için saldırgan, şifreleme algoritmasının çıktısındaki deseni ve veriyi analiz eder. Ardından, açık metin ve şifreli metin arasındaki ilişkileri çıkararak şifreleme anahtarını tahmin etmeye çalışır. Eğer saldırgan, doğru şifreleme anahtarını tahmin ederse, şifreli metni çözmek ve orijinal açık metni elde etmek mümkün olur.

Bilinen düz metin saldırıları, güvenli ve güçlü şifreleme algoritmalarına karşı uygulaması zor olan saldırılar arasındadır. Güçlü şifreleme algoritmaları, bu tür saldırılara dayanıklı olacak şekilde tasarlanır ve bilinen düz metin-şifreli metin çiftlerine dayanarak şifreleme anahtarını tahmin etmeyi zorlaştırır.

3.5.2. Sadece şifreli metin saldırısı (Cipher text only attack)

Sadece şifreli metin saldırısı, şifreleme algoritmasının güvenliğini etkilemek için sadece şifreli metni kullanır. Bu durumda, saldırganın elinde açık metin yoktur ve sadece şifreli metni inceleyerek şifreleme anahtarını bulmaya çalışır.

Sadece şifreli metin saldırısı gerçekleştirmek için saldırgan, şifreli metindeki deseni ve veriyi analiz eder. Ancak saldırganın elinde açık metin olmadığından, anahtar hakkında doğrudan bilgiye sahip değildir. Bu nedenle, sadece şifreli metin saldırısı, bilinen düz metin saldırısı gibi açık metin-şifreli metin çiftlerine dayanarak çalışan saldırılara göre daha zorlayıcıdır [30, 31].

3.5.3. Seçilmiş düz metin saldırısı (Chosen plain text attack)

Seçilmiş düz metin saldırısında, saldırganın şifreleme algoritmasına erişebildiği varsayılmaktadır. Saldırgan, şifreleme anahtarını bulmak için kendi seçtiği açık metinleri şifreleyip buna karşılık gelen şifreli metinleri elde eder [31, 32].

3.5.4. Anahtar uzayı (Key space)

Anahtar uzayı, şifreleme algoritmalarında kullanılan şifreleme anahtarlarının oluşturulabilecek tüm kombinasyonlarının sayısını ifade eden terimdir [28, 33].

Anahtar uzayı, şifreleme algoritmasının güvenliği ve kriptografik direnç açısından önemlidir. Anahtar uzayının büyüklüğü, bir saldırganın şifreleme algoritmasını kaba kuvvet saldırılarıyla kırmaya çalıştığı durumda geçerli anahtarı tahmin etme olasılığını belirler. Yani, anahtar uzayı ne kadar büyük olursa, kaba kuvvet saldırılarının başarılı olma olasılığı o kadar düşer.

Anahtar uzayı, anahtarın uzunluğuna ve kullanılan karakter kümesine bağlıdır. Örneğin, bir şifreleme algoritması 128 bit uzunluğunda anahtar kullanıyorsa, anahtar uzayı 2^{128} kombinasyonu içerir. Bu durumda, kaba kuvvet saldırılarıyla doğru anahtarı bulmak, 2^{128} kadar kombinasyonu denemek anlamına gelir. Böyle bir saldırıyla doğru anahtarı bulmak, günümüz bilgisayarlarında çok uzun süreceğinden, bu algoritma anahtar uzayı açısından güvenilirdir denebilir.

3.5.5. Kaba kuvvet saldırısı (Brute force attack)

Kaba kuvvet saldırısı şifreleme anahtarını bulmak için olası tüm kombinasyonları denemeye dayanan bir saldırı yöntemidir [28, 31].

Kaba kuvvet saldırısı, temel olarak bir deneme-yanılma yöntemidir ve tüm kombinasyonlar denendiği için çok zaman alabilir. Anahtar uzayının büyüklüğüne bağlı olarak bazen günler, haftalar veya yıllar sürebilir. Bu nedenle, güvenli şifreleme algoritmaları için genellikle kaba kuvvet saldırısı gibi saldırı türlerine karşı dayanıklı olacak şekilde tasarlanır ve anahtar uzayı mümkün olduğunca büyük yapılır.

3.5.6. Sözlük saldırısı (Dictionary attack)

Sözlük saldırısı, şifreleme anahtarını bulmak için bir sözlük veya kelime listesi kullanan bir saldırı türüdür. Özellikle kullanıcıların kriptografik açıdan zayıf veya kolay tahmin edilebilir şifreler kullandığı durumlarda etkili olabilir [31, 34].

Sözlük saldırısı, temel olarak kullanıcıların genellikle yaygın veya basit şifreleri kullanmaya yatkın olduğu gerçeğine dayanır. Saldırgan, bir sözlük veya kelime listesi kullanarak popüler veya yaygın şifre kombinasyonlarını sisteme uygular ve doğru şifreyi bulmaya çalışır. Bu tür saldırılar, kullanıcıların "123456", "password" ve "qwerty" gibi basit şifreler veya yaygın kelimeleri tercih etmeleri durumunda etkili olabilir.

Sözlük saldırısı, kaba kuvvet saldırılarından farklıdır. Kaba kuvvet saldırısı, tüm olası şifre kombinasyonlarını deneyerek şifreleme anahtarını bulmaya çalışırken, sözlük saldırısı belirli bir sözlük veya kelime listesi içinde yer alan şifreleri deneyerek şifreleme anahtarını bulmaya çalışır.

Sözlük saldırısı, güçlü şifrelerle karşı karşıya geldiğinde daha az etkili olur. Güçlü şifreleme algoritmaları, şifreleri tahmin etmeyi zorlaştırmak için gelişmiş güvenlik önlemleri içerir ve kullanıcıların karmaşık ve benzersiz şifreler seçmelerini teşvik eder. Kullanıcıların güçlü şifreler kullanması ve düzenli olarak şifrelerini değiştirmesi, sözlük saldırısından korunmada önemlidir.

3.5.7. Gürültü saldırısı (Noise attack)

Gürültü saldırısı, görüntü şifreleme algoritmalarında kullanılan bir saldırı türüdür. Bu saldırıda, orijinal görüntüye rasgele veya istenmeyen bilgi eklenir. Böylece görüntü bozulur ve şifreleme işleminin işlevi azalır [35, 36].

Gürültü Saldırısı, görüntü şifreleme işlemini etkilemek için farklı şekillerde gerçekleştirilebilir:

Ekleme gürültüsü: Görüntüye rasgele piksel değerleri veya renk değişiklikleri eklenir. Bu durum, görüntüde rasgele noktaların farklı renklere sahip olması veya piksel değerlerinin

sapmasıyla sonuçlanabilir.

Çarpma gürültüsü: Görüntüye rasgele çarpma işlemleri uygulanarak parlaklık ve kontrast gibi özellikler bozulur.

Tuz ve biber (Salt and pepper) gürültüsü: Görüntüde rasgele piksel değerleri siyah veya beyaz renklerle değiştirilir, böylece tuz ve biber benzeri bir desen oluşur.

Gürültü saldırısından korunmak için güvenli ve güçlü şifreleme algoritmalarının kullanılması önemlidir. Ayrıca, görüntü şifreleme algoritmalarında gürültü önleme ve filtreleme teknikleri de kullanılarak gürültü saldırılarına karşı koruma sağlanabilir.

4. DİJİTAL GÖRÜNTÜ ŞİFRELEME

Bu bölümde dijital görüntü şifreleme ile ilgili konular açıklanmıştır.

4.1. Dijital Görüntü

Dijital görüntü, görsel bir sahnenin veya nesnenin dijital bir biçimde temsilidir. Genellikle, dijital görüntünün her pikselinin renk ve parlaklık değerlerine karşılık gelen bir sayı değeri kümesidir. Bu değerler, JPEG, PNG veya TIFF gibi çeşitli dosya formatlarında saklanabilir ve çeşitli yazılım programları ve cihazlar tarafından işlenip çeşitli uygulamalarda kullanılabilir. Dijital görüntüler; dijital kameralar, tarayıcılar ve bilgisayar grafiği yazılımı gibi çeşitli yöntemlerle oluşturulabilir.

Dijital görüntü, piksellerden oluşan iki boyutlu bir dizidir. Her biri kendine özgü bir renk ve parlaklık değerine sahip olan bu pikseller, genellikle kırmızı, yeşil ve mavi (RGB; Kırmızı Yeşil Mavi; Red Green Blue) değerlerinin bir kombinasyonu ile temsil edilir. Parlaklık, renk piksellerinin belirli bir oranda bir araya getirilip birleştirilmesiyle ifade edilir. Dijital görüntünün çözünürlüğü, piksel başına inç (PPI; Pixel per inch) veya nokta başına inç (DPI; Dot per inch) olarak ölçülür. Görüntüdeki piksellerin sayısı, ayrıntı ve netliğin seviyesini belirler. Belirli bir ekrandaki ve görüntüdeki piksel sayısı ile ayrıntı ve netlik arasında doğru orantı vardır [28].

Dijital görüntüler, dosya boyutu azaltılarak daha kolay iletmek ve saklamak için sıkıştırılabilir. Kayıpsız sıkıştırma yöntemleri, PNG gibi, görüntünün tüm orijinal bilgisini ve kalitesini korurken, kayıplı sıkıştırma yöntemleri, JPEG gibi, daha az önemli bilgileri atmak suretiyle daha küçük bir dosya boyutu elde etmeyi amaçlar.

Dijital görüntüler genellikle raster ve vektör türlerine ayrılır. Raster görüntüler, piksel tabanlı olarak oluşturulur ve boyutları değiştirildiğinde kalite kaybına neden olur. Örnekleri: JPEG, PNG, GIF vb. Vektör görüntüleri ise matematiksel formüller kullanarak oluşturulur ve boyutları değiştirildiğinde kalite kaybı olmaz. Örnekleri: SVG, AI, EPS vb.

Raster görüntüler, piksel tabanlı olarak oluşturulur. Bu, görüntü dosyasının her bir pikseli

için renk bilgisi içerdiği anlamına gelir. Örneğin, bir JPEG dosyası, görüntünün her bir pikseli için renk bilgisi içerir. Raster görüntülerin boyutları değiştirildiğinde kalite kaybı olur çünkü pikseller yeniden boyutlandırıldığında ek bilgi kaybedilir.

Vektör görüntüler, matematiksel formüller kullanılarak oluşturulur. Bu, görüntünün her bir parçasının matematiksel olarak tanımlanmasını sağlar. Örneğin, bir SVG dosyası, görüntünün her bir noktasının koordinatlarını içerir. Vektör görüntüler boyutları değiştirildiğinde kalite kaybı olmaz çünkü görüntü, matematiksel olarak yeniden çizilir.

Dijital görüntü türleri

Dijital görüntüler bit sayısına göre temelde 3 gruba ayrılır [31]:

İkili (Binary) görüntüler: İkili görüntüler, her piksel için sadece iki olası değer, genellikle siyah ve beyaz, içeren dijital görüntülerdir. Bu tür görüntüler, her piksel için tek bir bit kullanılarak temsil edilir, 0 siyahı ve 1 beyazı temsil eder. İkili görüntüler, görüntü verilerini basitleştirmek ve işlemek için sıklıkla görüntü işleme ve bilgisayar görüsü uygulamalarında kullanılır. Örneğin, optik karakter tanıma (OCR; Optical Character Recognition) sistemlerinde, ikili görüntüler metni arka plan gürültüsünden ayırmak için kullanılır. Nesne tanıma işlemlerinde, ikili görüntüler nesneleri arka plandan ayırmak için kullanılabilir.

Gri tonlu (Grayscale) görüntüler: Bu tür görüntüleri temsil etmek için gri tonlar kullanılır. Her piksel, siyah (0) ile beyaz (255) arasında bir dizi olası değer alır ve aradaki tüm değerler gri tonları ifade eder. Gri tonlu görüntüler her piksel için 8 bit kullanılarak temsil edilir, 0 ile 255 arasındaki her değer farklı bir gri tonu temsil eder. Gri tonlu görüntüler sıklıkla görüntü işlemede, tıbbi görüntüleme işlemlerinde ve bilimsel görselleştirmede kullanılır. Örneğin, gri tonlu görüntüler bir görüntünün kontrastını arttırmak, gürültüyü azaltmak veya belirli özellikleri çıkarmak için kullanılır. Dijital bir görüntünün kontrastı, dijital görüntüdeki en koyu piksel ile en açık piksel arasındaki fark ile tanımlanır.

Renkli (Color) görüntüler: Renkli görüntüler, aynı zamanda RGB görüntüler olarak bilinir. Kırmızı, yeşil ve mavi renklerinin kombinasyonunu kullanarak görüntüyü temsil eden dijital görüntülerdir. Bir renkli görüntüde her piksel üç değer içerir. Üç renk kanalı

(kırmızı, yeşil ve mavi) bir araya gelerek tüm renklerin temsil edilmesine izin verir.

Renkli görüntüler fotoğraf, video ve grafik tasarımı gibi alanlarda sıklıkla kullanılır. RGB renk modeli, bilgisayar ekranlarında, televizyonlarda veya diğer elektronik görüntülerde görüntüleri oluşturmak için kullanılır ve ayrıca kameralar, tarayıcılar ve diğer dijital cihazlarda da kullanılır.

Görüntü şifrelemenin kullanım alanları

Dijital görüntü şifreleme, çeşitli amaçlar için kullanılabilir. Özellikle bu amaçlar aşağıdaki gibi olabilir:

Gizlilik: Kişisel veya özel bilgileri içeren görüntülerin gizliliğinin korunması amacı ile kullanılabilir. Örneğin, bir banka hesap bilgilerini içeren bir görüntü gibi.

Güvenlik: Önemli veya hassas bilgileri içeren görüntülerin güvenliğini sağlamak amacı ile kullanılabilir. Örneğin, bir devlet sırrı olarak kabul edilen bir proje görüntüsü gibi.

İletişim: Özel bilgileri içeren mesajların gizli iletimi amacı ile kullanılabilir. Örneğin, iş ortakları arasında gizli bilgileri içeren bir görüntü iletişimi gibi.

E-ticaret: Önemli veya hassas bilgileri içeren sipariş bilgileri, kredi kartı bilgileri gibi, e-ticaret sitelerinde kullanılabilir. Bu bilgilerin güvenliğini sağlamak amacı ile görüntü şifreleme kullanılabilir.

Sağlık: Sağlık sektöründe, kişisel sağlık bilgileri içeren görüntülerin gizliliğini sağlamak amacı ile görüntü şifreleme kullanılabilir. Örneğin, bir hastanın radyoloji görüntüleri gibi.

4.2. Görüntü Şifreleme Yöntemleri

Dijital görüntülerin şifrelenmesi, görüntünün güvenliğini arttırmak için kullanılan bir yöntemdir. Dijital görüntülerin şifrelenmesi, özellikle kişisel veya özel bilgileri içeren görüntülerin gizliliğini koruma amacı ile kullanılır.

Dijital görüntülerin şifrelenmesi için kullanılan yöntemler arasında en yaygın olanlar şunlardır:

Simetrik şifreleme: Bu yöntem, dijital görüntüyü şifrelemek için kullanılan anahtarın hem şifreleme hem de şifre çözme işlemlerinde kullanılmasını gerektirir. Örneğin, Advanced Encryption Standard (AES) gibi yöntemler bu tür şifrelemelerde kullanır.

Asimetrik şifreleme: Bu yöntemde, dijital görüntüyü şifrelemek için açık anahtar kullanılır. Şifrelenmiş görüntünün şifresini çözme işlemi için gizli anahtar kullanılır. Örneğin, eliptik eğri kriptografisi ve RSA gibi yöntemler bu tür şifrelemelerde kullanır.

Steganografi: Steganografi, görüntünün verilerini görünmez hale getirmek için kullanılan bir yöntemdir. Görüntünün renk değerleri kullanılarak verilerin gizlenmesi bu yöntemle gerçekleştirilir.

4.3. Görüntü Değerlendirme Parametreleri

Görüntü değerlendirme parametreleri görüntü şifreleme uygulamasının performansını ölçmek ve güvenlik açısından gücünü ölçmek için kullanılır [28, 31].

4.3.1. Piksel sayısı değişim oranı (NPCR; Number of pixel change rate)

NPCR metriği, orijinal görüntü ile şifrelenmiş veya filigran eklenmiş görüntü arasındaki piksellerin değişim yüzdesini ölçer. Filigran, genellikle bir belge, fotoğraf, kağıt para veya diğer görüntülerin üzerine eklenen ve çoğu zaman transparan bir şekilde görünen bir desendir. Filigranlar, bir görüntünün sahipliğini veya kaynağını belirtmek, izinsiz kullanımı önlemek veya görüntünün orijinalliğini korumak için kullanılır.

NPCR, özellikle steganografi ve filigran alanında görüntü veya veri şifreleme algoritmalarının kalitesini ve etkinliğini değerlendirmek için kullanılır. Steganografi ve filigrandaki amaç, insan gözü tarafından algılanamayacak şekilde bilgiyi bir görüntü içine gizlemektir ve aynı zamanda orijinal görüntünün görsel kalitesini korumaktır [28].

NPCR hesaplanırken aşağıdaki işlem adımları gerçekleştirilir:

1. Bir görüntünün A_1 ve A_2 şeklinde iki kopyası alınıp A_1 görüntüsünün bir piksel değeri değiştirilir.
2. Şifreleme algoritması A_1 ve A_2'ye uygulanarak sırasıyla B_1 ve B_2 şifrelenmiş görüntüleri oluşturulur.
3. NPCR Eş 4.1'deki gibi hesaplanır:

$$\mathrm{NPCR} = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N} D(x,y)}{K} \times 100 \tag{4.1}$$

Burada $D(x,y)$ değeri B_1 ve B_2 görüntülerinin aynı konumdaki piksel değerinin karşılaştırılmasını ifade eder. x ve y değerleri görüntülerin piksel koordinatını ifade eder. K değeri B_1 veya B_2 görüntüsündeki toplam piksel sayısını ifade eder. B_1 ve B_2 şifrelenmiş görüntülerindeki aynı konumdaki pikseller aynı ise $D(x,y)$ değeri 0 olur, farklı ise 1 olur.

Daha yüksek bir NPCR değeri, şifreleme algoritmasının piksellerde önemli değişiklikler yaptığını gösterir. Bu, gizli bilginin daha etkili bir şekilde gömüldüğü anlamına gelir. Düşük NPCR değerleri, algoritmanın pikselleri yeterince değiştiremediğini ve daha az güvenli olduğunu gösterir.

4.3.2. Histogram analizi

Histogram analizi, bir veri kümesindeki değerlerin frekans dağılımını görselleştiren bir grafik türüdür. Görüntü işleme ve veri analizi gibi alanlarda kullanılan önemli bir yöntemdir [28].

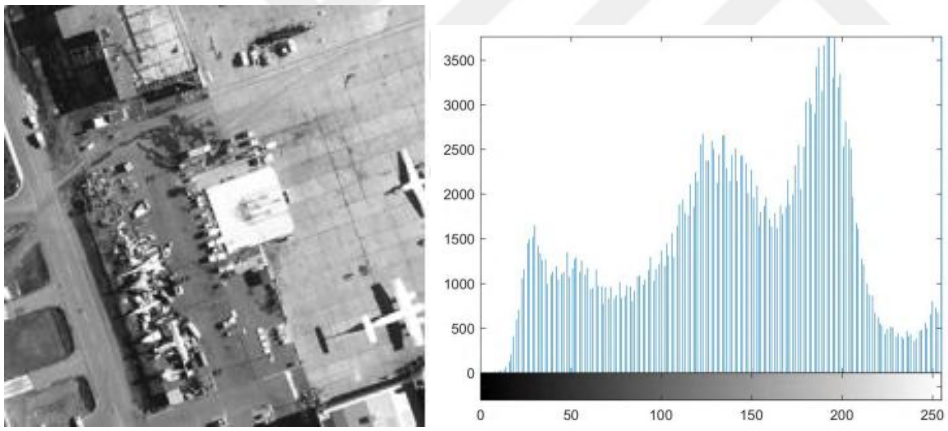
Bir görüntünün histogramı, piksellerin yoğunluk seviyelerinin farklı değerlere sahip olma sayısını gösterir. Yoğunluk seviyeleri genellikle gri tonlamalı görüntülerde 0 ile 255 arasındaki değerlerle temsil edilir. Renkli görüntülerde ise kırmızı, yeşil ve mavi bileşenlerin her biri için ayrı histogramlar oluşturulabilir.

Histogram analizi, bir görüntünün renk dağılımını incelemek ve farklı özelliklerini anlamak için kullanılır. Bu analiz yöntemi, bir görüntünün kontrastı, parlaklığı, renk dengesi ve renk dağılımı gibi özelliklerini anlamada önemli bir rol oynar.

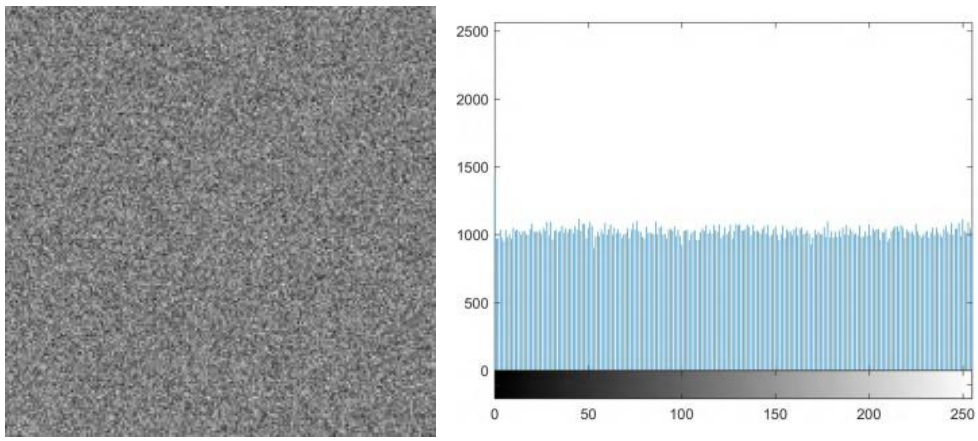
Histogram analizi, bir görüntüdeki öne çıkan nesneleri bulmak, arka planı belirlemek, görüntüyü aydınlatmak ya da karartmak, kontrastı artırmak veya azaltmak gibi bir dizi görüntü işleme ve analiz işleminde kullanılabilir.

Görüntü şifreleme uygulamalarında histogram analizi şifreleme algoritmasının performansını ölçmek için kullanılır. Güçlü şifrelemeye sahip bir algoritmadan çıkan şifrelenmiş görüntünün histogramının üniform bir şekilde dağılmış olması gerekir. Şifrelenmiş görüntünün histogramının üniform dağılmaması durumunda saldırganlar orijinal görüntü ile ilgili bilgi edinebilirler.

Şekil 4.1'de bir gri tonlu görüntü ve histogramı, Şekil 4.2'de ise gri tonlu görüntünün şifreli hali ve histogramı yer almaktadır. Görüldüğü üzere görüntü şifrelendikten sonra elde edilen histogramdan herhangi bir bilgi alabilmek mümkün değildir.



Şekil 4.1. Orijinal görüntü ve orijinal görüntünün histogramı



Şekil 4.2. Şifreli görüntü ve şifreli görüntünün histogramı

4.3.3. İlinti katsayısı (Correlation coefficient)

İlinti katsayısı, iki veri kümesi arasındaki ilişkiyi ve benzerliği ölçmek için kullanılan bir istatistiksel ölçüdür. Görüntü şifrelemede, orijinal görüntü ile şifrelenmiş görüntü arasındaki ilişkiyi belirlemek için ilinti katsayısı kullanılabilir. Bu katsayı, şifreleme algoritmalarının etkinliğini değerlendirmek için kullanılan bir metrik olarak önemli bir rol oynar.

Dijital görüntülerde anlamlı bir görüntünün ortaya çıkması için pikseller arası ilintinin yüksek olması yani genelde 1'e yakın olması gerekir. Görüntü şifreleme uygulamaları orijinal görüntüdeki yüksek ilintiyi minimum yapacak şekilde görüntüyü şifrelemelidir. Pikseller arası ilintinin azaltıldığı özellikle 0'a yakın olduğu şifreleme uygulamaları güçlü şifreleme algoritmalarıdır [28].

İlinti katsayısının nasıl hesaplanacağı ile ilgili formül Eş 4.2'de yer almaktadır.

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{4.2}$$

$$\operatorname{cov}(x,y) = \frac{\sum_{i=1}^{K}(x_i - E(x))(y_i - (E(y))}{K} \tag{4.3}$$

$$D(x) = \frac{1}{K}\sum_{i=1}^{K}(x_i - E(x))^2 \tag{4.4}$$

$$D(y) = \frac{1}{K}\sum_{i=1}^{K}(y_i - E(y))^2 \tag{4.5}$$

Eş. 4.3'de *x* ve *y* değerleri görüntünün koordinatını ifade ederken cov(*x*,*y*) ile ifade edilen parametre *x* ve *y* arasındaki ilintidir. *K* değeri görüntünün piksel sayısını ifade eder. Eş. 4.3, Eş. 4.4, Eş. 4.5'de ifade edilen *E*(*x*) ve *E*(*y*) parametreleri sırasıyla *x* ve *y*'nin ortalaması (mean) iken *D*(*x*) ve *D*(*y*) parametreleri sırasıyla *x* ve *y*'nin standart sapmasıdır.

4.3.4. Enformasyon entropisi (Information entropy)

Enformasyon entropisi, bir veri kümesinin düzensizliğini veya belirsizliğini ölçen bir istatistiksel kavramdır. Shannon entropisi olarak da adlandırılır ve genellikle enformasyon teorisi ve veri sıkıştırma alanlarında önemli bir rol oynar.

Görüntü şifrelemede, enformasyon entropisi, orijinal görüntüdeki piksellerin dağılımının ne kadar düzenli veya rasgele olduğunu belirlemeye yardımcı olur. Düşük enformasyon entropisi, piksellerin daha düzenli ve tahmin edilebilir olduğu anlamına gelirken, yüksek enformasyon entropisi, piksellerin daha rasgele ve tahmin edilemez olduğu anlamına gelir.

Enformasyon entropisi, şifreleme algoritmasının etkinliğini değerlendirmek için kullanılabilir. Eğer şifreleme işlemi yeterince güvenliyse, şifrelenmiş görüntüdeki piksellerin dağılımı orijinal görüntüden farklı ve daha rasgele olacaktır, bu da daha yüksek bir enformasyon entropisi değeriyle sonuçlanacaktır. Güçlü bir algoritma olarak nitelendirilen bir uygulamada şifrelenen 8 bit bir görüntünün entropisi 8'e çok yakın olmalıdır [31, 37].

Enformasyon entropisi $H(S)$ ile gösterilir ve Eş. 4.6'da olduğu gibi verilir.

$$H(S) = -\sum_{i=0}^{N}(P(s_i) \times \log_2 P(s_i)) \tag{4.6}$$

Burada $P(s_i)$, s_i enformasyonunu taşıyan parametrelerin bulunma olasılığıdır. N ise görüntüdeki bir pikselin alabileceği en yüksek değeri ifade etmektedir. Örnek olarak 8 bit bir görüntüde N=255 olacaktır.

4.3.5. Uygulama hızı (Execution time)

Uygulama hızı genellikle bir şifreleme algoritmasının ne kadar sürede çalıştığını belirlemek için kullanılan bir metriktir. Bu metrik, bir şifreleme işleminin tamamlanma süresini ölçmek ve şifreleme algoritmasının performansını değerlendirmek için kullanılır.

Şifreleme algoritmaları, verileri şifrelemek ve korumak için matematiksel işlemler ve algoritmalardan oluşur. Bu işlemler, şifreleme algoritmasının karmaşıklığına, kullanılan

anahtar uzunluğuna ve veri boyutuna bağlı olarak farklı sürelerde tamamlanabilir.

İşlem süresi, şifreleme algoritmasının hızını ve etkinliğini belirlemeye yardımcı olur. Daha hızlı bir şifreleme algoritması, verilerin daha hızlı bir şekilde şifrelenmesini ve çözülmesini sağlar. Bu özellik, uygulamaların ve sistemlerin performansını artırabilir ve daha hızlı veri işleme sağlayabilir.

Özellikle görüntü şifreleme uygulamaları görüntülerin boyutu nedeniyle uzun süre alan işlemlerdir. Bu tarz şifreleme uygulamalarında hız, kullanıcı ve sistem açısından daha önemli hale gelmiştir [31, 4].

Ancak, işlem süresi, tek başına şifreleme algoritmasının güvenliğini belirlemek için yeterli değildir. Diğer güvenlik metrikleri ve performans değerlendirmeleri ile birlikte ele alınmalıdır.

4.3.6. Bit doğruluk oranı (BCR; Bit correct ratio)

BCR, orijinal veri ile şifrelenmiş veri arasındaki bit seviyesindeki benzerliği ölçer. Şifreleme işlemi sırasında verilerin değiştiği veya hatalı bir şekilde kodlandığı durumlar, güvenlik ve doğruluk açısından önemli olabilir. BCR, bu tür hataları veya değişiklikleri belirlemek ve değerlendirmek için kullanılır. Bu metrik, şifreleme algoritmalarının doğruluğunu değerlendirmek için kullanılan bir ölçüdür [31, 38].

BCR hesaplanırken orijinal veri ve şifrelenmiş veri arasındaki bit seviyesindeki farklar tespit edilir. Toplam bit sayısına göre, doğru olarak şifrelenmiş bitlerin yüzdesi hesaplanır.

BCR'nin hesaplama yöntemi Eş. 4.7'de verilmiştir.

$$\mathrm{BCR} = 1 - \left(\frac{\sum_{x=1}^{M} \sum_{y=1}^{N} [O(x,y) \oplus R(x,y)]}{MN} \right) \tag{4.7}$$

Burada $M \times N$ görüntünün boyutunu vermektedir. x ve y görüntüdeki piksel koordinatlarını ifade eder. O ve R sırasıyla orijinal görüntüyü ve şifresi çözülmüş görüntüyü gösterir. $\oplus$ işareti XOR operasyonunu ifade eder.

Yüksek bir BCR, şifreleme algoritmasının verileri doğru bir şekilde koruduğunu ve doğruluk açısından güvenli olduğunu gösterir. Düşük bir BCR değeri ise, şifreleme algoritmasının doğrulukta sorunlar yaşayabileceğini veya verilerin hatalı bir şekilde şifrelendiğine işaret edebilir.

BCR, görüntü şifrelemede olduğu gibi çeşitli veri şifreleme uygulamalarında ve diğer şifreleme yöntemlerinde de değerlendirme için kullanılan önemli bir metriktir. BCR, şifreleme algoritmasının performansını anlamak ve geliştirmek için önemli bir araçtır.

4.3.7. Ortalama kare hatası (MSE; Mean squared error)

MSE, orijinal bir görüntü ile şifrelenmiş görüntü arasındaki farkı ölçmeye yardımcı olur ve bu farkın büyüklüğünü değerlendirir.

MSE'nin hesaplama yöntemi Eş. 4.8'de verilmiştir.

$$\mathrm{MSE} = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}[O(x,y) - R(x,y)]^2 \tag{4.8}$$

Burada $M \times N$ görüntünün boyutunu vermektedir, x ve y görüntüdeki piksel koordinatlarını ifade eder. O ve R sırasıyla orijinal görüntüyü ve şifresi çözülmüş görüntüyü gösterir. MSE değeri 0 ile $M \times N$ arasında değer alabilir. Güçlü algoritmaya sahip olarak bilinen bir şifreleme uygulamasında MSE değeri 0'a yakın olmalıdır [31, 39].

MSE değeri, ne kadar küçük olursa, şifreleme işleminin daha az hata içerdiği ve daha yüksek kalite elde edildiği anlamına gelir. MSE değeri, piksel değerlerinin orijinal görüntüye göre ne kadar değiştiğini ölçer ve bu nedenle bir şifreleme algoritmasının doğruluğunu ve performansını değerlendirmede önemli bir rol oynar.

4.3.8. Tepe sinyal gürültü oranı (PSNR; Peak signal to noise ratio)

PSNR, görüntü şifrelemede özellikle görüntü kalitesini değerlendirmek için kullanılan bir metriktir. PSNR, orijinal görüntü ile şifresi çözülmüş görüntü arasındaki benzerliği ölçmeye yardımcı olur [31, 40].

Orijinal görüntü ile şifresi çözülmüş görüntü arasındaki fark gürültü olarak değerlendirilir. Gürültü, şifreleme sırasında meydana gelen bilgi kaybını veya bozulmayı ifade eder. Bu nedenle yüksek bir PSNR değeri, şifrelenmiş görüntünün orijinal görüntüye çok yakın olduğu ve şifreleme kalitesinin yüksek olduğu anlamına gelir.

PSNR'nin hesaplanması Eş. 4.9'daki gibidir.

$$\mathrm{PSNR} = 10 \log_{10} \frac{(2^n - 1)^2}{\mathrm{MSE}} \tag{4.9}$$

Burada *n* bir görüntünün bit sayısını ifade eder. Bu çalışmada *n*=8 olarak alınmıştır.

PSNR, genellikle dB birimi ile ifade edilir ve daha yüksek değerler, daha iyi kalite ve daha düşük bilgi kaybı anlamına gelir. Düşük PSNR değerleri ise, daha fazla bilgi kaybı ve kalite düşüşü olduğunu gösterir.

4.3.9. Sinyal bozulma oranı (SDR; Signal to distortion ratio)

SDR, görüntü şifreleme veya diğer görüntü işleme uygulamalarında, veri sıkıştırma ve kalite değerlendirmelerinde kullanılan bir parametredir. SDR, orijinal görüntü ile şifrelenmiş görüntü arasındaki benzerliği ve kaliteyi ölçmek için kullanılır [31, 41].

SDR, benzer bir şekilde PSNR gibi bir metriktir. Ancak SDR, görüntü işleme uygulamalarında sıklıkla veri sıkıştırma veya kodlama performansını değerlendirmek için kullanılırken, PSNR genellikle şifreleme ve kalite değerlendirmelerinde tercih edilir.

SDR'nin hesaplanması Eş. 4.10'daki gibidir.

$$\mathrm{SDR} = 10 \log_{10} \frac{\sum_{x=1}^{M} \sum_{y=1}^{N} [O(x,y)]^2}{\sum_{x=1}^{M} \sum_{y=1}^{N} [O(x,y) - R(x,y)]^2} \tag{4.10}$$

Burada *O* ve *R* sırasıyla *M*×*N* piksele sahip orijinal görüntüyü ve *M*×*N* piksele sahip şifresi çözülmüş görüntüyü gösterir. *x* ve *y* görüntünün piksel koordinatlarını ifade eder.

SDR, genellikle dB birimi ile ifade edilir ve daha yüksek değerler, daha iyi kalite ve daha az bilgi kaybı anlamına gelir. Düşük SDR değerleri, daha fazla bilgi kaybı ve kalite düşüşü olduğunu gösterir.

Görüntü şifrelemede veya veri sıkıştırmada, SDR değeri, algoritmanın performansını değerlendirmek ve farklı algoritmaları karşılaştırmak için kullanılan önemli bir metriktir. Ancak SDR gibi tek bir metrik, genellikle bir işlemin kalitesini eksiksiz olarak değerlendiremez. Bu nedenle, şifreleme algoritmalarının performansını ölçmek için birden fazla metrik ve kalite ölçütü bir arada kullanılmalıdır.

4.3.10. Yapısal benzerlik katsayısı (SSIM; Structural similarity index)

SSIM, görüntü şifrelemede kullanılan önemli bir kalite değerlendirme parametresidir. SSIM, orijinal bir görüntü ile şifresi çözülmüş görüntü arasındaki benzerliği ve kaliteyi ölçmeye yardımcı olur [31, 40].

PSNR ve SDR gibi metrikler, sadece piksel değerlerinin farkını hesaplar ve benzerlikleri tam olarak ölçemez. SSIM, bu tür durumlarda daha etkili bir kalite değerlendirmesi sağlar çünkü daha fazla insan görsel algılamasını yansıtır.

SSIM, görüntüdeki yapısal benzerliği değerlendirmek için farklı parametreler ve farklı ölçümler kullanır. Piksel değerlerinin yanı sıra, görüntüdeki parlaklığı, kontrastı ve yapının farkını ölçer. Bu nedenle SSIM, insan gözünün algıladığı görsel benzerliği daha iyi temsil eder ve daha doğru sonuçlar verir.

SSIM'nin hesaplanması Eş. 4.11'deki gibidir.

$$\mathrm{SSIM} = \frac{(2\mu_O\mu_R + C_1)(2\sigma_{OR} + C_2)}{(\mu_O^2 + \mu_R^2 + C_1)(\sigma_O^2 + \sigma_R^2 + C_2)} \tag{4.11}$$

Burada μ_O ve μ_R sırasıyla O orijinal görüntünün ve R şifresi çözülmüş görüntünün Gauss ortalamasıdır. σ_O^2 ve σ_R^2 sırasıyla O ve R'nin varyansını ifade eder. σ_{OR}, O ve R'nin kovaryansını ifade eder. C_1 ve C_2 sırasıyla $(0.01P)^2$ ve $(0.03P)^2$ değerlerini alan regülarizasyon sabitidir. P değeri ise görüntüler arasındaki dinamik aralıktır.

SSIM değeri, -1 ile 1 arasında bir değer alır. 1, orijinal görüntü ile şifresi çözülmüş görüntü arasındaki tam benzerliği gösterirken, -1 ise iki görüntü arasında hiç benzerlik olmadığını gösterir.

Görüntü şifrelemede, SSIM değeri, algoritmanın performansını değerlendirmek ve farklı algoritmaları karşılaştırmak için yaygın olarak kullanılan önemli bir metriktir.

4.3.11. Kök ortalama kare hatası (RMSE; Root mean squared error)

RMSE, görüntü şifreleme ve görüntü işleme alanında kullanılan bir metriktir. RMSE, orijinal bir görüntü ile şifresi çözülmüş görüntü arasındaki farkı ölçmeye yardımcı olur ve bu farkın büyüklüğünü değerlendirir [31, 42].

RMSE değeri, farkın büyüklüğünü belirler ve küçük olması, şifreleme işleminin daha az hata içerdiği ve daha kaliteli olduğu anlamına gelir. RMSE değeri, piksel değerlerinin orijinal görüntüye göre ne kadar değiştiğini ölçer ve buradan hareketle bir şifreleme algoritmasının doğruluğunu ve performansını değerlendirmede önemli bir rol oynar.

RMSE'nin hesaplanması Eş. 4.12'deki gibidir.

$$\mathrm{RMSE} = \sqrt{\frac{\sum_{x=1}^{M}\sum_{y=1}^{N}[O(x,y) - R(x,y)]^2}{MN}} \tag{4.12}$$

Burada O ve R sırasıyla M×N piksele sahip orijinal görüntüyü ve M×N piksele sahip şifresi çözülmüş görüntüyü gösterir. x ve y parametreleri O ve R görüntülerinin piksel koordinatlarını ifade eder.

4.3.12. Sinyal gürültü oranı (SNR; Signal to noise ratio)

SNR görüntü şifreleme ve diğer görüntü işleme uygulamalarında kullanılan önemli bir metriktir. SNR, bir sinyalin gürültüye olan oranıdır. Burada gürültü, orijinal görüntü ile şifresi çözülmüş görüntü arasındaki fark cinsinden ifade edilmektedir [31, 44].

Görüntü şifrelemede, SNR, orijinal görüntü ile şifresi çözülmüş görüntü arasındaki

benzerliği ve veri kaybını ölçmeye yardımcı olur. SNR, dB birimi ile ifade edilir. Daha yüksek SNR değerleri, sinyal kısmının gürültü kısmına göre daha güçlü olduğunu ve daha az veri kaybı olduğunu gösterir. Dolayısıyla, daha yüksek SNR değerleri, daha yüksek kalite ve daha az veri kaybı anlamına gelir.

SNR'nin hesaplanması Eş. 4.13'deki gibidir.

$$\mathrm{SNR} = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}[O(x,y)]^2}{\sum_{x=1}^{M}\sum_{y=1}^{N}[O(x,y)-R(x,y)]^2} \tag{4.13}$$

Burada O ve R sırasıyla $M \times N$ piksele sahip orijinal görüntüyü ve $M \times N$ piksele sahip şifresi çözülmüş görüntüyü gösterir. x ve y parametreleri O ve R görüntülerinin piksel koordinatlarını ifade eder.

5. ELİPTİK EĞRİ KRİPTOGRAFİSİ İLE DİJİTAL GÖRÜNTÜ ŞİFRELEME

Bu bölümde eliptik eğri kriptografisi kullanılarak dijital görüntü şifreleme uygulaması tasarlanmıştır. Önerilen algoritmanın işlem adımlarına yer verilmiştir. Önerilen algoritmanın güvenlik ve performans açısından diğer şifrelemelerle olan kıyas bilgileri de bu bölümde sunulmuştur. Önerilen algoritmanın farklı görüntüler üzerinde çalıştığını göstermek amacıyla babun ve biberler görüntüsü olmak üzere iki farklı görüntü kullanılmıştır.

Önerilen algoritma C++ programlama dilinde yazılmıştır. Derleyici olarak MSVC (Microsoft Visual C++) kullanılmıştır [44]. Görüntü şifreleme için gerekli kütüphaneler olarak OpenCV (Open Computer Vision) ve Boost kütüphaneleri kullanılmıştır. OpenCV kütüphanesi dijital görüntünün piksel değerlerine erişmek, piksel değerlerini değiştirmek, dijital görüntü oluşturmak gibi işlemleri gerçekleştirmek için kullanılmıştır [45]. Boost kütüphanesi C++ programlama dilinde çok büyük tamsayıların kullanılabilmesi amacıyla kullanılmıştır [46].

Uygulamanın çalıştığı Lenovo marka dizüstü bilgisayarın özellikleri şunlardır:

i. AMD Ryzen 7 CPU - 2 GHz
ii. 16 GB RAM
iii. 64 bit işletim sistemi

Bu bölümde kullanılan parametrelere ilişkin bilgiler Çizelge 5.1'de verilmiştir.

Çizelge 5.1. Şifreleme uygulama parametreleri

Parametre	Tanım
$y^2=x^3+ax+b \pmod p$	Uygulamada kullanılan eliptik eğri denklemi
a	Eliptik eğri denklemindeki a değeri
b	Eliptik eğri denklemindeki b değeri
p	Eliptik eğri denklemindeki yeterince büyük p asal sayısı

Çizelge 5.1. (devam) Şifreleme uygulama parametreleri

G	Başlangıç parametresi (Generator point)
A	Şifreleme yapan taraf
B	Şifre çözen taraf
n_A	A'nın gizli anahtarı
n_B	B'nin gizli anahtarı
P_A	A'nın açık anahtarı
P_B	B'nin açık anahtarı
K	Ortak anahtar
büyük tamsayı	Pikseller gruplandırılarak oluşturulan 512 bit sayı
T	Tohum değeri (seed)
x	Görüntünün satır koordinat değeri
y	Görüntünün sütun koordinat değeri
L	Eliptik eğrinin bit uzunluğu
M	Şifreli büyük tamsayı
D	Şifresi çözülmüş büyük tamsayı

Önerilen şifreleme algoritmasında L=512 bit uzunluğunda eliptik eğri kripto sistemi kullanılmıştır yani p değeri 512 bittir.

Görüntü şifreleme uygulamasında kullanılan gizli anahtarlar Çizelge 5.2'de gösterilmiştir.

Çizelge 5.2. Görüntü şifreleme uygulamasında kullanılan gizli anahtarlar

n_A	94268904488832477456261857430572424738096937640789516634942387772947070700232237988829761592077291198236058505886084604294126475673608974091172098560224 01
n_B	96192759682482119853328425949563698712343813919172976158104477319333745612481875498805879175589072651261284189679678167647067832308974867524089740051 33

Görüntü şifreleme uygulamasında kullanılan NIST (National Institute of Standards and Technology) parametreleri Çizelge 5.3'de gösterilmiştir.

Çizelge 5.3. Görüntü şifreleme uygulamasında kullanılan NIST parametreleri

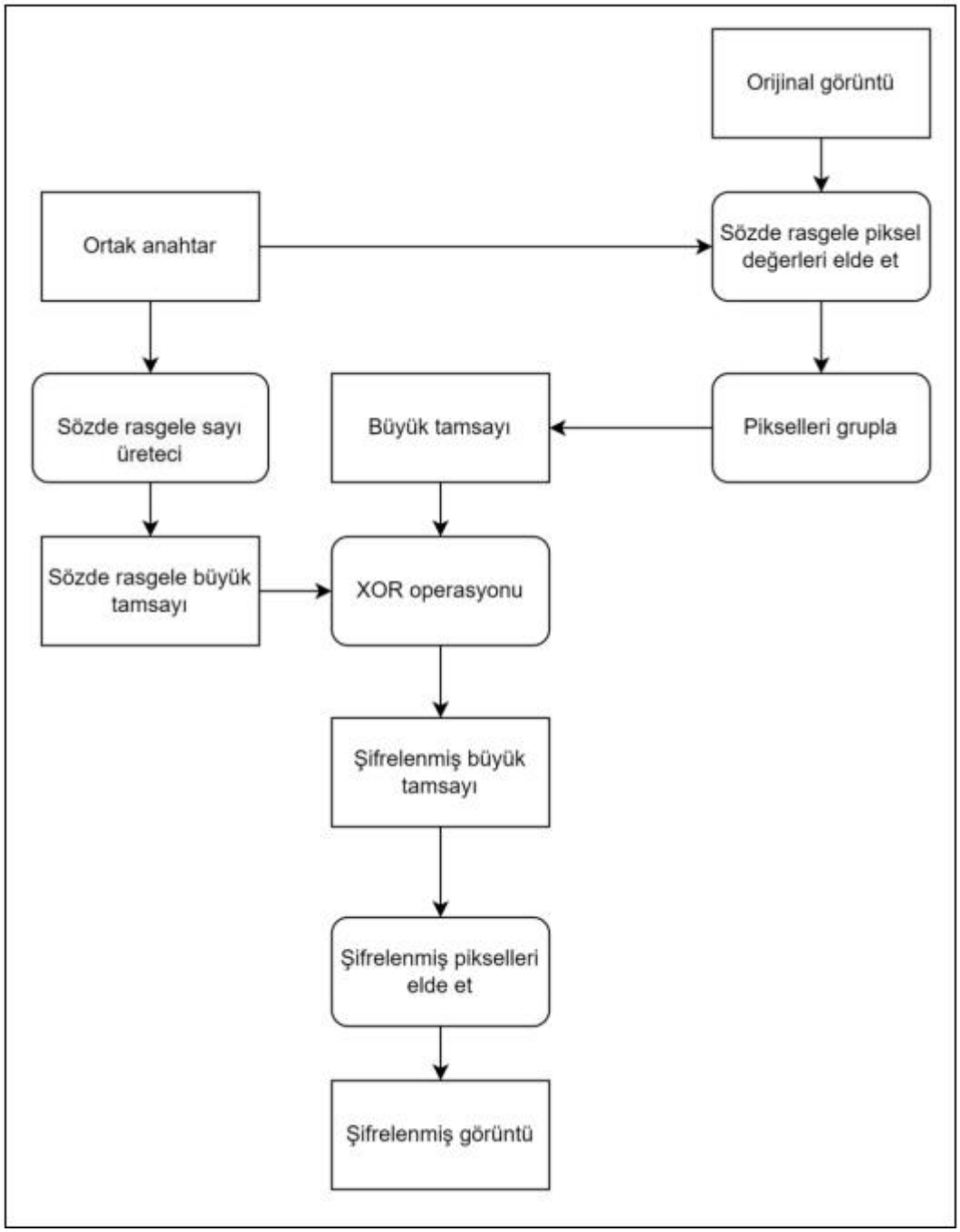
Parametre	Değer
a	629486055797306322766642130647637932407471577062274622713 691044545030191428127609802799096840798396269115185367856 387783422183402743971823806572584426413 8
b	324578900832896705927484958434207791653190900963750191832 832366873617917658326349646352512848828261155980077350697 377179776481149883499523434153086228662 7
p	894896220765023255165660281515915342216260964409835451134 459718720005701041355243991793430419195694276544653038642 734593796389430992392853607053460781694 7
G	679205914042457517443564043126919508784315339010252188146 802301273204748257985307754564744627286679493637152241077 453268658248461794601392887429684435152 2, 659224455524011287332474838142961034131271294032626633132 744506668701054541525646109770748328865021699261309018504 295771631830118015923478850430762850933 0

Önerilen algoritma, dijital görüntü şifreleme ve şifreli dijital görüntüyü çözme şeklinde iki adımdan oluşmaktadır.

5.1. Dijital Görüntü Şifreleme

Bu bölümde önerilen algoritmanın dijital görüntü şifreleme kısmındaki işlem adımları açıklanmıştır.

Şekil 5.1'de önerilen algoritmanın dijital görüntüyü şifrelemeye dair akış diyagramı bulunmaktadır.



Şekil 5.1. Dijital görüntü şifreleme akış diyagramı

Ortak anahtar oluşturma ve anahtar değişimi

Önerilen algoritmada anahtar değişimi yapılabilmesi için Diffie-Hellman anahtar değişim protokolü kullanılmıştır. Şifreleme algoritmasında eliptik eğri kriptografisi kullanıldığı için anahtar değişimi sırasında uygulanan çarpım işlemleri eliptik eğri nokta toplama işlemi olacak şekilde gerçekleştirilmiştir.

Ortak anahtar oluşturma ve anahtar değişim işlemleri aşağıda anlatılmıştır:

Şifreleme uygulamasında G başlangıç noktası seçilir. Eş. 5.1'de A'nın gizli anahtarı n_A ile G'nin çarpım işlemi sonucunda açık anahtar P_A elde edilir. Eş. 5.2'de B'nin gizli anahtarı n_B ile G'nin çarpım işlemi sonucunda B'nin açık anahtarı P_B elde edilir. Eş. 5.3'de P_B ile n_A'nın çarpım işlemi sonucunda ortak anahtar K oluşturulur. Benzer şekilde Eş. 5.4'de P_A ile n_B çarpım işlemi sonucunda K oluşturulur. Böylece her iki taraf da ortak anahtar olan K değerini elde etmiş olur.

$$P_A = n_A G \quad (5.1)$$

$$P_B = n_B G \quad (5.2)$$

$$K = P_B n_A \quad (5.3)$$

$$K = P_A n_B \quad (5.4)$$

Ortak anahtar oluşturma ve anahtar değişimi işlemleri şifreleme ve şifre çözme işleminden önce yapıldığı ve aynı işlem olduğu için şifre çözme kısmında tekrar anlatılmamıştır.

Sözde rasgele piksel değerleri elde etme

Önerilen algoritmada piksel değerlerinin gruplandırılması işleminden önce K, görüntünün piksel konum bilgileri x ve y sözde rasgele sayı üretecine girdi olarak verilerek görüntünün üç renk kanalının piksel değerleri için farklı sözde rasgele sayılar üretilmiştir. Böylece büyük tamsayı oluşturmadan önce piksel değerleri arasındaki ilinti azaltılmıştır.

Sözde rasgele piksel değerlerinin hesaplanması için aşağıdaki işlemler gerçekleştirilir:

T tohum bilgisinin hesaplanması için K, x ve y Eş. 5.5'deki gibi çarpılır. Elde edilen T değeri sözde rasgele sayı üretecine girdi olarak kullanılır. Eş. 5.6'da sözde rasgele sayının mod 256 değeri bulunur. Bunun sebebi şifreleme yapılan görüntü 8 bit olduğu için çıkan değerin 0 ile 255 arasında olması gerekliliğidir.

$$T = K * x * y \quad (5.5)$$

$$\text{Sözde rasgele piksel değeri} = \text{Sözde rasgele sayı üreteci}(T) \pmod{256} \quad (5.6)$$

Piksel gruplama

Dijital görüntü şifreleme yaparken her bir piksel üzerinde ayrı ayrı kriptografik işlem gerçekleştirilmesi büyük piksel sayıları için çok fazla zaman harcanmasına neden olacaktır. Bu nedenle, pikselleri gruplandırarak üzerinde işlem yapmak zaman açısından tasarruf sağlayacaktır.

Piksellerin gruplandırılması, kullanılan eliptik eğri parametrelerine bağlıdır. L eliptik eğri parametresi ne kadar büyükse, daha fazla piksel gruplandırılabilir. Gruplandırılacak maksimum piksel sayısı Eş 5.7'deki gibi bulunabilir. Örneğin, 512 bit ECC sisteminde, bir görüntüde 63 piksel ya da 256 bit ECC sisteminde 31 piksel bir araya getirilip gruplandırılabilir. Önerilen algoritmada da 512 bit ECC sistemi kullanıldığı için pikseller 63'lü gruplar halinde gruplandırılmıştır.

$$\text{Gruplandırılacak maksimum piksel sayısı} = (L / 8) - 1 \tag{5.7}$$

Önerilen algoritmada kullanılan 8 bit 3 kanallı renkli görüntünün her bir kanalının bir piksel değeri maksimum 255 olabilir. Buradan hareketle pikseller gruplandırılırken her bir 63 piksel, 256 tabanında bir basamak olacak şekilde alınıp büyük tamsayıya eklenmiştir. Eş 5.8'de P_{mxn} piksellerinin gruplandırılmasının nasıl yapıldığı gösterilmiştir.

$$\text{büyük tamsayı} = 256^0 * P_{0x0} + 256^1 * P_{0x1} + 256^2 * P_{0x2} + \ldots + 256^{62} * P_{0x62} \tag{5.8}$$

Görüntüdeki bütün pikseller için aynı işlem uygulanır. Görüntünün bir satırından ve bir renk kanalından toplamda 9 adet büyük tamsayı elde edilir. Görüntü 512 satır olduğu için ve ayrıca görüntüde 3 renk kanalı olduğu için toplamda 13824 adet büyük tamsayı elde edilir.

Sözde rasgele sayı üreteci

Dijital görüntüdeki piksellerin gruplandırılmasıyla elde edilen büyük tamsayıların sürekli aynı K ile XOR işlemine tabi tutulması, şifrelenen görüntüdeki pikseller arası ilinti katsayısının beklenenden yüksek seviyede olmasına sebep olacaktır. Bu sebeple gruplandırılan piksellerden elde edilen büyük tamsayıların farklı K değerleri ile XOR

işlemine tabi tutulması gerekmektedir. Fakat farklı K değerleri, açık anahtar ve gizli anahtar sayısını çok arttıracağından ve anahtar paylaşım işlemini çok zorlaştıracağından, K_{temp} şeklinde ortak gizli anahtar değerleri kullanılmıştır.

K_{temp} değerleri hesaplanırken sözde rasgele sayı üretecine girdi olarak K değeri ve piksellerin konum bilgisi verilmiştir. Böylece her büyük tamsayı için farklı K_{temp} değerleri elde edilmiştir. Sözde rasgele sayı üreteci için gerekli T_{temp} tohum değerinin oluşturulması için K, büyük tamsayının konum bilgisinin satır değeri $x_{büyük\ tamsayı}$ ve büyük tamsayının konum bilgisinin sütun değeri $y_{büyük\ tamsayı}$ Eş. 5.9'daki gibi çarpılır. Eş. 5.10'da gösterildiği gibi sözde rasgele sayı üretecinin K_{temp} değerini üretmesi için T_{temp} değeri kullanılıp mod p işlemi gerçekleştirilir.

$$T_{temp} = K * x_{büyük\ tamsayı} * y_{büyük\ tamsayı} \tag{5.9}$$

$$K_{temp} = \text{sözde rasgele sayı üreteci}(T_{temp}) \ (\text{mod } p) \tag{5.10}$$

XOR operasyonu

M şifreli büyük tamsayısını elde etmek için sözde rasgele sayı üretecinden elde edilen K_{temp} sayılarıyla, piksel gruplamasından elde edilen büyük tamsayılar sırayla XOR operasyonuna tabi tutulur. Eş. 5.11'de M şifreli büyük tamsayısının elde edilişi gösterilmiştir.

$$M = K_{temp} \oplus \ \text{büyük tamsayı} \tag{5.11}$$

Şifrelenmiş büyük tamsayıdan piksel değerlerinin elde edilmesi

M şifreli büyük tamsayısından piksel değerleri elde edilirken piksel gruplandırma işlem adımında yapılan operasyonun tam tersi yapılmaktadır. mod 256 işleminin, M'ye 63 defa uygulanması sonucunda şifrelenmiş piksel değerleri elde edilmektedir. Bu, iteratif bir işlem olduğundan dolayı her mod 256 işleminden sonra elde edilen sonuç E_{mxn} şifreli görüntünün bir piksel değerini gösterir. M'nin 256'ya bölünmesiyle M_{temp} değeri elde edilir. M_{temp} değeri ile tekrar mod 256 işlemi yapılarak bir sonraki piksel değeri elde edilir. Eş. 5.12'de şifreli piksel değerlerinin elde edilme yöntemi gösterilmiştir.

$E_{0x0}=M \pmod{256}$, $M_{temp}=M/256$,

$E_{0x1}=M_{temp} \pmod{256}$, $M=M_{temp}$, $M_{temp}=M/256$,

$E_{0x2}=M_{temp} \pmod{256}$, $M=M_{temp}$, $M_{temp}=M/256$,

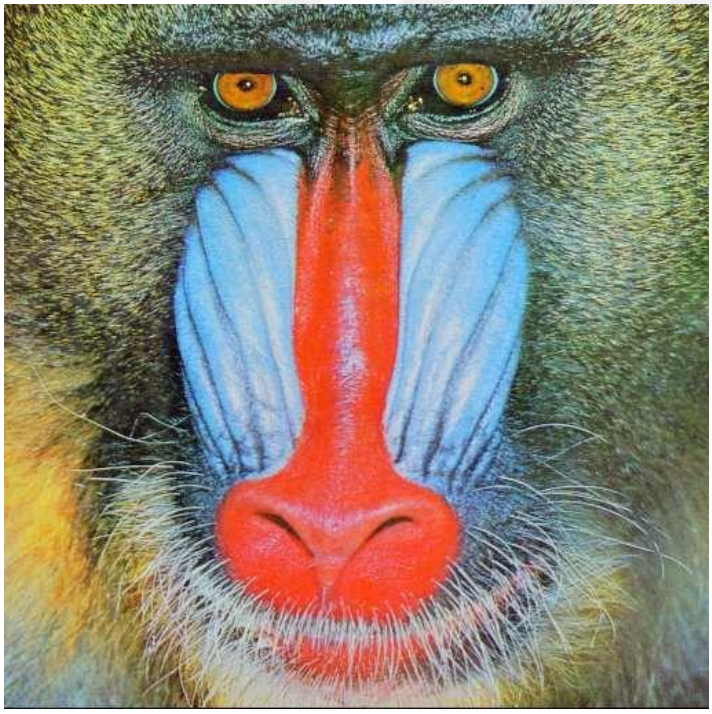
.....

$E_{0x62}=M_{temp} \pmod{256}$ (5.12)

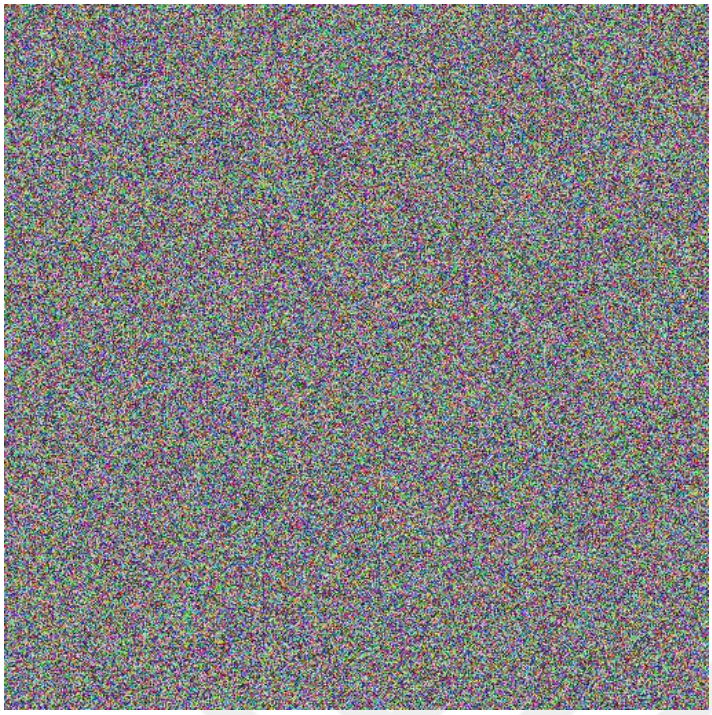
Bütün bu adımlardan sonra, elde edilen şifrelenmiş piksel değerleri yeni bir matrise eklenerek şifrelenmiş görüntü elde edilir.

Ayrıntıları yukarıda verilen algoritma örnek olarak bir babun görüntüsüne ve bir biberler görüntüsüne uygulanmıştır.

Şekil 5.2'de babun görüntüsünün orijinal hali, Şekil 5.3'de babun görüntüsünün şifrelenmiş hali yer almaktadır.



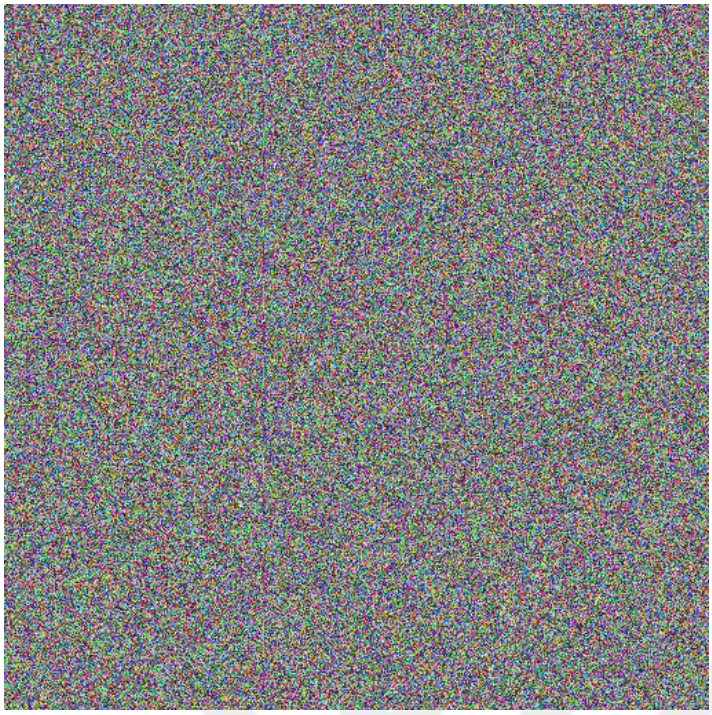
Şekil 5.2. Babun görüntüsünün orijinal hali



Şekil 5.3. Babun görüntüsünün şifrelenmiş hali

Şekil 5.4'de biberler görüntüsünün orijinal hali, Şekil 5.5'de biberler görüntüsünün şifrelenmiş hali yer almaktadır.

Şekil 5.4. Biberler görüntüsünün orijinal hali



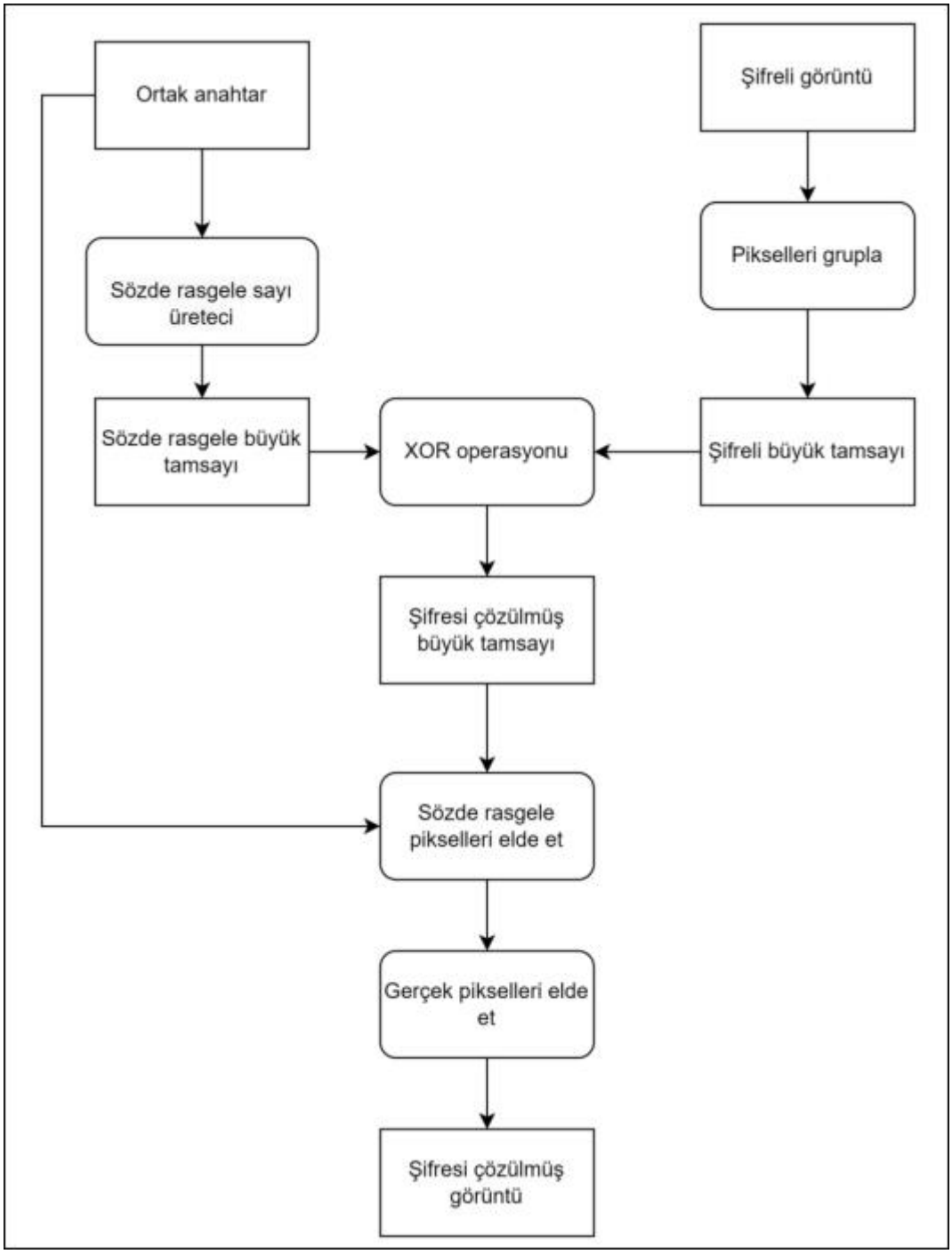
Şekil 5.5. Biberler görüntüsünün şifrelenmiş hali

Şekil. 5.3'ten ve Şekil 5.5'ten önerilen şifreleme algoritmasının başarılı olduğu, şifrelenmiş görüntülere bakıldığında orijinal görüntülere ilişkin herhangi bir belirti olmadığı görülmektedir.

5.2. Şifreli Dijital Görüntüyü Çözme

Bu bölümde önerilen algoritmanın şifreli dijital görüntünün çözümü kısmındaki işlem adımları yer almaktadır.

Şekil 5.6'da önerilen algoritmadaki şifreli dijital görüntüye çözmeye dair akış diyagramı bulunmaktadır.



Şekil 5.6. Dijital görüntü şifre çözme akış diyagramı

Sözde rasgele sayı üreteci

Şifrelenmiş dijital görüntüdeki pikseller gruplandırılarak elde edilen şifreli büyük tamsayıların şifresinin çözülmesi için şifreleme sırasında elde edilen K_{temp} değerlerinin elde edilmesi gerekmektedir. Bunu yapabilmek için sözde rasgele sayı üreteci kullanılmıştır. Sözde rasgele sayı üretecinin çalışması için gerekli işlem adımları ve parametreler dijital

görüntü şifreleme kısmındaki işlem adımları ve parametrelerle aynı olduğu için burada tekrar anlatılmamıştır.

Piksel gruplama

E_{mxn} şifreli dijital görüntüdeki pikseller 63 piksellik gruplar olacak şekilde gruplandırılır. Her 63 piksel 256 tabanında bir basamak olacak şekilde hesaplanıp M şifreli büyük tamsayıya eklenir. Eş 5.13'te E_{mxn} piksellerinin gruplandırılmasının nasıl yapıldığı gösterilmiştir.

$$M = 256^{0}*E_{0x0} + 256^{1}*E_{0x1} + 256^{2}*E_{0x2} + ... + 256^{62}*E_{0x62} \quad (5.13)$$

Görüntüdeki bütün pikseller bitinceye kadar aynı işlem uygulanır. Görüntünün bir satırından ve sadece bir renk kanalından toplamda 9 adet M değeri elde edilir. Görüntü 512 satır olduğu için ve ayrıca görüntüde 3 renk kanalı olduğu için toplamda 13824 adet M değeri elde edilir.

XOR operasyonu

M değerinin şifresini çözmek için sözde rasgele sayı üretecinden elde edilen K_{temp} sayılarıyla, şifreli piksel gruplanmasından elde edilen M değerleri sırayla XOR operasyonuna tabi tutulur. Böylece şifresi çözülmüş D büyük tamsayısı elde edilir. Eş. 5.14'te D'nin hesaplama yöntemi gösterilmiştir.

$$D = K_{temp} \oplus M \quad (5.14)$$

Sözde rasgele piksel değerlerini elde etme

D değerinden sözde rasgele piksel değerleri elde edilirken piksel gruplandırma işlem adımında yapılan operasyonun tam tersi yapılmaktadır. D'nin mod 256 işlemine 63 defa tabi tutulması sonucu sözde rasgele piksel değerleri elde edilmektedir. Bu işlem iteratif bir işlem olduğundan dolayı her mod 256 sonucundan sonra elde edilen değer, görüntü şifreleme aşamasında elde edilen sözde rasgele piksel değerini gösterir. D'nin 256'ya bölünmesiyle D_{temp} değeri elde edilir. D_{temp} değeri ile tekrar mod 256 işlemi yapılarak bir

sonraki piksel değeri elde edilir. Eş 5.15'te R_{mxn} sözde rasgele piksellerinin nasıl hesaplandığı gösterilmiştir.

$R_{0x0}=D \pmod{256}$, $D_{temp} = D / 256$,
$R_{0x1}=D_{temp} \pmod{256}$, $D=D_{temp}$, $D_{temp} = D / 256$,
$R_{0x2}=D_{temp} \pmod{256}$, $D=D_{temp}$, $D_{temp} = D / 256$,
.....
$R_{0x62}=D_{temp} \pmod{256}$ (5.15)

Gerçek piksel değerlerini elde etme

Sözde rasgele piksel değerlerinden gerçek piksel değerlerini elde etmek için sözde rasgele sayı üreteci kullanılmıştır. Eş. 5.16'da görüldüğü üzere T değerinin hesaplanması için K değeri, x değeri ve y değeri çarpılmıştır.

$$T = K * x * y \quad (5.16)$$

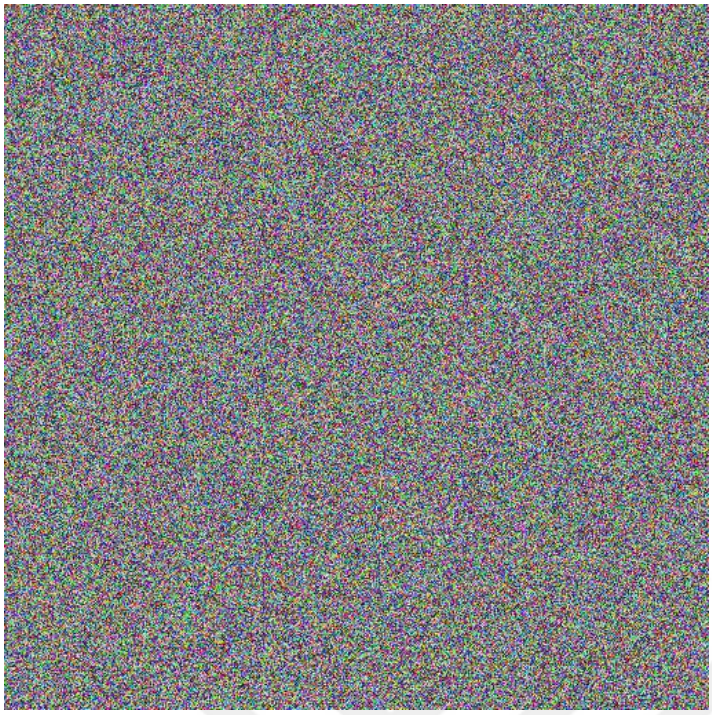
Sözde rasgele sayı üretecine T değeri verildikten sonra çıkan sözde rasgele değerin mod 256 işlemi sonucu şifresi çözülmüş piksel değeri elde edilir. Eş 5.17'de şifresi çözülmüş piksel değerlerinin nasıl hesaplandığı gösterilmiştir.

Şifresi çözülmüş piksel değeri= sözde rasgele sayı üreteci(T) (mod 256) (5.17)

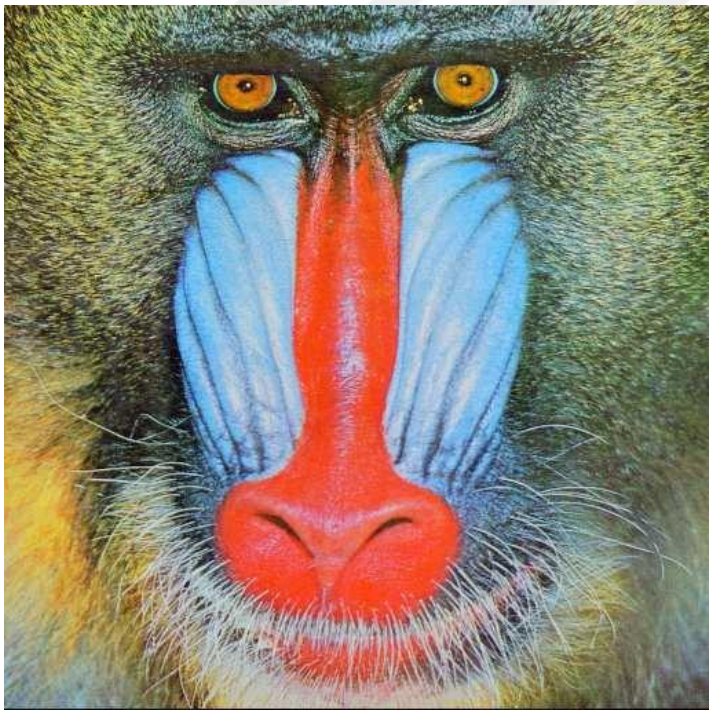
Bütün şifre çözme işlem adımlarından sonra elde edilen şifresi çözülmüş piksel değerleri yeni bir matrise eklenerek şifresi çözülmüş görüntü elde edilmiş olur.

Ayrıntıları yukarıda verilen algoritma örnek olarak şifrelenmiş bir babun görüntüsüne ve şifrelenmiş bir biberler görüntüsüne uygulanmıştır.

Şekil 5.7'de babun görüntüsünün şifrelenmiş hali, Şekil 5.8'de babun görüntüsünün şifresi çözülmüş hali yer almaktadır.

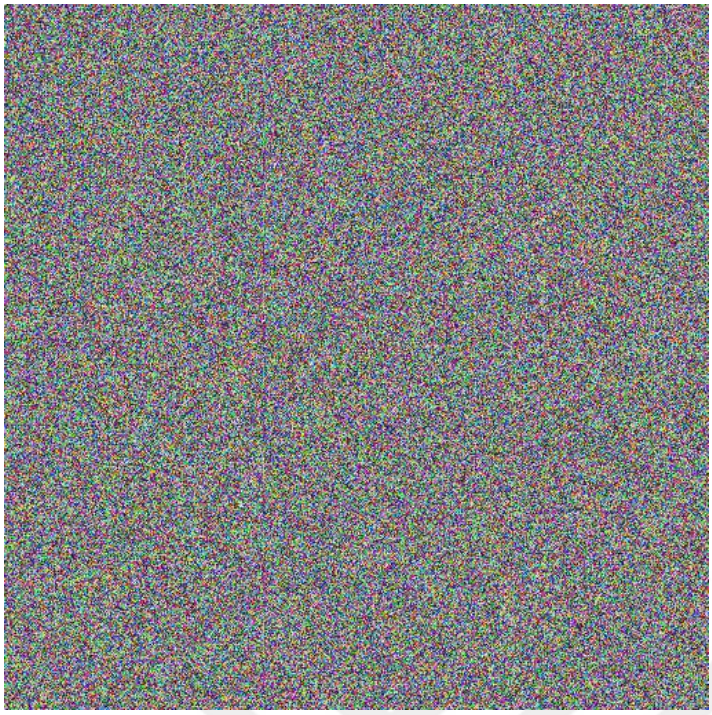


Şekil 5.7. Babun görüntüsünün şifrelenmiş hali



Şekil 5.8. Babun görüntüsünün şifresi çözülmüş hali

Şekil 5.9'da biberler görüntüsünün şifrelenmiş hali, Şekil 5.10'da biberler görüntüsünün şifresi çözülmüş hali yer almaktadır.



Şekil 5.9 Biberler görüntüsünün şifrelenmiş hali

Şekil 5.10. Biberler görüntüsünün şifresi çözülmüş hali

Şekil. 5.8'e ve Şekil 5.10'a bakıldığında önerilen şifre çözme algoritmasının başarılı olduğu, şifresi çözülmüş görüntülere bakıldığında orijinal görüntülerle birebir aynı olduğu

görülmektedir. Şifresi çözülmüş görüntü ile orijinal görüntünün birbiriyle aynı olduğu yazılan bir bilgisayar programı aracılığıyla gösterilmiştir.

5.3. Algoritma Değerlendirme Parametreleri

Bu alt bölümde önerilen uygulamanın hız analizi, histogram analizi, anahtar uzunluğu, anahtar hassasiyeti, ilinti katsayısı, entropi analizi ve PSNR analizi gibi parametreler incelenmiştir.

Hız analizi

Şifreleme algoritmalarının hızı algoritmanın tasarımına, tasarlayıcının programlama becerisine, uygulamanın çalıştığı donanıma vb. etkenlere bağlı olarak değişkenlik gösterir.

Eliptik eğri kriptografisi ile şifreleme yapılırken en çok zaman alan işlem eliptik eğri nokta çarpımlarıdır. Piksellerden elde edilen büyük tamsayıların nokta çarpımlarıyla şifrelenmesi bir algoritmaya büyük işlem yükü getireceğinden, önerilen algoritmada bu yöntem kullanılmamıştır. Bunun yerine eliptik eğri kullanılarak oluşturulan ortak anahtar ile XOR operasyonları yapılarak algoritmanın bu işlem yüklerinden kurtulması sağlanmıştır.

Önerilen algoritmada şifreleme ve şifre çözme işlemlerinin ortalama süreleri Çizelge 5.4'de verilmiştir. Ortalama süreler 1000 farklı denemenin sonucu olarak hesaplanmıştır.

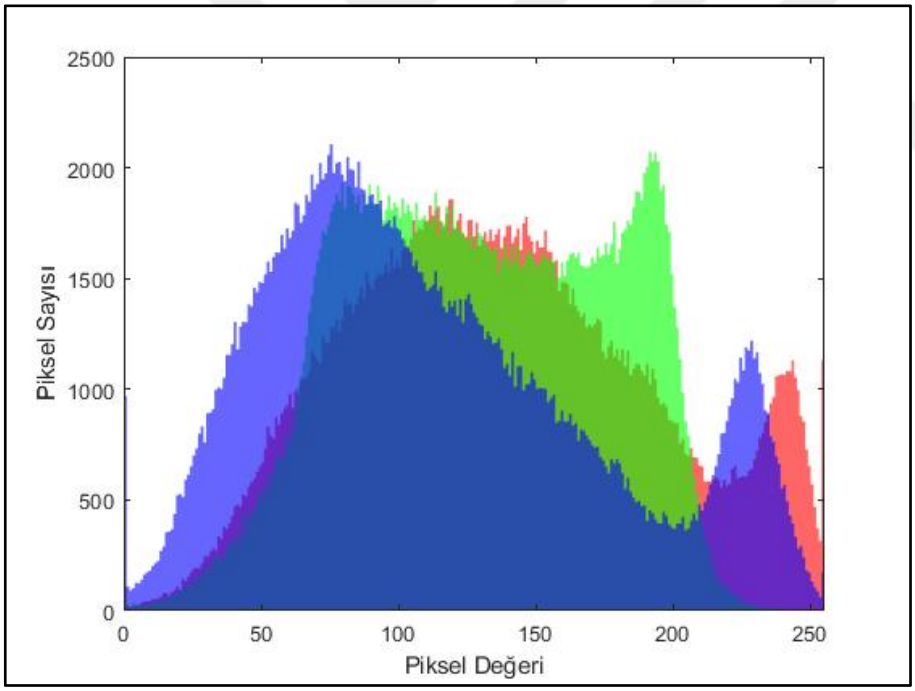
Çizelge 5.4. Şifreleme ve şifre çözme süreleri

Görüntü	İşlem	Süre (s)
babun	şifreleme	0,57
babun	şifre çözme	0,60
biberler	şifreleme	0,57
biberler	şifre çözme	0,59

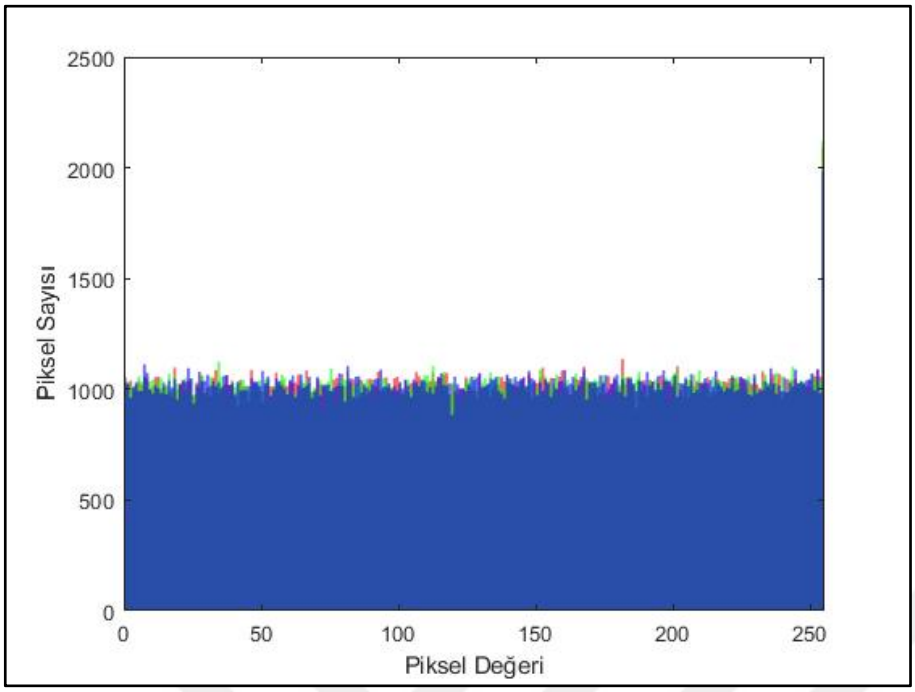
Histogram analizi

Önerilen algoritmada kullanılan sözde rasgele sayı üreteci sebebiyle hem sürekli aynı *K* değeri (Eş. 5.10) ile şifreleme yapılmamış hem de sözde rasgele piksel değerleri (Eş. 5.6) elde edilerek pikseller arası ilinti azaltılmıştır. Bu rasgele sayılar sebebiyle şifreli görüntüdeki piksel değerleri 0 ile 255 değerleri arasında üniform bir şekilde dağılmıştır. Bu sonuç ise önerilen uygulamadaki şifreleme yönteminin histogram analizi açısından güçlü bir yöntem olduğunu göstermektedir.

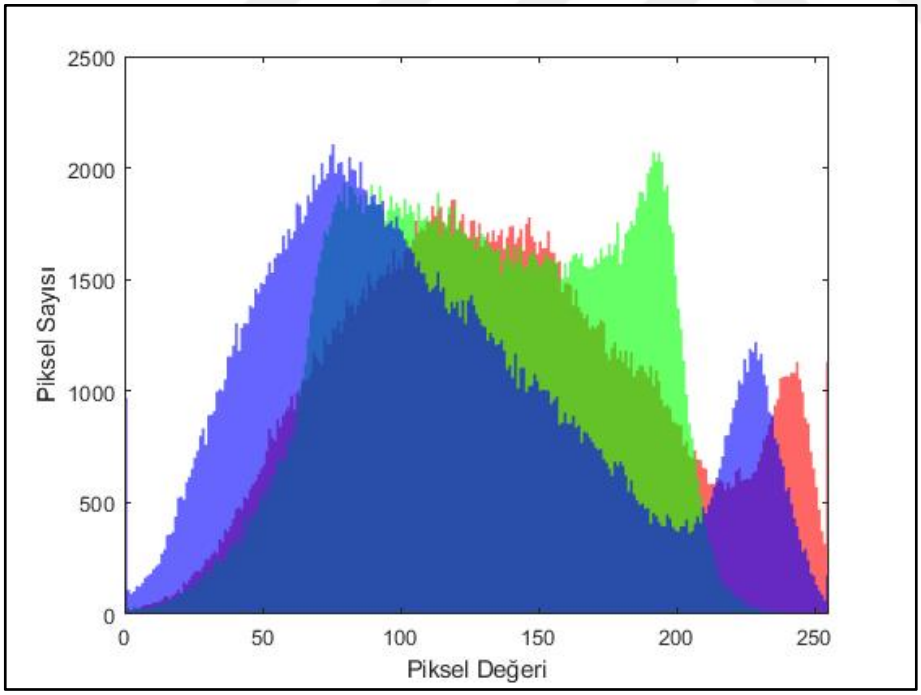
Şekil 5.11'de orijinal babun görüntüsünün histogramı, Şekil 5.12'de şifrelenmiş babun görüntüsünün histogramı ve Şekil 5.13'de şifresi çözülmüş babun görüntüsünün histogramı verilmektedir.



Şekil 5.11. Orijinal babun görüntüsünün histogramı

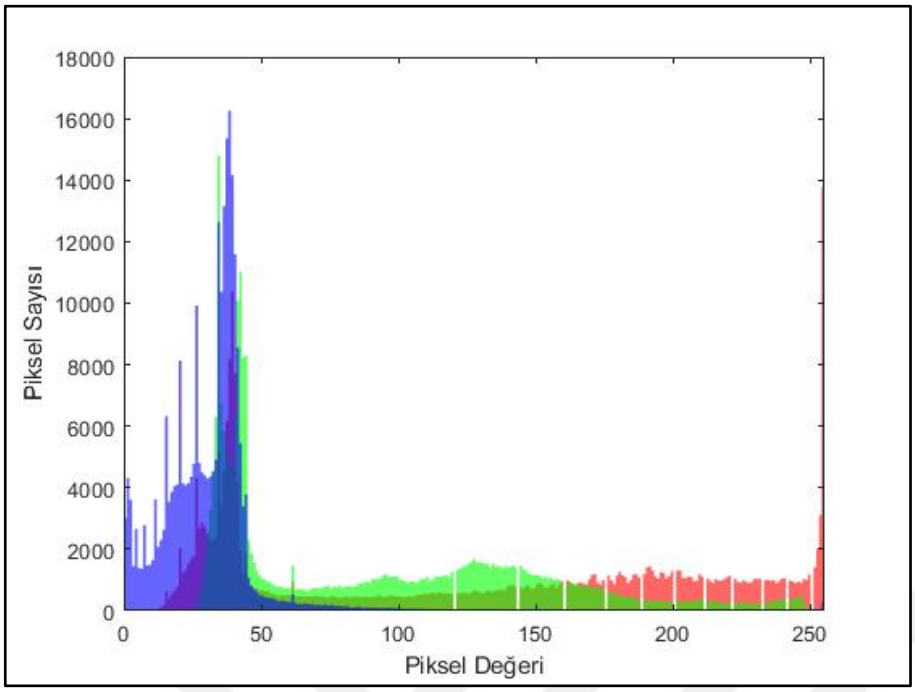


Şekil 5.12. Şifrelenmiş babun görüntüsünün histogramı

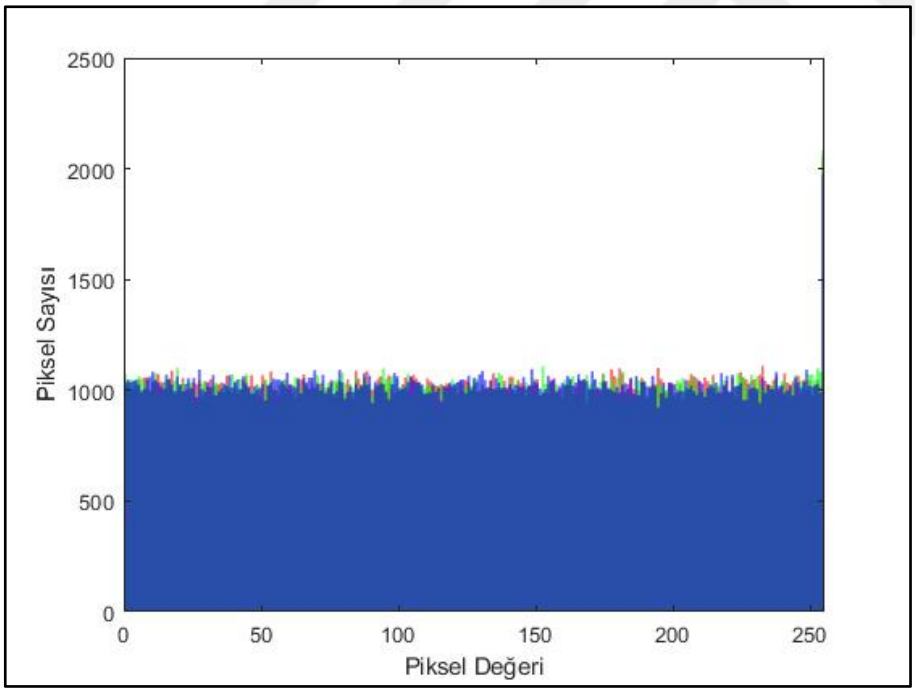


Şekil 5.13. Şifresi çözülmüş babun görüntüsünün histogramı

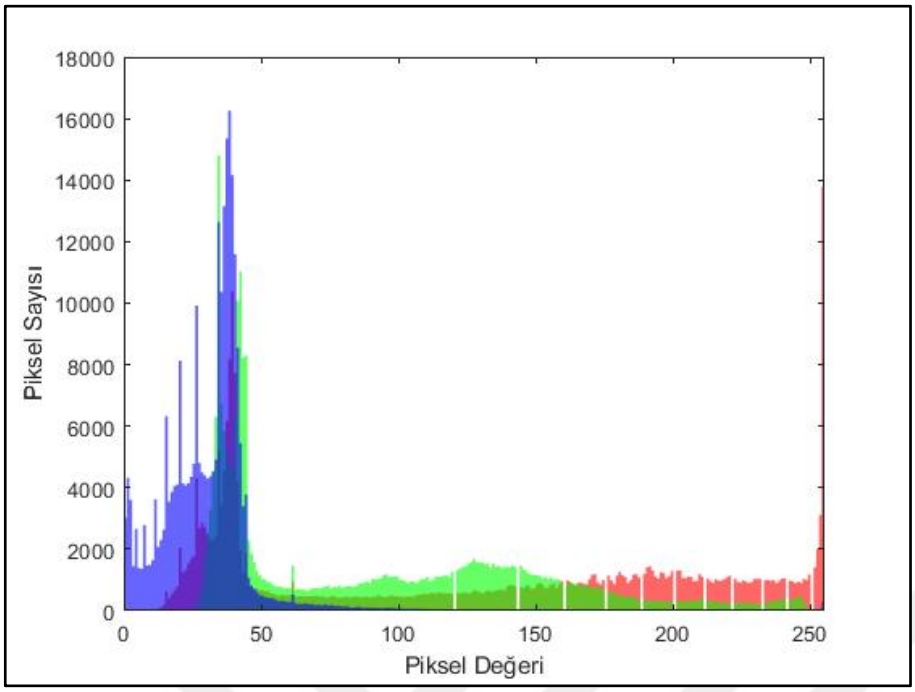
Şekil 5.14'de orijinal biberler görüntüsünün histogramı, Şekil 5.15'te şifrelenmiş biberler görüntüsünün histogramı ve Şekil 5.16'da şifresi çözülmüş biberler görüntüsünün histogramı verilmektedir.



Şekil 5.14. Orijinal biberler görüntüsünün histogramı



Şekil 5.15. Şifrelenmiş biberler görüntüsünün histogramı



Şekil 5.16. Şifresi çözülmüş biberler görüntüsünün histogramı

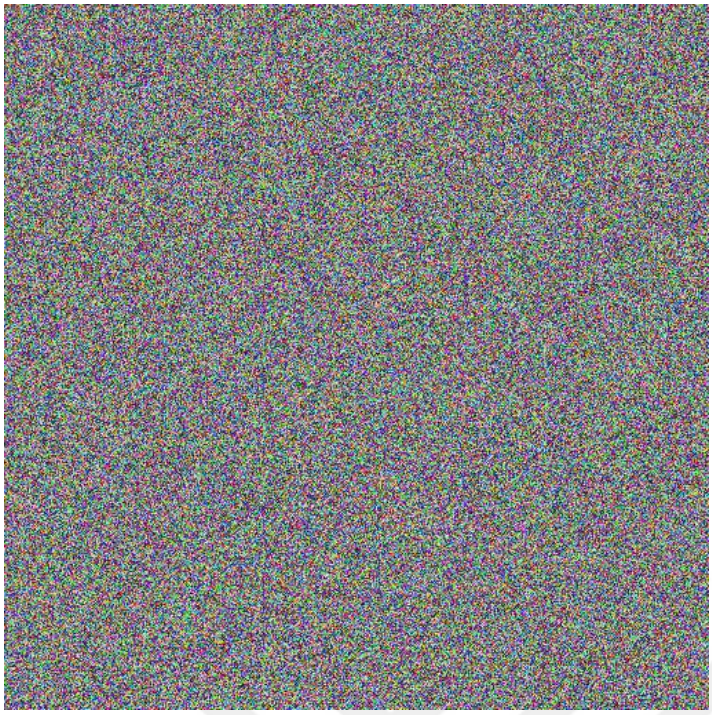
Anahtar uzunluğu

ECC, anahtar boyutuna bağlı olarak üssel olarak artan eliptik eğri ayrık logaritma problemine dayanmaktadır. Önerilen algoritmada, gerekli güvenliği sağlamak için kullanılan 512 bitlik bir eliptik eğri, anahtar boyutu açısından yeterli güvenlik sağlamaktadır.

Anahtar hassasiyeti

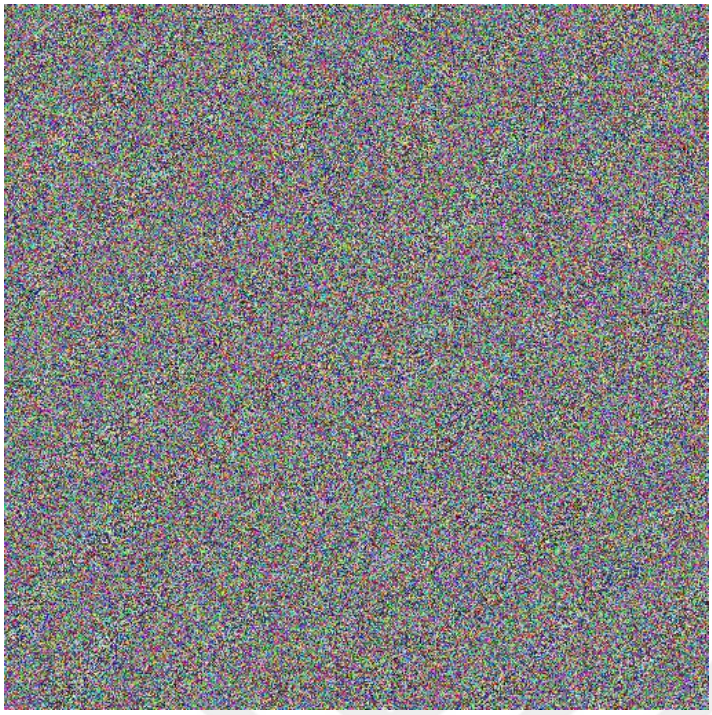
Önerilen algoritmada dijital görüntünün şifrelemede ve dijital görüntünün şifresini çözme işleminde kullanılan ortak anahtarda en ufak bir değişiklik, şifresi çözülmüş görüntü üzerinde büyük bir etki oluşturmalıdır.

Şekil 5.17, orijinal ortak anahtarla şifrelenmiş şifreli babun görüntüsünü, Şekil 5.18 orijinal ortak anahtar kullanılarak şifreli görüntüden elde edilen şifresi çözülmüş babun görüntüsünü ve Şekil 5.19 orijinal ortak anahtardan sadece 1 eksik olacak şekilde kullanılan sayıyla elde edilen şifresi çözülmüş görüntüyü ifade eder.



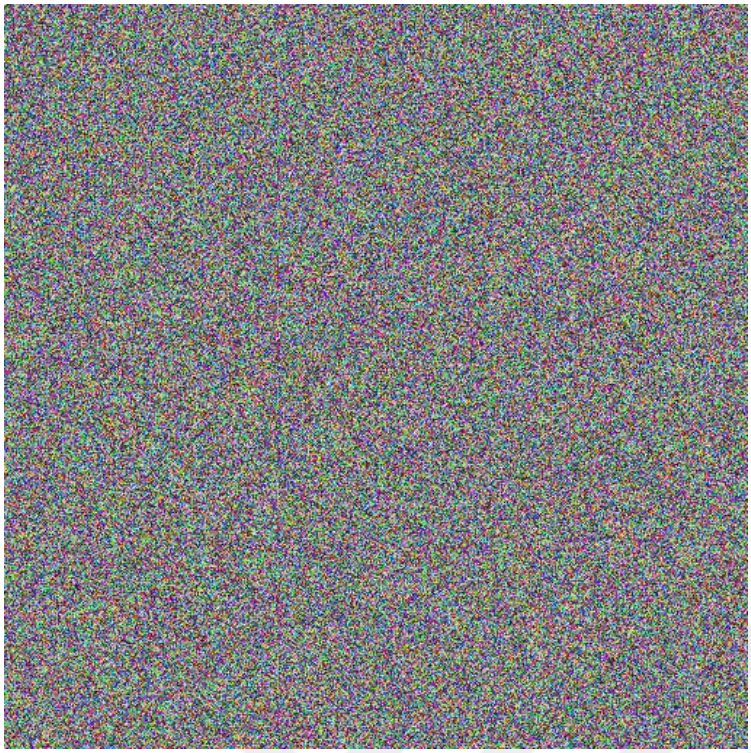
Şekil 5.17. Babun görüntüsünün *K* anahtarıyla şifrelenmiş hali

Şekil 5.18. Şifrelenmiş babun görüntüsünün *K* anahtarıyla şifresi çözülmüş hali



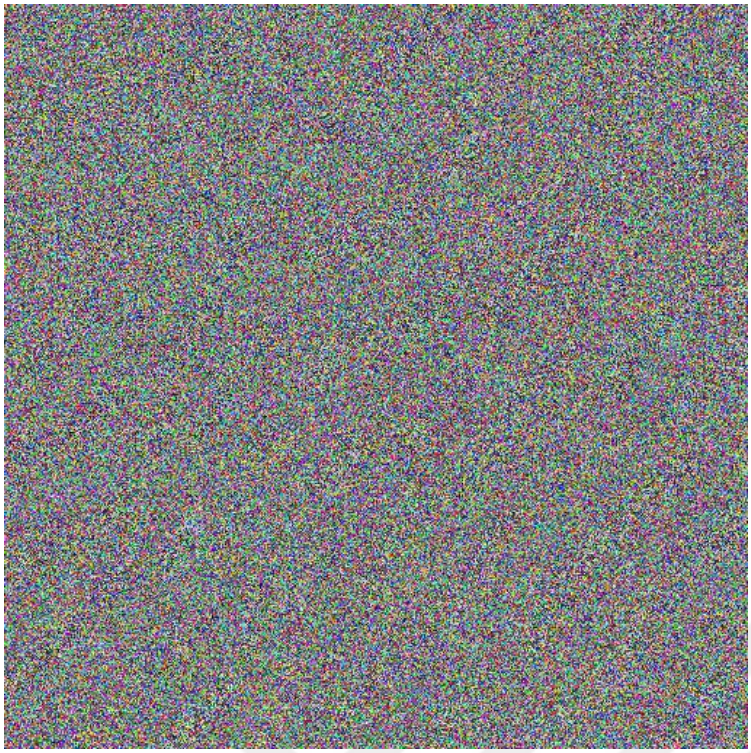
Şekil 5.19. Şifrelenmiş babun görüntüsünün (*K*-1) anahtarıyla şifresi çözülmüş hali

Şekil 5.20 orijinal ortak anahtarla şifrelenmiş şifreli biberler görüntüsünü, Şekil 5.21 orijinal ortak anahtar kullanılarak şifreli görüntüden elde edilen şifresi çözülmüş biberler görüntüsünü ve Şekil 5.22 orijinal ortak anahtardan sadece 1 eksik olacak şekilde kullanılan sayıyla elde edilen şifresi çözülmüş görüntüyü ifade eder.



Şekil 5.20. Biberler görüntüsünün *K* anahtarıyla şifrelenmiş hali

Şekil 5.21. Biberler görüntüsünün *K* anahtarıyla şifresi çözülmüş hali



Şekil 5.22. Biberler görüntüsünün (*K*-1) anahtarıyla şifresi çözülmüş hali

İlinti katsayısı

Dijital görüntülerde anlamlı bir görüntü ortaya çıkması için piksellerin belirli bir benzerlik düzeyine sahip olması gerekir.

Çizelge 5.5'de görüldüğü üzere orijinal babun görüntüsünün yatay ve dikeyde olan piksellerinin ilintisinin 1'e çok yakın olduğu görülmektedir. Bu değerler görüntüdeki yatay ve dikey ilintinin çok yüksek olduğunu göstermektedir.

Çizelge 5.5. Orijinal babun görüntüsünün ilinti katsayıları

İlinti	İlinti Katsayısı
Yatay İlinti (Kırmızı)	0,93999
Yatay İlinti (Yeşil)	0,90896
Yatay İlinti (Mavi)	0,93818
Dikey İlinti (Kırmızı)	0,86861
Dikey İlinti (Yeşil)	0,77846
Dikey İlinti (Mavi)	0,89683

Çizelge 5.5. (devam) Orijinal babun görüntüsünün ilinti katsayıları

Köşegen İlinti (Kırmızı)	0,87257
Köşegen İlinti (Yeşil)	0,80042
Köşegen İlinti (Mavi)	0,88530

Çizelge 5.6'da görüldüğü üzere orijinal biberler görüntüsünün yatay ve dikeyde olan piksellerinin ilintisinin 1'e çok yakın olduğu görülmektedir. Bu değerler görüntüdeki yatay ve dikey ilintinin çok yüksek olduğunu göstermektedir.

Çizelge 5.6. Orijinal biberler görüntüsünün ilinti katsayıları

İlinti	İlinti Katsayısı
Yatay İlinti (Kırmızı)	0,99645
Yatay İlinti (Yeşil)	0,99368
Yatay İlinti (Mavi)	0,95585
Dikey İlinti (Kırmızı)	0,99680
Dikey İlinti (Yeşil)	0,99486
Dikey İlinti (Mavi)	0,97886
Köşegen İlinti (Kırmızı)	0,99468
Köşegen İlinti (Yeşil)	0,99446
Köşegen İlinti (Mavi)	0,96265

Dijital görüntü şifreleme algoritmalarında şifrelenen görüntünün ilintisinin 0'a yakın olması, ilintinin çok düşük olduğunu gösterir. İlintinin 0'a yakın olmadığı durumlarda şifreleme algoritmasının kriptoanaliz yöntemlerine dayanıklı olduğu söylenemez.

Önerilen algoritma kullanılarak oluşturulan şifreli babun görüntüsünün ilinti katsayıları Çizelge 5.7'de görüldüğü üzere 0'a oldukça yakındır. Bu ise uygulamanın kriptoanaliz yöntemlerine dayanıklı olduğunu göstermektedir.

Çizelge 5.7. Şifreli babun görüntüsünün ilinti katsayıları

İlinti	İlinti Katsayısı
Yatay İlinti (Kırmızı)	-0,0175940

Çizelge 5.7. (devam) Şifreli babun görüntüsünün ilinti katsayıları

Yatay İlinti (Yeşil)	0,0270670
Yatay İlinti (Mavi)	-0,0545500
Dikey İlinti (Kırmızı)	-0,0288750
Dikey İlinti (Yeşil)	0,00613470
Dikey İlinti (Mavi)	-0,0158450
Köşegen İlinti (Kırmızı)	0,03382700
Köşegen İlinti (Yeşil)	0,00093329
Köşegen İlinti (Mavi)	-0,0381910

Önerilen algoritma kullanılarak oluşturulan şifreli biberler görüntüsünün ilinti katsayıları Çizelge 5.8'de görüldüğü üzere 0'a oldukça yakındır. Bu ise uygulamanın kriptoanaliz yöntemlerine dayanıklı olduğunu göstermektedir.

Çizelge 5.8. Şifreli biberler görüntüsünün ilinti katsayıları

İlinti	İlinti Katsayısı
Yatay İlinti (Kırmızı)	0,0333140
Yatay İlinti (Yeşil)	-0,0054729
Yatay İlinti (Mavi)	-0,0157270
Dikey İlinti (Kırmızı)	-0,0447090
Dikey İlinti (Yeşil)	-0,0092240
Dikey İlinti (Mavi)	-0,0480030
Köşegen İlinti (Kırmızı)	0,0207980
Köşegen İlinti (Yeşil)	0,0050615
Köşegen İlinti (Mavi)	0,0182340

Entropi analizi

Önerilen algoritmada şifrelenmiş görüntünün piksel değerlerinin sözde rasgele olması kriptografik açıdan önemli bir parametredir. Entropi analizi şifrelenmiş görüntüdeki piksellerin sözde rasgele olma oranını ölçmektedir. Kriptoanaliz yöntemlerine karşı dayanıklı olan bir şifreleme uygulamasıyla şifrelenmiş bir görüntüdeki entropi değeri 8'e oldukça yakın olmalıdır.

Önerilen algoritma ile şifrelenmiş babun görüntüsünün renk kanallarına ait ortalama entropi değerleri Çizelge 5.9'de verilmiştir.

Çizelge 5.9 Şifreli babun görüntüsünün entropi değerleri

Kanal	Entropi
Kırmızı Kanal	7,9992
Yeşil Kanal	7,9993
Mavi Kanal	7,9992
Ortalama	7,9992

Önerilen algoritma ile şifrelenmiş biberler görüntüsünün renk kanallarına ait ortalama entropi değerleri Çizelge 5.10'da verilmiştir.

Çizelge 5.10 Şifreli biberler görüntüsünün entropi değerleri

Kanal	Entropi
Kırmızı Kanal	7,9993
Yeşil Kanal	7,9993
Mavi Kanal	7,9994
Ortalama	7,9993

Bu değerlere bakıldığında önerilen uygulamanın kriptoanaliz uygulamalarına dayanıklı olduğu söylenebilir.

PSNR analizi

Önerilen algoritmada orijinal görüntü ile şifresi çözülmüş görüntü arasındaki PSNR değerleri sonsuz olarak hesaplanmıştır. Bu değerler, önerilen algoritmada şifreleme ve şifre çözme aşamalarında herhangi bir piksel değerinin kaybolmadığını göstermektedir.

6. SONUÇ VE ÖNERİLER

Bu tez çalışmasında eliptik eğri kriptografisi ile dijital görüntü şifreleme algoritması tasarlanmıştır. Yapılan tasarımda renkli görüntüler başarıyla şifrelenmiş ve şifrelenen görüntülerin şifresi başarılı bir şekilde çözülmüştür.

Önerilen algoritmada anahtar değişimi için Diffie-Hellman anahtar değişim protokolü uygulanmıştır.

Bu çalışmada şifreleme algoritmasının görüntü şifreleme değerlendirme parametreleri açısından incelemesi yapılmıştır.

Literatürdeki benzer çalışmalar ayrıntılı bir şekilde incelenmiştir. İnceleme sonucunda uygulamanın rakiplerine nazaran şifreleme ve şifre çözme algoritmalarında yaklaşık %10 oranında bir hızlanma olduğu görülmüştür. Buradaki hız artışının en büyük sebebi diğer eliptik eğri kriptografisi kullanan şifreleme algoritmalarında eliptik eğri nokta çarpımının fazla olmasıdır. Önerilen algoritmada eliptik eğri nokta çarpımı sayısı minimum tutularak işlem yükü azaltılmış ve algoritmanın daha hızlı çalışması sağlanmıştır.

Histogram analizi bakımından incelendiğinde, önerilen algoritma ile şifrelenen görüntünün histogramının üniform bir dağılıma sahip olduğu görülmüştür. Bu durum önerilen algoritmanın histogram analizi bakımından güçlü bir algoritma olduğunu göstermektedir.

Önerilen algoritma anahtar hassasiyeti bakımından incelenmiş, şifrelenen görüntünün kullanılan orijinal anahtardan bir eksik olacak şekilde yeni bir anahtar ile şifresi çözüldüğünde ortaya anlamsız bir görüntü ortaya çıkmıştır. Bu sonuç, önerilen algoritmanın anahtar hassasiyetinin yüksek olduğunu göstermektedir.

Anahtar uzunluğunun 512 bit olması önerilen algoritmanın, anahtar uzunluğu değerlendirme parametresi bakımından güçlü bir algoritma olduğunu göstermektedir.

Önerilen algoritma ile şifrelenen görüntülerin ilinti katsayılarının 0'a çok yakın çıkması, algoritmanın ilinti katsayısı açısından güçlü olduğunu göstermektedir.

Önerilen algoritma ile şifrelenen görüntülerin entropi analizlerinin incelenen örnek görüntüler için 8'e çok yakın çıkması algoritmanın entropi analizi açısından güçlü olduğunu göstermektedir.

Önerilen algoritma ile şifrelenen görüntülerin tepe sinyal gürültü oranının sonsuz olarak hesaplanması algoritmanın tepe sinyal gürültü oranı değerlendirme parametresi açısından güçlü olduğunu göstermektedir.

Önerilen algoritmaya benzer algoritmalarda ortak anahtar şifreleme amaçlı kullanılır ve bütün görüntü aynı anahtar ile şifrelenir. Bu durumun güvenlik açısından bir zafiyet olduğu tespit edilip belli periyotlarla bu ortak anahtar tohum olarak kullanılıp sözde rasgele sayılar oluşturulmuştur. Dijital görüntü bu sözde rasgele sayılarla şifrelendiği için algoritmanın ilinti katsayısı ve histogram analizi gibi değerlendirme parametreleri bakımından güçlü olduğu görülmüştür.

Ayrıca görüntüdeki piksel değerleri şifrelenmeden önce ortak anahtar katkısı ile üretilen sözde rasgele piksel değerlerine dönüştürülüp şifreleme algoritmasına girdiği için algoritmanın entropi, ilinti katsayısı ve histogram analizi değerlendirme parametreleri bakımından güçlü olduğu görülmüştür.

Bundan sonra yapılacak çalışmalarda; eliptik eğri kriptografisi kullanılarak kaotik hesaplamalarla elde edilen kaotik dijital görüntülerin şifrelenmesi konusu incelenebilir. Anahtar değişimi için yine bu çalışmada olduğu gibi Diffie-Hellman anahtar değişimi protokolü kullanılabilir.

KAYNAKLAR

1. Ye, G., Liu, M., and Wu,M. (2022). Double image encryption algorithm based on compressive sensing and elliptic curve. *Alexandria Engineering Journal*, 61(9), 6785-6795.

2. Dawahdeh, Z. E., Yaakob, S. N., and bin Othman, R. R. (2018). A new image encryption technique combining elliptic curve cryptosystem with hill cipher. *Journal of King Saud University-Computer and Information Sciences*, 30(3), 349-355.

3. Nagaraj, S., Raju, G. S. V. P., and Rao, K. K. (2015). Image encryption using elliptic curve cryptograhy and matrix. *Procedia Computer Science*, 48, 276-281.

4. Abd El-Latif, A. A., and Niu, X. (2013). A hybrid chaotic system and cyclic elliptic curve for image encryption. *AEU-International Journal of Electronics and Communications*, 67(2), 136-143.

5. Singh, L. D., and Singh, K. M. (2015). Image encryption using elliptic curve cryptography. *Procedia Computer Science*, 54, 472-481.

6. Reyad, O., Kotulski, Z., and Abd-Elhafiez, W. M. (2016). Image encryption using chaos-driven elliptic curve pseudo-random number generators. *Appl. Math. Inf. Sci*, 10(4), 1283-1292.

7. Liu, Z., Xia, T., and Wang, J. (2018). Image encryption technique based on new two-dimensional fractional-order discrete chaotic map and Menezes–Vanstone elliptic curve cryptosystem. *Chinese Physics B*, 27(3), 030502.

8. Obaid, Z. K., and Al Saffar, N. F. H. (2021). Image encryption based on elliptic curve cryptosystem. *International Journal of Electrical and Computer Engineering*, 11(2), 1293.

9. Chen, L., Chen, X., and Peng, Z. (2014). A novel public key encryption scheme for large image. *IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*.

10. Luo, Y., Quyang, X., Liu, J., and Cao, L. (2019). An image encryption method based on elliptic curve ElGamal encryption and chaotic systems. *IEEE Access*, 7, 38507-38522.

11. Bashir, Z., Malik, M. G. A., Hussain, M., Iqbal, N. (2021). Multiple RGB images encryption algorithm based on elliptic curve, improved Diffie Hellman protocol. *Multimedia Tools and Applications*, 1-31.

12. Zhang, X., and Wang, X. (2018). Digital image encryption algorithm based on elliptic curve public cryptosystem. *IEEE Access*, 6, 70025-70034.

13. Ibrahim, S., and Alharbi, A. (2020). Efficient image encryption scheme using henon map, dynamic S-boxes and elliptic curve cryptography. *IEEE Access*, 8, 194289-194302.

14. Hafsa, A., Sghaier, A., Malek, J., and Machhout, M. (2021). Image encryption method based on improved ECC and modified AES algorithm. *Multimedia Tools and Applications*, 80(13), 19769-19801.

15. Parida, P., Pradhan, C., Gao, X. Z., Roy, D. S., and Barik, R. K. (2021). Image encryption and authentication with elliptic curve cryptography and multidimensional chaotic maps. *IEEE Access*, 9, 76191-76204.

16. Laiphrakpam, D. S., and Khumanthem, M. S. (2017). Medical image encryption based on improved ElGamal encryption technique. *Optik*, 147, 88-102.

17. Azam, N. A., Ullah, I., and Hayat, U. (2021). A fast and secure public-key image encryption scheme based on Mordell elliptic curves. *Optics and Lasers in Engineering*, 137, 106371.

18. Jasra, B., Saqib, M., and Moon, A. H. (2021). *Mapping images over elliptic curve for encryption*. 6th International Conference for Convergence in Technology (I2CT).

19. Gupta, K., and Silakari, S. (2010). *Performance analysis for image Encryption using ECC*. International Conference on Computational Intelligence and Communication Networks.

20. Wu, J., Liao, X., and Yang, B. (2017). Color image encryption based on chaotic systems and elliptic curve ElGamal scheme. *Signal Processing*, 141, 109-124.

21. Afacan, E. (2021). *Kriptografiye Giriş* (Üçüncü Baskı). Ankara: Epos Yayınları, 82-122.

22. Genç, Y., and Afacan, E. (2021). *Implementation of new message encryption using elliptic curve cryptography over finite fields*. International Congress of Advanced Technology and Engineering (ICOTEN), 1-6.

23. Shih, F. Y. (2017). *Digital watermarking and steganography: fundamentals and techniques*. Boca Raton: CRC press, 80-121.

24. James, F. (1990). A review of pseudorandom number generators. *Computer Physics Communications*, 60(3), 329-344.

25. Çallıalp, F. (2011). *Örneklerle Soyut Cebir*. İstanbul: Birsen Yayınevi, 24-281.

26. Koblitz, N. (1987). Elliptic curve cryptosystems. *Math. Comput.*, 48(177), 202–203.

27. Miller, V. S. (1986). Use of Elliptic Curves in Cryptography. *In Advances in Cryptology- CRYPTO '85 Proceedings*, 25-45.

28. Abd El-Samie, F. E., Ahmed, H. E. H., Elashry, I. F., Shahieen, M. H., Faragallah, O. S., El-Rabaie, E. M., and Alshebeili, S. A. (2014). *Image Encryption A Communication Perspective.* London: CRC Press, 34-42.

29. Li, C., and Lo, K. (2011). Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. *Signal processing*, 91(4), 949-954.

30. Katti, R.S., Srinivasan, S. K., and Vosoughi, A. (2010). On the security of randomized arithmetic codes against ciphertext-only attacks. *IEEE Transactions on Information Forensics and Security*, 6(1), 19-27.

31. Habek, M., Genc, Y., Aytas, N., Akkoc, A., Afacan, E., and Yazgan, E. (2022). Digital image encryption using elliptic curve cryptography: a review. *In 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 1-8.

32. Zhang, Y., and Xiao, D. (2013). Cryptanalysis of s-box-only chaotic image ciphers against chosen plaintext attack. *Nonlinear Dynamics*, 72(4), 751- 756.

33. Ghebleh, M., Kanso, A., and Noura, H. (2014). An image encryption scheme based on irregularly decimated chaotic maps. *Signal Processing: Image Communication* 29(5), 618-627.

34. Bosnjak, L., Sre's, J., and Brumen, B. (2018). *Brute-force and dictionary attack on hashed real-world passwords*. 41st international convention on information and communication technology, electronics and microelectronics (mipro).

35. Reddy, P. R., Prasad, M. V., and Rao, D. S. (2009). Robust digital watermarking of color images under noise attacks. *International Journal of Recent Trends in Engineering*, 1(1), 334.

36. Kaur, M., and Kumar, V. (2020). A comprehensive review on image encryption techniques. *Archives of Computational Methods in Engineering*, 27(1), 15-43.

37. Zhang, W., Wong, W., Yu, H., Zhu, Z. (2013). An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion. *Communications in Nonlinear Science and Numerical Simulation*, 18(8), 2066-2080.

38. Li, X. W., Cho, S. J., and Kim, S. T. (2014). A 3D image encryption technique using computer-generated integral imaging and cellular automata transform. *Optik*, 125(13) 2983-2990.

39. Mehra, I., and Nishchal, N. K. (2015). Optical asymmetric image encryption using gyrator wavelet transform. *Optics Communications*, 354, 344-352.

40. Pehlivanlı, Ş. (2019). *Dalgacık yöntemine dayalı görüntü füzyon teknikleri*, Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara, 38-41.

41. Abbas, N. A. (2016). Image encryption based on independent component analysis and arnold's cat map. *Egyptian informatics journal*, 17(1), 139-146.

42. X. Cao, X. Wei, R. Guo, C. Wang. (2017). No embedding: a novel image cryptosystem for meaningful encryption. *Journal of Visual Communication and Image Representation*, 44, 236-249.

43. Khan, M., and Shah, T. (2014). A novel statistical analysis of chaotic S-box in image encryption. *3D Research*, 5(3), 1-8.

44. İnternet: Microsoft Visual C++, URL: https://www.visualstudio.microsoft.com, Son Erişim Tarihi: 10.03.2024.

45. İnternet: OpenCV Library, URL: https://www.opencv.org, Son Erişim Tarihi: 10.03.2024.

46. İnternet: Boost Library, URL: https://www.boost.org, Son Erişim Tarihi: 10.03.2024.

Gazili olmak ayrıcalıktır