T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLER ENSTİTÜSÜ

GRİ SEVİYE GÖRÜNTÜLERDE KRİPTOGRAFİK UYGULAMALAR

YÜKSEK LİSANS TEZİ

Hatice İmer GÜLERYÜZ
(101131106)
Anabilim Dalı : Elektronik ve Bilgisayar Eğitimi
Tez Danışmanı: Doç. Dr. Engin AVCI
OCAK - 2014

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLER ENSTİTÜSÜ
ELEKTRONİK VE BİLGİSAYAR EĞİTİMİ
ANABİLİM DALI

GRİ SEVİYE GÖRÜNTÜLERDE KRİPTOGRAFİK UYGULAMALAR

YÜKSEK LİSANS TEZİ

Hatice İmer GÜLERYÜZ
(101131106)

Tezin Enstitüye Verildiği Tarih :
Tezin Savunulduğu Tarih :

Tez Danışmanı : Doç. Dr. Engin AVCI
Diğer Jüri Üyeleri : Yrd. Doç. Dr. Murat KARABATAK
Yrd. Doç. Dr. Ferhat BAHÇECİ

OCAK - 2014

ÖNSÖZ

Bu tez çalışmasındaki genel amaç, bilginin her şeyden daha önemli olduğu günümüzde, bilgi gizliliğini en üst düzeye çıkarma çalışmalarına katkı sağlamaktır.

Çalışmalarım süresince benden yardımlarını, desteğini, sabrını ve bilgisini esirgemeyen, tezimi sonuçlandırmamı sağlayan değerli danışmanım Doç. Dr. Engin AVCI' ya, uygulama geliştirme esnasında bana katkıda bulunan hocam Türker TUNCER'e teşekkürü bir borç bilirim.

H. İmer GÜLERYÜZ

Elazığ - 2014

İÇİNDEKİLER

Sayfa No

ÖNSÖZ I

İÇİNDEKİLER III

ÖZET VI

SUMMARY VII

ŞEKİLLER LİSTESİ VIII

KISALTMALAR LİSTESİ IX

1. GİRİŞ 1

2. KRİPTOLOJİ 3

2.1. Kriptografi 3

2.1.1. Gizlilik (Privacy / Confidentiality) 4

2.1.2. Kimlik Belirleme (Authentication / Identification) 4

2.1.3. Bütünlük (Integrity) 4

2.1.4. Reddedilmezlik (Non-Repudation) 5

2.1.5. Erişim Kontrolü (Access Control) 5

2.2. Kripto Analiz 5

2.1.1. Kaba Kuvvet Yöntemi (Brute Force Attack) 6

2.1.2. Diferansiyel Kripto Analiz 6

3. KRİPTOLOJİ TARİHİ 7

4. KRİPTOLOJİ TERMİNOLOJİSİ 12

5. KRİPTOLOJİ ALGORİTMALARI 14

5.1. Simetrik Şifreleme Algoritmaları 14

5.1.1. Blok Şifreleme Algoritmaları 16

5.1.1.1. Lucifer Şifreleme Algoritması 17

5.1.1.2. Des Şifreleme Algoritması (Data Encryption Standard / Veri Şifreleme Standardı) 17

5.1.1.3 Aes Şifreleme Algoritması (Advanced Encryption Standard / Gelişmiş Şifreleme Standardı) 18

5.1.1.4. Blowfish (Balon Balığı) Şifreleme Algoritması 20

5.1.1.5. Camellia Şifreleme Algoritması 20

5.1.1.6. Feistel Şifreleme Algoritması 20

5.1.1.7. IDEA Şifreleme Algoritması (International Data Encryption Algorithm / Uluslar Arası Veri Şifreleme Algoritması) 21
5.1.1.8. Skipjack Şifreleme Algoritması 21
5.1.1.9. Playfair Şifreleme Algoritması 21
5.1.1.10. Permutation (Permütasyon) Şifreleme Algoritması 21
5.1.2. Dizi Şifreleme Algoritmaları 22
5.1.2.1. RC/4 Şifreleme Algoritması 22
5.1.2.2. A5/1 ve A5/2 Şifreleme Algoritmaları 22
5.2. Asimetrik Şifreleme Algoritmaları 23
5.2.1. Dijital İmza 24
5.2.2. RSA (Rivest, Shamir ve Adleman) Şifreleme Algoritması 25
5.2.3. Diffie Hellman Şifreleme Algoritması 26
5.2.4. DSA (Digital Signature Algorithm/Dijital İmza Algoritması) Şifreleme Algoritması 26
5.2.5. Elgamal Şifreleme Algoritması 27
5.2.6. Eliptik Eğri (Eliptic Curve) Şifreleme Algoritması 27
5.3. Karışık Algoritmalar 27
5.3.1. Sezar Şifreleme Algoritması 27
5.3.2. Vigenere Şifreleme Algoritması 28
5.3.3. Afin Şifreleme Algoritması 28
6. SAYISAL GÖRÜNTÜ VE GÖRÜNTÜ FORMATLARI 29
6.1. Sayısal Görüntü 29
6.2. Piksel 29
6.3. Nokta Ve Nokta Aralığı 30
6.4. Çözünürlük 31
6.5. Rezolasyon 32
6.6. Görüntü Formatları 32
6.6.1. JPG Görüntü Formatı 32
6.6.2. BMP Görüntü Formatı 32
6.6.3. PICT Görüntü Formatı 33
6.6.4. EPS Görüntü Formatı 33
6.6.5. GIF Görüntü Formatı 33
6.6.6. PNG Görüntü Formatı 34

6.6.7. PSD Görüntü Formatı 34
6.6.8. TIFF Görüntü Formatı..... 34
7. RENK KAVRAMLARI 36
7.1. Renk Modelleri 36
7.1.1. RGB Renk Modeli 36
7.1.2. CMYK Renk Modeli..... 37
7.1.3. CIE Renk Modeli 38
7.1.4. HSV Renk Modeli..... 38
7.1.5. HSL Renk Modeli 39
8. GÖRÜNTÜ ŞİFRELEME 40
8.1. Şifrelenmiş Resimlere Karşı Yapılan Saldırı Tipleri 41
8.2. Görüntü Şifreleme Yöntemleri Ve Algoritmaları..... 42
8.2.1. Dijital İmza Kullanılarak Görüntü Şifreleme 42
8.2.2. Vektör Kuantumlama Teknikleri İle Görüntü Şifreleme 43
8.2.3. SCAN Dili Kullanılarak Görüntü Şifreleme 44
8.2.4. Kaotik Görüntü Şifreleme Algoritmaları 45
9. UYGULAMA 48
10. SONUÇ VE ÖNERİLER 63
KAYNAKLAR 64
ÖZGEÇMİŞ 69

ÖZET

Bilgi geçmişten günümüze değerli görülmüş uğruna çok rekabet edilmiştir. Teknolojinin ilerlemesiyle en büyük güç haline gelen bilginin aktarılmasının gizliliği ve güvenilirliği büyük önem kazanmıştır. Bu güvenlik gereksinimini sağlamak için çok çeşitli şifreleme yöntemleri geliştirilmiştir.

Günümüzde kullanılan şifreleme yöntemleri güvenliği üst seviyelere çıkarmak için karmaşık teknikler içermektedir. Geliştirilen her şifreleme yöntemi aynı zamanda bu şifrelerin çözümü için gerekli olan analiz yöntemlerinin de gelişmesini sağlamaktadır. Öncekilerden daha güvenli olduğu düşünülerek ortaya çıkan yeni yöntemlerin zamanla güvenlik açıklarının olduğu, en nihayetinde bu şifrelerin kırıldığı görülmektedir. Böylelikle her seferinde kırılamayan şifreleme teknikleri arayışı verilere uygulanan yöntemlerin sayısını arttırmaktadır.

Bu çalışmada görüntü şifreleyebilmek için SCAN algoritması ve kaos tabanlı sistemler kullanılmaktadır. SCAN algoritması ile piksellerinin yeri değiştirilen resimler, Kaos tabanlı sistemlerle üretilen anahtar kullanılarak şifrelenmektedir. Bu metotlar gri seviyeli resimlere uygulanmaktadır. PSNR, NPCR, UACI ölçütleri kullanılarak şifrelemenin başarımı hesaplanmaktadır. Şifrelenmiş resimlerin histogramları çıkarılarak elde edilen sonuçların algoritmik güvenliği analiz edilmektedir. Yapılan analizler neticesinde en iyi sonuçların gerçekleştirilen hibrit metotla elde edildiği görülmektedir. Ancak performans analizi yapabilmek için metodun geniş bir alanda uygulanması gerekmektedir.

Anahtar Sözcükler: Kriptoloji, Kriptografi, Kripto Analiz, Kriptoloji Algoritmaları, Görüntü Şifreleme, Kaotik Sistemler, Scan Algoritması, Renkler, Renk modelleri, Sayısal Görüntü

SUMMARY

GRAY LEVEL IMAGES OF CRYPTOGRAPHIC APPLICATIONS

The information has always been valuable, being a subject of the competititon between companies and organizations. With progression of technology which has become the greatest power of information transmitted and reliability have gained immense importance. That the security requirements provide with many different ciphering methods had been developed.

Encryption methods which are used for nowadays, include complicated techniques to improve the security to the highest level. At the same time, each developed encryption method provides improving of analysis methods that is needed. Even if the new methods are thought that they are safier than the old ones, they also have some security gaps. Because of that reason, these passwords are hacked. Thus, each time the unhacked encryption techniques rise the number of the methods which is applied data.

In this study scan algorithm and chaos based system were used. These methods are applied to gray-level images. PSNR, NPCR, UACI performance metrics are calculated using the encryption. Histograms of encrypted images subtracted that algorithmic results obtained showed that there were analyzed.

Key Words: Cryptology, Cryptography, Analysis of Crypto, Cryptography Algorithms, Image Encryption, Chaotic Systems, Scan Algorithm, Colours, Colours, Models, Digital Images.

ŞEKİLLER LİSTESİ

Sayfa No

Şekil 1.1. Kriptolojinin ana yapısı 3
Şekil 3.1. Skytale aracının yapısı 7
Şekil 3.2. Enigma makinesi....9
Şekil 5.1. Şifreleme algoritmalarının genel diyagramı 14
Şekil 5.2. Simetrik şifreleme algoritmalarının genel yapısı....15
Şekil 5.3. Blok şifreleme algoritmalarının genel yapısı....16
Şekil 5.4. AES şifreleme algoritmasının genel yapısı 19
Şekil 5.5. Asimetrik şifreleme algoritmalarının genel yapısı....23
Şekil 6.1. Sayısal görüntüde pikselin gösterimi 29
Şekil 6.2. İkili görüntü 30
Şekil 6.3. 256 X 256 piksel 31
Şekil 6.4. 128 x 128 piksel....31
Şekil 6.5. 64 X 64 piksel....31
Şekil 6.6. 32 x 32 piksel....31
Şekil 7.1. RGB renk modeli 37
Şekil 7.2. CMYK renk modeli....38
Şekil 7.3. HSV renk modeli 39
Şekil 8.1. SCAN dilindeki temel tarama desenleri 45
Şekil 9.1. Uygulamada kullanılan lojistik harita 49
Şekil 9.2. Resimlerin orijinal halleri....50
Şekil 9.3. Resimlerin 256 bitlik kaotik anahtarla şifrelenmiş halleri 51
Şekil 9.5. Analiz edilmiş resimler 53
Şekil 9.6. Orjinal resimlerin histogramları....54
Şekil 9.7. Kaos tabanlı rastgele sayı üreteci kullanılarak şifrelenen resimlerin histogramları....54
Şekil 9.9. SCAN algoritması kullanılarak şifrelenen resimler 56
Şekil 9.10. SCAN algoritması kullanılarak şifrelenen resmin histogramları....57
Şekil 9.12. Geliştirilen hibrit metotla şifrelenen resimler....59
Şekil 9.13. Geliştirilen hibrit metotla şifrelenen resmin histogramları 60

KISALTMALAR LİSTESİ

ABD : Amerika Birleşik Devleti

FBI : Federal Bureau of Investigation (Federal Soruşturma Bürosu)

NSA : National Security Agency (Ulusal Güvenlik Ajansı)

DES : Data Encryption Standard (Veri Şifreleme Standardı)

RSA : Rivest Shamir Adleman

IDEA : International Data Encryption Algorithm (Uluslararası Veri Şifreleme Algoritması)

PGP : Pretty Good Privacy (Mükemmel Şifreleme)

ASCII : American Standard Code for Information Interchange (Bilgi Değişimi İçin Amerikan Standart Kodlama Sistemi)

SHA-1 : Secure Hash Algorithm (Güvenli Karma Algoritma)

NIST : National Institute of Standard and Technology (Ulusal Standartlar ve Teknoloji Enstitüsü)

AES : Advanced Encryption Standard (Gelişmiş Şifreleme Standardı)

IBM : International Business Machines (Uluslararası İş Makineleri)

NTT : Nippon Telegraph and Telephone (Nippon Telgraf ve Telefon Şirketi)

RC4 : Rivest Cipher 4 (Rivest Şifresi 4)

GSM : Global System for Mobile Communications (Mobil İletişim İçin Küresel Sistem)

MIT : Massachusetts Institute of Technology (Üniversitesi)

DSA : Digital Signature Algorithm (Dijital İmza Algoritması)

JPG : Joint Photographic Experts Group (Birleşik Fotoğraf Uzmanları Grubu)

BMP : Bitmap (Görüntüyü bit bit tanımlayan sıkıştırılmamış resim dosyası)

PCX : Personal Computer Exchange (Kişisel Bilgisayar Borsası)

EPS : Encapsulated PostScript (Kapsüllenmiş Elyazısı)

GIF : Graphics Interchange Format (Grafik Değiştirme Biçimi)

PNG : Portable Network Graphics (Taşınabilir Ağ Grafiği)

PSD : Photoshop Document (Photoshop Belgesi)

TIFF	**:** Tagged Image File Format (Etiketli Resim Dosya Formatı)
NM	**:** Nanometre
RGB	**:** Red Green Blue (Kırmızı, Yeşil, Mavi)
CIE	**:** Commission Intenationale de I'Eclairage (Uluslararası Işıklandırma Komisyonu)
HSV	**:** Hue Saturation Value (Ton, Doygunluk, Değer)
HSL	**:** Hue Saturation Lightness (Ton, Doygunluk, Parlaklık)
BCH	**:** Binary Coded Hexadecimal (İkilik Sayıdan Onaltılık Sayıya Kodlama)
NPCR	**:**The Number of Changing Pixel Rate (Değişen Piksel Oranı Sayısı)
UACI	**:** The Unified Averaged Change Intensity (Birleştirilmiş Ortalama Değişim Yoğunluğu)
PSNR	**:** Peak Signal to Noise Ratio (İşaret Gürültü Oranı)
FIPS46	: Federal Information Processing Standard (ABD Bilgi İşlem Standardı Enstitüsü)

1. GİRİŞ

Bilgiyi korumak, saklamak her dönemde çok önemli bir konu olarak görülmüştür. Bilgileri korumak, saklamak, kötü niyetli kişilerin eline geçmesine engel olmak için yapılan çalışmalar kriptografi bilimi içerisinde yer almaktadır. Kriprografik metotlar sayesinde bilgi anlaşılmaz bir hale dönüştürülmekte, şifrelenmekte ve emniyetli bir şekilde hedefe ulaştırılmaktadır. Ulaştırılan hedefte de istenildiği takdirde, bilgi tekrar eski orijinal haline çevrilmekte, şifresi çözülmektedir.

Gizliliği önemli olan bilgilerin internet kanalıyla yoğun olarak gönderildiği günümüzde kriptografinin önemi daha da artmaktadır. Bu durumun başlıca sebebi internet üzerinden gönderilen verilerin halka açık bir ağdan geçmesi, verilerin istenmeyen kişilerin erişimine uygun olmasıdır. Dolayısıyla kullanılan şifreleme yöntemleri güvenliği arttırmak için karmaşık teknikler içermekte ve matematiksel temellere dayanmaktadır.

Geliştirilen her şifreleme yöntemi aynı zamanda bu şifrelerin çözümü için gerekli olan analiz yöntemlerinin, kripto analizin gelişmesini sağlamaktadır. Kripto analiz, şifrelenmiş bir sistemi inceleyerek şifrelenmiş olan bilginin açık halini elde etmeye, şifreyi kırmaya çalışmaktadır. Öncekilerden daha güvenli olduğu düşünülerek ortaya çıkan yeni yöntemlerin zamanla güvenlik açıklarının olduğu ve en nihayetinde bu şifrelerin kırıldığı görülmektedir. Böylelikle her seferinde kırılamayan şifreleme yöntemleri arayışı yeni yöntemlerin sayısını arttırmaktadır. Bu yeni yöntemler sadece metin değil, günlük hayatımızda çok geniş kullanım alanına sahip olan ses, resim ve diğer multimedya bilgileri de kapsamaktadır.

Bu tez çalışmasının hazırlanmasındaki genel amaç; bilginin her şeyden daha önemli olduğu günümüzde, bilgi gizliliğini en üst düzeye çıkarma çalışmalarına katkı sağlamaktır. Kriptolojinin resim dosyaları üzerindeki uygulamaları bu tez kapsamında ele alınmaktadır. Görüntü şifrelemede genellikle simetrik şifreleme metotları kullanılmaktadır. Simetrik şifreleme metotlarında sabit bir anahtarla resim doğrudan XOR işlemine tabi tutulmaktadır. Bu metotların en büyük dezavantajı ise resim doğrudan XOR işlemine tabi tutulduğunda resmin ana hatlarının belirginliğini koruması ve böylece sağlam bir şifreleme gerçekleştirilememesidir. Şifrelemenin doğru yapıldığını gösterebilmek için ekstradan resmin piksel değerleri ile oynanmaktadır. Bu uygulamalar 9. bölümde net bir şekilde anlatılmaktadır. Bu dezavantajları giderebilmek için SCAN algoritması kullanılmaktadır.

Tez düzeni genel hatlarıyla şöyledir; 1. bölüm giriş bölümüdür. 2. bölümde kriptoloji, kriptografi, kriptoanaliz kavramları, 3. bölümde kriptoloji tarihinde geçmişten günümüze doğru yaşanan gelişmeler, 4. bölümde kriptoloji terminolojisi, 5. bölümde geleneksel kriptoloji algoritmaları, 6. bölümde sayısal görüntü ve görüntü formatları, 7. bölümde renk kavramları, renk modelleri, 8. bölümde görüntü şifreleme açıklanmaktadır. 9. bölümde SCAN algoritmasıyla, Kaos tabanlı sistemler kullanılarak görüntü şifreleme uygulamaları yapılmaktadır. 10. ve son bölüm ise sonuç ve öneriler bölümüdür.

2. KRİPTOLOJİ

Kriptoloji gizli, şifreli belgeler bilimi olarak adlandırılmaktadır. Köken olarak Yunanca "Kryptos Logos" kelimelerinden türetilmektedir. "Kryptos" kelimesi gizli dünya, "logos" kelimesi ise sebep - sonuç ilişkisi kurma anlamı taşımaktadır. Kriptoloji kelimesinin dünya dillerindeki karşılığı da genellikle bu orijinal halini korumaktadır [1].

Kavram olarak kriptoloji şöyle ifade edilmektedir. Haberleşen birden fazla sistemin güvenli bilgi alışverişinde bulunabilmeleri için kullandıkları, temeli zor matematiksel problemlere dayalı tekniklerin bütünüdür. 2 farklı ana dalı vardır [2, 3] . Bunlar;

1. Kriptografi
2. Kripto Analiz

Şekil 1.1. Kriptolojinin ana yapısı

2.1. Kriptografi

Kriptografi, şifreleme tekniklerinin tamamını inceleyen bilim dalına denilmektedir. Yunanca gizli, saklı anlamına gelen "kript" ve yazı anlamına gelen "graf" kelimelerinden türetilmektedir. Şifre yazımı anlamına gelmektedir. Bu bilime ortaya çıktığı ilk zamanlarda

daha çok askeri alanlarda ihtiyaç duyulmuştur. Ancak günümüzde teknolojinin gelişimiyle en büyük güç haline gelen bilginin şifrelenmesi her alanda önemli olmaktadır.

Kriptografi; gizlilik, kimlik denetimi, bütünlük gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemler bütünü olarak da ifade edilebilmektedir. Bu yöntemler, bir bilginin iletimi esnasında karşılaşılabilecek aktif ya da pasif ataklardan bilgiyi, dolayısıyla bilgi ile beraber bilginin göndericisini ve alıcısını da koruma amacı gütmektedir . Diğer bir ifade ile kriptografi, okunabilir durumdaki bir bilginin istenmeyen taraflarca okunamayacak bir hale dönüştürülmesinde kullanılan tekniklerin tümü olarak düşünülebilmektedir[4].

2.1.1. Gizlilik (Privacy / Confidentiality)

Taşınan, gönderilen bilginin, bilgiyi görme yetkisi olanlar dışındaki herkesten saklanmasıdır. Bilginin gizli kalması, üçüncü kişiler tarafından okunamamasıdır. Gizlilik, bilgi güvenliği için gerekli olan temel ölçütlerdendir. Bilginin gizliliğini sağlayabilmek için birçok veri gizleme ve şifreleme yöntemleri geliştirilmiştir[4].

2.1.2. Kimlik Belirleme (Authentication / Identification)

Bilgiyi gönderen kişinin gerçekten mesajı gönderen kişi olup olmadığının doğrulanmasıdır. Şifreleme teknikleri ile gönderilen mesajlar üzerine özel imzalar eklenerek, mesajı gönderen kişinin doğru kişi olduğundan emin olunması sağlanabilmektedir.

Çeşitli algoritmalarla oluşturulan bu özel imzalar, alıcı kişi tarafından belirli tekniklerle doğrulanabilmektedir. Bu imza oluşturma ve doğrulama işlemi dijital imza olarak adlandırılmaktadır [5].

2.1.3. Bütünlük (Integrity)

Bilginin saklanması, iletilmesi vs. süreçlerinde bilginin gönderildiği gibi olduğunun, üzerinde hiçbir değişiklik yapılmadığının garantisidir. Bilginin içeriğinde meydana gelebilecek küçük bir değişiklik bazen tamamıyla bilgiyi anlamsızlaştırabilmektedir[4].

2.1.4. Reddedilmezlik (Non-Repudation)

Alıcı veya gönderici tarafından iletilen mesajın inkâr edilememesidir. Mesaj gönderildiğinde alıcı taraf gönderen tarafın mesajı gönderdiğini, aynı şekilde gönderen tarafta alıcı tarafın mesajı aldığını ispatlayabilme imkânına sahip olmaktadır[4].

2.1.5. Erişim Kontrolü (Access Control)

İzinsiz kişilerin erişimlerinin yasak olduğu kaynaklara erişemeyeceklerinin garantisidir. Erişim kontrolü servisleri, kimlik denetimi yapılmış varlıkların kaynaklara ancak kendilerine izin verilen şekilde erişebilecekleri garantisini vermekle yükümlüdür [4].

2.2. Kripto Analiz

Şifrelenmiş bir metni veya sistemi çözebilmek için yapılan bütün saldırıları inceleyen bilim dalı olarak ifade edilmektedir. Kripto analiz, şifrelenmiş bir sistemi inceleyerek şifrelenmiş olan mesajın açık halini elde etmeye çalışmaktadır. Kısaca şifre kırma bilimidir. Kriptoloji bilimi içerisinde oldukça önemli bir yere sahiptir[6].

Bilinen ilk kripto analiz çalışması 9. yüzyılda matematikçi Ebu Yusuf Yakup tarafından yazılan "A Manuscript on Deciphering Cryptographic Messages" adlı eserde yer almaktadır. İkinci Dünya Savaşıyla kripto analiz biliminin önemi daha çok artmıştır. Kripto analizle Almanların Enigma şifresi kırılmış ve savaşın gidişatı değişmiştir[7].

Kripto analiz konusunda devrim yapan olay Kindi'nin yazmış olduğu "Şifreli Mesajların Kırılması Üzerine" adlı eserdir. Bu eserin bir bölümünde "Sıklık Analizi Yöntemine" şöyle açıklık getirilmektedir. "Hangi dilde yazıldığı bilinen şifreli mesajları çözebilmek için; aynı dilde yazılmış bir sayfayı dolduracak uzunlukta farklı bir düz yazı bulmak ve bu yazıda her bir harfin kaç kere geçtiğini saymak gerekir. En çok geçen harfe "birinci", sonraki en çok geçen harfe "ikinci", en çok geçen üçüncü harfe "üçüncü" şeklinde örnekte geçen bütün harfler tanımlanarak sıralanmalıdır. Çözülmek istenen şifreli metin örnek metindeki sembollerle aynı şekilde sınıflandırılır. En çok geçen sembolün yerine örnek metindeki "birinci" harf, ikinci en çok geçen sembolün yerine "ikinci" harf konularak tüm harfler tamamlanana kadar devam edilir. Çözüm sağlanmaya çalışılır."

Kripto analiz çalışması sırasında, kripto analiz yapan kişinin elinde genellikle çok az bilgi vardır. Bu bilgilerin değişik durumları şunlardır:

1. Şifrelenmiş Mesajın Analizi: Kripto analiz yapan kişinin elinde sadece şifrelenmiş mesaj bulunmaktadır. Mesajın açık haliyle ilgili ipucu dahi yoktur.

2. Tam Bir Açık Mesajın Analizi: Kripto analiz yapan kişi mesajın hem açık hem de şifreli halinin tamamına sahiptir.

3. Yarım Olarak Elde Edilmiş Açık Mesajın Analizi: Kripto analiz yapan kişinin elinde mesajın açık halinin bir kısmı ile şifreli halinin tamamı mevcuttur.

4. İstenen Açık Mesajın Şifrelenmiş Halinin Analizi: Kripto analiz yapan kişi istediğinde, açık olan mesajın şifreli halini elde edebilmektedir.

5. Şifrelenmiş Mesajın Şifreleme Algoritması Bilinerek Yapılan Analizi: Kripto analiz yapan kişi mesajın hangi yöntemle şifrelendiği bilgisine sahiptir.

Kripto analiz Yöntemleri Şunlardır:

2.1.1. Kaba Kuvvet Yöntemi (Brute Force Attack)

Kriptografi biliminde bir şifreyi çözmek için kullanılan en basit saldırı yöntemidir. Bu yöntemde bütün ihtimaller tek tek veya belirli bir mantığa göre deneme yanılma yoluyla denenmektedir. Şifrenin çözülmesi zorluk derecesine göre zaman almaktadır. Eski bir yöntem olsa da günümüzde halen kullanılmaktadır[1].

2.1.2. Diferansiyel Kripto Analiz

İlk kez 1990 yılında Eli Biham ve Adi Shamir tarafından yayımlanan "Des Benzeri Şifre Sistemlerinin Diferansiyel Kriptoanalizi / (Differantial Cryptanalysis of Des Live Cryptosytems)" adlı makalelerinde kamuoyuna açıklanan bir saldırı yöntemidir. Bu yöntem bilinen açık ve şifreli mesaj çiftleri arasındaki farkların hesaplanmasına dayanmaktadır[1].

3. KRİPTOLOJİ TARİHİ

Kriptoloji insanlığın var oluşundan bu yana çeşitli evreler geçirerek günümüze kadar gelmiştir. Kısaca insanlık ne zaman var olmuşsa kriptolojide o zaman var olmuştur. Ancak asıl ivme son yüzyılda, özelliklede bilgisayar çağı olarak adlandırılan son 50 yılda kat edilmiştir.

M.Ö. 1900'lü yıllarda bir Mısırlı kâtibin yazdığı kitabelerde standart dışı hiyeroglif işaretler bulunmuştur.

Sıkı askeri disiplinleri ile bilinen kuzey Yunanistan'daki Sparta adlı tarihi şehirde M.Ö. 475 yılında bilinen ilk kriptografik iletişim aracı "Skytale" geliştirilmiştir[8].

Skytale; Antik Yunanlıların savaşlarda kullandığı bir iletişim aracıdır. Basit olduğu kadar o günün şartlarına göre dâhice bir cihazdır. Skytale adı verilen sabit genişlikte bir sopa üzerine, şifrelenecek mesaj yatay olarak yazılmakta kalan boşluklarda rastgele harflerle doldurulmaktadır. Daha sonra bu kâğıt sopadan çıkarılıp karşı tarafa gönderilmektedir. Alıcının bu mesajı okuyabilmesi için kâğıdın aynı genişlikteki bir "Skytale" ile sarılması gerekmektedir. Sopa daha geniş veya daha dar olursa doğru metin okunamamaktadır.

Şekil 3.1. Skytale aracının yapısı

M.Ö. 60 – 50 dolaylarında Julius Caesar normal alfabede bulunan harflerin yerini değiştirerek oluşturduğu şifreleme yöntemini devlet haberleşmesinde kullanmıştır. Bu yöntemde açık metindeki her harf, alfabede kendisinden 3 harf sonraki harfle değiştirilerek şifrelenmektedir. Günümüzde Sezar şifreleme olarak bilinmektedir[9].

1000 – 1200'lü yıllara gelindiğinde Gaznelilerden günümüze ulaşmış bazı dokümanlarda şifrelenmiş metinlere rastlanmıştır. Tarihçilerin bu dönemle ilgili kaleme

aldıkları yazılarına göre devletin üst düzey görevlilerine yeni görev yerlerine giderlerken özel şifreleme bilgileri verilmektedir.

1586 yılında Fransız şifreci Blaise de Vigenere tarafından şifreleme bilimi hakkında bir kitap yazılmıştır. Bu kitapta ilk olarak açık ve şifreli metin için otomatik anahtarlama yönteminden bahsedilmiştir.

1623 yılına gelindiğinde Sir Francis Bacon, 5 bit ikili kodlamayla karakter tipi değişikliğine dayanan stenografi yöntemini bulmuştur.

Gizli bilgileri şifrelemenin kolay yollarından biride 16.yy'da yaşamış olan ünlü İtalyan matematikçi, yazar Girolamo Kardano tarafından bulunmuştur. Metodunun çalışması şöyledir: Bir kâğıda belirli aralıklarla delikler açılıp "Kardano Kalıbı" oluşturulmaktadır. Bu kalıp boş kâğıt üzerine yerleştirilmekte ve her harf bir deliğe konulacak şekilde şifreli mesaj yazılmaktadır. Daha sonra bu kalıp kaldırılıp şifreli mesajın arasındaki boşluklar, anlamlı bir metin elde edilecek şekilde harflerle doldurulmaktadır. Böylece şifrelenmiş mesaj bir metnin arasına sıkıştırılmaktadır. Kardano kalıbı şifreli mesajın ulaştırılacağı kişide de varsa şifrenin çözülmesi kolay olmaktadır.

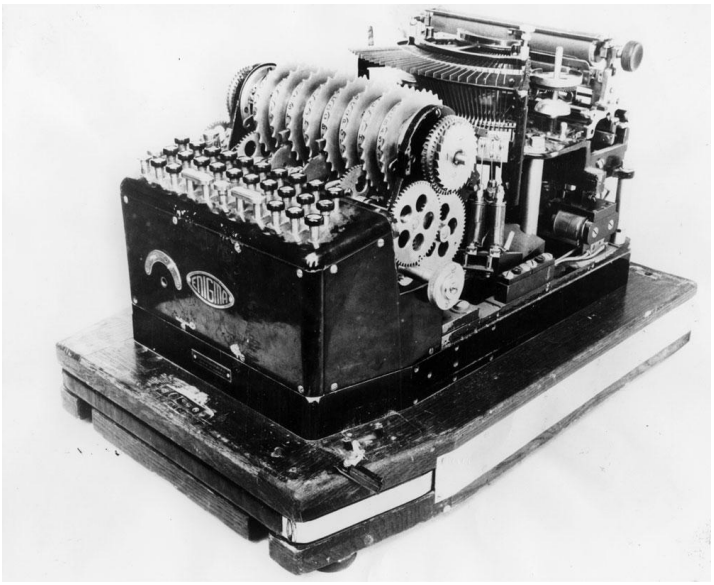
Aynı mantıktan hareketle daha yakın tarihten örnek verirsek; gazeteci, yazar İlhan Selçuk'un 1980 yılında tutuklu bulunduğu sürede benzer bir yöntemle hapishane dışındakilere şifreli mektuplar yazdığı bilinmektir. İlhan Selçuk yazdığı mektuplarda her noktadan sonra 7. sıraya sakladığı harflerle, iletmek istediği yazıların cezaevi yönetiminden geçmesini sağlayarak dışarıya haber vermiştir.

1790 yılında ise Thomas Jefferson, Strip Cipher adında bir makine geliştirmiştir. Bu makine II. Dünya savaşında ABD donanması tarafından kullanılmıştır.

1917'ye gelindiğinde Joseph Mauborgne ve Gilbert Vernam mükemmel şifreleme sistemi olan "one –time pad"i bulmuşlardır. One-time pad (one-time password/tek kullanımlık şifre) yöntemi isminden de anlaşılacağı üzere, her kimlik denetimi yapılması gerektiğinde kullanıcının yeni tek kullanımlık bir şifre ile sisteme tanıtılmasını sağlayan yapıdır. Bu sistemde kullanıcının şifresi kötü niyetli kişilerin eline geçse bile hiçbir anlam ifade etmemektedir. Çünkü bir sonraki seferde o şifre geçersiz olmaktadır.

1918'de Alman mühendis Arthur Scherbius tarafından bir kripto cihazı icat edilmiş ve cihaza "muamma, bilmece" anlamına gelen Enigma ismi verilmiştir. Enigma Makinesi verinin şifrelenmesinde kullanılmıştır. Ancak bu makine İngiliz matematikçi, bilgisayar biliminin kurucusu kabul edilen, kriptolog Alan Matthison Turing ve ekibi tarafından, Colossus adlı ilk tüplü bilgisayar yardımıyla çözülmüştür. Bu sayede bazı tarihçiler savaşın

bir yıl daha erken bittiğini söylemektedir. Ve Alan Turing, bu şifreleme yöntemini kırarak savaş üzerinde çok önemli bir rol oynadığı için savaşın kahramanı ilan edilmiştir.



Şekil 3.2. Enigma makinesi

Enigma makinesinden kısaca bahsetmek gerekirse gizli mesajların şifrelenmesi ve çözülmesi amacıyla kullanılan, 10 kg ağırlığında, elektro-mekanik bir makinedir. Olasılık üreten bir mekanizmaya sahiptir. Daktilo klavyesine benzer klavye tuşlarına basıldığında olasılık üreten mekanizmaları dönerek şifreler üretmektedir.

1920 ve 1930'larda ise FBI, içki kaçakçılarının haberleşme sistemini çözebilmek için araştırmalar yapmak üzere bir ofis kurmuştur. William Frederick Friedman, Riverbank laboratuarlarını kurmuş ve ABD için kripto analiz çalışmaları yaparak, II. Dünya savaşında Japonların Purple Machine şifreleme sistemini çözmüştür.

1948-1949 yılları kriptografinin matematiksel olarak formülize edildiği yıllardır. Shannon tarafından bu alanda yayımlanan ilk bildiri çağdaş kriptografinin temellerini oluşturmaktadır.

04.11.1952 yılında ABD'de ulusal güvenlik teşkilatı (NSA) kurulmuştur. Bu teşkilat bilgi toplamak için internet, telefon görüşmeleri ve e-postaları izlemiştir. İllegal olarak sivillerin telefon görüşmelerini kaydettikleri ve telekomünikasyon şirketlerinden telefon kayıtlarını aldıkları ortaya çıkmıştır.

1970 yılında Alman kriptolog Horst Feister, IBM firmasında yaptığı çalışmalar sırasında DES algoritmasının temelini oluşturan, dünyanın halka açık ilk simetrik şifreleme standardı olan Lucifer algoritmasını geliştirmiştir.

1976 yılında 56 bit anahtar uzunluğu ile bilinen DES algoritması ABD Bilgi İşlem Standardı Enstitüsünce (FIPS 46/Federal Information Processing Standard) standartlaştırılmıştır.

Yine aynı yıl Whitfield Diffie ve Martin Hellman açık anahtar sistemini anlattıkları makalelerini yayınlanmışlardır.

1978 yılında Ronald L Rivest, Adi Shamir ve Leonard M. Adleman 1976 yılında temelini attıkları ve isimlerinin baş harflerinden oluşan RSA (Rivest – Shamir - Adleman) algoritmasını bulmuşlardır.

1985 yılına gelindiğinde ise Neal Koblitz ve Victor S. Miller yaptıkları çalışmalarda Eliptik Eğri Şifreleme Algoritmasını duyurmuşlardır.

1990'da Çinli Profesör Xuejia Lai ve ABD'li Profesör James Massey IDEA Blok Şifreleme Algoritmasını bulmuşlardır.

1991 yılında ABD'li Phil Zimmerman PGP sistemini geliştirip yayınlamıştır.

PGP (Pretty Good Privacy/Mükemmel Şifreleme) günümüzde en çok kullanılan şifreleme ve sayısal imzalama programıdır. Birçok işletim sistemi ile çalışma özelliğine sahip olduğu için dünyada kabul görmüş bir yazılımdır. Temeli ilerleyen bölümlerde anlatılacak olan "RSA" asimetrik şifreleme algoritmasına dayanmaktadır. Çok güçlü algoritmalar içerdiği için güvenlik düzeyi oldukça yüksektir. PGP yönteminin en önemli özelliklerinden biri şifrelenen mesajın başına zaman damgaları koymasıdır. Bu yöntemle gönderilen dosyaların başkası tarafından kopyalanıp, farklı bir zamanda farklı bir alıcıya gönderilmesi engellenmiş olunmaktadır.

PGP programı şifreleme işlemini 3 adımda gerçekleştirmektedir.

İlk olarak gönderici taraf sahip olduğu gizli anahtar sayesinde mesajın özünü imzalamakta daha sonra mesajı sıkıştırmaktadır. Son olarak da sıkıştırılan mesaj şifrelenmekte ve gizli anahtarla alıcının anahtarı da şifrelenip, şifrelenmiş olan mesaj paketinin başına eklenmektedir. Bu işlemlerden sonra paket elle ASCII formatına (ASCII formatı, Latin alfabesi üzerine kurulu olan 7 bitlik bir karakter setidir.) çevrilmektedir. Mesaj alıcıya ulaştığında basamak sondan başa doğru tekrarlanmaktadır.

1995'de SHA-I Özet Algoritması (Secure Hash Algorithm/Güvenli Karma Algoritma) ABD'nin NIST (National Institute of Standarts and Technology/Ulusal

Standartlar ve Teknoloji Enstitüsü Kurumu) tarafından standartlaştırılmıştır. SHA-I özet algoritmasından kısaca bahsetmek gerekirse herhangi bir uzunluktaki metnin sabit uzunlukta özetini oluşturan, kimlik doğrulama ve veri bütünlüğü ile ilgili uygulamalarda temel yapı taşı olan bir özetleme fonksiyonudur. (NIST enstitüsünün amacı; ölçüm bilimini, standartlarını ve teknolojilerini ekonomik güvenliliği arttırıp, yaşam kalitesini iyileştirecek biçimde geliştirerek ABD'deki endüstriyel rekabet ve yeniliği teşvik etmektir.)

1997 yılında NIST Kurumu DES Algoritmasının yerini alabilecek yeni bir simetrik algoritma yarışı açmıştır. 2001 yılında bu yarışmayı kazanan Belçikalı kriptologlar Joan Daemen ve Vincent Rijmen, Rijndael Algoritmasını AES adıyla standart hale getirmişlerdir.

2005 yılında Çinli bir ekip tarafından, 1995 yılında geliştirilen SHA-I algoritmasının kırıldığı duyurulmuştur.

2007 yılına geldiğinde her programcı şifreleme algoritması geliştirebilmektedir. Geliştirilen bu algoritmalarında kırılamayacağı düşünülmektedir. Fakat hemen hemen hepside kırılmaktadır.

25-28 Şubat 2009'da Belçika Katholieke Üniversitesinde kriptografi konusunda dünyanın ilk olimpiyatları başlamıştır. Bu olimpiyatların amacı SHA-I ve benzeri şifreleme standartlarını kırmak ve dijital imza sistemleri ile mesajlaşmada, diğer uygulamalarda kullanılabilecek yeni sistemler geliştirmektir.

4. KRİPTOLOJİ TERMİNOLOJİSİ

Bir bilim, sanat veya teknik alanda özel olarak kullanılan terimlerin tümüne terminoloji denilmektedir. Bu başlıkta kriptoloji biliminde en çok kullanılan terimler, kriptoloji terminolojisi açıklanmaktadır.

Gizlilik: Verinin, ona erişme yetkisi olmayan herkesten gizli tutulmasıdır.

Özgünlük: Verinin üçüncü kişiler tarafından değiştirilmemesidir. Yani verinin orijinal halinin korunmasıdır.

Kaynak Kimlik Doğrulaması: Veriyi gönderen kişinin, gerçek kişi olduğunun tespit edilebilmesidir.

Hedef Kimlik Doğrulaması: Verinin ulaşacağı kişinin, doğru kişi olup olmadığının garanti edilebilmesidir.

İmza: Bilginin kaynağına ait olup olmadığını belirleyebilmek için gerekli araçtır.

İzin: Verinin taşınabilmesi için gerekli olan birimlerden alınacak onaydır.

Doğrulama: İznin zamandan bağımsız olmasıdır.

Erişim Kontrolü: İzin verilmeyen kişilerin, kaynaklara erişmesinin engellenmesidir.

Sertifikasyon: Sağlanan bilgilerin doğru olup olmadığının kanıtlanmasıdır.

İşlem Kaydı: Yapılan bütün işlemlerin kaydedilmesidir.

Şahitlik: Oluşturulan taraftan gelmemiş olan bilgilerin doğruluğunun garanti edilmesidir.

Onay: Bilginin hedefine ulaşıp, ulaşmadığının bilgisidir.

Sahiplik: Bir bilginin kullanım haklarına sahip olunmasına denilmektedir.

Anonimlik: Belirli işlemlerde birimin kimliğinin saklanmasıdır.

İnkâr Önlemleri: Kişinin yapmış olduğu bütün işlemleri inkâr etmesinin engellenmesidir.

Şifreleme(Encryption): Bilginin tanınmayacak şekilde gizlenmesidir.

Deşifreleme(Decryption): Bilginin tekrar orijinal haline dönüştürülmesi işlemidir.

Cipher: Kriptografide algoritma olarak bilinmekte, veriyi şifrelemek için kullanılan kodda denilmektedir. İlk zamanlar cipher'ları kırmak oldukça kolay iken, günümüzdekiler kırılması zor, karmaşık yapıdadır.

Düz Metin (Plain Text): Verinin ilk halidir. Düz metin bir metin dosyası olabileceği gibi resim, ses, görüntü dosyası da olabilmektedir. Sayısal ortamdaki her şey

düz metin olarak ifade edilebilmektedir. Bilgisayar ortamında düz metin ise, ikili (binary) bir bilgidir. Kısaca düz metin şifrelenecek bir iletidir.

Şifreli Metin (Cipher Text): Verinin özel algoritmalarla kriptolaştırılmasıdır. Şifreli metin ikili (binary) bir bilgidir. Genellikle düz metinle aynı boyuttadır. Şifreli metin, şifreleme işlemi ile düz metin üzerinden gerçekleştirilerek elde edilmektedir.

Anahtar (Key): Bilgiyi saklamayı veya orijinal haline dönüştürmeyi sağlayan ipuçlarıdır.

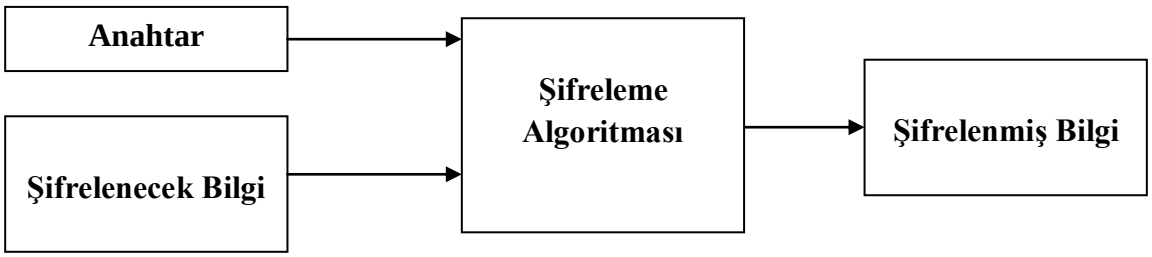
Genel Anahtar (Puplic Key): Herkes tarafından görülebilecek anahtardır.

Gizli Anahtar (Secret Key): Verinin şifrelenmiş halini görmeyi sağlayan anahtardır.

5. KRİPTOLOJİ ALGORİTMALARI

Kriptoloji algoritmaları şifrelemek ve şifre çözmek için kullanılan matematiksel temelli işlemlerdir. Bu algoritmalar ile bilgi matematiksel yöntemler kullanılarak kodlanmakta, başkalarının okuyamayacağı bir hale getirilmektedir.

Algoritmaların birçoğu, şifreleme ve şifre çözme işlemleri için şifrelenecek bilginin yanı sıra "anahtar" denen bir değer de kullanmaktadır. Anahtar "0" ve "1" lerden oluşan uzun bir bit dizisinden meydana gelmektedir ve çok çeşitli değerler alabilmektedir. Şifreleme anahtarlarının alabileceği olası değerlerden oluşan genişliğe anahtar uzayı denmektedir. Her algoritmanın kullandığı anahtar boyları farklılık göstermektedir. Genellikle, kullanılan anahtar boyu arttıkça şifreyi çözme güçleşmekte, şifreleme ve şifre çözme hızı yavaşlamaktadır[10].



Şekil 5.1. Şifreleme algoritmalarının genel diyagramı

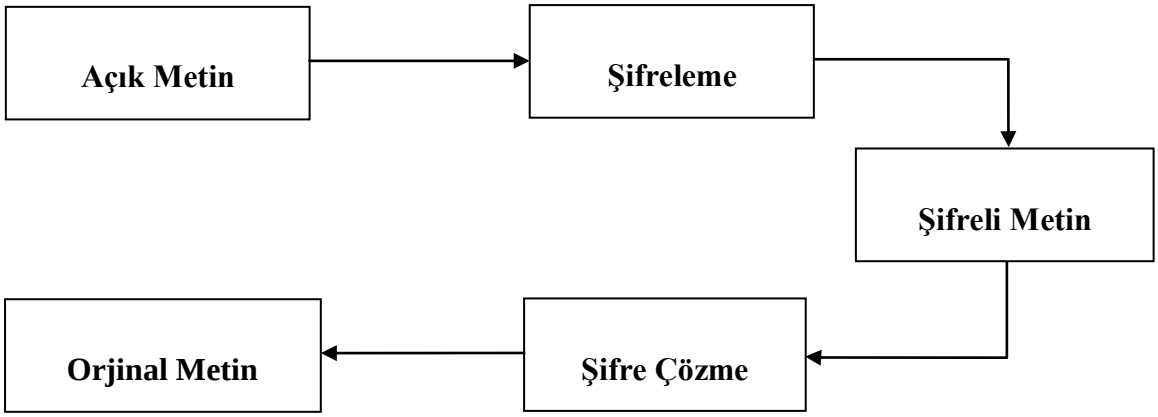
Kriptoloji algoritmaları şifreleme algoritmalarına, anahtar sayısına, şifrelenecek mesaj tipine göre sınıflandırılmaktadır. Anahtar yapısına göre algoritmalar Simetrik ve Asimetrik şifreleme algoritmaları olmak üzere ikiye ayrılmaktadır.

5.1. Simetrik Şifreleme Algoritmaları

Simetrik şifreleme algoritmalarına convential-anlaşmalı, gizli anahtar, tek veya özel anahtarlı, geleneksel şifreleme yöntemleri de denilmektedir.

Aynı ya da benzer olan kriptografik şifreleri kullanarak hem şifreleme hem de şifreyi çözme işlemi yapılmaktadır. Bu yöntemde şifreleme de kullanılan anahtarı gönderici ve alıcı taraftan başka kimsenin bilmemesi gerektiği için gizli anahtar veya özel anahtar şifreleme algoritması olarak da ifade edilmektedir.

Şifreleme ve şifre çözme işlemlerinde aynı anahtar ile birbirinin simetriği olan algoritmalar kullanıldığı için simetrik şifreleme algoritması olarak adlandırılan daha geleneksel bir şifreleme yöntemidir. Bu şifreleme algoritmasında güvenliği sağlayan unsur anahtardır. Çünkü şifreleme ve şifre çözme algoritmaları herkese açıkken, gizli olan tek şey anahtardır. Değişik anahtarlar kullanılarak, aynı mesaj ve aynı algoritma ile birbirinden farklı şifreli metinler oluşturulabilmektedir[11]. Bu algoritmada gönderilecek şifreli metinle beraber gizli anahtarda alıcı tarafa gönderilmekte ve şifre çözülmektedir.



Şekil 5.2. Simetrik şifreleme algoritmalarının genel yapısı

Simetrik şifreleme algoritmalarının en önemli avantajlarından bazıları basit, kolay uygulanabilir ve çok hızlı olmasıdır. Bundan dolayı yoğun hız gerektiren mesajların iletilmesinde büyük avantaj sağlamaktadır. Basit işlemler içerdiği için elektronik ortamlarda uygulanması kolaydır, ancak bu teknikte gizli anahtarın taraflar arasındaki iletimi probleme neden olmaktadır. Çünkü gizli anahtar, taraflar arasında iletilirken istenmeyen kişilerin eline geçebilmektedir. Dolayısıyla simetrik şifreleme algoritmalarının gücü anahtar uzunluğuyla doğru orantılı olarak ifade edilmektedir. 40 bit anahtar uzunluğu genellikle zayıf yöntemler olarak kabul edilirken, 128 bit ve üzeri anahtar uzunluğuna sahip olanlar ise kuvvetli yöntemler olarak kabul edilmektedir[7].

Simetrik şifreleme algoritmasının matematiksel olarak ifadesi şöyledir:

X : Orijinal Metin

Y : Şifrelenmiş Metin

K : Anahtar

E : Şifreleme Algoritması

D : Şifre Çözme Algoritması

EK (X) = Y (Anahtar Kullanılarak Şifreleme)

DK (Y) = X (Anahtar Kullanılarak Şifre Çözme)

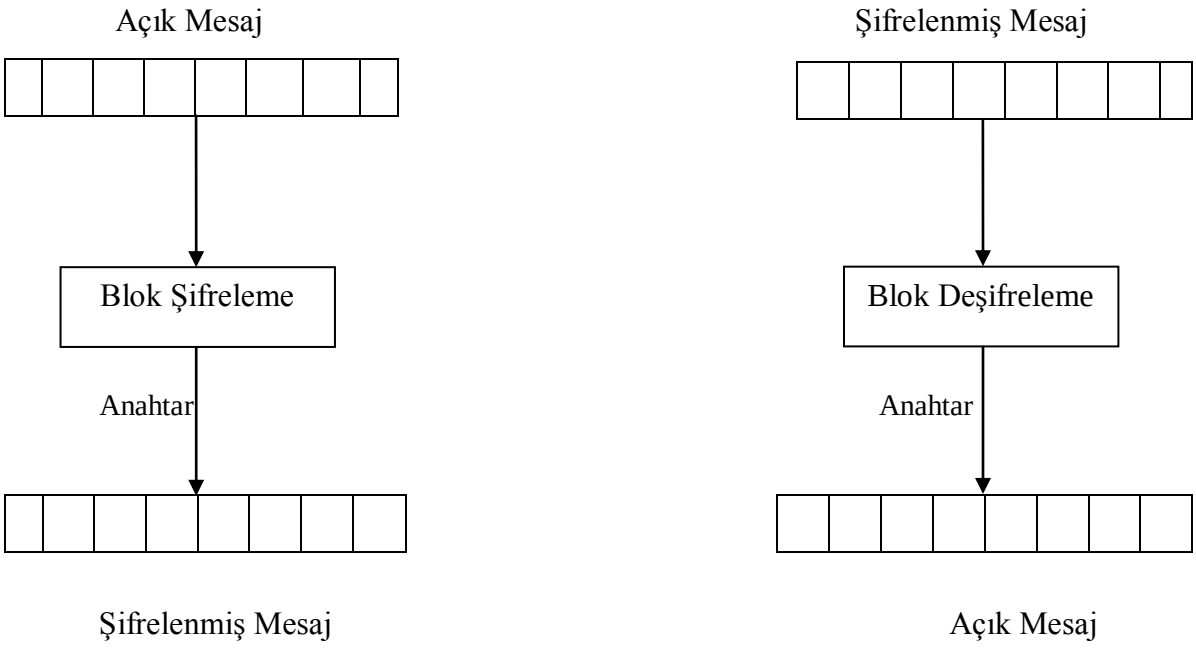
Buradan şu sonuca ulaşılmaktadır:

DK (EK (X)) = X

Simetrik şifreleme algoritmaları, Blok ve Dizi şifreleme algoritmaları olmak üzere ikiye ayrılmaktadır.

5.1.1. Blok Şifreleme Algoritmaları

Blok şifreleme algoritmaları veriyi bloklar halinde işlemektedir. Veri sabit uzunluktaki bloklara bölünmekte ve her bir blok birbirinden bağımsız bir şekilde şifrelenmektedir. Bu blokların boyutu genellikle 64 bit uzunluğundadır. Şifreleme işlemi gizli bir anahtarla yapılmaktadır. Şifre çözme işlemi de yine aynı gizli anahtar kullanılarak gerçekleştirilmektedir. Blok şifreleme algoritmaları birden fazla şifreleme işleminin birleşmesi ile oluşturulmaktadır. Her şifreleme adımına döngü denilmektedir. Genellikle her döngüde farklı anahtar materyali kullanılmaktadır. Bu algoritmalarda hafıza olmadığı için hafızasız şifreleme algoritmaları da denilmektedir.



Şekil 5.3. Blok şifreleme algoritmalarının genel yapısı

Blok şifreleme algoritmaları, Shannon'un önerdiği karıştırma ve yayılma tekniklerine dayanmaktadır. Karıştırma şifreli ve şifrelenmemiş metin arasındaki ilişkiyi olabildiğince karıştırarak, bu ilişkiyi gizli tutmayı amaçlarken, yayılma şifrelenmemiş metindeki izlerin şifreli metinde fark edilmemesini sağlamak için kullanılmaktadır[12].

Blok Şifreleme Algoritmaları şunlardır;

5.1.1.1. Lucifer Şifreleme Algoritması

1970'lerde IBM'de çalışan Alman kriptolog Horst Feistel başkanlığındaki bir grup tarafından geliştirilen şifreleme sistemidir. Dünyanın halka açık ilk simetrik şifreleme standardı olarak kabul edilmektedir. 1973 yılında NIST sivil kullanım için bir standart belirlemek üzere çeşitli firmaları davet etmiş ve yapılan incelemeler sonucunda amaca en yakın çözüm LUCIFER algoritması olarak bulunmuştur. 128 bitlik şifreleme anahtarına sahip olan LUCIFER algoritması üzerinde uzmanlar çalışarak bazı düzenlemeler yapmış ve anahtar uzunluğunu 56 bit'e indirmişlerdir. Bu yeni algoritma DES olarak adlandırılmaktadır[13].

5.1.1.2. Des Şifreleme Algoritması (Data Encryption Standard / Veri Şifreleme Standardı)

1970'lerde NIST tarafından geliştirilen DES algoritması kriptoloji ve kripto analiz bilimlerinin askeri olmayan çalışmalarının başlangıcı kabul edilmektedir. Geliştirildiği zamanlarda en çok kullanılan şifreleme algoritmalarından olmasına rağmen günümüzde modern bilgisayarlar tarafından yapılan saldırılar sonucunda güvenini kaybetmiştir. Ancak genel olarak bakıldığı zaman aşırı güvenlik gerektirmeyen uygulamalarda rahatlıkla kullanabilecek bir algoritma olduğu görülmektedir.

DES algoritmasında veriler 64 bitlik bloklar halinde gruplanarak şifrelenmektedir. Mesajın 64 bitten az olması durumunda mesaja "0"bitleri eklenerek 64 bite tamamlanmaktadır. Mesajın 64 bitten fazla olması durumunda ise 64 bitlik bloklara ayrılmakta ve her biri 16 defa dönen döngü ile ayrı ayrı şifreleme işlemine tabi tutulmaktadır. Sonuçta yine 64 bitten oluşan şifrelenmiş veri elde edilmektedir. DES algoritmasında şifreleme yapabilmek için kullanıcı tarafından oluşturulan 64 bitlik özel bir anahtar kullanılmaktadır. Bu anahtarda her 8. bit göz ardı edilmektedir. Dolayısıyla etkin

anahtar uzunluğu 56 bittir, ancak her durumda 64 bitlik gruplar esas alınmakta ve bu gruplar DES'in temelini oluşturmaktadır.

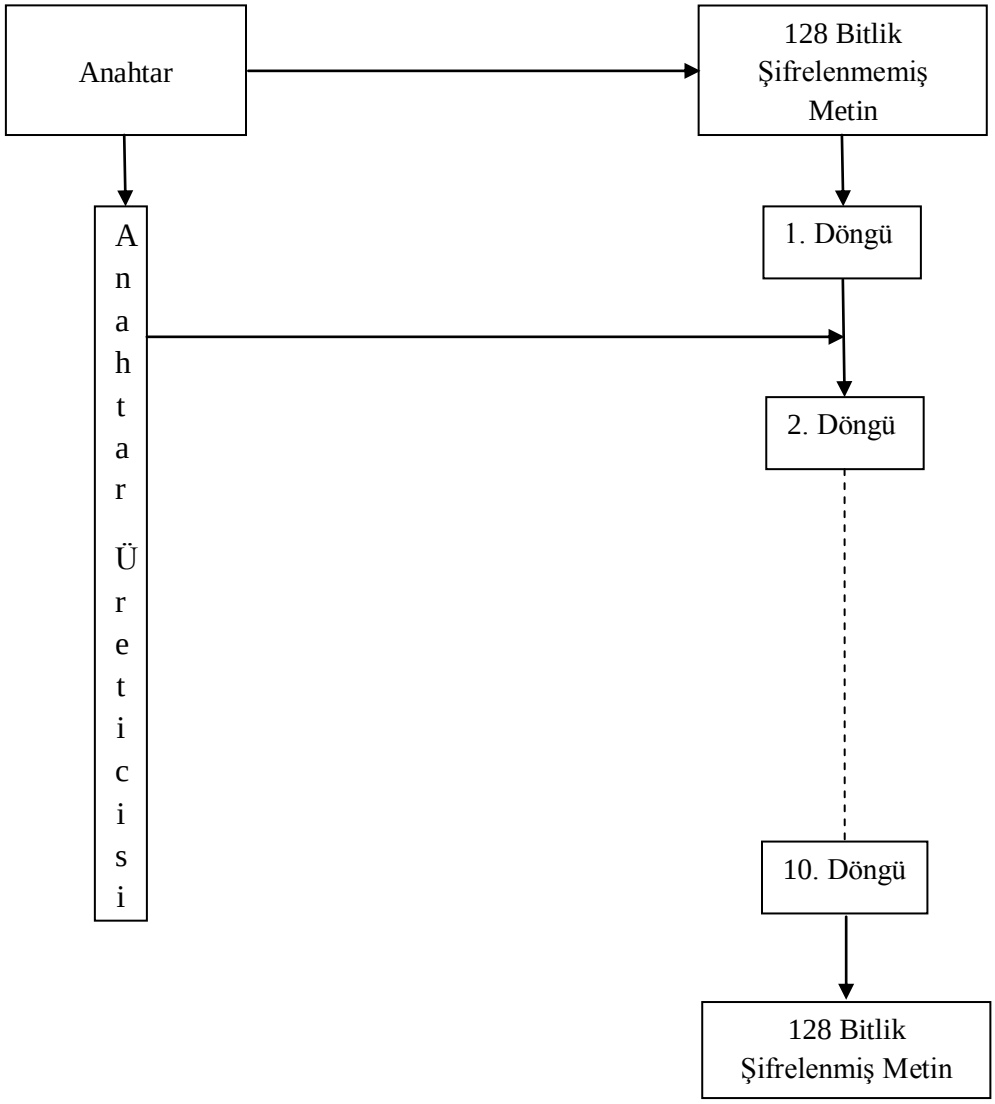
Şifreleme ve şifre çözme işlemleri için permütasyon, yer değiştirme gibi bazı işlemler yapılmaktadır. Bu işlemlerin sırası şifreleme ve şifre çözme işlemlerinde birbirinin tam tersi sırada gerçekleştirilmektedir[14].

56 bitlik anahtar uzunluğuna sahip olan DES algoritması kırılınca onun yerine anahtar uzunluğunun 128 bit olduğu 3 DES uygulaması IBM firması tarafından geliştirilmiştir. 3 DES algoritması DES algoritmasının 3 defa artarda çalıştırılmasıdır. Dolayısıyla DES algoritmasına göre 3 kat daha yavaş çalışmaktadır.

5.1.1.3 Aes Şifreleme Algoritması (Advanced Encryption Standard / Gelişmiş Şifreleme Standardı)

DES şifreleme algoritmasına karşı Vincent Rijmen ve Joan Daemen tarafından geliştirilmiştir. Şuana kadar bilinen güçlü algoritmalar arasında yer almaktadır.

Aşağıda 10 döngüden oluşan AES şifreleme algoritmasının genel görünümü verilmektedir [15].



Şekil 5.4. AES şifreleme algoritmasının genel yapısı

AES şifreleme algoritmasında, şifreleme işlemi için 128 bitlik veri blokları kullanılmaktadır. Şifrelenecek olan veri bu algoritmada 128 bitten oluşan bloklara ayrılmakta ve bu 128 bitlik veri blokları 128, 192, 256 bitlik anahtar seçenekleriyle şifrelenmektedir.

Döngü sayısı veriyi şifrelemede kullanılan anahtar büyüklüğüne göre belirlenmektedir. 128 bitlik anahtar için 10 döngü ile şifreleme yapılırken, 192 bitlik anahtar için 12 ve 256 bitlik anahtar için ise 14 döngüde şifreleme yapılmaktadır. Her döngüde 4 farklı işlem gerçekleştirilmektedir. Bunlar sırasıyla şöyledir; byte değiştirme, satırları kaydırma, sütunları karıştırma ve döngü anahtarı ile toplama [12].

Örneğin 128 bitlik anahtar için 10 döngü sonunda algoritmaya giren veri işlenmiş olarak çıkmaktadır. 1. Döngüde anahtar ilk haliyle döngüye katılmakta diğer döngülerde ise anahtar üreticisi tarafından yeni üretilen anahtarlar döngüye sokulmaktadır[16].

5.1.1.4. Blowfish (Balon Balığı) Şifreleme Algoritması

1993 yılında şifreleme ve güvenlik uzmanı olan Bruce Schnider tarafından DES şifreleme algoritmasına alternatif olarak geliştirilmiştir. Ücretsiz ve patentsiz olarak kullanıma sunulmuş güvenli ve hızlı bir algoritmadır. Bu özelliklerinden dolayı geniş kullanıcı kitleleri tarafından kabul görmektedir.

Blowfish şifreleme algoritmasında veriler DES şifreleme algoritmasında olduğu gibi 64 bitlik bloklar halinde şifrelenmekte ve bu 64 bitlik veri 32 bitlik iki parçaya ayrılmaktadır. Ayrıca 32 bitten oluşan 18 farklı alt anahtar bulunmaktadır. Veriler, basit bir fonksiyonun 16 defa kullanılmasıyla şifrelenmektedir[17].

5.1.1.5. Camellia Şifreleme Algoritması

2000 yılında NTT ve Mitsubishi Electric Şirketleri tarafından ortak geliştirilmiş bir şifreleme algoritmasıdır. Bütün şifre çözme saldırılarına karşı koyabilmek için tasarlanmış hızlı bir algoritmadır. Bu şifreleme yönteminde veriler 128 bitlik bloklara ayrılmakta ve bu bloklar için 128, 192 veya 256 bitlik anahtarlar kullanılmaktadır.

128 bitlik anahtar kullanıldığında veriyi şifrelemek ve şifreyi çözmek için 18 döngüden oluşan bir yöntem kullanılırken, 192 veya 256 bitlik anahtarlarda 24 döngü kullanılmaktadır[2].

5.1.1.6. Feistel Şifreleme Algoritması

Adını Alman şifreleme uzmanı olan Horst Feistel'den almaktadır. Bilinen Blok şifreleme algoritmalarının temelini oluşturmaktadır. Bu yapıda da şifrelenecek veri, eşit uzunluktaki iki bloğa ayrılmakta ve şifreleme, şifre çözme işlemleri yapılmaktadır. Feistel şifreleme algoritmasının en büyük avantajı şifreleme ve şifre çözme işlemlerinin çok benzer hatta bazen tamamen aynı olmasıdır [18].

5.1.1.7. IDEA Şifreleme Algoritması (International Data Encryption Algorithm / Uluslar Arası Veri Şifreleme Algoritması)

1990'lı yıllarda Xuejia Lai ve James Massey tarafından İsveç Federal Teknoloji Enstitüsünde geliştirilmiştir. 128 bit anahtar uzunluğuna sahip yüksek güvenlikli ve hızlı bir algoritmadır. Veriyi 64 bitlik bloklara bölerek şifrelemektedir[2]. Kaynak kodu ücretsiz olmasına rağmen ticari amaçlı olan kullanımlarda lisans gerektirmektedir[2].

5.1.1.8. Skipjack Şifreleme Algoritması

1987 yılında NSA tarafından geliştirilen 1993 yılında kullanılmaya başlanan ancak 1998 yılına kadarda gizli tutulan bir algoritmadır[2].

Bu algoritmada 64 bitlik bloklara ayrılan veri 80 bit uzunluğundaki anahtar kullanılarak 32 döngü sonunda şifrelenmektedir. Anahtar uzunluğu ve döngü sayısının fazla olmasına rağmen az işlem gerektiren bir algoritma olması önemli bir avantaj sağlamaktadır[2].

5.1.1.9. Playfair Şifreleme Algoritması

Çok basit bir blok şifreleme algoritmasıdır. Bu yöntemde 5x5 büyüklüğünde bir matris alınarak, bu matrisin içerisine kullanılacak anahtar sırasıyla yerleştirilmekte, geri kalan harfler rastgele sıralanmaktadır[2]. Şifrelenecek olan veri 2'lik bloklara bölünmekte ve oluşturulan 5x5'lik anahtar, bu matrise çeşitli şekillerde yerleştirilerek şifreleme işlemi yapılmaktadır.

5.1.1.10. Permutation (Permütasyon) Şifreleme Algoritması

İlkel bir blok şifreleme yöntemidir. Çünkü şifrelenmiş metin oldukça kısa bir sürede çözülebilmektedir. Şifrelenecek olan metnin, seçilen anahtara göre basitçe yer değiştirmesi mantığına dayandığı bir şifreleme algoritmasıdır[2].

5.1.2. Dizi Şifreleme Algoritmaları

Dizi şifreleme algoritması; şifrelenecek mesajdaki her bir biti, özel algoritmalar kullanılarak üretilmiş olan ve zamanla değişen anahtar ile sırayla şifrelemektedir. Bu algoritmanın en önemli girdisi anahtardır. Bu şifreleme sisteminin yapısı, zamana bağlı durum değiştirebilen bir makine gibi düşünülmektedir. Bu sistemde mesaj biriminin küçük olması istenmektedir. Genellikle kullanılan mesaj birimi Latin alfabesinin bir karakteri ya da tek bitlik sayılardır.

Blok şifreleme algoritmalarına göre daha hızlı çalışmaktadır. En çok kullanılan dizi şifreleme algoritmaları şunlardır;

5.1.2.1. RC/4 Şifreleme Algoritması

1987 yılında Ronald Linn Rivest tarafından bulunmuştur. Ancak 1994 yılında bilinmeyen kişiler tarafından internet ortamında bu şifreleme algoritmasının kaynak kodları yayınlanmıştır. Kullanımı lisans gerektirmektedir.

RC/4 şifreleme algoritması belirli bir uzunluktaki anahtar ile veriyi şifrelemektedir. Anahtar uzunluğu sabit değildir. 128 bitlik anahtar uzunluğu ile yapılan RC4 şifreleme algoritmasının güçlü olduğu belirtilmektedir. Şifreleme hızı yüksek olduğu için hız gerektiren uygulamalarda, bankacılık ve dokümantasyon işlemlerinde yaygın olarak kullanılmaktadır[19].

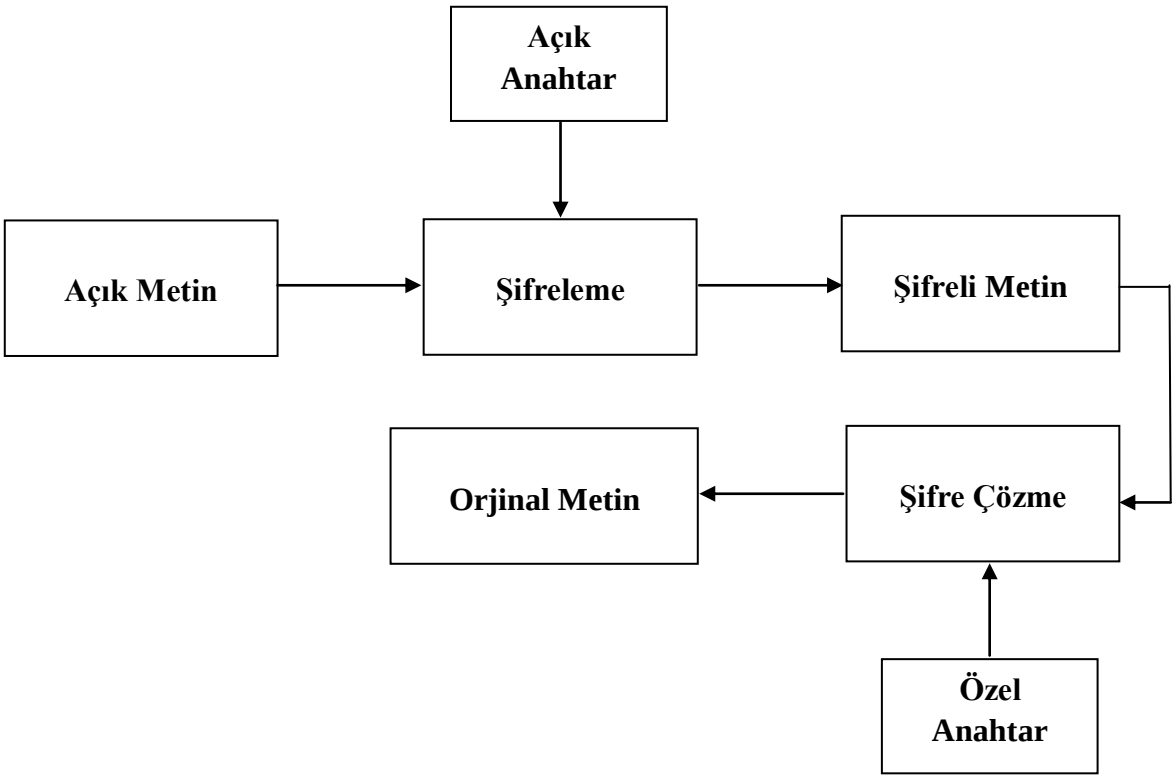
5.1.2.2. A5/1 ve A5/2 Şifreleme Algoritmaları

GSM sisteminde kullanılan şifreleme algoritmalarıdır. A5/2 şifreleme algoritması A5/1'in güvensizliğinden dolayı hazırlanmıştır. Bu şifreleme algoritmalarının amacı baz istasyonu ile mobil cihaz arasındaki veri alış-verişinde verileri şifrelemek ve şifrelenmiş olan bu verileri hava kanalı üzerinden göndermektir[20].

Diğer dizi şifreleme algoritmaları şunlardır: Chameleon, FISH, Helix, ISAAC, MUGI, Panoma, Phelix, Pike, SEAL, SOBER ve WAKE.

5.2. Asimetrik Şifreleme Algoritmaları

1976 yılında Standford Üniversitesinde görev yapan Martin Hellman, Whitfield Diffie adlı araştırmacılar tarafından önerilmiş bir yöntemdir. Asimetrik şifreleme algoritmalarının gelişimi kriptografi tarihindeki önemli olaylardan biri olarak kabul edilmektedir. Bu algoritmalar temellerini matematikten almaktadır. Hatta matematiğin çözüm getiremediği bazı durumları kullanarak güvenlik sağlamaktadır. Günümüzde kullanılan bütün asimetrik şifreleme sistemleri, güçlü bilgisayarlar tarafından bile, kısa sürede çözülmesi imkansız belirli matematik problemlerine dayanmaktadır.



Şekil 5.5. Asimetrik şifreleme algoritmalarının genel yapısı

Asimetrik şifreleme algoritmalarında şifreleme ve şifre çözme işlemleri farklı anahtarlarla yapılmaktadır. Bu farklı anahtarlardan biri veriyi şifrelemek için kullanılan açık (public key) anahtar, diğeri ise şifreyi çözmede kullanılan özel (private key) anahtardır. Bu iki anahtar beraber üretilmesine rağmen özel anahtarın gizli tutulması gerekirken, açık anahtar gerekli kişilere dağıtılabilmektedir. Bu özelliğinden dolayı da Açık Anahtar Şifreleme Algoritmaları da denilmektedir. Açık anahtara sahip bir kişi bilgiyi sadece şifreleyebilmekte, ancak çözememektedir. Çözebilmesi için özel anahtara da sahip

olması gerekmektedir. Kullanılan anahtarların boyu ne kadar uzun olursa, şifrenin kırılma ihtimalide o kadar azalmaktadır. Ancak anahtar boyutunun uzun olması bu şifreleme algoritmasında zaman zaman sorun çıkarabilmektedir[21].

Asimetrik şifreleme algoritmaları, simetrik şifreleme algoritmalarına göre daha güvenilir ve kırılması daha zordur. Çünkü asimetrik şifreleme algoritmasının temelini oluşturan matematiksel problemleri çözmek zordur. Asimetrik şifreleme algoritmalarının en büyük dezavantajı matematiksel yapılarından dolayı simetrik şifreleme algoritmalarına göre daha yavaş olmalarıdır[22].

Asimetrik şifreleme sistemlerinin avantajlarından biri veri şifreleme ve şifre çözme işlemlerini yapmasının yanında dijital imza olarak doğrulama işlemlerinde kullanılmasıdır. Şifrelenmiş bir veri gönderilmesi gereken yere ulaşıp şifre çözme işlemi yapıldıktan sonra karşılaşılabilecek en büyük sorun bu şifreli verinin doğru kişiden gelip gelmediğinin doğrulanmasıdır. Bu doğrulama işlemi dijital imzalar sayesinde gerçekleştirilmektedir.

Asimetrik şifreleme algoritmaları şunlardır:

5.2.1. Dijital İmza

Açık anahtar şifreleme algoritmalarının gelişmesiyle yaygınlaşan dijital imza, açık ve özel anahtarlar ile elektronik ortamda iletilen veriye vurulan bir mühürdür. Günlük hayatta kullanılan imzalarda olduğu gibi, dijital imzalar da elektronik ortamda gönderilen bilginin kime ait olduğunu göstermektedir. Yani veriyi gönderenin kimliğinin kesin bir biçimde teyit edilmesini sağlamaktadır.

Dijital imzalar kişinin el yazısı ile attığı imzaya eşdeğerdir, elle atılan imzanın elektronik ortamdaki karşılığıdır, aynı amaçla kullanılmaktadır. Ancak el yazısı ile atılan imzanın taklit edilmesi kolay iken dijital imzanın taklit edilmesi nerdeyse mümkün değildir. Dolayısıyla elle atılan imzalara göre daha güvenilirdir. Bu güvenilirliği sağlayan unsur ise dijital imzalama yönteminde kullanılan matematiksel algoritmalardır.

Dijital imza, imzalayan kişinin gizli anahtarıyla şifrelenerek elde edildiği için, imza veya imzalanan belge değişikliğe uğradığında bu kolayca anlaşılmakta, belge reddedilmektedir. Bu da belgenin bütünlüğü ve kaynağı konusunda alıcı tarafa garanti vermektedir[23].

5.2.2. RSA (Rivest, Shamir ve Adleman) Şifreleme Algoritması

RSA şifreleme yöntemi 1978 yılında "Dijital İmza Elde Etme Yöntemi ve Açık Anahtarlı Kripto Sistemler" (A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, February 1978) adlı bir makale ile yayınlanmıştır ve MIT Üniversitesi'nde görevli olan Ronald L. Rivest, Adi Shamir ve Leonard Adleman isimli araştırmacılar tarafından bulunmuştur. Bu şifreleme yöntemi adını, bulanların soyadlarının baş harflerinden almaktadır.

RSA şifreleme algoritması geliştirilen ilk asimetrik şifreleme algoritmalarından olmasına rağmen halen güvenilirliğini korumaktadır. Çok büyük sayıların çarpanlarına ayrılmasına dayalı basit bir mantığı vardır ve anahtar iki büyük asal sayıdan üretilmektedir. İki büyük asal sayı çarpıldığında ortaya çıkan sonucun, hangi iki asal sayının çarpılmasından elde edildiğini bulmak neredeyse imkansızdır. Dolayısıyla RSA şifreleme algoritmasının güvenliği bu büyük asal sayıları üretme ve bunları çarpanlarına ayırmanın zorluğuna dayanmaktadır. Ancak bu asal sayılar seçilirken sadece güvenlik değil performansında düşünülmesi gerekmektedir. Bu özelliklere rağmen RSA şifreleme algoritması mükemmel değildir[24].

RSA şifreleme algoritmasının genel yapısı şöyledir.

1. p ve q olarak ifade edilen ve çok büyük olan iki asal sayı seçilmektedir.

2. n=p*q ve z=(p-1)*(q-1)

işlemi hesaplanmaktadır.

3. z ile ilişkili asal bir sayı bulunmakta ve bulunan bu sayıda d olarak adlandırılmaktadır.

4. e*d=1 (mod z)

eşitliğini sağlayan e sayısı bulunmaktadır.

Bu aşamalardan sonra şifreleme işlemi yapılmaktadır. Bu algoritmaya zarar verecek durum, bilinen en etkili p ve q'nun bulunmasıdır. Ancak p ve q çok büyük asal sayılardan seçildiği için bulunmasının çok zor olduğu konusunda matematikçiler hemfikirdir. Bunun yanında bilgisayar teknolojisinde yaşanan hızlı gelişmelerden ötürü p ve q'nun dikkatli seçilmesi gerekmektedir[24].

5.2.3. Diffie Hellman Şifreleme Algoritması

1976 yılında Whitfield Diffie, Martin Hellman bulmuş ve "New Directions in Cryptography" isimli makaleleri ile de duyurmuşlardır. Dünyaya ilk duyurulan asimetrik şifreleme algoritmasıdır. Bu algoritma sayesinde simetrik şifreleme algoritmalarında büyük problem olarak görülen gizli anahtarı koruma ve dağıtma konularına büyük ölçüde çözüm getirilmiştir. Birçok ticari uygulamada bu algoritma kullanılmıştır. Algoritmanın amacı kullanıcıların bir ortak gizli anahtarı güvenli şekilde birbirlerine iletmeleri ve iletilen bu anahtar yardımıyla da şifreli mesajların gönderilebilmesidir. Ortak gizli anahtarın güvenilirliği, anahtar oluştururken çok büyük asal sayılar seçmeye bağlıdır. Gizli anahtar oluştururken aşağıda örnek üzerinde açıklanan ayrık algoritma yöntemi kullanılmaktadır[25].

Ortak gizli anahtar basitçe şu şekilde oluşturulmaktadır.

1. Kişi tarafından $0 \leq A \leq p-2$ eşitsizliğini sağlayan tesadüfî bir A sayısı seçilmekte ve $x=g^A \pmod p$ hesaplanıp B'ye gönderilmektedir.

2. kişi tarafından ise $0 \leq B \leq p-2$ eşitsizliğini sağlayan yine tesadüfi olarak bir B sayısı seçilmektedir.

$Y=g^B \pmod p$ hesaplanarak hesaplama sonucunu B'de A'ya göndermektedir.

Kullanılacak ortak anahtarda h olarak kabul edilirse 1. kişi kullanılacak ortak anahtarı;

$h=y^A = (g^B)^A$ şeklinde hesaplamaktadır.

2. kişi ise kullanılacak ortak anahtarı şöyle hesaplamaktadır.

$h=x^B=(g^A)^B$

Böylelikle 1. ve 2. kişi aralarında ortak kullanacakları gizli anahtarı yani "h"ı hesaplamış olmaktadır.

5.2.4. DSA (Digital Signature Algorithm/Dijital İmza Algoritması) Şifreleme Algoritması

NIST tarafından yayınlanan ve ABD'de kullanılan bir şifreleme algoritmasıdır. Asimetrik anahtar alt yapısını kullanarak şifreleme yapmaktan çok imzalama amaçlı kullanılmaktadır[2].

5.2.5. Elgamal Şifreleme Algoritması

1984 yılında Tahar ElGamal tarafından önerilmiştir. Diffie Hellman şifreleme algoritmasını temel alan bir asimetrik şifreleme algoritmasıdır. Olasılıksal bir şifreleme metodudur, temeli farklı logaritmik problemler üzerine dayandırılmaktadır. Şifreleme ve dijital imza algoritmalarından oluşmuştur. İletilecek mesaj, çok sayıda farklı gizli anahtar kullanılarak şifrelenebilmektedir[2].

5.2.6. Eliptik Eğri (Eliptic Curve) Şifreleme Algoritması

Eliptik eğri şifreleme algoritmasının en önemli özelliği, diğer asimetrik şifreleme algoritmalarından daha küçük boyutlu anahtarlar kullanmasıdır. Örneğin 128 Byte'lık anahtar kullanan RSA şifreleme algoritmasının sağlayabildiği güvenliği, Eliptik Eğri şifreleme algoritması sadece 20 Byte kullanarak sağlayabilmektedir. Örnekte açıklanan bu özellik asimetrik şifreleme algoritmalarında çok önemli bir avantajdır[26].

Günümüzde yeni gelişen teknolojilerden olan kablosuz ağların büyük anahtar değerlerine sahip şifreleme algoritmalarını kullanmaları zor olduğundan dolayı Eliptik Eğri şifreleme algoritmalarının kablosuz ağlarda kullanımı çok uygundur. Donanım ve yazılım ile etkin bir biçimde uygulanabilmektedir. Ancak şu anda Eliptik Eğri şifreleme algoritması yayınlanmış olmasına rağmen pratikte pek kullanılmamaktadır[27].

5.3. Karışık Algoritmalar

Akla gelebilecek her türden şifreleme teknikleri kullanılarak, yeni üretilen, eskiden kullanılan, simetrik ve asimetrik algoritmaları içine alan algoritmalar olarak ifade edilebilir. Bu bölümde simetrik ve asimetrik şifreleme algoritmalarının dışında kalan karışık algoritmalardan bahsedilmektedir[2].

5.3.1. Sezar Şifreleme Algoritması

Şifreleme algoritmasının adından da anlaşılacağı üzere eski Roma İmparatoru Julius Caesar tarafından savaş zamanlarında askeri bilgileri gönderirken sorun

yaşanmaması için üretilmiştir. İlk şifreleme algoritmalarından biri olarak kabul edilmektedir. Şifrelenecek mesajdaki her karakter, 'anahtar' olarak belirlenen değer kadar ötelenerek şifreli mesaj elde edilmektedir. Örneğin anahtar değeri 3 ise orijinal mesajdaki her harf kendisinden 3 sonra gelen harfle yer değiştirmektedir. Böylelikle şifreli mesaj elde edilmektedir[28].

5.3.2. Vigenere Şifreleme Algoritması

Sezar şifreleme algoritmasının geliştirilmiş halidir. 1553 yılında Giovan Batista Belasa tarafından tanıtılmış ve 16. Yüzyılda Blaise de Vigenere tarafından kullanılmıştır. Böylelikle yöntemin adı Vigenere şifreleme algoritması olarak kalmıştır[2].

Şifreli mesajın oluşturulabilmesi için çoklu alfabe kullanılmıştır. Uzun zaman boyunca güvenilir bir algoritma olarak bilinmiştir. Ancak 1863 yılında Friedrich Kasiski, Vigenere şifreleme yöntemini açıklamıştır[2].

5.3.3. Afin Şifreleme Algoritması

Afin şifreleme algoritması geometride doğru denklemi olarak ifade edilen y=ax+b doğrusal fonksiyonunu kullanarak şifreleme yapmaktadır. Denkleme göre x şifrelenecek mesajı, y ise şifrelenmiş mesajı ifade etmektedir. b ise anahtarı oluşturmaktadır[2].

Örneğin şifrelenecek mesaj x=abi, anahtar (2,3) olsun. Şifreli mesaj şöyle oluşturulmaktadır.

a harfi birinci harf olarak kabul edilirse y=1*2+3=5 bulunmaktadır. Böylelikle a harfinin karşılığının alfabenin 5. harfi olduğu kabul edilmektedir. Bu harfte e'ye karşılık gelmektedir. Benzer şekilde b ve i harflerinin de karşılıkları bulunarak abi kelimesi egv şeklinde şifrelenmektedir.

6. SAYISAL GÖRÜNTÜ VE GÖRÜNTÜ FORMATLARI

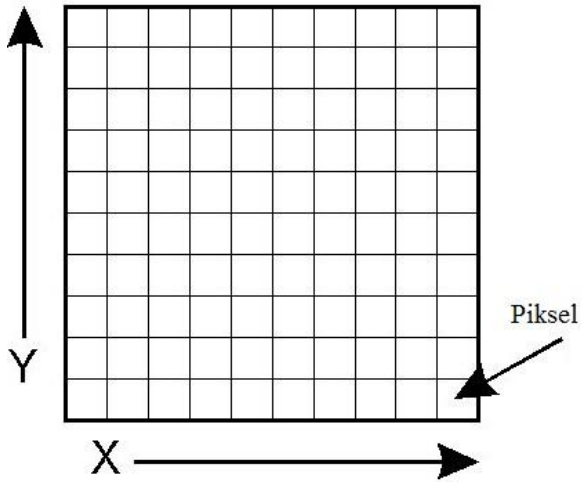
6.1. Sayısal Görüntü

Sayısal görüntü, a(x,y) gibi bir fonksiyonla ifade edilen basit iki değişken olarak tanımlanmaktadır. Bu fonksiyondaki a parlaklık gibi bir şiddet birimini, x değişkeni görüntünün satırlarını (enini) ve y değişkeni ise sütunlarını (boyunu) temsil etmektedir. Kısaca sayısal görüntü yatay ve dikey biçimde yan yana sıralanmış piksellerden oluşan elektronik bir fotoğraftır. Her piksel; siyah, beyaz, grinin tonu ya da herhangi bir rengi içeren renk tonu ile temsil edilmektedir[29].

6.2. Piksel

Piksel kelimesi İngilizce Picture Element (resim elemanı) kelimelerinin ilk hecelerinin bileşiminden türetilmiştir. Tüm sayısal görüntülerin temeli olan, ekranda kontrol edilebilen en küçük noktalara denmektedir.

Bir piksel kırmızı, yeşil ve mavi renklerin karışımından oluşmaktadır. Görüntü ne kadar çok sayıda ve küçük piksellerden oluşmuşsa o kadar kaliteli ve net olmaktadır. Görüntüdeki piksel sayısı arttıkça görüntü kalitesi de artmaktadır. Çok fazla arttırıldığında ise dosyanın kapasitesinin artmasına, görüntünün yazıcıdan çıktısı alınırken zaman kaybına ve mürekkep sarfiyatına neden olmaktadır[29].



Şekil 6.1. Sayısal görüntüde pikselin gösterimi

Bir görüntünün temel yapı taşı olan pikseller bir araya gelerek, resmi oluşturmaktadır. Görüntü deyince akla m x n boyutlu piksellerden oluşan bir matris gelmektedir[29].

Siyah-Beyaz resim yani ikili görüntü sadece iki değerden oluşan bir resimdir. İkili bir görüntüde her piksel ya siyah ya da beyaz olarak ifade edilmektedir. Sembolik olarak beyaz pikseller 1, siyah pikseller 0 değeri ile gösterilmektedir.

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	0	0	0	0	0	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	0	0	0	0	0	1	1	1	1	1	1	1	1
1	1	1	1	1	1	0	0	0	0	0	0	1	1	1	1	1	1	1	1
1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
1	1	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
1	1	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
1	1	0	0	0	0	1	1	0	0	0	0	1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Şekil 6.2. İkili görüntü

Şekil 6.2.'de ikili bir görüntüye ait piksellerin 0 ve 1 değeri olarak kodlanmış hali verilmektedir. Bu şekilde 0 ve 1 değerleri ile kodlanmış piksellerden oluşan görüntülere ikili görüntü denilmektedir.

6.3. Nokta Ve Nokta Aralığı

Pikselleri oluşturan kırmızı, mavi ve yeşil renklerin her birine nokta (dot), bir pikseldeki bu üç rengin birbirine olan uzaklığına ise nokta aralığı (dot pitch) denilmektedir.

6.4. Çözünürlük

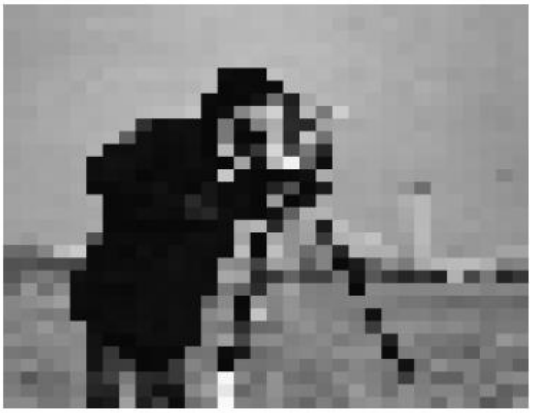
Bir görüntüyü oluşturan piksellerin birbirine olan uzaklıklarının ölçüsüne çözünürlük denilmektedir. Bir defada ekranda görüntülenebilen piksel sayısıdır. Çözünürlük arttıkça (yani görüntüdeki piksel sayısı arttıkça) görüntü kalitesi artmaktadır. Fiziksel olarak aynı büyüklüğe sahip olan görüntüler aynı çözünürlükte olmayabilirler[30].

Aşağıdaki görüntüler çözünürlük piksel sayısı ilişkisine örnek olarak verilebilir.

Şekil 6.3. 256 X 256 piksel

Şekil 6.4. 128 X 128 piksel

Şekil 6.5. 64 X 64 piksel



Şekil 6.6. 32 X 32 piksel

Görüntünün çözünürlük değeri, örneğin 400 X 200 piksel olarak verildiğinde, bu görüntüde 400 sütun ve 200 satır kullanıldığını göstermektedir. Bunların çarpımı olan 80.000 değeri ise görüntüdeki toplam piksel sayısını vermektedir.

6.5. Rezolasyon

Bir resmin piksel yoğunluğudur yani 1 inç karede (1 inç = 2.54 cm) bulunan piksel sayısıdır[31].

6.6. Görüntü Formatları

Yaygın olarak kullanılan görüntü formatlarından bazıları şunlardır:

6.6.1. JPG Görüntü Formatı

Türkçe'ye "Birleşik Fotoğraf Grubu" olarak çevrilen İngilizce "Joint Photographic Group" kelimelerinin baş harflerinden oluşmaktadır. İmge işleme programlarının yüksek megabaytlı dosyaları sıkıştırarak disk üzerinde kayıt edebileceği, profesyonel fotoğrafçılar için geliştirilmiş, internette yaygın olarak kullanılan bir görsel formattır. Gerçek renk değerleri içerdiği için fotoğrafik görüntülemede kullanılmaktadır.

JPEG sıkıştırma yöntemi, görüntünün algılanabilmesi için zorunlu olmayan detayları bulup atan ve dosyayı böyle sıkıştıran bir format olduğundan dolayı kayıplı formatlar arasında yer almaktadır. Kaybolan ayrıntılar ve sıkıştırma oranı arasında bağlantı bulunduğundan bu dengenin iyi korunması gerekmektedir. Daha fazla sıkıştırma daha fazla veri kaybı, daha az sıkıştırma ise daha büyük boyutlu dosya demektir[32].

6.6.2. BMP Görüntü Formatı

BMP, herhangi bir sıkıştırma yapmadan resimlerin özeliklerini tutan Windows ve Microsoft'un PCX formatını değiştirerek geliştirdiği bir resim dosyası biçimidir. Sıkıştırma yapmadığı için dosya boyutu diğer resim türlerine göre çok büyüktür. BMP formatı 1-24 bit arasında değişen piksel derinliğini içerebilmektedir[32].

6.6.3. PICT Görüntü Formatı

PICT formatı bütün programlar tarafından ortak olarak kullanılan dosya formatıdır. Bu format herhangi bir uygulama programına aktarıldığında resim bilgisi sayfaya dâhil olmaktadır[31].

6.6.4. EPS Görüntü Formatı

İngilizce Encapsulated PostScript kelimelerinin baş harflerinden oluşturulan EPS formatı hemen hemen bütün çizim ve sayfa düzenleme programları tarafından desteklenen vektör yapısındaki grafik dosyalardır. İstenildiği kadar büyütülebildiği için büyük çaplı grafiklerin tasarlanmasında özelliklede logo tasarımlarında kullanılmaktadır. Eskiden bu tür dosyalar sadece Macintosh bilgisayarların dosya sistemi ile uyumlu çalışan bir formatken şuanda Windows altında da açılabilmektedir[33].

6.6.5. GIF Görüntü Formatı

GIF, CompuServe firması tarafından geliştirilen, İngilizce Grafik Değiştirme Biçimi anlamına gelen Graphics Interchange Format kelimelerinin kısaltmasıdır. JPEG ile birlikte bilgisayar dünyasında oldukça yaygın kullanılan, sayısal resim saklama biçimlerinden biridir.

Az sayıda renk içeren dokümanlarda kayıpsız sıkıştırma sağlaması, animasyonlarda zamanlama ve farklı boyutlardaki imgeleri bir arada tutma desteği, saydam renk tanımlaması bu formatı popüler yapan nedenlerdendir. Ancak "Adobe Photoshop" gibi görüntü işleme programlarının çoğu GIF formatının tüm özelliklerini kullanamamaktadır. Bu nedenle GIF formatıyla çalışırken sıklıkla başka programlara ihtiyaç duyulmaktadır.

Gerçek renk desteği yoktur. 8 bit yani 256 renge kadar renk desteği vermektedir. Az renk içermesinden dolayı genellikle grafiklerin saklanmasında bu görüntü formatından yararlanılmaktadır. Web sayfalarında piksel tabanlı animasyonlu resimler oluşturmak için kullanılmaktadır. Resim kalitesi düşüktür[34].

6.6.6. PNG Görüntü Formatı

PNG, İngilizce Portable Network Graphics kelimelerinin baş harflerinden kısaltılmış, taşınabilir ağ grafikleri anlamına gelen, kayıpsız sıkıştırma yapan, görüntü işleme yazılımı programlarında düzenlenebilen ve görüntülerin web'de gösterilmesi için kullanılan bir görüntü formatıdır. Sıkıştırma için değişik filtreleme algoritmaları kullanmaktadır. GIF görüntü formatına, patentsiz bir alternatif olarak geliştirilmiştir. PNG 24 bit görüntüleri desteklemekte ve kenarları pürüzlü olmayan bir arka plan saydamlığı oluşturmaktadır. Ancak bazı web tarayıcıları PNG formatındaki görüntüleri desteklememektedir[31].

6.6.7. PSD Görüntü Formatı

PSD (Photoshop Document/Photoshop belgesi) Photoshop fotoğraf düzenleme yazılımı ile hazırlanmış bir formattır. İçersinde katmanlar, maskeler, çeşitli renk tonları ve fotoğraf parçaları bulunabilmektedir[31].

6.6.8. TIFF Görüntü Formatı

1986 yılında Aldus isimli şirket tarafından geliştirilen Tagged Image File Format kısaca TIFF isimli bir formattır. Grafik, fotoğraf gibi dosyalar için kullanılan, tüm boyama, görüntü düzenleme ve sayfa mizanpajı uygulamaları tarafından desteklenen, esnek ve uyarlanabilir bir bitmap görüntü dosyasıdır. TIFF formatının gerçek anlamda yaygınlaşması ve dünya çapında popüler hale gelmesi, Aldus şirketinin 1994 yılında "Adobe Systems" ile birleşmesiyle gerçekleşmiştir.

TIFF biçimi birden fazla sayfayı desteklediği için, çok sayfalı dokümanlar ayrı ayrı dosyalar yerine tek bir TIFF dosyası olarak kaydedilebilmektedir. Bu özelliği ile de reklamcılık, grafikerlik ve matbaacılık gibi profesyonel çalışma alanlarında çok kullanılmaktadır.

TIFF dosyaları, görsel kalitesinde kayıp yaşamadan görüntü depolama özelliğine sahip olduğundan dolayı bu dosya formatıyla son derece kaliteli görsellerden oluşan bir görüntü arşivi yapılabilmektedir. Web sitelerinde her ne kadar JPEG gibi boyuttan tasarruf sağlayan formatlar tercih edilse de, kaliteli görsellere ihtiyaç duyulan alanlarda TIFF

formatı ideal biçimleme yöntemidir. JPEG biçimleme ile görsel kalitede kayıp yaşanırken TIFF biçimleme de bu tür sıkıştırma kayıpları yaşanmamakta ve yüksek kaliteli resimleme yapılabilmektedir. Görüntü kalitesinde herhangi bir kayıp olmaksızın görsellerin depolanmasını veya değiştirilmesini sağlayan TIFF biçimleme, bu özelliği nedeniyle baskı işlerinde adeta bir gereksinim haline gelmektedir. Ancak TIFF içinde yer alan JPEG görsellerde görüntü kalitesinin düşeceği de unutulmamalıdır.

TIFF, diğer dosya biçimlerine kıyasla çok daha fazla disk alanına ihtiyaç duyması ve içerdiği "tampon bellek taşması (buffer overflow)" gibi zayıflıkları nedeniyle giderek azalan bir kullanıma sahiptir. TIFF belgelerinin en büyük dosya boyutu 4 GB'tır[35].

7. RENK KAVRAMLARI

Işığın maddelere çarptıktan sonra yansıyarak gözümüzde uyandırdığı etkiye renk adı verilmektedir. Renk ışığın meydana getirdiği fiziksel bir olgudur. İnsanlarda renk duygusunun oluşması için bir cismin göze ışık göndermesinin yanı sıra, gelen ışık karşısında normal çalışan bir göz ve beyinde kusursuz bir görme merkezi gerekmektedir. Göz tarafından algılanan ışık, retinada sinirsel sinyallere dönüştürülüp, buradan görme siniri yoluyla beyindeki görme merkezine iletilmektedir. Renklerin algılanışı dış koşullara bağlı olarak değişmektedir. Güneş ışığında belli bir renk tonunda görülen bir cisim, ampul ışığında değişik, mum ışığında daha değişik renk tonlarında algılanabilmektedir. Fakat insanın görme duyusu ışığın kaynağına uyum sağlayarak, onların her iki koşulda da aynı renk olarak algılanmasına neden olmaktadır.

İnsan gözü elektromanyetik spektrum içinde 380 ile 780 nanometre dalga boyunu algılamaktadır. Tüm dalga boylarının birden göze ulaşması ile beyaz, herhangi bir dalga boyunun ulaşmaması durumunda ise siyah olarak algılanılmaktadır. Göz, üç temel birleştirici renk olan 600 - 700 nm civarındaki dalga boylarını kırmızı, 500 - 600 nm civarındakileri yeşil ve 400 - 500 nm civarindakileri de mavi olarak algılamaktadır. Bilgisayar dünyasında bu üç temel renk RGB olarak tanınmaktadır. Diğer renkler bu üç rengin dalga boyunun farklı yoğunluklarda kullanılmasıyla elde edilmektedir[36].

7.1. Renk Modelleri

Renk modelleri, renkleri tanımlamak için kullanılan matematiksel modellerdir. Renk modellerinin amacı, bazı standartlara göre genel kabul görmüş bir şekilde renk belirtimini kolaylaştırmaktır. Renk modelleri bütün renkleri temsil edecek şekilde oluşturulmuştur[37].

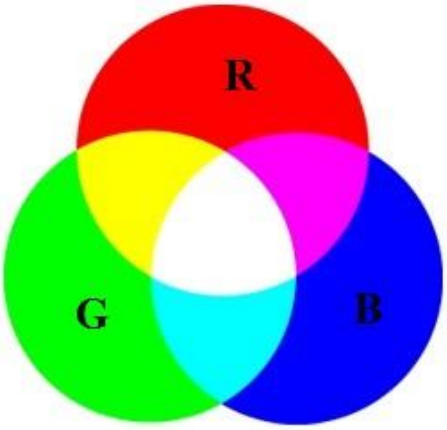
Temel kabul edilen renk modelleri, şunlardır;

7.1.1. RGB Renk Modeli

İsmini İngilizce kırmızı, yeşil, mavi anlamına gelen Red – Green – Blue kelimelerinin baş harflerinden almaktadır. Bu renk modelinde tüm renkler; kırmızı, yeşil ve mavi renklerin farklı kombinasyonları ile elde edilmekte yani diğer renkler bu üç temel

renkten oluşmaktadır. RGB renk modeli renkli elektronik ekranlarda, bilgisayar grafikleri üzerinde yoğun olarak kullanılmaktadır.

Şekil 7.1.'de RGB renk modeline örnek bir görüntü verilmektedir.



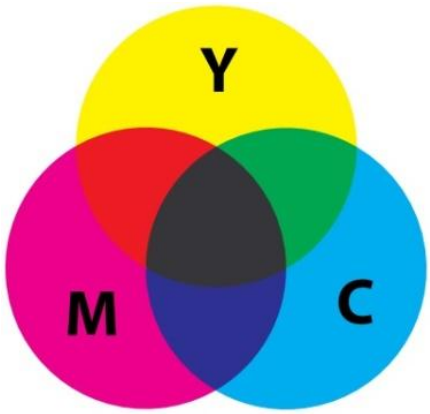
Şekil 7.1. RGB renk modeli

Kırmızı,yeşil ve mavi, ışık birincil renklerin kümesidir. Bu üç renk eşit olarak karıştırıldığında beyaz elde edilmekte ve diğer oranlarda karıştırıldıklarında ise farklı bir ışık renk dizisi üretilmektedir.

7.1.2. CMYK Renk Modeli

CMYK renk modeli, RGB modelinin bir altkümesi olarak düşünülebilir. CMYK; siyan, macenta ve sarı ile birlikte siyah için kullanılan bir kısaltmadır. Siyan "C", macenta "M" ve sarı "Y" ve siyah "K" ile gösterilmektedir. Eklemeli renk modeli olan RGB'nin aksine, CMYK çıkarmalı bir renk modelidir. Genellikle renkli baskı üretiminde kullanılan CMYK renk modelinde siyan, macenta, sarı eklemeli renk teorisinde siyahı vermektedir. Ancak üç ana rengin (CMY) kombinasyonu tam doygun siyah üretmek için yeterli olmadığından, siyah kullanılmaktadır. Siyaha bunun için "anahtar" denilmektedir ve teorideki siyahın varlığı İngilizcedeki anahtar (key) kelimesinin baş harfi "K" ile gösterilmektedir[37].

Şekil 7.2.'de CMYK renk modelini gösteren örnek bir görüntü yer almaktadır.



Şekil 7.2. CMYK renk modeli

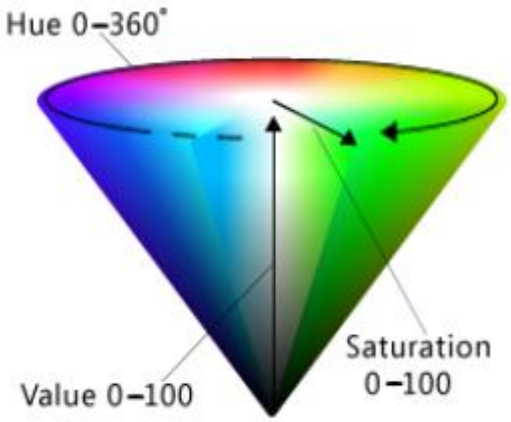
7.1.3. CIE Renk Modeli

CIE renk modeli insanın renk algılayışını düzgün bir biçimde gösterebilmek amacıyla CIE (Commission Intenationale de l'Eclairage) tarafından üretilmiştir. İnsan gözünün algılayabileceği tüm renkleri tanımlamak için özel olarak geliştirilmiştir. Bu renkler herhangi bir tarayıcıya bağımlı olmayıp, tarayıcılarda, monitörlerde ve yazıcılarda aslına uygun olarak üretilebilmektedir. Bilgisayarda kullanımları rahat olduğundan oldukça geniş bir renk yelpazesi bulunmaktadır[37].

7.1.4. HSV Renk Modeli

HSV 1978 yılında Alvy Ray Smith tarafından duyurulan, renkler arasındaki ilişkiyi açıklayan bir modeldir. HSV Ton (H; hue), doygunluk (S; saturation) ve değer (V; value) olmak üzere, üç boyutlu rengi göstermektedir. Ton (Hue); rengin kendisini tanımlar. Ton ekseni; kırmızı ile başlayan, yeşil ve mavi ile devam eden ve tekrar kırmızı da biten bütün ara renkler ile araları doldurulmuş 0 ile 360 arasında değişen bir çemberdir. Doygunluk (Saturation); nötr griye kadar olan değer derecesini göstermektedir. Doygunluk, belirli bir renk tonunun tam doygun olduğu 1, hiç doygun olmadığı 0, dereceleri arasındaki değerlerle belirtilmektedir. Değeri (Value); dikey ekseni belirtir ve V = 0 siyah renge, V= 1 ise beyaz renge karşılık gelmektedir[37].

Şekil 7.3.'de HSV renk modeline örnek bir görüntü yer almaktadır.



Şekil 7.3. HSV renk modeli

7.1.5. HSL Renk Modeli

HSV renk modeli gibi, HSL'de Alvy Ray Smith tarafından duyurulmuştur. Bu model RGB modeline benzemekte ve resim üzerinde detay kaybetmeden renk değişiklikleri yapma imkanı tanımaktadır. HSL renk modelinde, renkler üç parametre ile temsil edilmektedir. Bunlar; Ton (Hue; H), Doygunluk (Saturation; S) ve parlaklıktır (Lightness; L). Bu model, HSV modeli ile aynı renk düzlemini kullanmaktadır. HSL renk modeli üst tepesinde beyaz ve altında siyah bir çift altıgen koni ile temsil edilmektedir[37].

8. GÖRÜNTÜ ŞİFRELEME

Gelişen teknoloji internet kullanımının yaygınlaşmasına, bilgisayar ağlarının olağanüstü derecede büyümesine neden olmuştur. Kurulan bu bilgisayar ağları birbirlerine internet aracılığı ile bağlanmakta ve veri alışverişinde bulunmaktadır. Teknolojik ilerlemelere paralel olarak her geçen gün internetteki veri akışı da artmaktadır. Yaşanan bu gelişmeler karşısında bilgisayar ağlarının en önemli konularından biri son derece önemli olan bilgilerin, yetkisiz kişilerin eline geçmesini engellemek olmuştur. Bu nedenle de geçmişten günümüze çok çeşitli şifreleme yöntemleri geliştirilmiştir. İnternet üzerinden iletilen veri sadece metin değil, aynı zamanda ses, resim ve diğer multimedya bilgilerini de içermektedir. Dolayısıyla geliştirilen şifreleme yöntemleri sadece metinlere yönelik değildir, diğer multimedya araçlarını da kapsamaktadır.

Günlük hayatımızda resimler çok geniş bir kullanım alanına sahiptir. Resimlerin daha yoğun kullanılmaya başlandığı ve internet üzerinden yapılan veri alış verişine dahil edildiği zaman, onların güvenliğini sağlamak çok önemli bir konu haline gelmiştir. Günümüzde, mevcut olan birçok şifreleme sistemleri düz metin verilerini korumak için tasarlanmıştır. Orjinal açık metin, rastgele anlamsız şifreli metinlere dönüştürülmektedir. Şifreli metin üretildikten sonra istenilen yere iletilmektedir. Şifreli metin alındığında ise, şifre çözme algoritması kullanılarak orijinal haline dönüştürülmektedir.

Resim verileri, metin verilerinden farklı bir yapıya sahip olduğundan dolayı resimleri direk olarak şifrelemek (RSA ve DES gibi geleneksel şifreleme yöntemleri kullanılmasına rağmen) uygun değildir. Metin verileri ile resim verileri arasındaki farklılıklar aşağıdaki gibidir[38].

1. Resimlerin boyutları metinlere göre çok daha büyüktür. Dolayısıyla geleneksel şifreleme sistemleri, resmi direk olarak şifrelemek için daha fazla zamana ihtiyaç duymaktadır. Metinler direk şifrelenirken, resimleri şifreleme zamanını azaltmak için genellikle önce resim sıkıştırma yöntemlerinden faydalanılmaktadır.

2. Şifrelenen görüntü ile şifresi çözülen görüntü birebir aynı olmak zorunda değildir. Makul düzeydeki veri kayıplarını insan gözü algılayamadığı için bu kayıplar yok sayılabilmektedir. Oysa şifrelenmiş metin, orijinal metne eşit olmak zorundadır. Çünkü şifreleme ve şifre çözme esnasında oluşabilecek en küçük bir veri kaybı bazen metinsel verilerde büyük bozulmalara neden olmaktadır.

3. Metinsel veriler kelimelerden oluşmaktadır. Dolayısıyla metinler direk şifrelenebilmektedir. Ancak resimler genellikle iki boyutlu dizi şeklinde ifade edilmektedir. İki boyutlu bir diziyi klasik şifreleme yöntemleriyle şifreleyebilmek için bu iki boyutlu dizinin tek boyutlu bir diziye dönüştürülmesi gerekmektedir. Böylesi bir durum ise görüntülerin klasik yöntemlerle şifrelenmesinde ekstra zaman demektir.

Görüntülerin güvenli olarak şifrelendiğini kabul edebilmek için bilgi güvenliği alanında kullanılan gizlilik (mesajın görme yetkisi olmayan kişilerce okunamaması), bütünlük (mesajın yetkisiz kişilerce değiştirilememesi, bozulamaması yani bilginin üzerinde hiçbir değişiklik yapılamaması) ve kullanılabilirlik (mesajın iletilmek istenen kişi tarafından tam olarak ulaşılabilir halde olması) koşullarının dışında aşağıda verilen temel bazı koşulların sağlanması gerekir.

1. Şifreleme sistemi hesaplama bakımından çok güvenli olmalıdır. Şifreyi kırmak çok büyük hesaplama zamanı gerektirmelidir.

2. Şifreleme ve şifre çözme algoritmaları sistemin performansını olumsuz yönde etkilemeyecek kadar hızlı, kişisel bilgisayara sahip kullanıcılar tarafından uygulanabilecek kadarda basit olmalıdır.

3. Güvenlik mekanizması esnek ve mümkün olduğunca geniş kullanım alanına sahip olmalıdır.

4. Şifrelenmiş resim verilerinin boyutu çok fazla artmamalıdır[39].

8.1. Şifrelenmiş Resimlere Karşı Yapılan Saldırı Tipleri

Resim şifreleme sistemlerine karşı yapılan 5 saldırı tipi mevcuttur. Bu saldırı tiplerinin hepsinde şifreyi çözmeye çalışan kişinin, kullanılan şifreleme algoritmalarını bildiği varsayılmaktadır. Saldırı tipleri şunlardır[38, 39]:

1. Sadece Şifrelenmiş Resme Yönelik Saldırı: Bu saldırı yönteminde yetkisiz kullanıcının şifreli resmi ağ ortamından aldığı gizli anahtara sahip olmadığı ve gizli anahtarı, sadece ele geçirdiği şifrelenmiş resmi kullanarak elde edebileceği kabul edilmektedir.

2. Bilinen Düz Resim Saldırısı: Yetkisiz kullanıcının, düz ve şifreli resim çiftini ele geçirdiği kabul edilmektedir. Şifreyi çözmeye çalışan kişi, düz resimleri şifrelemek için kullanılan anahtarı belirlemeli ya da aynı anahtarla yeni şifrelenen resimleri çözebilecek bir algoritma geliştirmelidir.

3. Seçilen Düz Resim Saldırısı: Bu yöntem bilinen düz resim saldırısı yönteminden çok daha etkili bir yöntemdir. Çünkü saldırgan, şifreyi çözebilmek için gereken bazı özel, düz ve şifreli resimleri kendisi seçebilmektedir. Dolayısıyla gizli anahtar hakkında daha fazla bilgi edinebilmektedir.

4. Kesik Parçaları Birleştirme Saldırısı: Bu saldırı yönteminde saldırgan şifrelenmiş resmi küçük parçalara ayırıp, bu küçük parçaları teker teker kırmaktadır. Küçük parçalara ayrılan her bir alanı kırmak için gereken hesaplama zamanı şifreli resmi kırmak için gereken hesaplama zamanından çok daha azdır. Dolayısıyla bu yöntem diğer saldırı yöntemlerinden daha güçlüdür.

5. Komşu Saldırılar: Saldırganın resmin bir parçasını bildiği kabul edilmektedir. Birçok resmin alan sınırları düzgün bir yapıda olduğu için şifre çözücü bu özelliği kullanarak komşu olan alanların sınırlarını hızlı bir şekilde seçebilmekte ve resmin bilinen kısımları üzerinden tüm şifreli resim çözülebilmektedir[40].

8.2. Görüntü Şifreleme Yöntemleri Ve Algoritmaları

Kriptografik sistemlerin çoğu metinsel verileri şifrelemek üzere tasarlanmıştır. Ancak günümüzde teknolojinin ilerlemesiyle birlikte görsel veriler daha yoğun kullanılmaya başlanmış ve bunların güvenliğini sağlamak giderek önem kazanmıştır.

Görsel verileri şifrelemek için kullanılan belli başlı yöntemler şunlardır:

1. Dijital İmza Kullanılarak Şifreleme
2. Vektör Kuantumlama Teknikleri ile Şifreleme
3. SCAN Dili Kullanılarak Şifreleme
4. Kaotik Resim Şifreleme Algoritmaları

8.2.1. Dijital İmza Kullanılarak Görüntü Şifreleme

Dijital imzalar, kişinin el yazısı ile attığı imzaya eşdeğerdir, elle atılan imzanın elektronik ortamdaki karşılığıdır ve aynı amaçla yani kimlik doğrulama amacıyla kullanılmaktadır. Dijital imza, imzalanacak metin ve imzalayacak kişinin gizli anahtarı kullanılarak matematiksel algoritmalarla elde edilen bir dizi karakterden oluşmaktadır. Dijital imzanın başkaları tarafından taklit edilmesi çok zordur ve kim tarafından imzalandığı da şüpheye yer bırakmayacak şekilde ispatlanabilmektedir. Ayrıca güvenli

olarak imzalanmış elektronik veride sonradan bir değişiklik yapılıp yapılmadığının tespitide sağlanabilmektedir.

Oluşturulan dijital imza şifreleme sırasında şifrelenmemiş resmin kodlanmış verisine bit düzeyinde özel veya işlemi ile eklenmektedir. Resmin kodlama işlemi BCH gibi uygun bir hata kodlama yöntemiyle yapılmaktadır. Dijital imza, hata kontrol kodlama yönteminden sonra resme eklenen bir gürültüdür. Resmin şifresi çözüldükten sonra dijital imza kullanılarak resmin doğruluğu onaylanmaktadır[41].

8.2.2. Vektör Kuantumlama Teknikleri İle Görüntü Şifreleme

Kuantum şifreleme, güvenli iletişimi garanti edebilmek için kuantum mekaniğinin temel kuramlarından olan Heisenberg Belirsizlik Prensibini kullanmaktadır. Bu belirsizlik prensibine göre kuantum boyutlarındaki sistemde bir değişkenin, aynı anda iki niceliğinin (konum ve momentum) ölçülmesi, diğer nicelikleri değiştirmektedir. Matematiğin aksine fiziğe daha fazla güvenmesi bakımından geleneksel kriptografik sistemlerden farklıdır. İletişimin optik hatlar üzerinden en küçük ışık parçacığı olan fotonlar sayesinde gerçekleştirildiği gizli anahtar dağıtım yöntemidir.

Kuantum şifreleme sistemi, mesajın iletilmesinden ziyade mesajın şifrelenmesinde ve şifrelenen mesajın çözülmesinde kullanılan anahtarın güvenli bir şekilde alıcı ve verici arasında iletimi ile ilgilenmektedir. Bu sistemde iletişim kuran iki taraf, sadece kendilerinin bileceği rastgele ortak bir bit dizisi üretmekte, bu bit dizisini verinin şifrelenmesinde veya şifrelerinin açılmasında kullanmaktadır. Kuantum kriptografinin önemli özelliklerinden biri, şifreleme anahtarını ele geçirmeye çalışan üçüncü bir tarafın varlığını, iletişim kuran iki tarafında tespit edebilmesidir [42, 43].

Kuantum kriptografi tekniği güvenli bir protokole sahip olsada uygulanabilirliği şu an için yüksek maliyet gerektirmektedir. Dolayısıyla günümüzde kısıtlı imkanlarla daha çok askeri amaçlı olarak kullanılmaktadır[44].

8.2.3. SCAN Dili Kullanılarak Görüntü Şifreleme

SCAN, hızlı ve çok sayıda scan tarama desenlerinden oluşmuş, iki boyutlu ve biçimsel dil temelli bir yaklaşımdır. İkili ve gri resim türlerinde herhangi bir kayıp olmadan sıkıştırma ve şifreleme işlemleri yapmaktadır. Resmin sıkıştırma ve şifreleme algoritması, SCAN yönteminden elde edilen çeşitli SCAN desenlerine bağlıdır.

Şifrelenen bir resmin sıkıştırma ve şifreleme algoritmaları gizli tutulabildiği sürece şifresi çözülememektedir. Ancak günümüz de birçok sıkıştırma ve şifreleme yönteminin algoritmaları bilinmektedir. Günümüzde varolan yöntemler şifreleme algoritmasının gizliliğine değil de gizli bir anahtara bağlıdır. Güvenli bir şifreleme için hem sıkıştırma hem de anahtar tabanlı şifreleme yapılmalıdır[45].

Bu yöntemde ikili bir resim, resimde kodlanmış olarak belirtilen tarama yolu ve bu yol üzerindeki bit dizileri kodlanarak sıkıştırma işlemi yapılmakta, şifrelenmektedir. Resim üzerindeki tarama yolu, resmin her pikselinden sadece bir kere geçilerek elde edilen sıradır. Böylelikle şifreleme işlemi gizli tutulan bir dizi tarama yolu kullanılarak yapılmakta, kullanılan bu tarama yolları şifreleme anahtarını oluşturmaktadır. Sıkıştırma yönteminin temelinde, kodlanmış tarama yolunu ve bu yol üzerindeki kodlanmış bit dizisini ifade etmek için gereken bit sayısını minimize edecek uygun tarama yolunu belirleyebilmek yatmaktadır.

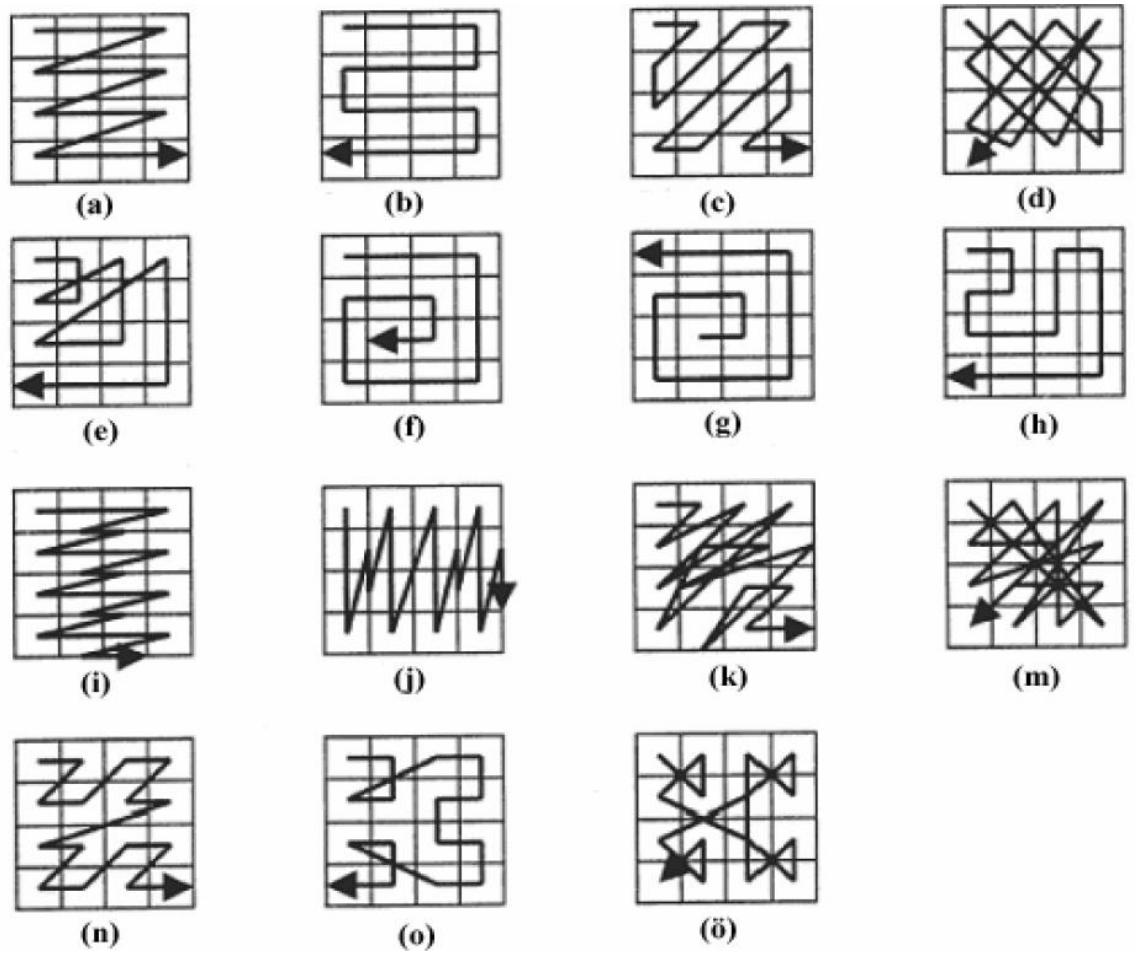
SCAN dilinin basitçe kullanımı aşağıdaki gibidir.

İki boyutlu bir diziyi taramak demek (Matematiksel olarak nxn boyutlu bir dizi (nxn)! farklı şekilde taranabilmektedir.) dizinin her elemanına sadece bir kez erişmektir. Bunun için kullanılan fonksiyon şöyledir:

Pmxn= {p(i,j): $1 \leq i \leq m$, $1 \leq j \leq n$} den {1, 2,..,mn – 1, mn} şeklinde gösterilir.

Yukarıdaki fonksiyon kullanılarak oluşturulan 15 temel tarama deseni aşağıda verilmektedir.

Özel uygulamalar için bu tarama desenlerinin sayısı çok daha fazla arttırılabilmektedir. Tarama desenlerinin 6 çeşit dönüşümü vardır. Bunlar kendisi, yatay yansıma, dikey yansıma, 90, 180, 270 derece döndürülmelerinden ve bunların çeşitli bileşenlerinden oluşmaktadır[38].



Şekil 8.1. SCAN dilindeki temel tarama desenleri

8.2.4. Kaotik Görüntü Şifreleme Algoritmaları

Kaos teorisi, doğrusal olmayan dinamik sistemlerde bulunan, başlangıç koşullarına aşırı duyarlılık gösteren, görünüşte rastgele davranışlar sergileyen ancak tamamen deterministik olan yani bir sonraki durumun bir önceki duruma göre belirlendiği sistemler olarak tanımlanmaktadır. Kısaca kaos teorisi, görünüşte rastgele olan veriler içerisindeki düzeni bulma ile ilgilidir.

Kaotik sistemlerin en önemli karakteristiklerinden biri sistem parametrelerine ve/veya başlangıç koşullarına duyarlı olmasıdır[46]. Sistem parametrelerinde ve/veya başlangıç koşullarında yapılan küçücük bir değişiklik dahi sistem yörüngelerinde büyük değişimlere sebep olmaktadır. Kaosun bu temel karakteristiği; Shannon'un mükemmel gizlilik teorisi için vurguladığı ve modern şifreleme sistemleri içinde temel karakteristiklerden olan karıştırma ve yayılma özellikleri ile örtüşmektedir [47, 48].

Karıştırma özelliğini kullanan şifreleme sistemlerinde; her anahtar için açık metin ve şifreli metin arasındaki yapılarda istatistiksel bağlılığın olmadığı şifreleme algoritması seçilmektedir. Bu özelliğin olabilmesi için anahtarın ve açık metnin her bitinin şifreli metni etkilemesi gerekmektedir[49].

Yayılma özelliğine sahip bir şifreleme sisteminde ise; şifreli metin ile anahtar arasındaki ilişki mümkün olduğunca karmaşık hale getirilmelidir. Yani yayılma, anahtarın açık ve şifreli metne bağlılığının kript analiz için faydalı olamayacak kadar karmaşıklaştırılması, doğrusal olmaması demektir. Böylelikle şifreleme algoritmasından anahtarı bulabilmek imkansız olmaktadır [49].

Kaosun açıklanan bu özellikleri, kaotik sistemlerde uzun süre tahmin yapmayı zorlaştırmaktadır. Bu durumda kaosun kriptografi alanında kullanılma sebeplerinden biridir. Kaotik sistemlerin kriptografinin bazı özellikleri ile oldukça benzer yönleri bulunmaktadır. Bilimin birçok dalında uygulama alanı bulan kaos teorisi kriptolojik sistemlerin tasarlanmasında da yaygın kullanıma sahiptir[50].

1990'lardan bu yana blok şifreleme ve görüntü şifreleme algoritmaları gibi birçok klasik şifreleme sisteminin tasarlanmasında kaos tabanlı sistemler kullanılmaktadır. Klasik şifreleme teknikleriyle, kaotik senkronizasyon kullanılarak şifreleme yapılmaktadır. Bu teknikte şifrelenecek veriler kaotik sistemle üretilen işaretler kullanılarak seçilen şifreleme algoritmasıyla şifrelenmekte ve alıcı tarafa gönderilmektedir. Alıcı tarafta şifreli veri kaotik senkronizasyon bilgisi ile ayıklanarak şifre çözme işlemi gerçekleştirilmektedir.

Kaotik tabanlı sistemlerde kullanılan algoritmalar düşük hesaplama maliyetini sahiptir, genellikle çok basittir dolayısıyla sistem hızı oldukça yüksektir, görüntü şifreleme konusunda gayet başarılıdır, anahtar değişikliğine karşı çok hassas olduğu içinde daha güvenilirdir[51].

Kaos tabanlı güvenli haberleşme sistemlerinin çoğunda şifreleme işleminde kullanılan anahtarlar, sistemin başlangıç şartlarından veya sistem parametrelerinden üretilmektedir. Bu anahtarları kesin olarak belirleyebilmek için derin incelemeler sonucunda önceden oluşturulmuş anahtar uzayı kullanılmaktadır. Anahtar uzayının boyutu kriptolojik sistemlerce erişilebilen ve şifreleme, deşifreleme işlemleri için kullanılan anahtarların sayısıyla ifade edilmektedir. Anahtar uzayı oldukça büyüktür ve doğrusal değildir. Anahtar uzayının matematiksel ifadesi şöyledir:

$$K=\{k1, k2 , k3 ,..., kr\}$$

Burada k_i oluşturulmuş anahtarlar içinde herhangi bir anahtar, K'de, bu anahtarların topluluğu yani anahtar uzayıdır.

Genellikle sayı teorisine göre çalışan geleneksel şifreleme sistemlerinde şifreleme anahtarı, bazı otomatik işlemler sonucu üretilen rastgele geniş ancak sınırlı sayı dizisinden elde edilen bir stringdir. Çoğu mevcut kaos tabanlı kripto sistemlerde ise anahtar uzayının kaotik davranışlar gösteren bölgelerinden, donanım imkanları ölçüsünde rasyonel sayı aralıklarından seçilen anahtarlar kullanılmaktadır. Bu anahtarlar eşit güçlükte değildir. Bir anahtar seçerken göz önünde bulundurulması gereken birden fazla parametrenin varlığı düşünüldüğünde, bu parametrelerin birbirine bağımlılıklarını, hangi aralığın en iyiyi üreteceğini belirlemek oldukça zordur. Eğer, m parametreye bağlı bir anahtardan söz ediliyorsa, anahtarın seçileceği uzay en az m boyutlu olmalıdır[51, 52].

Yukarıda açıklanmaya çalışılan kaotik sistemlerle şifrelenen verilere karşı geleneksel kripto analiz metotları etkisiz kalmaktadır. Geleneksel kripto analiz metotları; kaba kuvvet, diferansiyel kripto analiz gibi tekniklerle şifreli veriyi çözmeye çalışmaktadır. Ancak bu tür teknikler kaotik şifreleme sistemlerine uygulanamamaktadır. Çünkü kaos rastgele benzeri davranış gösterme özelliği sayesinde geleneksel kripto analize karşı dirençlidir[53,54].

9.UYGULAMA

Bu tez çalışmasında SCAN algoritmasıyla, Kaos tabanlı sistemler kullanılarak görüntü şifreleme uygulaması yapılmaktadır. Sistemin verimliliğini ve güvenilirliğini değerlendirmek için aşağıda verilen ölçütler kullanılmaktadır.

NPCR, UACI ve PSNR görüntü şifreleme yöntemlerinin gücünü değerlendirmek için kullanılan ölçütlerdir. NPCR ve UACI test sonuçları ne kadar yüksek olursa şifreleme yönteminin diferansiyel saldırılara karşı direnci o kadar yüksek olmaktadır.

NPCR ve UACI test sonuçlarının matematiksel hesaplaması aşağıdaki gibidir:

$$D(i,j) = \begin{cases} 0, if\, C^1(i,j) = C^2(i,j) \\ 1, if\, C^1(i,j) \neq C^2(i,j) \end{cases} \quad \textbf{(9.1)}$$

$$\text{NPCR: } \mathcal{N}(C^1, C^2) = \sum_{i,j} \frac{D(i,j)}{T} \times 100\% \quad \textbf{(9.2)}$$

$$\text{UACI: } \mathcal{U}(C^1, C^2) = \sum_{i,j} \frac{|C^1(i,j) - C^2(i,j)|}{F \cdot T} \times 100\% \quad \textbf{(9.3)}$$

C^1: Orijinal resim

C^2: Şifrelenmiş resim

i,j: Resmin piksel değerleri

T: Toplam piksel sayısı

F: Satır ve sütun sayılarının çarpımı

D(i,j): Yeni oluşturulan matrisin değerleri (Yeni oluşturulan matris piksel değerleri değişmiş ise 1, değişmemişse 0 değerini alan, 0 ve 1'lerden oluşan matristir.)

PSNR değerlerinin yüksek olması resimde çok fazla bozulma olmadığını göstermektedir.

$$MSE = \sum_{i,j} (P_{i,j} - \bar{P}_{i,j})^2 \quad \textbf{(9.4)}$$

$$PSNR = 10.\log.\frac{M \cdot N \cdot Max(P_{i,j}^2)}{\sum_{i,j} (P_{i,j} - \bar{P}_{i,j})^2} \quad \textbf{(9.5)}$$

P: Orijinal resim

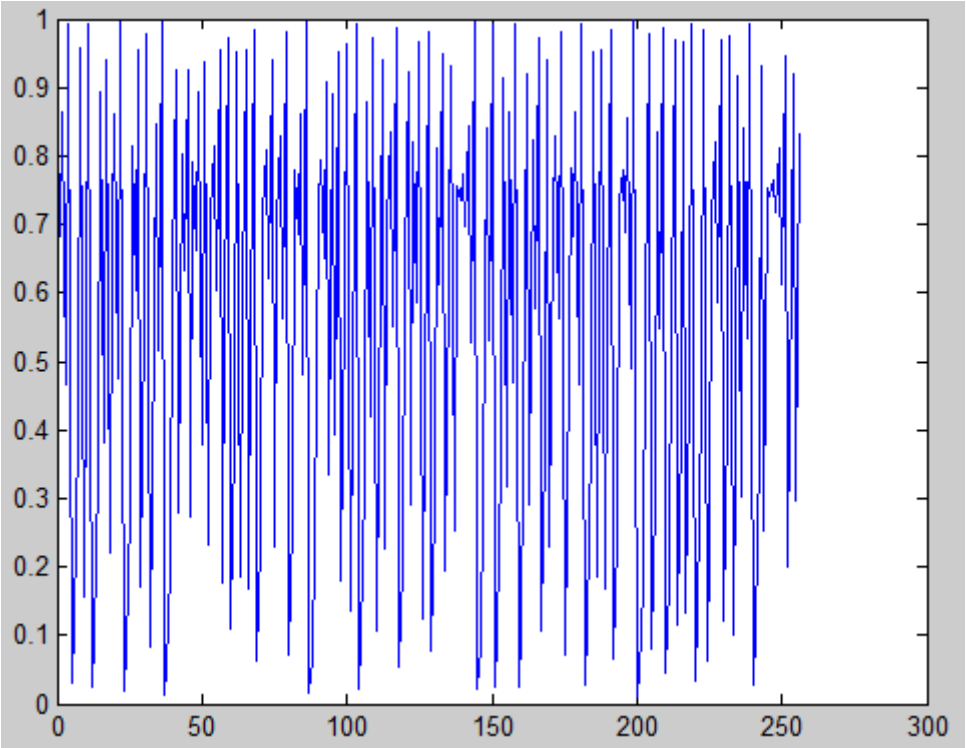
$\bar{P}$: Şifrelenmiş resim

Kaos tabanlı sistemlerde aşağıdaki formül kullanılarak rastgele sayı üretilmektedir. Üretilen bu rastgele sayı dizisiyle şifrelenecek resim XOR (özel veya) işlemine tabi tutulmaktadır. Burada üretilen sayı dizisi şifrelemede kullanacağımız 128 bitlik anahtarımızı oluşturmaktadır.

$$x_{n+1} = kx_n(1 - x_n) \tag{9.6}$$

Yukarıdaki formülde kullanılan k katsayısı kaos katsayısıdır ve 3.5 ile 4 arasında değerler alabilmektedir.

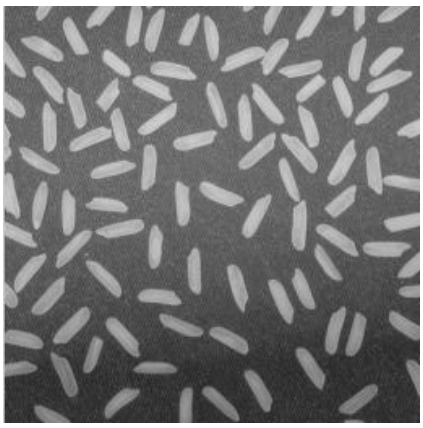
Şekil 9.1.'de denklem 9.6 kullanılarak oluşturulan kaos tabanlı bir rastgele sayı üreticinin karakteristiği verilmektedir. Şekil 9.1.'den de anlaşılacağı üzere sistem kararsız olduğundan dolayı, şifreleme için uygun görülmektedir. Bu lojistik haritada k değeri 3,99 ve başlangıç değeri x_1 0,682 seçilmektedir.



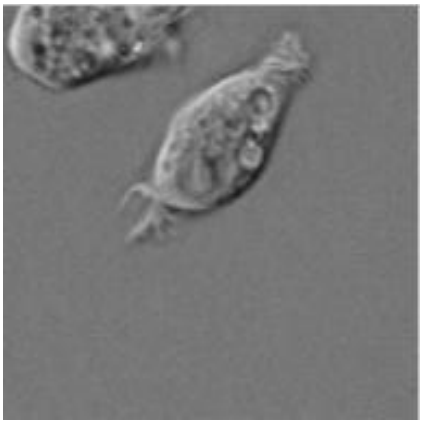
Şekil 9.1. Uygulamada kullanılan lojistik harita

Şekil 9.2.' de görüntü şifreleme uygulamasında kullanılan resimlerin orijinal halleri, Şekil 9.3.' te Kaos tabanlı rastgele sayı üreteci kullanılarak üretilen 256 bitlik kaotik anahtarla şifrelenen resimler gösterilmektedir.

(a)

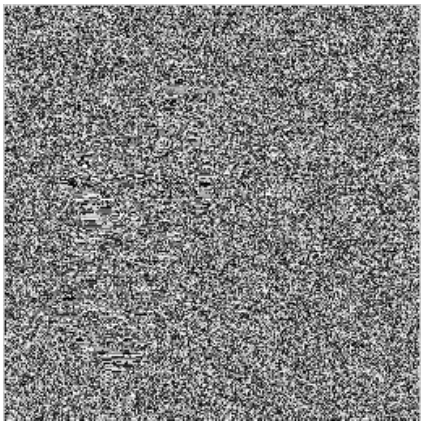


(b)

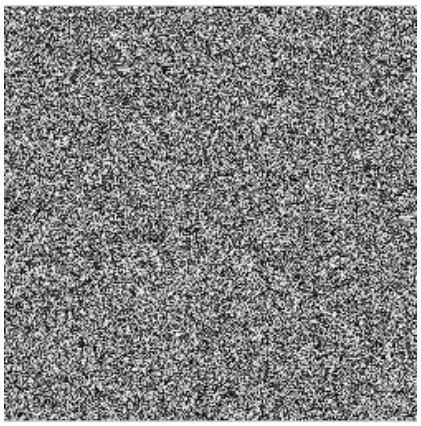


(c)

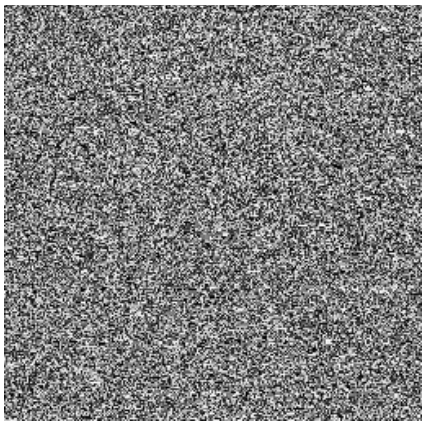
Şekil 9.2. Resimlerin orijinal halleri: (a) Cameraman, (b) Rice, (c) Cell



(a)



(b)



(c)

Şekil 9.3. Resimlerin 256 bitlik kaotik anahtarla şifrelenmiş halleri: (a) Cameraman, (b) Rice, (c) Cell

Kaos tabanlı sistemler kullanılarak yapılan simetrik şifreleme işlemi sonucunda resimler Şekil 9.3.‘ te görüldüğü gibi anlaşılmaz bir şekle dönüşmektedir. Şifrelenen bu resimleri çözebilmek için, şifreleme anahtarına ihtiyaç vardır ve bu uygulamada kullanılan

anahtar 256 bittir. Pratikte bu uzunluktaki anahtarlar kaba kuvvet saldırısıyla çözülememekte, şifreleme işlemi başarılı olarak kabul edilmektedir.

Yapılan şifreleme işleminin görünüşte başarılı olduğu düşünülebilir. Ancak şifreli resimlerin bitleri üzerinde oynama yapılarak resmin ana hatlarına ulaşmak mümkündür. Resmin ana hatlarına ulaşmak için ise aşağıdaki algoritma kullanılmaktadır.

Adım 1: Şifrelenmiş resmin piksel değerleri 8 bitlik binary değer olarak kodlanmaktadır.

Adım 2: Elde edilen binary resmin en anlamlı bitleri aşağıda verilen Şekil 9.4' teki gibi çarpılarak yeniden kodlanmaktadır.

MSB							LSB

Şekil 9.4. 8 bitlik binary sayı dizisi

Normalde binary' den onluk sisteme çevirim aşağıdaki gibi yapılmaktadır.

$11010101 = 1.2^7+1.2^6+0.2^5+1.2^4+0.2^3+1.2^2+0.2^1+1.2^0$

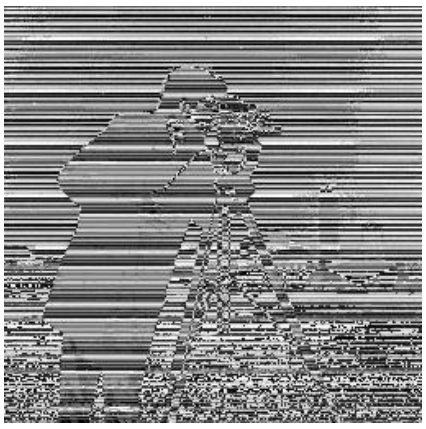
Gerçekleştirilen analiz yönteminde ise dönüşüm yukarıdaki örneğin tam tersi sırada gerçekleştirilmektedir.

$11010101 = 1.2^0+1.2^1+0.2^2+1.2^3+0.2^4+1.2^5+0.2^6+1.2^7$

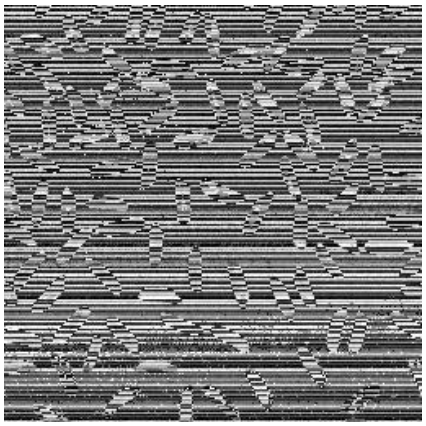
Adım 3: Resmin tüm piksellerine adım 2' deki işlem uygulanmaktadır.

Adım 4: Yeni resim elde edilmektedir.

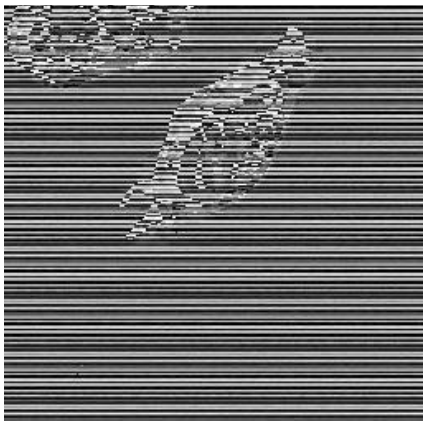
Elde edilen resimler ise şekil 9.5.' te gösterilmektedir.



(a)



(b)

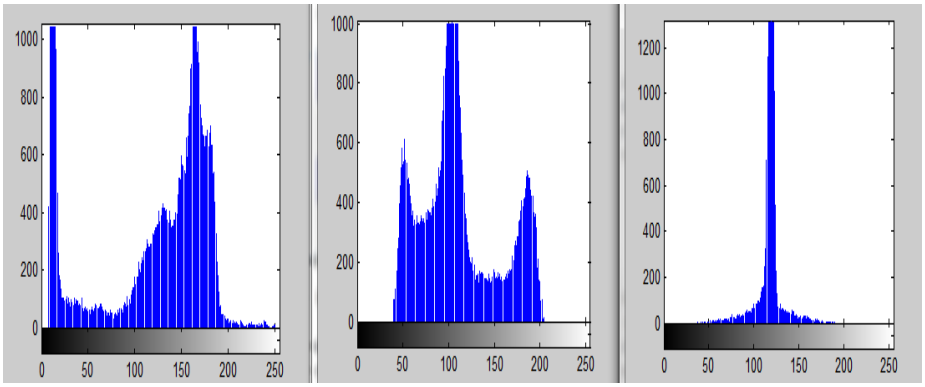


(c)

Şekil 9.5. Analiz edilmiş resimler: (a) Cameraman, (b) Rice, (c) Cell

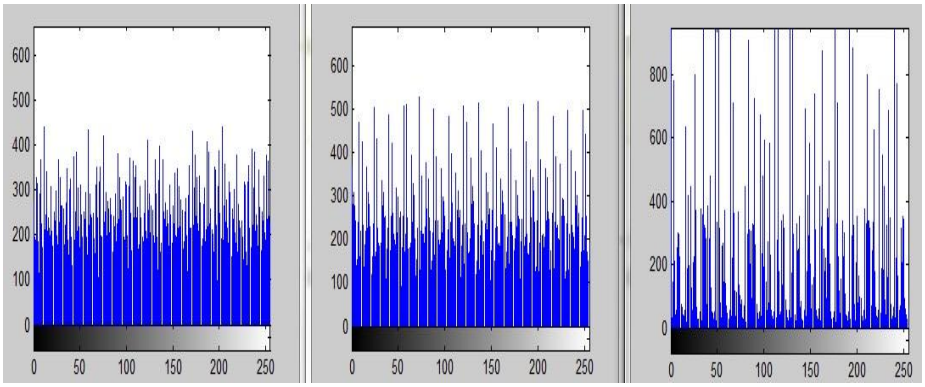
Anahtarı tahmin etmeden sadece resmin piksel değerleri üzerinde önerilen algoritma kullanılarak, resmin ana hatları tahmin edilebilmektedir. Buda kaotik sistem kullanılarak şifreleme yapmanın önemli bir dezavantajı olarak görülmektedir.

Resimlerin orijinal hallerinin ve kaos tabanlı sistemler kullanılarak şifrelenen resimlerin histogram sonuçları aşağıda yer alan Şekil 9.6. ve Şekil 9.7.'de verilmektedir.



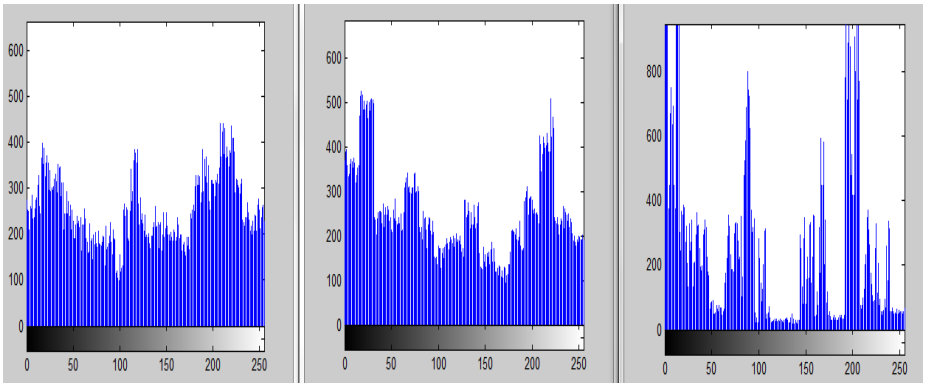
(a) (b) (c)

Şekil 9.6. Orjinal resimlerin histogramları: (a) Cameraman, (b) Rice, (c) Cell



(a) (b) (c)

Şekil 9.7. Kaos tabanlı rastgele sayı üreteci kullanılarak şifrelenen resimlerin histogramları: (a) Cameraman, (b) Rice, (c) Cell

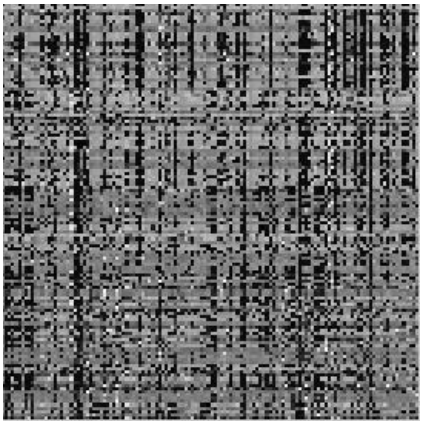


(a) (b) (c)

Şekil 9.8. Gerçekleştirilen analiz yöntemi sonucunda elde edilen resimlerin histogramları: (a) Cameraman, (b) Rice, (c) Cell

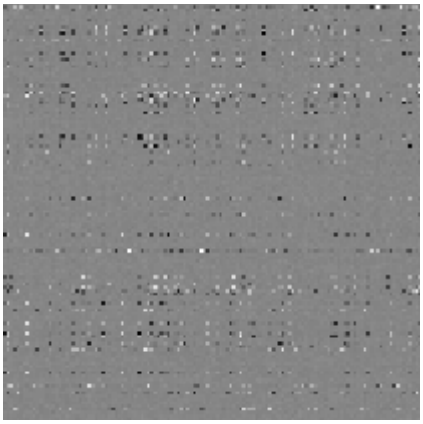
Şekil 9.8.'den de görüldüğü gibi analiz yöntemiyle elde edilen histogramlar asıl histogramları yakınsamakla birlikte tepe ve çukur noktaları da belirgin hale getirmektedir. Böylelikle resmin tahmin edilebilmesi kolaylaştırılmaktadır. Scan algoritması kullanılarak kaosun bu dezavantajı giderilmeye çalışılmaktadır.

SCAN algoritmasında kullanılan tarama desenlerinden bir desen belirlenmekte ve belirlenen tarama deseni kullanılarak resim şifrelenmektedir. SCAN algoritmasıyla yapılan şifreleme sonucunda elde edilen şifreli resimler Şekil 9.9.' da gösterilmektedir. Şekil 9.9.'de şifrelenmiş hali verilen resimlerin orijinal halleri Şekil 9.2.'de verilen resimlerdir.



(a)

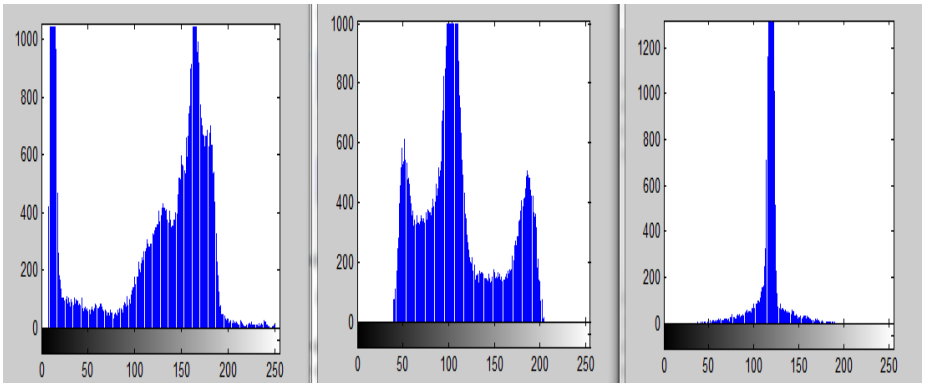
(b)



(c)

Şekil 9.9. SCAN algoritması kullanılarak şifrelenen resimler: (a) Cameraman, (b) Rice, (c) Cell

SCAN algoritması kullanılarak şifrelenen resimlerin histogram sonuçları aşağıda yer alan Şekil 9.10.'da verilmektedir.



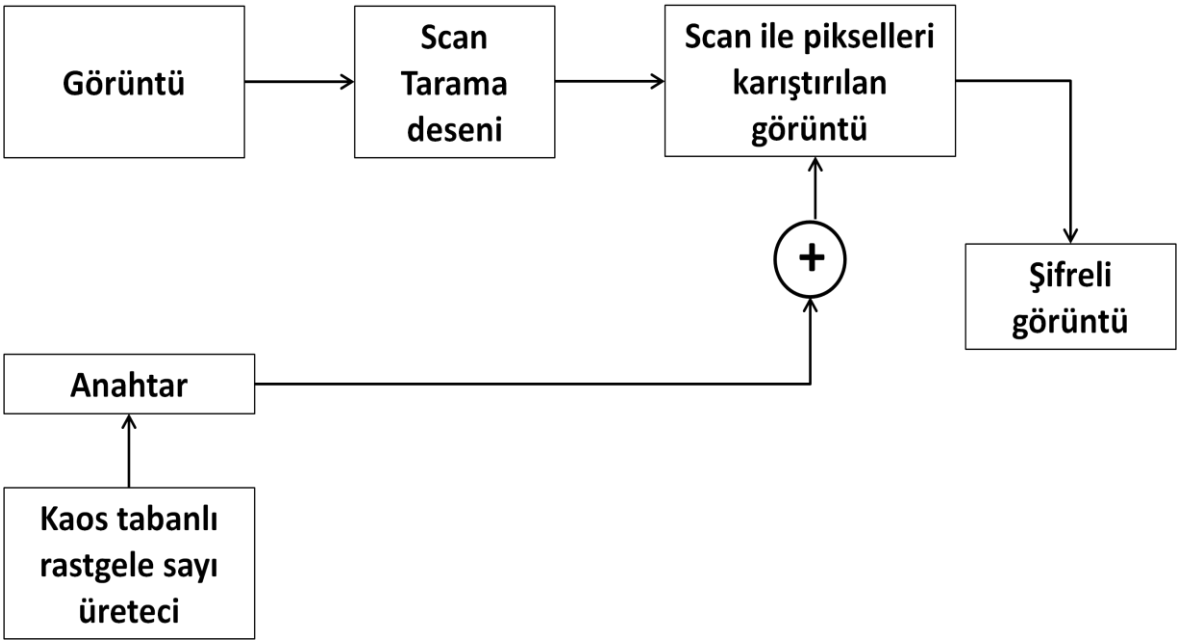
(a) (b) (c)

Şekil 9.10. SCAN algoritması kullanılarak şifrelenen resmin histogramları: (a) Cameraman, (b) Rice, (c) Cell

Gerçekleştirilen çalışmalardan da görüldüğü gibi SCAN algoritmasıyla yapılan şifreleme işleminin resmin renk değerlerine bir etkisi yoktur. Çünkü Şekil 9.6 ve Şekil 9.10.'da verilen histogram sonuçları birbirinin aynısıdır.

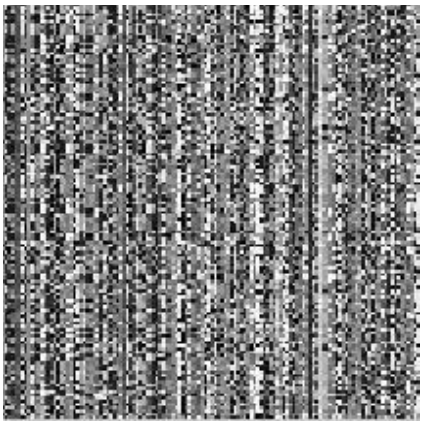
Kaos tabanlı sistemler kullanılarak yapılan şifreleme işlemindeki sorun şifrelenen resmin tahmin edilebilmesidir. Kaos tabanlı şifreleme görüntüyü bozmaktadır.

Bu iki şifreleme algoritmasının avantajlarını kullanabilmek için hibrit bir metot geliştirmek gerekmektedir. Öncelikle SCAN algoritması kullanılarak pikseller farklı konumlandırılmaktadır. Ardından kaos tabanlı sayı üretecinden elde edilen anahtarla resim XOR işlemine tabi tutularak şifreleme işlemi gerçekleştirilmektedir. Geliştirilen hibrit metot kullanılarak yapılan şifreleme işleminin blok diyagramı şöyledir:

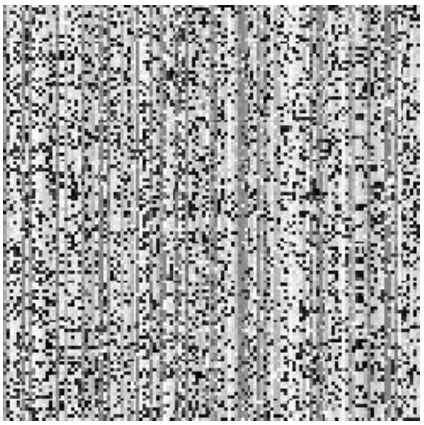


Şekil 9.11. Geliştirilen hibrit metot kullanılarak yapılan şifreleme işleminin blok diyagramı

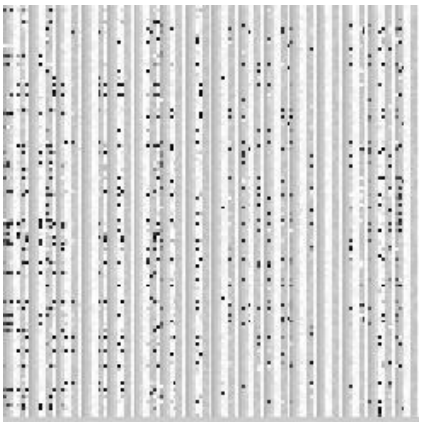
Şekil 9.12.'de geliştirilen hibrit metotla şifrelenmiş olan resimler görülmektedir.



(a)

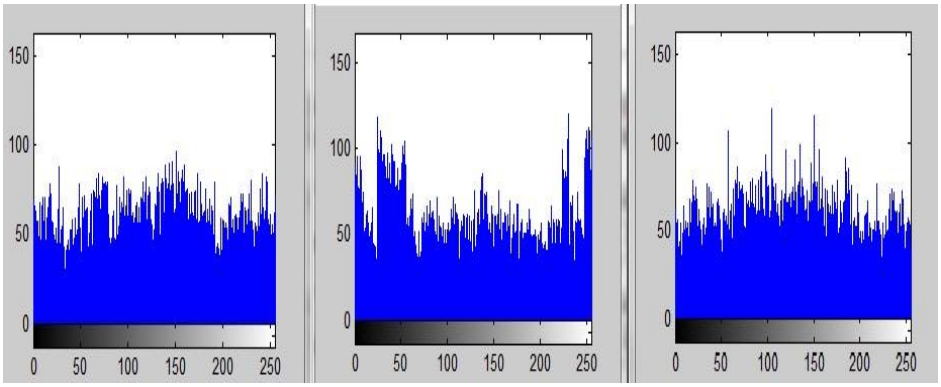


(b)



(c)

Şekil 9.12. Geliştirilen hibrit metotla şifrelenen resimler: (a) Cameraman, (b) Rice, (c) Cell



Şekil 9.13. Geliştirilen hibrit metotla şifrelenen resmin histogramları: (a) Cameraman, (b) Rice, (c) Cell

Görüntülerin histogramlarında aşırı uç tepe ve çukur noktaları görüntüler hakkında bilgi vermektedir. Şifrelenmiş resimlerin histogramlarında bu noktaların bulunması halinde, bu noktalar üzerine yapılan kripto analiz çalışmaları ile şifrelenmemiş görüntüler elde edilebilmektedir. Dolayısıyla şifreli görüntülerin histogramlarının dalgalı bir yapıdan ziyade düz olması beklenir. Buda yapılan şifrelemenin güçlü olduğunu göstermektedir. Çünkü bu durumda şifreli görüntüye yapılan saldırılar sonucu görüntülerin orijinalini elde etmek zordur.

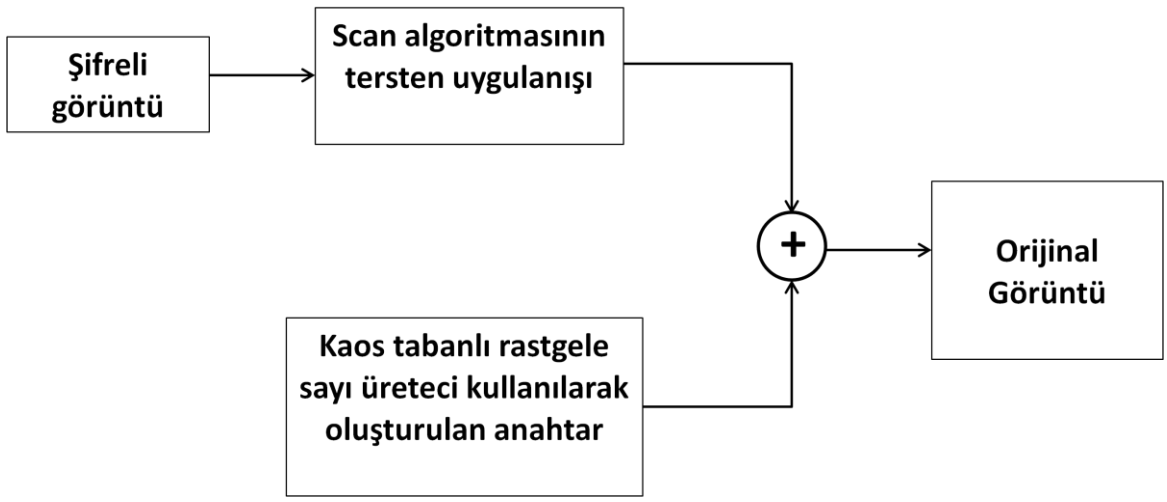
Yapılan tez çalışmasında önerilen hibrit metot sonucunda şifrelenen resmin histogramında (Şekil 9.13.'te geliştirilen hibrit metotla şifrelenmiş resimlerin histogramları verilmiştir.) aşırı dalgalanmanın olmadığı gözlenmektedir. Buda görüntünün, yapılacak saldırılara karşı güçlü olduğunu göstermektedir.

Aşağıdaki tabloda Kaos tabanlı sistemle, SCAN algoritmasıyla ve geliştirilen hibrit metotla yapılan şifreleme işlemlerinin NPCR, UACI, PSNR ölçütlerine göre analiz sonuçları verilmektedir. Tablodaki sonuçlardan da anlaşılacağı üzere en iyi sonuçlar hibrit metotla yapılan şifrelemeden elde edilmektedir.

Tablo 9.1. Scan Algoritması ve Kaos Tabanlı Rastgele Sayı Üreteci Kullanılarak Şifrelenen Resimlerin NPCR, UACI ve PSNR Sonuçları

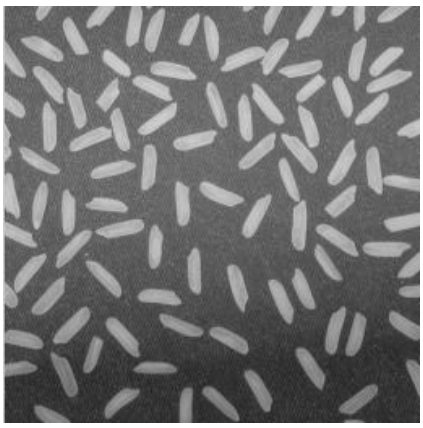
Kullanılan Resim	Ölçüt	Kaos Tabanlı Şifreleme	Scan Algoritması	Hibrit Metot
Cameraman	NPCR	99,6399	98,8403	99,7300
	UACI	$6{,}28.10^{-4}$	$1{,}60.10^{-4}$	$1{,}83.10^{-5}$
	PSNR	7,9888	9,6743	7,8806
Rice	NPCR	99.4263	98,8464	99,7803
	UACI	0,0040	$7{,}71.10^{-5}$	$8{,}05.10^{-7}$
	PSNR	9,8662	11,1114	7,9157
Cell	NPCR	99.8657	89,6484	99,9695
	UACI	0,0020	$7{,}18.10^{-5}$	$2{,}97.10^{-5}$
	PSNR	9,6843	21,7420	7,9439

Geliştirilen hibrit metotla şifrelenen resmin şifresinin çözülmesi:

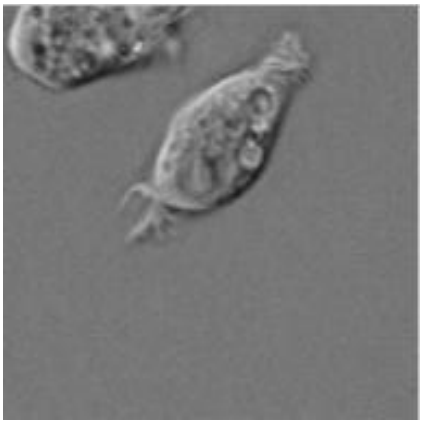


Şekil 9.14. Geliştirilen hibrit metot kullanılarak yapılan şifre çözme işleminin blok diyagramı

(a)



(b)



(c)

Şekil 9.15. Şifre çözme işleminden sonra elde edilen resimler: (a) Cameraman, (b) Rice, (c) Cell

10. SONUÇ VE ÖNERİLER

Bilginin güvenliğini sağlama geçmişten günümüze kadar her dönemde çok önemli bir konu olmuştur. Günümüzde teknolojinin gelişmesiyle bilgi alışverişinin bilgisayar ağları üzerinden yapılması, bilgi güvenliğinin önemini daha da arttırmıştır. Bilginin kötü niyetli kişilerin eline geçmesine engel olmak, bilgiyi korumak, saklamak için anlaşılmaz bir hale dönüştürülmesi, şifrelenmesi gerekmektedir. Bu amaca hizmet etmek için şu ana kadar birçok şifreleme tekniği geliştirilmiştir.

Bu tez çalışmasında, Kaos tabanlı şifrelemenin tek başına yeterli olamayacağı anlaşılmaktadır. Dolayısıyla Kaos tabanlı sistemlerle birlikte SCAN algoritması da kullanılmaktadır.

Bu çalışmada ilk olarak veri şifreleme teknikleri incelenmekte daha sonrada SCAN algoritmasıyla uygun tarama desenleri kullanılarak resmin pikselleri karıştırılmaktadır. Kaos tabanlı sistemlerin özelliklerinden yararlanılarak random (rastgele) bir dizi üretilmekte ve bu dizilerde şifrelemede kullanılmaktadır. Kullanılan tekniklerin eksik yönleri görülmekte ve bu eksiklikleri giderebilmek için hibrit bir metot geliştirilmektedir. Bu metotlar gri seviyeli resimlere uygulanmaktadır.

PSNR, NPCR, UACI ölçütleri ve histogram analizi kullanılarak şifrelemenin başarımı hesaplanmaktadır. Şifrelenmiş resimlerin histogramları çıkarılarak elde edilen sonuçların algoritmik güvenliği analiz edilmektedir. Yapılan analizler neticesinde en iyi sonuçların geliştirilen hibrit metotla elde edildiği görülmektedir.

Önerilen metot optimizasyon teknikleri ışığında geliştirilerek ve bir donanım yardımıyla gerçekleştirildiği zaman, günlük hayatta rahatlıkla kullanılabilecek güçlü bir şifreleme aygıtı oluşturulabileceği düşünülmektedir. Bu aygıt resim ve video şifrelemede kullanılabilir. Böylece asimetrik video şifreleme cihazlarına alternatif bir şifreleme aygıtı geliştirilebilir.

Yapılan incelemeler sonucunda gizliliğin son derece önemli olduğu ve teknolojinin geldiği nokta itibariyle bilgi hırsızlığının had safhaya ulaştığı günümüzde veri şifrelemenin her geçen gün daha çok gelişeceği ve kriptoloji tekniklerinin sayısının da artarak güçleneceği gözlenmektedir.

KAYNAKLAR

[1] Ersin, G.: "TÜBİTAK UEKAE Açık Anahtar Altyapısı Eğitim Kitabı", Mayıs, 2006

[2] Kriptoloji – Kriptoğrafi Seminerleri Sonuç Bildirgesi 20 – 29 Temmuz 2009

[3] http://www.savaskartal.com/2010/04/11/kriptoloji-nedir/ (Son Erişim Tarihi: 28.03.2013)

[4] Çimen, C.; Akleylek, S.; Akyıldız, E.: "Şifrelerin Matematiği: Kriptografi",ODTÜ Geliştirme Vakfı Yayıncılığı (Adana/2009 (4. Basım))

[5] Menezes, A.; Van Oorschot, P., C. and Vanstone, S., A., Handbook of Applied Cryptography, CRC Press, October 1996.

[6] http://tr.wikipedia.org/wiki/Kriptoloji (Son Erişim Tarihi: 01.04.2013)

[7] Sakallı, M. T. : " Modern Şifreleme Yöntemlerinin Gücünün İncelenmesi", Doktora Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne, Türkiye, 2006

[8] Kahn, D.: "The Codebreakers", Macmillan, 1967, Sf. 82

[9]Tılborg H.C.A.: "Fundamentals of Cryptology", Kluwer Academic Publishers, 2000

[10] Bilişim Güvenliği [online], Pro-G ve Oracle
http://www.pro-g.com.tr/whitepapers/bilisim-guvenligi-v1.pdf (Son Erişim Tarihi: 03.11.2013)

[11] Hellman, M.E.: "An Overview of Puplic Key Cryptography" IEEE Communications Society Magazine

[12] Şahin, A.; Buluş, E.; Sakallı, M.T.: "Modern Blok Şifreleme Algoritmalarının Gücünün İncelenmesi", II. Mühendislik Bilimleri Genç Araştırmacılar Kongresi - MBGAK'2005, İstanbul, Türkiye, 2005

[13] http://en.wikipedia.org/wiki/Lucifer_(cipher) (Son Erişim Tarihi 15.12.2013)

[14] Akyıldız, E.; Doganaksoy, A.; Keyman, E.; Uguz, M.: "Kriptografi Ders Notları, ODTÜ Uygulamalı Matematik Enstitüsü", Şubat, 2004

[15] Gladman, B.: "A Speciation for Rijhndeal", The AES Algorithm, Mayıs, 2002, 2-20

[**16] Daemen, J.; Rijmen, V.:** "The Design of Rijndael AES-The Advanced Encryption Standard Series: Information Security and Cryptography"**,** Springer Verlag 2002.

[17] Schneier, B.: "The Blowfish Encryption Algorithm", Dr. Dobb's Journal, pp. 38-40, April 1994.

[18] Spies, T.: "Feistel Finite Set Encryption Mode" Voltage Security, Inc.

[19] Stallings, W.: "The RC4 Stream Encryptıon Algorithm" 2005

[20] Biham, E.; Dunkelman, O.:"Cryptanalysis of the A5/1 GSM Stream Cipher" 2000

[21] Yerlikaya, T.; Buluş, E.; Arda, D.: "Asimetrik Kripto Sistemler ve Uygulamaları", II.Mühendislik Fakültesi Genç Arastırmacılar Kongresi, Kasım, 2005

[22] Salomaa, A.: "Public-Key Cryptography", Springer Verlag, New York, 1990

[23] Biçkin, İ.: "Elektronik İmza ve Elektronik İmza ile İlgili Yasal Düzenlemeler", TBB Dergisi, Sayı 63, 2006

[24] Yerlikaya, T., Buluş, E.: "AES Finalistlerinin Karşılaştırılması - RSA Şifreleme Algoritmasının İncelenmesi ve Kriptanalizi", 20. Türkiye Bilişim Kurultayı, İstanbul-TÜRKİYE, 2003

[25] Bozkurt F.:"Elektronik Güvenlik, Şifreleme Teknikleri ve Algoritması Açık Olan Şifreleme Teknikleri", Dokuz Eylül Üniversitesi, 2005

[26] Yerlikaya, T., Buluş, E.: "New Generation Public Key Crypto: Elliptic Curve Cryptography", International Scientific Conferance, Gabrovo, 2004

[27] Çetin, Ö.: "Eliptik Eğri Kriptografisi", Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara, Türkiye, Mayıs, 2006, 44-49

[28] http://fahriv.home.uludag.edu.tr/pdf_notlari/bp1/fahriv_bp2_hafta_7.pdf(Son Erişim Tarihi 25.11.2013)

[29] Parker, J.R.: "Algorithm For İmage Processing And Computer Vision", Wiley Computer Publishing, 1997

[30] Buğday, A.: "Gerçek Zamanlı Videolarda Ön Plan Arka Plan Ayrımı", Yüksek Lisans Tezi, Ankara 2010.

[31]http://mebk12.meb.gov.tr/meb_iys_dosyalar/42/03/175302/dosyalar/2013_02/14110159_grntleme.pdf (Son Erişim Tarihi 03.12.2013)

[32] http://www.webdersleri.com/sayfa.asp?id=623(Son Erişim Tarihi 05.12.2013)

[33] http://en.wikipedia.org/wiki/Encapsulated_PostScript (Son Erişim Tarihi 15.11.2013)

[34] http://tr.wikipedia.org/wiki/Graphics_Interchange_Format (Son Erişim Tarihi 01.12.2013)

[35] http://tr.wikipedia.org/wiki/TIFF(Son Erişim Tarihi 03.12.2013)

[36] http://renk.nedir.com/#ixzz2maXnSvpn (Son Erişim Tarihi 05.12.2013)

[37] Polat, H. H.:" Grafik Tasarım Sürecinde Kullanılan Aygıtların Renk Modelleri", İdil Dergisi, 2012

[**38] Güvenoğlu, E.:** "Görüntü Şifreleme Algoritmaları ve Performans Analizleri" , Yüksek Lisans Tezi, 2066

[39] Öztürk, İ.: " Görüntü Şifreleme" ,Institute of Technology Computer Engineering Department, 2003

[40] Chang C-C., Hwang M-S., Chen T-S.: "A New Encription Algorithm For İmage Cryptosystems", The Journal of Systems and Software, 22 August 2000

[41] Sinha, A., Singh, K.:"A Technique For İmage Encryption Using Digital Signature", Optics Communications, February 2003

[42] http://tr.wikipedia.org/wiki/Kuantum_kriptografi (Son Erişim Tarihi 21.12.2013)

[43] Sergienko, A.: "Quantum Communications And Cryptography", 2005

[44] Gümüş, E.: "Kuantum Kriptografi ve Anahtar Dağıtım Protokolleri", Akademik Bilişim 2011, Malatya, Şubat 2011

[45] Manıccam, S.S., Bourbakis, N.G.:"Lossless image compression and encryption using SCAN", Pattern Recognition, 2001

[46] Jakimoski, G., Kocarev, L.: "Chaos and cryptography: block encryption ciphers. IEEE Trans Circ Syst—I", 2001

[47] Amigo, J.M., Kocarev, L., Szczapanski, J.: "Theory and practice of chaotic cryptography, Physics Letters A", 2007

[48] Alvarez, G., Li, S.: "Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems", International Journal of Bifurcation and Chaos, 2006

[49] Paar, C., Pelzl, J.: "Understanding Cryptography: A Textbook for Students and Practitioners" Springer, 2010

[50] Yavuz, N.: "Kaotik Ortamlarda Güvenli Veri Transferi" 2006

[51] Kangwei, H., Lih, T., Parwani, C.: "Chaos and Cryptography: Applications and Analysis" 2003

[52] Guan, Z.H., Huang, F., Guan, W.: "Chaos based image encryption algorithm. Phys Lett A" 2005

[53] Milanı, M.M.R.A., Pehlivan, H., Pour S.H.: "Kaos Tabanlı Bir Şifreleme Yöntemi ve Analizi" Akademik Bilişim 2011, Malatya, Şubat 2011

[54] Özkaynak, F., Özer, A.B., Yavuz, S.: "Hücresel Otomata ve Kaos Tabanlı Bir Şifreleme Algoritmasının Güvenlik Analizi" 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara, Eylül 2013

[55] http://tr.wikipedia.org/wiki/SHA-1 (Son Erişim Tarihi 15.12.2013)

[56] Christof, P., Pelzl, J.: "Understanding Cryptography: A Textbook for Students and Practitioners"

[57] http://www.emo.org.tr/ekler/67cca0f32a34f11_ek.pdf (Son Erişim Tarihi: 25.11.2013)

[58] http://www.bilgisayarkavramlari.com/2008/06/07/blok-sifreleme-block-cipher (Son Erişim Tarihi: 25.11.2013)

[59] Cımato, S., Yang, C.N.: "Visual Cryptography and Secret Image Sharing"

[60] Naor, M., Shamir, A.: " Visual Cryptography"

[61] http://tr.wikipedia.org/wiki/Kriptografi (Son Erişim Tarihi 29.11.2013)

[62] Lin, C.C., Tsai, W.H.: " Visual Cryptography for Gray-Level Images by Dithering Techniques" Elsevier Science, Augustc2001

[63] http://tr.wikipedia.org/wiki/Dizi_%C5%9Fifresi (Son Erişim Tarihi (27.11.2013)

[64] http://jes.ksu.edu.tr/public/journals/1/backIssues/sayi/eski/sayi/81/81.35-40.pdf (Son Erişim Tarihi (29.11.2013)

[65] Yen, J.C., Guo, J.I.: "A new Chaotic Image Encryption Algorithm", National Lien-Ho College of Technology and Commerce, Miaoli,Taiwan

[66] Chang, C.C., Yu, T.X.: "Crypanalysis of an encryption scheme for binary images", Pattern Recognition Letters, 8 February 2002

[67] http://www.bidb.itu.edu.tr/?d=1002 (Son Erişim Tarihi 19.09.2013)

[68] http://acikfikir.org/2012/04/des-algoritmasi-kriptoloji-yazi-dizisi-4/ (Son Erişim Tarihi 25.09.2013)

[69] http://kriptoloji.net/matematik-ve-sifre (Son Erişim Tarihi: 21.10.2013)

[70] Wang, D., XiaoboLi, F.: "On General Construction For Extended Visual Cryptography Schemes"

[71] Yerlikaya T., Buluş E., Buluş N.: "Kripto Algoritmalarının Gelişimi Ve Önemi"

[72] Kodaz, H.: "RSA Şifreleme Algoritmasının Uygulaması" Konya, 2003

[73] Dalkılıç G., Yıldızoğlu G.: "Tek Anahtarlı Yeni Bir Şifreleme Algoritması Daha" İzmir, 2008

[74] http://www.bilgisayarkavramlari.com/2009/06/11/idea-uluslar-arasi-sifreleme-algoritmasi/ (Son Erişim Tarihi: 26.11.2013)

[75] Hou, Y.C.: " Visual Cryptography for Color Images" The Journal of the Pattern Recognition Society, 2003

[76] Güleryüz, H.İ., Tuncer, T., Avcı, E.: " Kaos ve SCAN Algoritması Tabanlı Görüntü Şifreleme Uygulaması", ISDFS'13, Elazığ, Mayıs 2013

ÖZGEÇMİŞ

14.04.1987 yılında Elazığ'da doğdum. İlk, orta ve lise öğrenimimi Elazığ'da tamamladıktan sonra 2006 yılında Fırat Üniversitesi, Teknik Eğitim Fakültesi, Elektronik Bilgisayar Eğitimi Bölümü, Bilgisayar Öğretmenliğini kazandım. 2010 yılında bu bölümden mezun oldum. Aynı yıl Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elektronik Bilgisayar Eğitimi Bölümü, Bilgisayar Sistemleri Anabilim Dalında yüksek lisans eğitimine hak kazandım. 2010 yılında Bingöl ilinin Genç ilçesindeki Kız Meslek Lisesinde bilgisayar öğretmeni olarak göreve başladım. 2013 yılı Eylül ayından itibaren Elazığ Merkez Uzuntarla Ortaokulunda öğretmenlik görevimi sürdürmekteyim.