
GAZİ ÜNİVERSİTESİ
Gazi
1926

MASKE TABANLI GÖRÜNTÜ ŞİFRELEME

Ali UZUN

YÜKSEK LİSANSTEZİ
ADLİ BİLİŞİM ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

AĞUSTOS 2022

Ali UZUN tarafından hazırlanan “MASKE TABANLI GÖRÜNTÜ ŞİFRELEME” adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Adli Bilişim Ana Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Doç. Dr. Hasan Hüseyin SAYAN

Elektrik Elektronik Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ..……

Başkan: Prof. Dr. Recep DEMİRCİ

Bilgisayar Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ……..

Üye: Prof. Dr. Pakize ERDOĞMUŞ

Bilgisayar Mühendisliği Ana Bilim Dalı, Düzce Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ……..

Tez Savunma Tarihi: 02/08/2022

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

……..…….

Prof. Dr. Aslıhan TÜFEKCİ

Bilişim Enstitüsü Müdürü

ETİK BEYAN

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

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

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

Ali UZUN
02/08/2022

MASKE TABANLI GÖRÜNTÜ ŞİFRELEME

(Yüksek Lisans Tezi)

Ali Uzun

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Ağustos 2022

ÖZET

Gelişen iletişim teknolojileriyle birlikte internet ve mobil ağların kullanımı da hızlı bir artış göstermiştir. Gelişen teknolojiler kullanıcılar için birçok avantaj sağlamasına rağmen, kullanım oranlarının artmasıyla bilgi güvenliği, konunun en önemli noktalarından biri haline gelmiştir. Geçmişten günümüze bilgi güvenliğine verilen önem katlanarak artmaya devam etmektedir. Teknolojik gelişmelerin ilerlemesiyle birlikte görüntülerin kullanım alanları artmakta ve görüntü günlük hayatımızda geniş bir kullanım alanına sahip olmaktadır. Artan görüntü kullanımı ile birlikte konunun önemli bir noktası olan güvenlik sorunu ortaya çıkmıştır. Bilginin güvenli bir biçimde iletilmesinde veya saklanmasında matematiksel yöntemler sıkça kullanılmaktadır. Kriptoloji matematiksel yöntemler kullanılarak verilerin korunmasını sağlayan şifreleme bilimidir. Kaos ve kriptografi arasındaki benzerlikler kullanılarak geliştirilen kriptografik bir uygulamada güvenli ve etkili sonuçlar için günümüzde sıklıkla kaotik sistemlere başvurulmaktadır.

Bu tezde, permütasyon ve kombinasyon işlemleri ile rastgeleliği arttırılırmış kaotik lojistik harita kullanarak bir görüntü şifreleme yöntemi geliştirilip ve yöntemin yeterliliği farklı testler ile incelenmiştir. Önerilen algoritma, kaotik bir lojistik haritanın başlangıç parametresi için rastgele oluşturulmuş gizli anahtarı kullanır. Bu parametreler kullanılarak maske görüntüsü üretilir. Daha sonra şifrelenecek görüntü maske görüntüsü ve XOR (Özel-VEYA) operatörü kullanılarak şifrelenir. Geliştirilen metodun yeterliliğini test etmek için; anahtar uzay analizi, histogram analizi, korelasyon analizi, bilgi entropisi analizi, sinyal gürültü oranı analizi, ortalama karesel hata analizi, ortalama mutlak hata analizi ve şifreleme kalitesi analizi testleri orijinal ve şifreli görüntüler arasında C# ortamında gerçekleştirilmiştir. Sonuçlar klasik lojistik harita ile karşılaştırıldığında önerilen yöntemin verimliliği doğrulanmıştır.

Bilim Kodu	:	92403
Anahtar Kelimeler	:	Kaotik lojistik harita, görüntü şifreleme, kaotik kriptografi, görüntü şifre çözme,
Sayfa Adedi	:	79
Danışman	:	Doç. Dr. Hasan Hüseyin SAYAN

MASK BASED IMAGE ENCRYPTION

(M. Sc. Thesis)

Ali UZUN

GAZİ UNIVERSITY

INFORMATICS INSTITUTE

August 2022

ABSTRACT

With the developing communication technologies, the use of the internet and mobile networks has also increased rapidly. Although developing technologies provide many advantages for users, information security has become one of the most important points of the subject with the increase in usage rates. From past to present, the importance given to information security continues to increase exponentially. With the advancement of technological developments, the usage areas of images are increasing and the image has a wide usage area in our daily life. With the increasing use of images, the security problem, which is an important point of the subject, has emerged. Mathematical methods are frequently used to transmit or store information securely. Cryptology is the science of encryption that protects data using mathematical methods. In a cryptographic application developed using the similarities between chaos and cryptography, chaotic systems are frequently used today for safe and effective results.

In this thesis, an image encryption method was developed using permutation and combination operations and a chaotic logistic map with increased randomness, and the adequacy of the method was examined with different tests. The proposed algorithm uses a randomly generated secret key for the starting parameter of a chaotic logistic map. Using these parameters, a mask image is generated. Then the image which will be encrypted is encrypted using the mask image and the XOR (Private-OR) operator. To test the adequacy of the developed method key space analysis, histogram analysis, correlation analysis, information entropy analysis, signal to noise ratio analysis, mean square error analysis, mean absolute error analysis and encryption quality analysis tests were performed between the original and encrypted images in C# application. The efficiency of the proposed method was confirmed when the results were compared with the classical logistic map.

ScienceCode : 92403

KeyWords : Chaotic logistic map, image encryption, chaotic cryptography, image decryption

PageNumber : 79

Supervisor : Assoc. Prof. Dr. Hasan Hüseyin SAYAN

TEŞEKKÜR

Tez çalışmam boyunca yanımda olan ve her zaman desteğini hissettiğim değerli danışmanım Doç. Dr. Hasan Hüseyin SAYAN'a sonsuz teşekkürlerimi sunarım. Tez çalışmam süresince bilgi birikimiyle beni yönlendiren ve fikirlerini esirgemeyen Prof. Dr. Recep DEMİRCİ'ye, eğitim hayatım boyunca her zaman yanımda olan sevgili aileme çok teşekkür ederim.

İÇİNDEKİLER

Sayfa

ÖZET iv
ABSTRACT v
İÇİNDEKİLER vii
ÇİZELGELERİN LİSTESİ ix
ŞEKİLLERİN LİSTESİ xv
SİMGELER VE KISALTMALAR xviii
1. GİRİŞ 1
2. KRİPTOLOJİ VE GÖRÜNTÜ ŞİFRELEME 5
2.1. Kriptolojinin Temelleri 5
2.1.1. Kriptografi 5
2.1.2. Kriptoanaliz 7
2.2. Kriptolojinin Gelişimi 7
2.2.1. Klasik şifreleme yöntemleri 9
2.2.2. Modern şifreleme yöntemleri 12
2.3. Görüntü Şifreleme 21
2.4. Görüntü Şifreleme Algoritmaları İçin Güvenlik Testleri 22
2.4.1. Anahtar uzayı analizi 22
2.4.2. Histogram analizi 22
2.4.3. Korelasyon (KR) 23
2.4.4. Bilgi entropisi analizi (BE) 23
2.4.5. Sinyal gürültü oranı (PSNR) ve ortalama karesel hata (MSE) analizi 24
2.4.6. Ortalama mutlak hata analizi (MAE) 24

Sayfa

2.4.7. Şifreleme kalitesi analizi (EQ) 25

2.5. Rastgele Sayı Üreteçleri (RSÜ) 25

2.5.1. Gerçek rastgele sayı üreteçleri (GRSÜ) 25

2.5.2. Sözde rastgele sayı üreteçleri (SRSÜ) 27

3. KAOTİK LOJİSTİK TABANLI ŞİFRELEME SİSTEMİ VE GELİŞTİRİLEN UYGULAMA ARAYÜZÜ 31

3.1. Kaotik Lojistik Şifreleme Sistemi 31

3.2. Önerilen Algoritma ve Geliştirilen Kullanıcı Arayüzü 34

3.2.1. Önerilen algoritma 34

3.2.2. Geliştirilen kullanıcı arayüzü 40

4. DENEYSEL SONUÇLAR VE GÜVENLİK ANALİZLER 49

4.1. Deneysel Sonuçlar 49

4.2. Güvenlik analizleri 54

4.2.1. Anahtar uzayı analizi 54

4.2.2. Histogram analizi 54

4.2.3. Korelasyon (KR) 62

4.2.4. Bilgi entropisi analizi (BE) 63

4.2.5. Sinyal gürültü oranı (PSNR) ve ortalama karesel hata (MSE) analizi 64

4.2.6. Ortalama mutlak hata analizi (MAE) 67

4.2.7. Şifreleme kalitesi analizi (EQ) 68

5. SONUÇ VE ÖNERİLER 71

KAYNAKLAR 73

ÖZGEÇMİŞ 79

ÇİZELGELERİNLİSTESİ

Çizelge **Sayfa**

Çizelge 2.1. AES algoritması anahtar uzunluğu döngü sayısı tablosu 17

Çizelge 3.1. Klasik lojistik harita ve önerilen lojistik harita ile oluşturulan sayıların ortalama, varyans ve standart sapma değerleri..... 35

Çizelge 4.1. Klasik lojistik harita ve önerilen lojistik harita ile şifrelenmiş görüntülerin korelasyon değerleri 63

Çizelge 4.2. Klasik lojistik harita ve önerilen lojistik harita ile şifrelenmiş görüntülerin bilgi entropisi değerleri 64

Çizelge 4.3. Klasik lojistik harita ve önerilen lojistik harita ile şifrelenmiş görüntülerin sinyal gürültü oranı değerleri 66

Çizelge 4.4. Klasik lojistik harita ve önerilen lojistik harita ile şifrelenmiş görüntülerin ortalama karesel hata değerleri 67

Çizelge 4.5. Klasik lojistik harita ve önerilen lojistik harita ile şifrelenmiş görüntülerin ortalama mutlak hata değerleri 68

Çizelge 4.6. Klasik lojistik harita ve önerilen lojistik harita ile şifrelenmiş görüntülerin şifreleme kalitesi değerleri 69

ŞEKİLLERİNLİSTESİ

Şekil **Sayfa**

Şekil 2.1. Şifreleme ve şifre çözme süreci 8

Şekil 2.2. Temel şifreleme algoritmaları 9

Şekil 2.3. Vigenere Tablosu 11

Şekil 2.4. ASCII Tablosu..... 12

Şekil 2.5. Simetrik şifreleme metodu..... 13

Şekil 2.6. RC4 algoritması blok diyagramı 14

Şekil 2.7. DES algoritması blok diyagramı 16

Şekil 2.8. AES algoritması adımları..... 18

Şekil 2.9. Asimetrik şifreleme metodu..... 18

Şekil 2.10. RSA şifreleme metodu..... 20

Şekil 2.11. Eliptik eğri algoritmasının şekli 21

Şekil 2.12. GRSÜ mimarisi 26

Şekil 3.1. Kaotik sistem çalışma prensibi..... 33

Şekil 3.2. Maske görüntü (a) klasik lojistik harita ile oluşturulan, (b) önerilen lojistik harita ile oluşturulan..... 35

Şekil 3.3. Maske görüntünün histogram grafiği (a) klasik lojistik harita ile oluşturulan, (b) önerilen lojistik harita ile oluşturulan..... 36

Şekil 3.4. Kod bloğu (a) klasik lojistik harita, (b) önerilen lojistik harita..... 37

Şekil 3.5. Anahtardan lojistik haritanın başlangıç değerlerini elde etme adımları 38

Şekil 3.6. Önerilen lojistik haritayı kullanarak maske görüntü elde etme adımları..... 39

Şekil 3.7. Düz metin görüntüsü ve maske görüntü ile şifreleme adımları 39

Şekil 3.8. Geliştirilen kullanıcı arayüz sayfası 40

Şekil 3.9. Şifreleme arayüz sayfası 40

Şekil 3.10. Resim seçilmiş şifreleme arayüz sayfası..... 41

Şekil 3.11. Lojistik harita ile şifreleme gerçekleştirilmiş arayüz sayfası 42

Şekil **Sayfa**

Şekil 3.12. Önerilen lojistik harita ile şifreleme gerçekleştirilmiş arayüz sayfası..... 42

Şekil 3.13. Güvenlik testleri 43

Şekil 3.14. Örnek güvenlik analizi testi 43

Şekil 3.15. Örnek histogram görüntüsü..... 43

Şekil 3.16. Şifre çözme penceresi 44

Şekil 3.17. Şifreli resim yüklenmiş arayüz görüntüsü 44

Şekil 3.18. Şifresi çözülmüş resim arayüz görüntüsü 45

Şekil 3.19. Rastgele sayı üretme penceresi arayüz görüntüsü..... 46

Şekil 3.20. Önerilen lojistik harita ile üretilen sayıların grafiğinin ekran görüntüsü..... 46

Şekil 3.21. Önerilen lojistik harita ile üretilen sayıların Fi grafiğinin ekran görüntüsü..... 47

Şekil 3.22. Önerilen lojistik harita ile üretilen sayıların Pi grafiğinin ekran görüntüsü..... 47

Şekil 4.1. Lena (a) orijinal görüntüsü, (b) lojistik harita ile şifrelenmiş şekli, (c) önerilen lojistik harita ile şifrelenmiş şekli 49

Şekil 4.2. Biberler (a) orijinal görüntüsü, (b) lojistik harita ile şifrelenmiş şekli, (c) önerilen lojistik harita ile şifrelenmiş şekli 50

Şekil 4.3. Papağan (a) orijinal görüntüsü, (b) lojistik harita ile şifrelenmiş şekli, (c) önerilen lojistik harita ile şifrelenmiş şekli 51

Şekil 4.4. Kuzey ışıkları (a) orijinal görüntüsü, (b) lojistik harita ile şifrelenmiş şekli, (c) önerilen lojistik harita ile şifrelenmiş şekli..... 51

Şekil 4.5. Gazi Üniversitesi rektörlük binası (a) orijinal görüntüsü, (b) lojistik harita ile şifrelenmiş şekli, (c) önerilen lojistik harita ile şifrelenmiş şekli . 52

Şekil 4.6. Meyveler (a) orijinal görüntüsü, (b) lojistik harita ile şifrelenmiş şekli, (c) önerilen lojistik harita ile şifrelenmiş şekli 53

Şekil 4.7. Çiçek (a) orijinal görüntüsü, (b) lojistik harita ile şifrelenmiş şekli, (c) önerilen lojistik harita ile şifrelenmiş şekli 53

Şekil 4.8. Lena görüntüsünün klasik lojistik harita ile şifrelenmiş halinin histogram analizi (a) kırmızı kanal, (b) yeşil kanal, (c) mavi kanal, (d) tüm kanallar; önerilen lojistik harita ile şifrelenmiş görüntünün histogram analizi (e) kırmızı kanal, (f) yeşil kanal, (g) mavi kanal, (h) tüm kanallar..... 55

Şekil **Sayfa**

Şekil 4.9. Biberler görüntüsünün klasik lojistik harita ile şifrelenmiş halinin histogram analizi (a) kırmızı kanal, (b) yeşil kanal, (c) mavi kanal, (d) tüm kanallar; önerilen lojistik harita ile şifrelenmiş görüntünün histogram analizi (e) kırmızı kanal, (f) yeşil kanal, (g) mavi kanal, (h) tüm kanallar 56

Şekil 4.10. Papağan görüntüsünün klasik lojistik harita ile şifrelenmiş halinin histogram analizi (a) kırmızı kanal, (b) yeşil kanal, (c) mavi kanal, (d) tüm kanallar; önerilen lojistik harita ile şifrelenmiş görüntünün histogram analizi (e) kırmızı kanal, (f) yeşil kanal, (g) mavi kanal, (h) tüm kanallar 57

Şekil 4.11. Kuzey ışıkları görüntüsünün klasik lojistik harita ile şifrelenmiş halinin histogram analizi (a) kırmızı kanal, (b) yeşil kanal, (c) mavi kanal, (d) tüm kanallar; önerilen lojistik harita ile şifrelenmiş görüntünün histogram analizi (e) kırmızı kanal, (f) yeşil kanal, (g) mavi kanal, (h) tüm kanallar..... 58

Şekil 4.12. Gazi Üniversitesi rektörlük binası görüntüsünün klasik lojistik harita ile şifrelenmiş halinin histogram analizi (a) kırmızı kanal, (b) yeşil kanal, (c) mavi kanal, (d) tüm kanallar; önerilen lojistik harita ile şifrelenmiş görüntünün histogram analizi (e) kırmızı kanal, (f) yeşil kanal, (g) mavi kanal, (h) tüm kanallar 59

Şekil 4.13. Meyveler görüntüsünün klasik lojistik harita ile şifrelenmiş halinin histogram analizi (a) kırmızı kanal, (b) yeşil kanal, (c) mavi kanal, (d) tüm kanallar; önerilen lojistik harita ile şifrelenmiş görüntünün histogram analizi (e) kırmızı kanal, (f) yeşil kanal, (g) mavi kanal, (h) tüm kanallar 60

Şekil 4.14. Çiçek görüntüsünün klasik lojistik harita ile şifrelenmiş halinin histogram analizi (a) kırmızı kanal, (b) yeşil kanal, (c) mavi kanal, (d) tüm kanallar; önerilen lojistik harita ile şifrelenmiş görüntünün histogram analizi (e) kırmızı kanal, (f) yeşil kanal, (g) mavi kanal, (h) tüm kanallar 61

SİMGELER VE KISALTMALAR

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

Kısaltmalar	Açıklamalar
AES	Gelişmiş şifreleme standardı (Advanced encrypted standard)
ASCII	Bilgi değişimi için Amerikan standart kod sistemi (American standard code information interchange)
BE	Bilgi entropisi değeri
DES	Veri şifreleme standardı (Data encrypted standard)
EQ	Şifreleme kalitesi (Encrypted quality)
GRSÜ	Gerçek rastgele sayı üreteçleri
IBM	Uluslararası iş makineleri (International business machines)
IP	Başlangıç permütasyonu (Initial permutation)
KGSRSÜ	Kriptolojik güvenli sözde rastgele sayı üreteçleri
KR	Korelasyon değeri
LFSR	Doğrusal geri beslemeli kaydedici (Linear feedback shift register)
MAE	Ortalama mutlak hata (Mean absolute error)
MIT	Massachusetts teknoloji enstitüsü (Massachusetts Institute of Technology)
MSE	Ortalama karesel hata (Mean squared error)
NIST	Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standard and Technology)
NSA	Ulusal Güvenlik Ajansı (National Security Agency)
PSNR	Sinyal gürültü oranı (Peak signal to noise ratio)
RSÜ	Rastgele sayı üreteçleri
SRSÜ	Sözde rastgele sayı üreteçleri
XOR	Özel veya (Exclusive OR)

1. GİRİŞ

Bilgi bir değerdir. Bu değeri korumak amacıyla yapılan çalışmaların bütünü bilgi güvenliği olarak adlandırılmaktadır. Geçmişten günümüze bilgi güvenliğine verilen önem katlanarak artmaya devam etmektedir. Bilginin güvenli bir biçimde iletilmesinde veya saklanmasında matematiksel yöntemler sıkça kullanılmaktadır. Kriptografi ve kripto analiz olmak üzere iki temel alandan oluşan kriptoloji, şifreleme bilimi olarak da adlandırılmaktadır [1].

Kriptografi verilerin şifrelenmesi için kullanılan yöntemlere verilen genel bir addır. Matematik, istatistik, elektrik, elektronik, bilgisayar bilimleri gibi birçok bilim dalını içinde barındıran disiplinler arası özel bir bilim dalıdır. Diğer bir ifadeyle, gizliliği olan bir veriyi üçüncü şahısların algılayamayacağı ve öğrenemeyeceği bir forma dönüştürme sürecidir. Bu süreç boyunca veri kaybı olmaması da önemli bir noktadır. Kriptoanaliz ise şifrelenmiş veriden orijinal veriyi elde etme sürecidir.

Kriptolojik uygulamaların temeli onlarca yıl öncesine dayanmaktadır. Teknolojik gelişmelere paralel olarak bu uygulamalar da gelişim göstermiştir. Bu gelişmeler ışığında uygulamalar klasik şifreleme algoritmaları ve modern şifreleme algoritmaları olarak temelde 2 başlık halinde incelenmektedir. Klasik algoritmalardan yaygın olarak Sezar, Vigenere, Vernam ve Hill şifreleme yöntemleri kullanılmaktadır. Modern algoritmalarda ise temel olarak DES (veri şifreleme standardı), AES(gelişmiş şifreleme standardı), RSA ve RC4 şifreleme yöntemleri kullanılmaktadır.

Sezar şifreleme yönteminde açık metinde şifrelenecek veri, anahtar olarak belirlenen sayı kadar kaydırma metodu ile şifreleme gerçekleşir. Şifre çözme işleminde ise, şifreli veriye şifrelemede kullanılan aynı anahtar kullanılarak ters yönde kaydırma işlemi uygulanır ve şifre çözme işlemi gerçekleştirilir [2].

Vigenere şifreleme yöntemi ile şifreleme işlemi gerçekleştirmek için özel Vigenere tablosu kullanılmaktadır. Bu tablo yardımı ile şifrelenecek her bir harf başka bir harf ile değiştirilerek şifreleme gerçekleştirilir. Vigenere şifreleme yönteminde Sezar şifrelemeden farklı olarak anahtar değerinin sabit bir değer değil bir vektör olmasıdır. Şifreleme işleminde anahtar olarak alfabe içerisinden belirlenen bir kelime kullanılır. Şifre çözme işlemi de yine anahtar kelime ve tablo kullanılarak gerçekleştirilir [3,4].

Vernam şifreleme yöntemi şifreleme ve şifre çözmede aynı anahtar kullanıldığı için simetrik bir yöntemdir [5]. Şifrelenecek mesaj 0 ve 1'lerden oluşan ikili sayı sistemine dönüştürülür ve XOR (özel veya) işlemine tabi tutulur. Şifre çözme işlemi ise şifreli mesaj ile anahtarın XOR işlemine tabi tutulmasıyla gerçekleşir. Şifrelemenin eşit olasılıklı XOR işlemi ile yapılmasından istatistiksel olarak iyi sonuçlar elde edilir.

Hill şifreleme yönteminde lineer cebir işlemleri kullanıldığı için kripto analiz süreci teoriktir. Şifrelenecek mesaj eşit uzunluklardaki bloklara ayrılır. Oluşturulan bloklar teker teker şifrelenir. Şifreleme işleminde anahtar olarak m*m boyutunda bir matris kullanılır. Burada m, blok uzunluğunu temsil etmektedir [6].

DES şifreleme yöntemi simetrik bir şifreleme yöntemidir. Şifreleme işlemini gerçekleştirmek için mesaj 64 bit ve anahtar 56 bit uzunluğunda olmalıdır [7]. Şifreleme işleminde her blok farklı bir anahtar kullanılarak gerçekleşmektedir. Gelişen teknoloji ile 56 bitlik anahtar uzunluğu yetersiz kalmış ve DES algoritması yerine 3DES algoritması kullanılmaya başlanmıştır.

AES şifreleme yöntemi DES ve 3DES yönteminin eksik yönlerini gidermek amacıyla geliştirilmiş birçok avantaja sahip blok şifreleme algoritmasına sahiptir. 128, 192 ve 256 bit uzunluğunda anahtar seçenekleri ile AES algoritması saldırılara karşı dayanıklıdır fakat AES algoritması resim gibi büyük boyuttaki multimedya verilerinin şifrelenmesi için uygun değildir [8].

RSA algoritması, bir tür açık anahtar şifreleme algoritmasıdır. Algoritmada simetrik şifrelemeden farklı olarak şifreleme ve şifre çözmede iki farklı anahtar kullanılmaktadır. Algoritma güvenliğini büyük sayıların asal çarpanlara ayrılması zorunluluğuna dayanmaktadır. Algoritmada kullanılan büyük sayılar algoritmanın güvenliği artırmasına karşın günümüz sıradan bilgisayarları ile şifreleme işlemlerinde hız problemini oluşturmaktadır [9].

RC4 algoritması simetrik bir akış şifreleme algoritmasıdır. Algoritma, şifreleme ve şifre çözmede aynı anahtar kullanılması dolayısıyla simetrik, verilerin bloklar halinde değil de bit bit veya byte byte şifrelenmesi nedeniyle akış şifreleme olarak adlandırılmaktadır. Algoritmada şifreleme işlemi için anahtar algoritması ve sözde rastgele üretim algoritması

olmak üzere iki temel bileşen bulunmaktadır. Sözde rastgele üretim algoritması, şifreleme işleminde kullanılmak üzere başlangıç değerlerine bağlı olarak sayılar üretmektedir. Üretilen bu sayılar birbirlerine bağlı olarak üretildikleri için saldırılara karşı istatistiksel olarak dayanıklı olmalıdır. Sayıların istatistiksel olarak dayanıklı olabilmesi için sayılar olabildiğince eşit olasılıklı ve rastgele olmalıdır. Rastgelelik özelliğinin zayıf olması durumunda saldırganlar şifrelemede kullanılan anahtar dizisini kolaylıkla elde edebilir [10]. RC4 algoritması, yapılan analizler sonucundan oldukça hızlı bir şifreleme işlemi gerçekleştirmektedir [11]. Şifrelemede kullanılacak anahtar daha güvenli hale getirilerek oldukça güvenlikli şifreleme işlemleri elde edilebilmektedir.

Kriptolojik gelişmelerin yakından takip edilmesi ve uygulamaların güncel kalması, şirketler, devlet kurumları ve özellikle askeri kurumlarda birimler arasındaki iletişimin güvenliğini sağlamak amacıyla oldukça önemlidir. Bu amaçlar doğrultusunda oluşabilecek güvenlik açıklarını ortadan kaldırmak ve bunu yaparken de iletişimi hızlı bir şekilde gerçekleştirebilmek amacıyla birçok kriptografik yöntem geliştirilmektedir. Geliştirilen bu yöntemlerde ileri düzey güvenlik sağlayanlar düşük hızlı olma, hızlı olanlar ise düşük güvenlik düzeyinde olma problemini oluşturmaktadır. Kriptolojik uygulamalarda bu iki temel bileşenin optimum olması uygulamaların temel hedef noktasıdır.

Farklı iletişim kanalları üzerinde gerçekleştirilen iletişimde, mesajın multimedya veri türünde olması, güvenliği sağlama konusunda birçok problem oluşturmaktadır. Bu durum, multimedya iletiminde güvenlik sağlayan uygulama geliştiricileri farklı güvenlik tedbirleri almak zorunda bırakmıştır. Günümüz sayısal sistemlerde bulunan ve bilgisayar ağları üzerinden iletilen multimedyaların gizlilik ve güvenliği, şifreleme yani kriptografik yöntemlerle sağlanmaktadır. Kriptografik uygulamalar ile multimedya veri, yetkisiz kişiler tarafından anlaşılamayacak forma dönüştürülür. Multimedya verileri büyük boyutlu verilerdir. Güvenli haberleşme, kanal kapasiteleri sınırlı boyutta olması sebebiyle bu büyük boyuttaki verilerin güvenli kanallar üzerinden iletilmesi zor ve maliyeti yüksektir. Bu sebeplerden dolayı multimedya verileri güvensiz haberleşme kanalı üzerinden iletilmek durumundadır. Güvensiz kanal üzerinde saldırganların veriye erişip izleme ve değiştirme ihtimalinin olması verilerin şifreli olarak iletilmesi zorunluluğunu ortaya çıkarmaktadır.

Günümüzde kullanılan birçok multimedya veri türü bulunmaktadır. Bir multimedya türü olan sayısal görüntü, günümüzde görsel haberleşmenin yaygınlaşmasıyla önemli bir

konuma gelmiştir. Görüntü verisi diğer veri türleri ile karşılaştırıldığında geleneksel simetrik ve asimetrik şifreleme teknikleri kullanılarak gerçekleştirilen şifreleme işlemleri, çok daha büyük boyutta olması sebebiyle bir takım sorunları ortaya çıkarmaktadır. Bu durum standart şifreleme yöntemleri ile görüntü şifreleme işleminin gerçekleştirilmesinde düşük verimliliğe sebep olmaktadır [12].

Görüntü şifreleme, yüksek veri kapasitesi ve ardışık piksel değerleri arasındaki yakınlık dolayısıyla sıradan metin şifreleme işlemlerinden farklı yapıdadır. Görüntüyü bu özelliklerinden dolayı sıradan şifreleme algoritmalarıyla şifrelemek güvenlik ve hız açısından pek uygun olmamaktadır.

Bu tezde de sayısal görüntüler yani, görüntü üzerinde arttırılmış güvenlikli maske tabanlı simetrik bir şifreleme üzerine çalışma yapılmıştır. Haberleşmede görsel unsurların artmasıyla görüntü şifreleme konuları da önemini daha çok artırmıştır. Önerilen çalışma ile kriptografik sistemlerin temel problemi olan güvenlik ve hız problemine çözüm bulmak amaçlanmıştır. Uygulamada, bir görüntüyü şifrelemek için resim ile boyutları birebir örtüşen bir maske resim kullanılarak şifreleme işlemi gerçekleştirilmiştir. Kullanılan maske görüntüyü üretmek için, kaotik sisteme dayalı sahte rastgele sayı üreteci algoritması temel alınmış ve bu algoritma üzerinde çeşitli seçme ve sıralama yani kombinasyon ve permütasyon işlemleri yapılarak daha güvenlikli bir algoritma tasarlama işlemleri gerçekleştirilmiştir.

2. KRİPTOLOJİ VEGÖRÜNTÜ ŞİFRELEME

Bu bölümde ilk olarak şifreleme bilimi olan kriptolojinin temelleri anlatılmış daha sonra kriptolojinin gelişim evreleri ile temel kriptolojik algoritmaları anlatılmıştır. Bölümün ilerleyen kısmında görüntü şifreleme uygulamalarının temelleri alınmış ve görüntü şifreleme algoritmaları için kullanılan güvenlik analizleri aktarılmıştır. Son olarak da kaotik haritaların temelini oluşturan rastgele sayı üreteçleri hakkında temel bilgilere yer verilmiştir.

2.1. Kriptolojinin Temelleri

Yunanca kökenli olan Kriptoloji kelimesi "kryptós" gizli ve "-logia" çalışmak kelimelerinin birleşmesinden oluşmuş iletişimde gizlilik bilimi olarak değerlendirilir. Kriptoloji, güvenli iletişim için matematiksel yöntem ve tekniklerin çeşitli uygulamalarıdır. Gizlilik ve güvenlik kriptolojinin temel hedef noktalarıdır. Kriptolojide iletişimi gerçekleştirenler arasında iletilen bilgilerin üçüncü tarafların erişememesi ve her iki tarafın da başka bir kaynaktan değil, birbirlerinden gelen bilgilere güvenebilmesinin sağlanması amaçlanmaktadır. Bu amaçların gerçekleştirilmesi amacıyla geçmişten günümüze matematik ve bilgisayar bilimi olanaklarından yararlanılarak pek çok farklı yöntem önerilmiş ve test edilmiştir. Şifreleme yöntemleri, iletilecek verinin yapısına ve iletim ağının yapısına bağlı olarak değişebilir. Veri yapısı ve iletim ortamında olan çeşitlilik dolayısıyla onlarca yeni yöntem önerilmiş ve kullanılmıştır [13].

Temeli zor matematiksel problemlere dayalı tekniklerden oluşan kriptolojinin, kriptografi ve kripto analiz olmak üzere 2 farklı ana dalı vardır.

2.1.1.Kriptografi

Kriptografi, bir verinin iletimi sürecinde karşılaşılabilecek aktif ya da pasif ataklardan veriyi ve veri ile beraber bilginin göndericisini ve alıcısını korumayı amaçlamaktadır. Kriptografi, güvenli veri iletimi temel güvenlik hedefleri doğrultusunda gerçekleştirilmektedir [14]. Bu güvenlik hedefleri; gizlilik, bütünlük, süreklilik, kimlik denetimi(doğrulama), inkâr edilemezlik ve izlenebilirliktir.

Gizlilik

Bilgiye erişim yetkisine sahip olanların erişimini sağlamaktır. İletilen bilginin, bilgiye erişme yetkisi olmayan herkesten saklanmasıdır. Diğer bir ifadeyle, bilginin gizli kalması, üçüncü şahıslar tarafından erişilememesidir. Gizlilik, güvenli bilgi iletiminin temel ölçütlerindendir. Gizli iletimin sağlanabilmesi için birçok veri gizleme ve şifreleme metotları geliştirilmiştir.

Bütünlük

Bilginin güvenli bir şekilde iletilmesi ve bilginin güvenli şekilde korunması süreçlerinde bilgi üzerinde hiçbir değişiklik yapılmamasıdır. Bilgide küçük bir değişiklik bazen çok büyük sorunlar ortaya çıkarabilmektedir.

Süreklilik

Bilginin zamanında ve güvenilir şekilde kullanımının sağlanmasıdır. Üçüncü taraflar haberleşen iki taraf arasındaki hattı veya haberleşme araçlarını kullanılmaz hale getirerek haberleşmenin sürekliliğini engellemeye çalışır.

Kimlik denetimi (Doğrulama)

Kullanıcıların iddia ettikleri kullanıcılar olduğunun ve bir sisteme erişen verinin güvenilir kaynaktan geldiğinin kontrolüdür. Saldırgan olarak da adlandırılan üçüncü taraflar alıcıya göndericinin kimliğini taklit ederek bir mesaj gönderdiğinde, eğer alıcı güvenilir bir kimlik doğrulaması yapmıyorsa yanlış mesajlarla kandırılabilir.

İnkar edilemezlik

Güvenli haberleşme esnasında mesaj gönderildiğinde alıcı taraf gönderen tarafın mesajı gönderdiğini, gönderen tarafta alıcı tarafın mesajı aldığını kanıtlayabilmesidir.

İzlenebilirlik

Bir güvenlik ihlali yapıldığında sorumlusunu ortaya çıkarmak için kullanıcı işlemlerinin

takibinin yapılmasının sağlanmasıdır [15].

2.1.2. Kriptoanaliz

Kripto analiz şifreli metinlerin saldırgan kişiler tarafından açık mesaj elde etme yöntemleri olarak tanımlanabilir. Kripto analiz klasik kripto analiz, uygulama atakları ve sosyal mühendislik olarak 3 gruba ayrılmaktadır.

Klasik kripto analiz

Matematiksel analiz yöntemleri kullanarak veya mevcut anahtarın olası bütün durumlarının denendiği literatürde Brute-Force olarak da anılan kaba kuvvet saldırıları ile gerçekleştirilir.

Uygulama atakları

Saldırganların akıllı kartlar gibi fiziksel erişime sahip olduğu kripto sistemler üzerinde gerçekleşir. İnternet tabanlı uzak erişim saldırıların çoğunda uygulama atakları genellikle bir sorun oluşturmamaktadır [16].

Sosyal mühendislik

Saldırganların hedeflerinde mesaj değil mesaj iletimini gerçekleştiren kişiler vardır. Mesajı iletecek kişiyi aldatarak, istediği bilgileri ele geçirmesini sağlayan bir saldırı tekniğidir. Sosyal mühendislik teknik olmayan bir terimdir.

2.2. Kriptolojinin Gelişimi

İnsanlık tarihi boyunca insanlar arası iletişim ihtiyacı hep var olmuştur. Geçmişten günümüze artarak devam eden bu ihtiyaç, sistemlerin de entegre olması ile güvenlik kavramı, bu süreçte kilit taşı konumunu hep korumaktadır. Güvenli veri iletimi, haberleşmenin başlıca amaçlarındandır. Güvenli haberleşmenin yolu, verinin şifrelenmesi ile gerçekleşmektedir. Bu sayede üçüncü taraf saldırganların açık olan haberleşme kanalına izinsiz erişmesi ile oluşabilecek olumsuz durumlar ortadan kaldırılmaktadır.

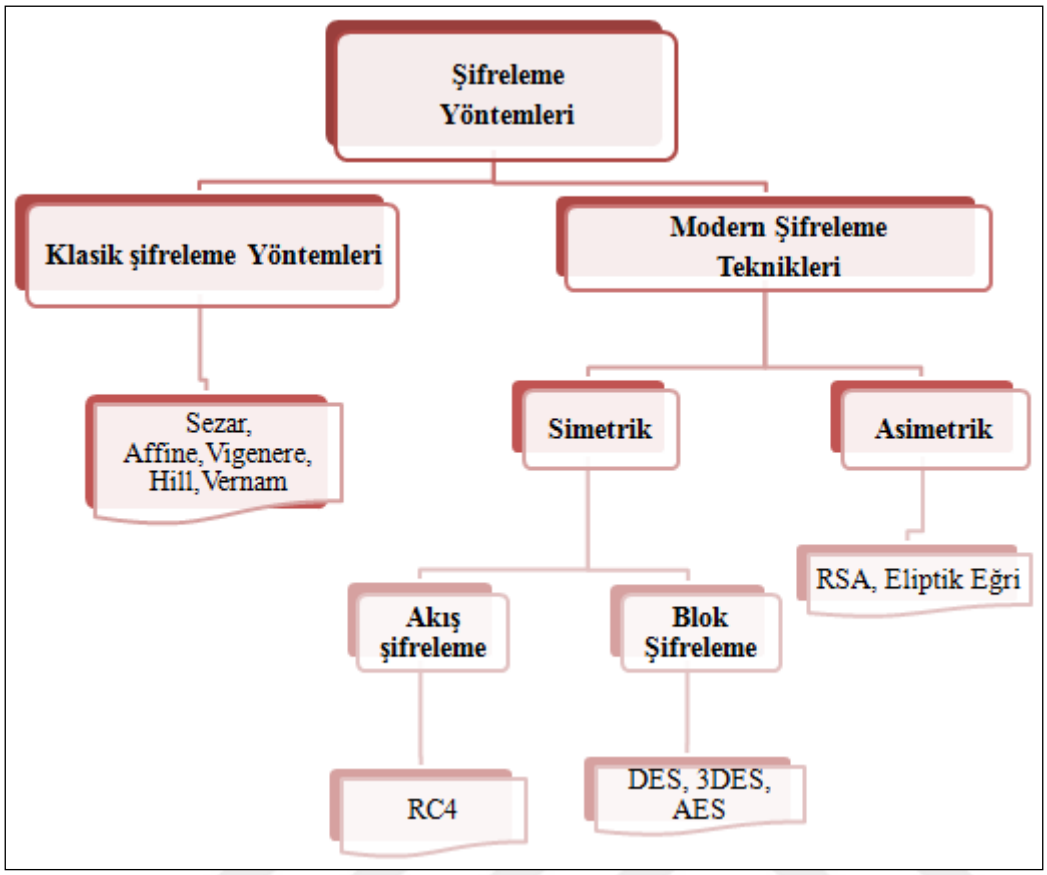
Verilerin şifrelenmesinin temeli, bilgilerin belirli kişilerden gizlenmesi amacına dayanmaktadır. Bilginin gizlenmesi, bir mesajın saldırganlarca elde edilse dahi kolay anlaşılamayacak bir şekle dönüştürülmesidir [17].

Açık ağlar üzerinden bir mesajın, üçüncü şahıslar tarafından izlenme, dinlenme ve üzerinde değişiklik yapılma tehdidi mevcuttur. Burada ifade edilen mesaj literatürde, plain text olarak da kullanılan açık mesajdır. Açık mesajın içeriğini gizlemek için yapılan işlemlere şifreleme denir. Şifreleme, açık mesajı anahtar kullanarak şifreli mesaja dönüştürmektedir. Başka bir ifadeyle, bilginin içeriğini başkaları tarafından anlaşılmayacak hale getirme işlemidir. Bir bilgiyi başka bir kişiye iletmek için veya bulunduğu yerde saklamak için şifreleme işlemi uygulanabilmektedir. Şifreleme süreci sonrasında cipher text olarak da kavramlaşmış olan şifreli mesaj elde edilir. Şifreli mesajdan yeniden açık mesaj elde etme işlemi şifre çözme işlemidir [18]. Şekil 2.1'de bu süreç gösterilmiştir.



Şekil 2.1. Şifreleme ve şifre çözme süreci

Şifreleme algoritmaları temelde anahtar kullanımına bağlı olarak gruplandırılmaktadır. Şekil 2.2' de temel şifreleme algoritmaları gruplaması görülmektedir.



Şekil 2.2. Temel şifreleme algoritmaları

2.2.1. Klasik şifreleme yöntemleri

Klasik şifreleme metotları basit işlemler kullanılarak oluşturulan algoritmaları içermektedir. Klasik yöntemlerde kullanılan metotlardaki algoritmalar gizlidir. Gizli tutulan bu algoritmalar düşük güvenlik seviyesi problemi oluşturabilmektedir. Bu yöntemde güvenlik düzeyini artırıcı ekstra önlemler kullanılmaktadır [19].

Sezar şifreleme

Yer değiştirme temeline dayanan bir yöntemdir. Mesajda bulunan her bir karakter belirlenen anahtar yardımı ile farklı bir karaktere dönüştürülerek şifrelenir. Şifre çözme işleminde de aynı anahtar kullanılarak aynı işlemler yapılır.

Eş. 2.1'de şifrelemek için kullanılan fonksiyon görülmektedir.

$$e_k(m) = \mathrm{m} + \mathrm{k} \left(\mathrm{mod}\, N\right) \tag{2.1}$$

Burada e_k *(m)* şifreli mesajı, *m* şifrelenecek mesajı, *k* anahtarı, *N* ise alfabe boyutunu temsil etmektedir.

Şifre çözmek için ise Eş.2.2 kullanılmaktadır.

$$d_k(m) = e_k - k(mod\ N) \tag{2.2}$$

Burada $d_k(m)$ şifresi çözülmüş mesajı, e_k şifreli mesajı, *k* anahtarı, *N* ise alfabe boyutunu temsil etmektedir.

Affine şifreleme

Sezar şifreleme yöntemine oldukça benzerdir. Affine şifreleme yönteminde $a.x+b$ şeklinde ifade edilen doğrusal bir fonksiyon ile şifreleme gerçekleştirilir. Şifre Çözme işlemi ise ters fonksiyon kullanılarak gerçekleştirilir. Eş. 2.3'te şifrelemek için kullanılan fonksiyon görülmektedir.

$$e_k(x) = a.x + b(\mathrm{mod}\ N) \tag{2.3}$$

Burada $e_k(x)$ şifreli mesajı, *x* şifrelenecek mesajı, *a* ve *b* anahtarları, *N* ise alfabe boyutunu temsil etmektedir.

Ayrıca burada $\mathrm{ebob}(a, \mathrm{N}) = 1$ olmalıdır.

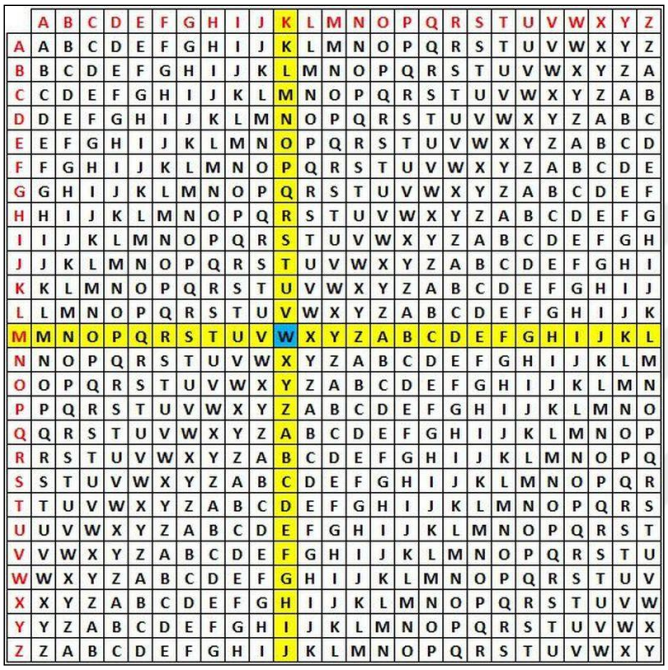
Şifre çözmek için ise Eş.2.4 kullanılmaktadır.

$$d_k(y) = a^{-1}.y^{-b}(\mathrm{mod}\ N) \tag{2.4}$$

Burada $d_k(y)$ şifresi çözülmüş mesajı, *y* şifreli mesajı, *a* ve *b* anahtarları, *N* ise alfabe boyutunu temsil etmektedir.

Vigenere şifreleme

Düz metinde bulunan harfler anahtar olarak seçilmiş bir kelime kullanılarak Vigenere tablosu yardımıyla şifrelenmektedir. Bu işlem sonrasında düz metindeki sözcükler için farklı şifre metinler oluşturulur. Şifre çözme işlemi de yine anahtar sözcük ve tablo kullanılarak yapılır. Şekil 2.3'te Vigenere tablosu görülmektedir.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Şekil 2.3. Vigenere Tablosu

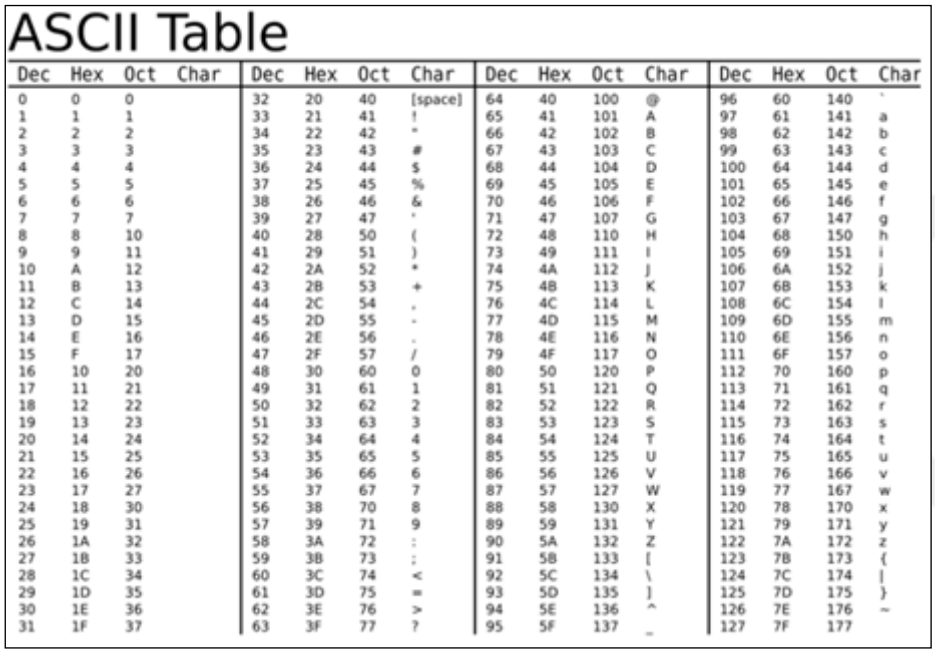
Hill şifreleme

Leste S. Hill tarafından tasarlanan çok alfabeli şifreleme yöntemidir. Hill şifresi, lineer cebir temeline dayandığı için kripto analiz süreci teoriktir. Saldırgan tarafından açık metin ve o açık metine ait şifrelenmiş metin ele geçirilirse, cebirsel işlemler yardımıyla anahtar hesaplanabilir [20].

Vernam şifreleme

1917'de Gilbert Vernam tarafından geliştirilen bu yöntem Vigenere yöntemine benzemektedir. Mesaj 0 ve 1'lerden oluşan ikili sayı sistemine dönüştürülür ve XOR işlemine tabi tutulur. Veri, rastgele belirlenmiş anahtarlar vasıtasıyla şifrelenir. Şifreleme işleminde ikili sistemde yazılmış ASCII (Bilgi Değişimi İçin Amerikan Standart Kodlama

Sistemi) adı verilen Tablo kullanılır. Şekil 2.4'te ASCII tablosu görülmektedir Kullanılan her bir karakter için ASCII kodu birbirinden farklıdır. Seçilen anahtar dizisinin ASCII karşılığı ve açık mesaj ASCII karşılığı XOR işlemi uygulanarak şifrelenir. XOR işleminin sonunda bitlerin 0 veya 1 çıkma olasılığı eşittir. Her iki bit aynı ise sonuç olarak 0 bit, her iki bit ayrı ise sonuç olarak 1 bit üretilir. Bu durum istatistiksel olarak iyi sonuçlar vermesine olanak sağlamaktadır [19].



ASCII Table

Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char
0	0	0		32	20	40	[space]	64	40	100	@	96	60	140	`
1	1	1		33	21	41	!	65	41	101	A	97	61	141	a
2	2	2		34	22	42	"	66	42	102	B	98	62	142	b
3	3	3		35	23	43	#	67	43	103	C	99	63	143	c
4	4	4		36	24	44	$	68	44	104	D	100	64	144	d
5	5	5		37	25	45	%	69	45	105	E	101	65	145	e
6	6	6		38	26	46	&	70	46	106	F	102	66	146	f
7	7	7		39	27	47	'	71	47	107	G	103	67	147	g
8	8	10		40	28	50	(	72	48	110	H	104	68	150	h
9	9	11		41	29	51	)	73	49	111	I	105	69	151	i
10	A	12		42	2A	52	*	74	4A	112	J	106	6A	152	j
11	B	13		43	2B	53	+	75	4B	113	K	107	6B	153	k
12	C	14		44	2C	54	,	76	4C	114	L	108	6C	154	l
13	D	15		45	2D	55	-	77	4D	115	M	109	6D	155	m
14	E	16		46	2E	56	.	78	4E	116	N	110	6E	156	n
15	F	17		47	2F	57	/	79	4F	117	O	111	6F	157	o
16	10	20		48	30	60	0	80	50	120	P	112	70	160	p
17	11	21		49	31	61	1	81	51	121	Q	113	71	161	q
18	12	22		50	32	62	2	82	52	122	R	114	72	162	r
19	13	23		51	33	63	3	83	53	123	S	115	73	163	s
20	14	24		52	34	64	4	84	54	124	T	116	74	164	t
21	15	25		53	35	65	5	85	55	125	U	117	75	165	u
22	16	26		54	36	66	6	86	56	126	V	118	76	166	v
23	17	27		55	37	67	7	87	57	127	W	119	77	167	w
24	18	30		56	38	70	8	88	58	130	X	120	78	170	x
25	19	31		57	39	71	9	89	59	131	Y	121	79	171	y
26	1A	32		58	3A	72	:	90	5A	132	Z	122	7A	172	z
27	1B	33		59	3B	73	;	91	5B	133	[	123	7B	173	{
28	1C	34		60	3C	74	<	92	5C	134	\	124	7C	174	|
29	1D	35		61	3D	75	=	93	5D	135	]	125	7D	175	}
30	1E	36		62	3E	76	>	94	5E	136	^	126	7E	176	~
31	1F	37		63	3F	77	?	95	5F	137	_	127	7F	177	

Şekil 2.4. ASCII Tablosu

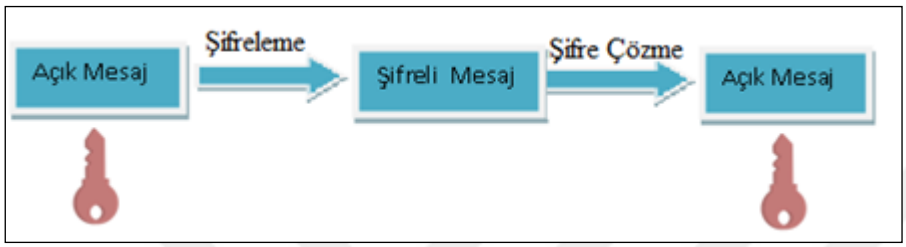
2.2.2. Modern şifreleme yöntemleri

Modern şifreleme yöntemleri klasik yöntem algoritmalarına göre daha kısa fakat daha karmaşık yapıdadırlar. Modern şifreleme algoritmalarında şifreleme ve şifre çözme algoritmalarında güvenlik, anahtar üzerinden sağlanır. Mesajın çözülme işlemi sadece uygun anahtar ile gerçekleşir.

Modern şifreleme yöntemleri anahtar kullanımına bağlı olarak ikiye ayrılır. Bunlar tek bir anahtarın kullanıldığı simetrik metotlar ve açık, gizli ikili anahtar çiftinin kullanıldığı asimetrik metotlardır [21].

Simetrik metotlar

Literatürde gizli anahtarlı şifreleme olarak da adlandırılan simetrik şifreleme metotlarında tek bir anahtar kullanılır. Şifreleme ve şifre çözme işlemi aynı anahtar ile gerçekleştirilir. Açık mesaj, anahtar kullanılarak şifreli mesaja dönüştürülür. Şifreli olarak iletilen mesaj tekrar aynı anahtar kullanılarak açık mesaja dönüştürülür [22]. Simetrik şifreleme metodu Şekil 2.5'te görülmektedir.



Şekil 2.5. Simetrik şifreleme metodu

Simetrik şifreleme algoritmaları kullanılan teknikler bakımından akış şifreleme ve blok şifreleme olmak üzere ikiye ayrılır.

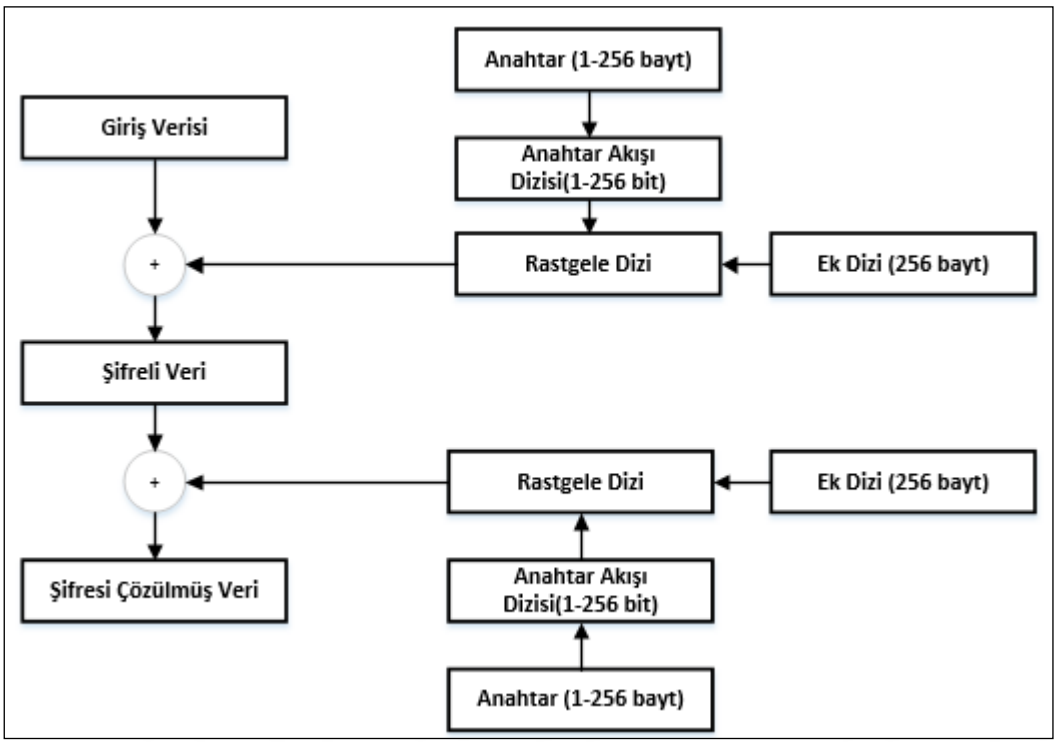
Akış şifreleme

Akış şifreleme algoritmaları, şifreleme işlemi rastsal olarak elde edilen bir dizi ile gerçekleştirilir. Yazılım verimliliği üst seviyede, donanım karmaşıklık seviyesi daha düşüktür. Bu sayede blok şifreleme yöntemlerine göre daha hızlı bir şifreleme gerçekleştirilir. Akış şifreleme işleminde başlangıç değeri ve seri devam eden işlemler ile anahtar dizisi elde edilir. Elde edilen dizi ile düz metinin her biti XOR işleminden geçirilerek şifreleme gerçekleştirilir. Şifre çözme işleminde de yine anahtar dizisi XOR işleminden geçirilerek açık metin elde edilir [23].

RC4

RC4, 1987 yılında Ronald Rivest tarafından tasarlanan yaygın akış şifreleme algoritmasıdır. Algoritma simetrik anahtarlama mantığı ile çalışan hızlı bir algoritma örneğidir. Algoritmada, anahtar uzunluğu genellikle 5-16 bayt arasıdır. RC4 algoritması, akış şifreleme işleminin temel mantığı olan anahtar dizisi ile açık mesajı XOR işlemine tabi tutarak şifreleme işlemini gerçekleştirmektedir. Hızlı ve kolay uygulanabilir olmasına

karşın birkaç güvenlik zafiyeti algoritmanın dezavantajdır. Algoritma temellerine ilave güvenlik tedbirleri ile güvenli hızlı ve kullanılabilir algoritmalar oluşturulabilir [24,25]. Şekil 2.6 'da algoritmanın blok diyagramı görülmektedir [25].



Şekil 2.6. RC4 algoritması blok diyagramı

Blok şifreleme

Blok şifreleme yöntemi, şifrelenmek istenen mesajı belirli uzunluklarda bloklar halinde şifrelemenin gerçekleştirildiği yöntemdir. Bloklar algoritma çeşitlerine bağlı olarak bir önceki bloğa bağlı ve bağlı olmayan bir şekilde şifrelenebilir. Belirli uzunluktaki blokların şifreleme işlemi sonrasında blok boyutlarında bir değişiklik meydana gelmez, aynı boyutta şifrelenmiş bloklar elde edilir. Blok şifreleme uygulamaları genellikle bütünlük ihtiyacı olan durumlarda kullanılmaktadır [26].

Blok şifreleme yönteminin temeli Shannon tarafından önerilen karıştırma ve yayılma tekniklerine dayanmaktadır. Karıştırma işleminde amaç, metnin şifreleme sonrası hali ile olan ilişkisini gizlemekken, yayılma işleminin amacı, mesajda bulunan izlerin anlaşılmamasını sağlamaktır [27].

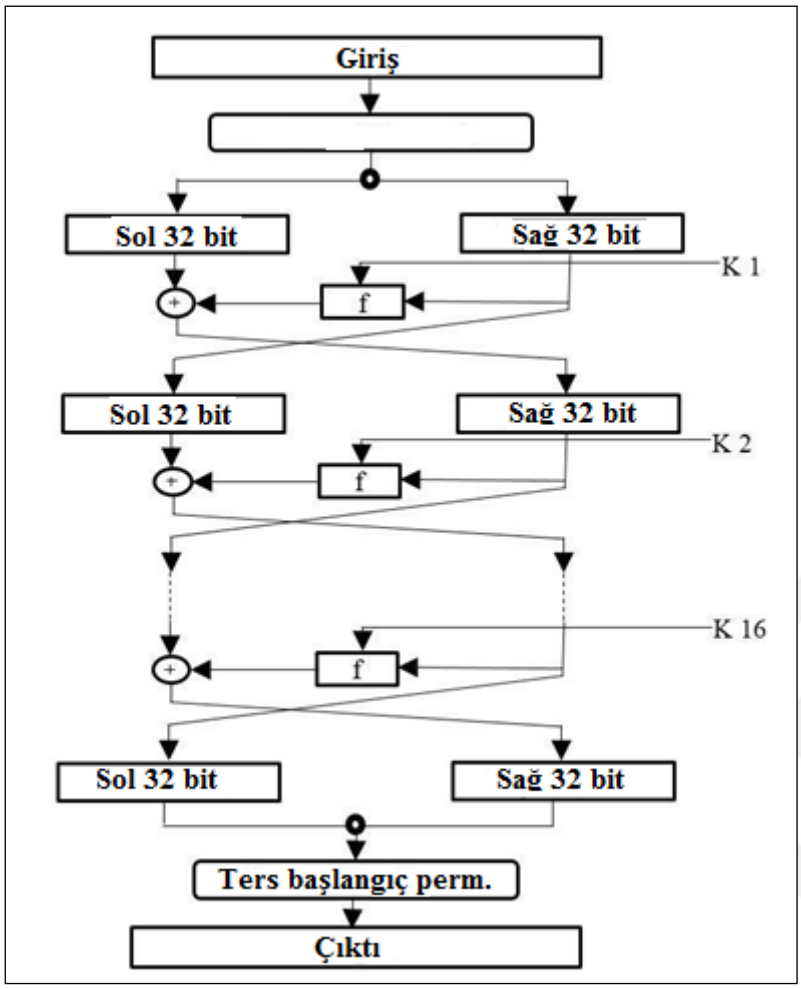
DES ve 3DES

DES algoritma 1974 yılında IBM(Uluslararası İş Makineleri) ve NSA (Ulusal Güvenlik ajansı) ortak çalışması sonucu ortaya çıkmıştır. Geçmişten günümüze hızla gelişen teknolojiler neticesinde algoritmanın temel hali günümüzde anahtar uzayı bakımından yetersiz kalması sebebiyle kullanılmamakta, değiştirilmiş halleri tercih edilmektedir [28].

DES algoritmasında mesaj, tek bir anahtar yardımıyla şifrelenir ve şifre çözülür. Dolayısıyla simetrik bir algoritmadır. Mesaj belirli uzunluktaki bloklar halinde şifrelendiği için blok şifreleme mantığında çalışmaktadır. Anahtar uzunluğu ile algoritmanın güvenliği doğru orantılıdır. Yani, anahtar uzunluğu arttıkça algoritma daha güvenli hale gelmektedir. DES algoritmasında 56 bit uzunluğunda anahtar kullanılmaktadır. Bu anahtar uzunluğunun günümüz teknolojileri ile kaba kuvvet saldırı karşısında dayanabildiği süre kısadır. Algoritmada şifrelenecek blokların uzunluğu 64 bittir ve her bir blok ayrı ayrı şifrelenir. Şifre çözme işleminde de yine aynı anahtar kullanılarak her bir blok üzerinde aynı işlemler yapılmaktadır. DES algoritmanın çalışma adımlarının sırası aşağıdaki gibidir:

1. Başlangıç permütasyonu yani IP (Başlangıç permütasyonu) çalıştırılır,
2. 64 Bit uzunluğundaki bloklar ikiye bölünür ve sağ R, sol L olarak adlandırılır,
3. Bloklar f fonksiyonuna sokulur ve 16 kez döngü sağlanır,
4. Döngüler sonrasında R ve L blokları yer değiştirilir,
5. Son adım olarak 64 bit veriye, ilk adımda oluşturulan IP vektörünün ters işlemi uygulanır.

Şekil 2.7'de algoritmanın bu adımları görülmektedir.



Şekil 2.7. DES algoritması blok diyagramı

DES algoritmasında, bloklarda farklı anahtar kullanılması bir avantaj olmasına rağmen, başlangıç anahtarı boyutunun kısa olması dezavantajdır. Bu dezavantajlardan kurtulmak adına günümüzde yeni ve daha güvenlikli Triple DES olarak bilinen 3DES algoritması kullanımı tercih edilmektedir. 3DES algoritmasında DES'in aksine 24 bayt anahtar kullanımı vardır. Baytın eşlik biti olması sebebiyle anahtar boyutu 168 bittir. DES algoritması işlemleri 3 kez tekrar edilerek 3DES algoritması oluşturulur. Bu tekrarlama işlemi ise bu algoritmanın zayıf yönü olan hız problemini ortaya çıkarmaktadır. Sonuç olarak hız ve güvenlik arasından çapraz bir ilişki ortaya çıkmaktadır. Yani güvenlik arttıkça hız azalmakta, hız arttıkça güvenlik azalmaktadır. Bu iki bileşenin optimum değerini bulmak ise kriptolojinin temel hedef noktasını oluşturmaktadır [26].

AES

AES, Kasım 2001 tarihinde NIST (Ulusal Standartlar ve Teknoloji Enstitüsü) tarafından, gelişmiş şifreleme standardı olarak kabul edilmiştir ve günümüzde de kullanılan kamuya açık ilk şifreleme algoritmasıdır. AES algoritması DES gibi simetrik bir blok şifreleme algoritmasıdır. Algoritmada blok uzunluğu 128 bit iken, anahtar 128, 192 ve 256 bitlik seçeneklere sahiptir. Kullanılan anahtar uzunluğuna bağlı olarak döngü sayısı değişmektedir [27]. Çizelge2.1'de bu değerler görülmektedir.

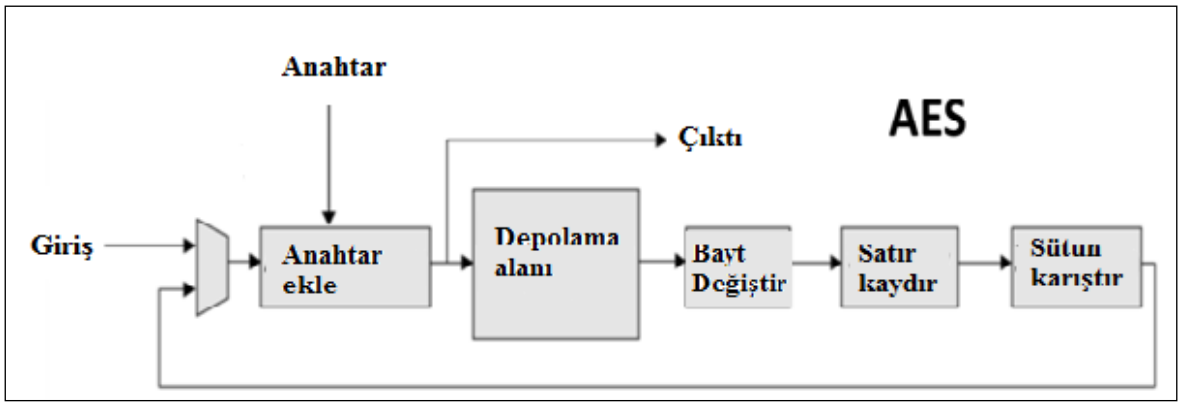
Çizelge 2.1. AES algoritması anahtar uzunluğu döngü sayısı tablosu

Anahtar uzunluğu (bit)	Döngü sayısı
128	10
192	12
256	14

AES algoritmasında döngülerde bayt değiştirme, satır kaydırma ve sütun değiştirme işlemleri yapılır. DES algoritması 3 gruba ayrılır. Çalışma adımları aşağıdaki gibidir:

1- İlk döngü: *Anahtar ekle: Durum ilk döngü anahtarı ile XOR işlemine tabi tutulur.
2-Diğer döngüler: *Bayt değiştir: Durum matrisindeki her bayt tabloya göre güncellenir.
*Sütun kaydır: Her satır belirli bir sayıda kaydırılır.
*Satır karıştır: Her bir sütundaki 4 bayt, birbiriyle karıştırılır.
*Anahtar ekle
3- Son döngü: *Bayt değiştir
*Satır karıştır
*Anahtar ekle

Şekil 2.8 'de algoritmanın adımları görülmektedir.

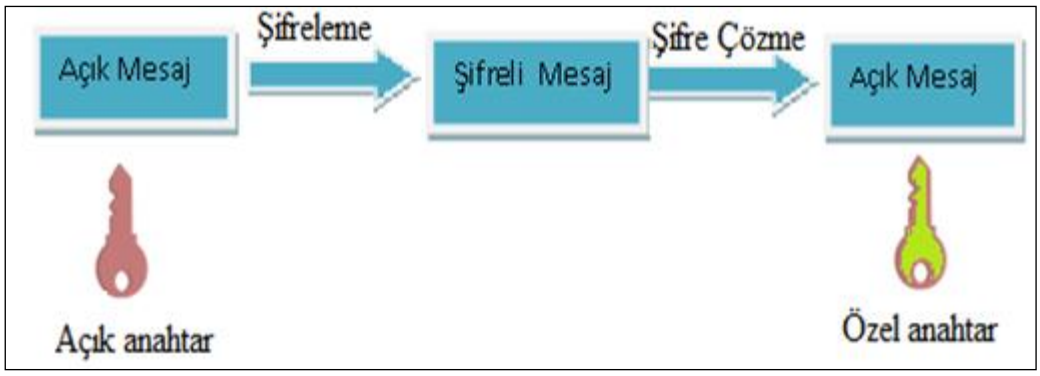


Şekil 2.8. AES algoritması adımları

Asimetrik metotlar

Asimetrik metotlar bir diğer adıyla açık anahtarlı şifreleme, simetrik şifrelemede olduğu gibi şifreleme ve şifre çözmek için tek anahtar kullanılmaz. Açık ve özel olmak üzere iki farklı anahtar kullanımı gerekmektedir. Algoritmaya açık anahtar denilmesinin sebebi şifrelemede kullanılan anahtarlardan birinin herkes tarafından bilinmesidir. Anahtar çiftinin diğeri ise yalnızca şifreleme yapan kullanıcıya ait olan gizli anahtardır. Anahtar şifreleri birbirleriyle tam uyum halinde çalışır. Yani, kullanıcının açık anahtarıyla şifrelenen mesaj yalnızca o açık anahtarın çifti olan özel anahtar ile çözülebilir.

Asimetrik şifreleme metodu Şekil 2.9'da görülmektedir.



Şekil 2.9. Asimetrik şifreleme metodu

RSA

RSA algoritması 1977 yılında MIT (Massachusetts Teknoloji Enstitüsü) çalışanı olan Ron Rivest, Adi Shamir ve Len Adleman tarafından geliştirilen en yaygın asimetrik şifreleme algoritmasıdır. RSA, şifrelemenin yanında imzalama kullanımı için de uygun bir algoritmadır. Algoritmada açık ve özel anahtar alıcı tarafından oluşturulur. Gönderici taraf, göndermek istediği kişinin açık anahtarı ile mesajı şifreler, alıcı taraf kendi özel anahtarını kullanarak şifre çözme işlemini gerçekleştirir.

Algoritma çalışma yapısı aşağıdaki gibidir:

- Anahtar oluşturma algoritması:

1. 0, 1, 2, 3, ... , n - 1 sayıları arasında, asal ve birbirinden farklı yeterince büyük *p* ve *q* sayıları seçilir.
2. $n = p.q$ hesaplanır.
3. $\Phi = (p-1).(q-1)$ değeri hesaplanır.
4. $2 < e < \Phi$ ve $ebob(\Phi, e) = 1$olacak şekilde bir *e* tamsayısı seçilir.
5. $e.d = 1 (mod\ \Phi)$ sağlayacak d değeri hesaplanır.
6. Özel anahtar: *(n,d)* ve açık anahtar: *(n, e)*'dir.

- Şifreleme algoritması:

1. Gönderici, veriyi alacak tarafın açık anahtarı olan *(n, e)*' yi kullanır.
2. Şifrelenecek veri olan *m*, $[0, n-1]$ arasında bir tamsayıya dönüştürülür.
3. Şifrelemek için verinin *mod n' e* göre *e*. kuvveti alınır.

$$c = m^{e} \pmod{n} \tag{2.5}$$

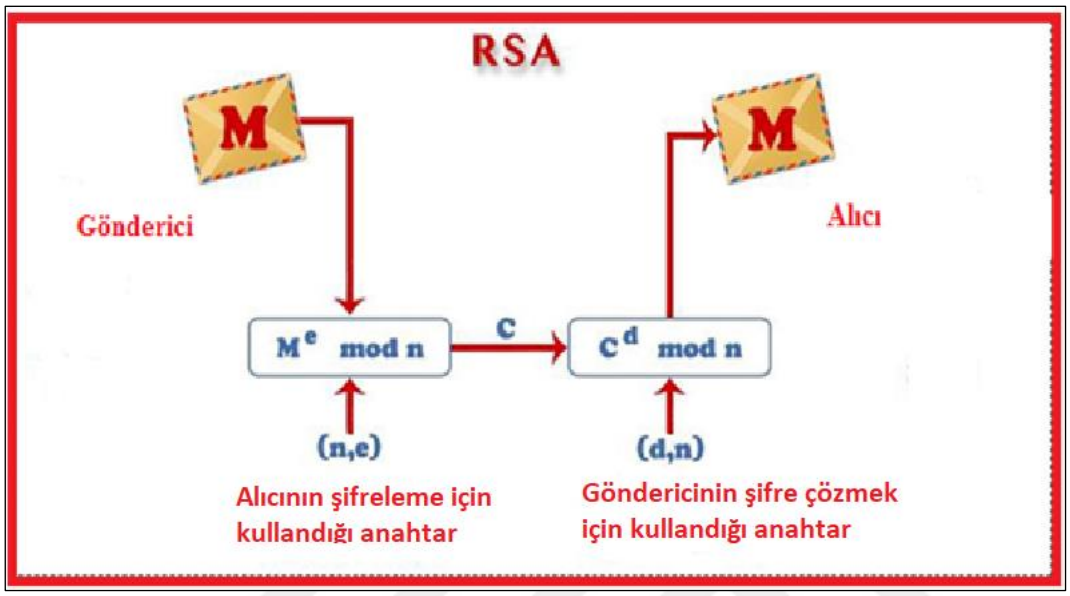
Burada c şifrelenmiş veridir.

- Şifre çözme algoritması:

1. Şifreli mesaj *c*,Eş. 2.6 kullanılarak açık mesaj elde edilir.

$$m = c^{d} \pmod{n} \tag{2.6}$$

Şekil 2.10 'da RSA algoritmasının çalışması görülmektedir.



Şekil 2.10. RSA şifreleme metodu

RSA algoritmasının güvenilirliğini artırmak için çok büyük asal sayılar kullanılmalıdır. Büyük sayılarda işlem yapmak güvenlik açısından iyi sonuçlar vermesine karşın çalışma hızını düşürmektedir. Bu sebeple büyük boyutlu verilerin şifrelenmesinde RSA algoritması çok uygun kabul edilmemektedir [29].

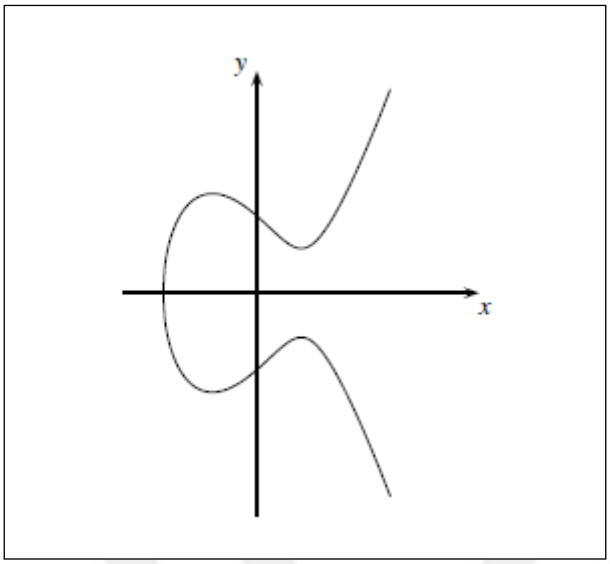
Eliptik eğri

Eliptik eğri algoritması Neal Koblitz ve Victor S. Miller tarafından 1985 yılında önerilmiş, geniş kullanımı 2004 yılında olmuştur. Eliptik eğri ile şifreleme algoritması eliptik eğrilerin cebirsel topolojisine dayanan bir açık anahtar şifreleme temeline dayanmaktadır. Eliptik eğri algoritması RSA algoritmasına göre daha düşük bir anahtar uzunluğuna sahiptir [30]. Eliptik eğri çalışma prensibi ayrık logaritma problemine dayanmaktadır.

Eliptik eğride şifreleme Eş.2.7 ile yapılır.

$$y^{2} = x^{3} + a.x + b \pmod{q} \tag{2.7}$$

Eliptik eğri algoritmasının şekli Şekil 2.11'de görülmektedir.



Şekil 2.11. Eliptik eğri algoritmasının şekli

2.3.Görüntü Şifreleme

Renkli görüntü *M* satır ve *N* sütun sayısı olmak üzere *M*N* adet pikselden oluşan bir matris ile temsil edilebilir. Matris elemanı olan her bir piksel 8 bitlik (yani 0-255 değer alan) kırmızı, yeşil ve mavi bileşenlerinden oluşmaktadır. Renkli görüntülerde oluşan büyük verilerin şifrelenmesi klasik şifreleme yöntemleri ile güvenli bir şekilde sağlanamaz [31]. Renkli görüntülerin klasik metotlarla şifrelenememesinin bir diğer nedeni de birbirine yakın pikseller arasındaki yüksek benzerliktir. Klasik metotlar ile şifreleme işlemi hız açısından da büyük bir dezavantaja sahiptir [32]. Büyük boyutlu bu verilerin güvenli bir şekilde şifrelenmesi için kaos şifreleme metotlarının güvenli sonuçlar vermesi nedeniyle uygulamalarda kullanımı giderek artmaktadır.

Görüntü boyutları metinden oldukça büyüktür ve bir görüntüyü şifrelemek çok daha fazla zaman gerektirir. Görüntü şifreleme algoritmaları geliştirmek için çalışan araştırmacılar, şifreleme sürecini hızlı bir şekilde gerçekleştirmek için geleneksel yöntemler yerine kaosa dayalı hızlı ve güvenli şifreleme yöntemlerine yönelmişlerdir. Son zamanlarda şifreleme alanında kaosun yaygınlaşması ve bu durumun diğer şifreleme sistemlerine göre daha iyi sonuçlar vermesi kaos uygulamalarına olan ilgiyi artırmaktadır [33].

Günümüzde hızla artan teknolojik gelişmelerle birlikte görüntülerin kullanım alanları artmakta ve görüntü günlük hayatımızda geniş bir kullanım alanına sahip olmaktadır. Görüntü kullanımında yaşanan artışla birlikte konunun önemli bir noktası olan güvenlik sorunu ortaya çıkmaktadır. Görüntülerin sık kullanımı ile saklanırken ve iletilirken güvenliğinin sağlanması konunun en önemli noktası haline gelmiştir. Görüntü güvenliğinin sağlanması kişilerden kurumlara kadar çok geniş bir kitle için hayati önem arz etmektedir. Görüntü güvenliği kurumlar için özellikle askeri alanda ve kamu güvenliğinin sağlanması için önemli iken bireyler için ise günümüzde belki de en değerli hazine olarak adlandırabileceğimiz kişisel bilgilerimizin korunması için önemli bir noktadır. İnsansız hava araçlarının çektiği görüntülerin aktarılması veya bir banka binasının planının görüntüsünün saklanması hususları konunun önemini daha iyi anlatmaktadır [34].

2.4. Görüntü Şifreleme Algoritmaları İçin Güvenlik Testleri

Görüntü şifreleme algoritmalarının güvenliği sağlamak ve saldırganlar tarafından uygulanan farklı saldırı tekniklerinin şifreleme algoritmasında zafiyete yol açıp açmadığını anlamak için algoritmalara bazı güvenlik testleri uygulanmaktadır [35].

2.4.1. Anahtar uzayı analizi

Resim şifreleme algoritmasının kaba kuvvet saldırılarına karşı dayanıklı olup olmadığını belirlemek için kullanılan analizdir. Anahtar boyutunun tahmin veya olası bütün sonuçları deneyerek elde edilemeyecek büyüklükte olması gerekmektedir. Literatürde genel olarak bu büyüklük, 2^{100} olarak kabul edilmektedir [36]. Bu boyuttan büyük olan anahtar güvenli olarak nitelendirilebilir.

2.4.2. Histogram analizi

Histogram analizi, görüntünün kırmızı, yeşil ve mavi renk bileşenlerinin piksel değerlerini grafik üzerinde çizerek piksel değerlerinin dağılımını göstermek için kullanılır. Şifrelenmiş görüntünün istatistiksel saldırılara karşı dayanıklı olabilmesi için pikseller düzgün dağılımlı olmalıdır.

2.4.3. Korelasyon (KR)

Bir görüntünün komşu pikselleri benzer değerdedir. Şifreli görüntünün istatistiksel saldırılara karşı dayanıklı olabilmesi için komşu pikseller arasındaki bağlantının minimum olması gerekmektedir. Görüntü pikselleri arasındaki bağlantının göstergesi olan KR Eş. 2.8'deki gibi hesaplanmaktadır [35,36].

$$KR = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{2.8}$$

$$\operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right) \tag{2.9}$$

$$E(x) = \frac{1}{N}\sum_{I=1}^{N} X_i \tag{2.10}$$

$$D(x) = \frac{1}{N}\left(x_i - E(x)\right)^2 \tag{2.11}$$

Burada x ve y iki komşu piksel arasındaki değeri N ise görüntüde seçilen piksel sayısını ifade etmektedir. KR değeri -1 ile +1 arasında değerler alabilmektedir. Değerin artı olması iki görüntü arasında pozitif ilişkinin olduğunu eksi olması ise negatif bir ilişkinin olduğunu göstermektedir. Algoritmanın saldırılara karşı dayanıklı olabilmesi için KR değeri sıfıra olabildiğince yakın olmalıdır.

2.4.4. Bilgi entropisi analizi (BE)

Bilgi entropisi şifrelenmiş görüntüde piksellerin rastgele dağılımın bir ölçüsüdür [35-37]. Bilgi entropisi BE Eş. 2.12'deki formül ile hesaplanmaktadır.

$$BE = \sum_{i=0}^{2^n-1} p(i)\log_2\frac{1}{p(i)} \tag{2.12}$$

Burada $p(i)$ her bir pikselin görüntü içinde olma olasılığını temsil etmektedir. BE değeri 8'e yaklaştıkça piksellerin rastgeleliği artmakta ve algoritma daha güvenli hale gelmektedir.

2.4.5. Sinyal gürültü oranı (PSNR) ve ortalama karesel hata (MSE) analizi

PSNR şifrelenmiş görüntüye saldırıdan sonra şifresi çözülen görüntünün kalitesini ölçmek için kullanılır. PSNR değeri ne kadar küçükse şifreli görüntü orijinal görüntüden o kadar uzak demektir ve iyi bir şifreleme sisteminde PSNR değeri oldukça küçük olmalıdır [12]. PSNR Eş. 2.13'deki MSE Eş. 2.14'deki formül ile hesaplanmaktadır.

Güvenli bir sistemde PSNR değeri 8,3875'den küçük olmalıdır. MSE ile iki görüntü arasındaki ortalama hata hesaplanmaktadır. MSE değeri şifreleme sisteminin kalitesi için kritik bir değerdir ve büyük MSE değeri güçlü bir şifreleme sistemi anlamına gelmektedir. Bilimsel çalışmalar MSE değerinin güvenlik ölçütünü 9555 değeri olarak kabul etmektedir. Bu değerin üzerindeki değerler güvenli olarak kabul edilmektedir [35,38-39].

$$PSNR = 10\,x \log\left(\frac{I_{MAX}}{MSE}\right)(dB) \tag{2.13}$$

$$MSE = \frac{1}{M\,x\,N}\sum_{i=1}^{m}\sum_{i=1}^{n}|\,C(i,j) - P(i,j)\,|^2 \tag{2.14}$$

Burada $C(i,j)$ şifreli görüntünün piksel değerlerini ve $P(i,j)$ orijinal görüntünün piksel değerlerini ve I_{MAX} görüntünün maksimum piksel değerini temsil etmektedir.

2.4.6. Ortalama mutlak hata analizi (MAE)

Ortalama mutlak hata analizi orijinal ve şifreli görüntü arasındaki değişimi gösteren bir analiz yöntemidir. MAE Eş. 2.15'deki formül ile hesaplanmaktadır.

$$MAE = \frac{1}{M\,x\,N}\sum_{i=1}^{m}\sum_{i=1}^{n}|\,C(i,j) - P(i,j)\,| \tag{2.15}$$

Burada $C(i,j)$ şifreli görüntünün piksel değerlerini ve $P(i,j)$ orijinal görüntünün piksel değerlerini temsil etmektedir. Bilimsel çalışmalarda güvenlik ve performans kriteri olarak MAE değerinin 80 ve üzerinde olduğunda şifreleme sisteminin güvenli bir sistem olduğu kabul edilmektedir [38,40].

2.4.7. Şifreleme kalitesi analizi (EQ)

Şifreleme kalitesi, orijinal görüntü ile şifrelenmiş görüntü arasındaki piksel değerlerindeki toplam değişimi ifade etmektedir. EQ Eş. 2.16'daki formül ile hesaplanmaktadır.

$$EQ = \frac{1}{256}\sum_{i=0}^{255}\left(H_L(C) - H_L(P)\right)^2 \tag{2.16}$$

Burada $H_L(C)$ şifreli görüntüde her bir pikselin oluşma sayısı ve $H_L(P)$ orijinal görüntüde her bir pikselin oluşma sayısını temsil etmektedir. Bilimsel çalışmalar EQ değerinin güvenlik ölçütü olarak 210'dan büyük olması gerektiği kabul etmektedir [38,40-41].

2.5. Rastgele Sayı Üreteçleri (RSÜ)

Rastgele sayılar, sonucunu önceden belirli yöntemlerle tahmin edemediğimiz sayılardır. Rastgele sayılar bilgisayar, şans oyunları, istatistik ve kriptografi gibi birçok alanda kullanılır. Rastgele sayılar çözülmesi zor matematiksel işlemlerden ve otomatik düzensizlik kaynaklarından yararlanılarak oluşturulmaktadır [42]. Rastgele sayıların aşağıdaki bazı temel özelliklere sahip olması gerekir.

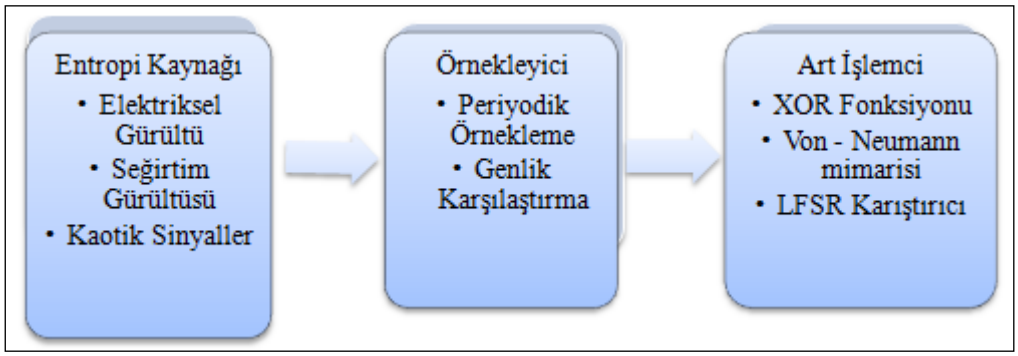
- Yüksek Rastgelelik (Entropi): Tahmin edilemezlik
- Düzgün dağılım: Her sayının olma olasılığının eşit olması
- Bağımsızlık: Ardışık üretilen sayılar arasında ilinti olmaması
- Uzun periyot: Sayıların tekrar etmemesi
- Kolay ve hızlı üretilebilirlik.

Rastgele sayı üreten aygıt ve algoritmalar rastgele sayı üreteci(RSÜ) olarak adlandırılmaktadır. RSÜ'ler gerçek rastgele sayı üreteci (GRSÜ)ve sözde rastgele sayı üreteci(SRSÜ) olmak üzere 2 gruba ayrılmaktadır.

2.5.1. Gerçek rastgele sayı üreteçleri (GRSÜ)

GRSÜ Donanımsal yani fiziksel olaylara dayanan belirleyici olmayan algoritmalardır. Kuantum, osilatör seğirtim gürültüsü, kaotik sistemlerin üretmiş olduğu sinyaller ve

elektriksel gürültü GRSÜ' ye örnek olarak verilebilir. GRSÜ mimari olarak üç bölümden oluşmaktadır. Şekil 2.12'de bu mimari görülmektedir.



Şekil 2.12. GRSÜ mimarisi

Entropi kaynakları

Elektriksel gürültü: * Yarı iletkendeki elektriksel gürültü entropi kaynağıdır.
* Genelde bant genişlikleri sınırlıdır.
* Çevresel parametrelerden kolayca etkilenirler.

Seğirtim gürültüsü: * Osilatör seğirtimi entropi kaynağıdır.
* Yüksek hızda sayı üretirler.
* Yüksek güç tüketirler.
* Elektromanyetik sinyal aşılama saldırılarından etkilenebilirler.

Kaotik sinyaller: * Kaotik sistemler bilgi kaynağı gibi davranabilirler.
* Yüksek hız veya düşük güç tüketecek şekilde tasarlanabilirler.
* Senkronizasyon saldırılarından etkilenebilirler.

Örnekleyici

Entropi kaynaklarının çeşitli yöntemler kullanılarak örnek oluşturma işlemi gerçekleştirmesidir.

Art İşlemci

RSÜ' lerin ürettiği sayıların ideal şartlarda eş olasılıklı ve düzgün dağılımlı olması gerekmektedir. Bu özellikler, üretim parametre saçılmaları, çevresel etkiler ya da saldırılar nedeniyle ideal durumdan sapma gösterebilir. Bu tür risklere karşı RSÜ'lerin çıkışlarına belirlenimci algoritmik bir art işlem fonksiyonu eklenir. Bu fonksiyonun çıkısını

gözlemleyerek ham RSÜ verisine ulaşılmaması gerekir. XOR fonksiyonu, Von- Neumann algoritması ve LFSR'ler yazılımsal ya da donanımsal olarak gerçeklenerek art işlemci olarak kullanılırlar. Art işlemciler güvenliği arttırıp, istatistiksel özellikleri iyileştirmelerine karşın sayı üretim hızını düşürürler.

2.5.2. Sözde rastgele sayı üreteçleri (SRSÜ)

SRSÜ algoritmik yapılardır. Yazılımsal ve donanımsal olarak deterministik olarak oluşturulabilen uygulamalardır. Algoritmalar tohum olarak adlandırılan bir başlangıç değerine ihtiyaç duyarlar [43]. SRSÜ ilk değerden başlayarak ardışık şekilde üretilen sayı dizileri çok uzun da olsa bir periyoda sahiptir. Üretilen sayılar bağımsız değildirler. Sayılar yüksek hızda kısa süre içinde üretilebilmektedir. Gerekli durumlarda aynı sayı dizisi yeniden oluşturulabilir. İlk değer ve algoritmanın bilinmesi ile sayılar oluşturulduğu için güvenlik riski mevcuttur. Kriptografik uygulamalarda daha güvenlikli SRSÜ olan kriptografik güvenli sözde rastgele sayı üreteci (KGSRSÜ) kullanılmaktadır. KGSRSÜ ilk değere az bağımlı ve çok uzun periyoda sahip algoritmalardır. Kesintisiz şifreleme algoritmaları, çeşitli SRSÜ'in kombinasyonları ve sayaç modda geri beslemeli blok şifreleme algoritmaları KGSRSÜ'ne örnek olarak verilebilir. Kriptolojik uygulamaların güvenliği rastgele sayının güvenliği ve tahmin edilemezliğine dayanmaktadır.

LFSR ile SRSÜ

LFSR, doğrusal geri beslemeli kaydedici olarak bilinen SRSÜ algoritmasıdır. LFSR uzun periyodikliği ve iyi istatistiksel sonuçları nedeniyle temel olarak kullanılan SRSÜ algoritmalarındandır. Kriptolojide anahtar oluşumu ve oturum yönetimi olmak üzere geniş bir kullanım alanına sahiptir. LFSR fonksiyonu ile yeni sayı üretmek için belirli bitlerinin XOR işlemine tabi tutulmasıyla bir bit oluşturur. Oluşturulan bu bitler yeni sayıyı oluşturmaktadır. Algoritmanın güvenilirliğini sayı değerlerinin başlangıç değeri ve bit kaydırma sırası belirlemektedir [44,45].

XOR fonksiyonu ile SRSÜ

XOR fonksiyonu ile rastgele sayı üretme işlemi Amerikalı matematikçi George Marsaglia tarafından geliştirilmiştir. XOR fonksiyonu ile SRSÜ doğrusal geri beslemeli kayan

yazmaçların altından geliştirilen bir fonksiyondur. XOR fonksiyonu ile SRSÜ işleminde yeni üretilecek sayı bir önceki sayıya bit kaydırma ve XOR işlemleri adımlarından oluşmaktadır. Bu işlemler algoritmayı modern sistemlerin gelişmesiyle oldukça hızlı hale getirmektedir. Algoritma, hızlı olmasının yanı sıra yapılan istatistiksel testlerin yetersiz sonuç vermesi nedeniyle kriptografik olarak uygun bir SRSÜ olarak kabul edilmemektedir [45,47].

LCG fonksiyonu ile SRSÜ

LCG, doğrusal eşlenik üreteci olarak bilinen SRSÜ algoritmasıdır. LCG oldukça temel matematik işlemlere dayanır. LCG ile sayı üretmek için Eş. 2.17 kullanılmaktadır.

$$X_1 = A.X_0 + B\left(\mathrm{mod}\, C\right) \tag{2.17}$$

Burada X_1, yeni üretebilecek sayıyı, X_0tohum değerini, A, B ve C başlangıç parametrelerini göstermektedir.

LCG algoritması ile yüksek miktarda sayı üretildiğinde istatistiksel olarak iyi sonuçlar alınmaktadır ancak orta ve düşük miktarda sayı üretimi gerçekleştirildiğinde istatistiksel zayıflıklar bulunmaktadır. LCG algoritmasının basit bir üretim algoritması olması sebebiyle kriptolojik uygulamalar için uygun değildir [48].

Lojistik kaotik tabanlı SRSÜ

Lojistik harita kaotik davranışlar gösterebilen genellikle ikinci dereceden polinom denklemidir. Lojistik harita ilk kez 1976 yılında Robert May tarafından bir makalede ortaya atıldı [49]. Klasik lojistik harita ile sayı üretmek için Eş. 2.18 kullanılmaktadır.

$$X_{n+1} = \mu.X_n.\left(1 - X_n\right) \tag{2.18}$$

Burada X_{n+1} yeni üretilecek sayıyı, X_n [0,1] aralığındaki başlangıç değerini ve μ ise [0,4] aralığında değer alan başlangıç parametre değerini temsil etmektedir.

Klasik lojistik harita ile üretilen sayılar kriptografik uygulamalarda kullanımı istatistiksel olarak gerekli şartları sağlayamadığı için pek uygun değildir. 1990'lı yıllarda ilerleyen teknolojik gelişmeler ile kaos tabanlı kripto sistemler ön plana çıkmaktadır. Kaotik sistemlerin başlangıç değerine karşı aşırı hassasiyeti bulunmaktadır. Bu durum SRSÜ için oldukça iyi bir durumdur. Lojistik harita basit ve doğrusal olmayan sistem yapısı ile kaotik kriptografide yaygın kullanıma sahiptir. Lojistik kaotik sistem karmaşık dinamik davranışı ile veri güvenliği ve güvenli veri iletimi için uygundur. Lojistik kaotik sistemde de sayı üretmek için klasik lojistik haritada kullanılan formül kullanılmaktadır. Fakat μ parametre değeri, sistemin kaos durumuna girebilmesi için, [3,5699, 4] aralığında olmalıdır.

Lojistik kaotik sistem başlangıç değerlerine oldukça duyarlıdır. Başlangıç değeri için seçilen iki nokta ne kadar yakın olursa olsun sistem tarafından üretilen yeni değerler birbirinden tamamen farklı olmaktadır [50].

3. KAOTİK LOJİSTİK TABANLI ŞİFRELEME SİSTEMİ VE GELİŞTİRİLEN UYGULAMA ARAYÜZÜ

Bu bölümde öncelikle kaotik lojistik şifreleme sisteminin temelleri ve gelişim evreleri anlatılmış ardından geliştirilen algoritma ve kullanıcı arayüzü hakkında bilgiler verilmiştir.

3.1. Kaotik Lojistik Şifreleme Sistemi

Kaos terimi dağınık, uyumsuz, biçimden yoksun karışık durumları tanımlamak için kullanılmaktadır. Kaos teorisi 18 yy. Yunan ve Çin bilim insanlarının oluşturduğu kaynaklara dayanmaktadır. Teori başlangıç koşullarındaki değişimlerin sistem çıktısındaki değişimlerini incelemektedir. Kaos teorisi başlangıç koşullarına bağlı dinamik sistem davranışlarını inceleyen çalışmalar gerçekleştirmektedir. Hesaplamaya gerek duyulmadan, karmaşık fakat kendi iç düzenine sahip süreçler kaotik olarak adlandırabilmektedir. Kaotik sistemlerde zamana bağlı çıktının tahmin edilebilmesi oldukça güçtür ancak bu değişimler deterministik olmaları sebebiyle başlangıç koşullarıyla belirlenmektedir [51].

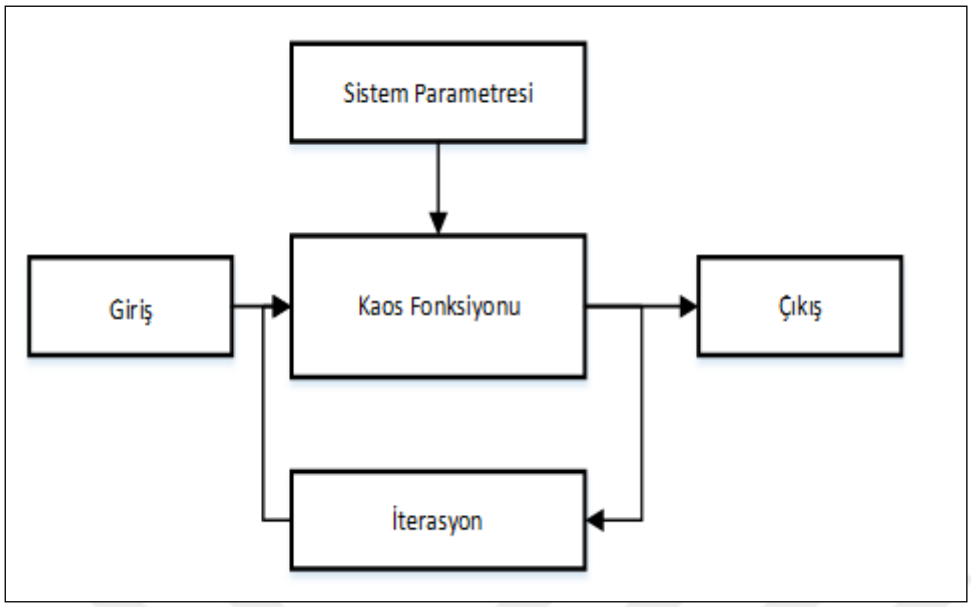
Başlangıç koşullarına duyarlı, topolojik geçişkenlik ve periyodik nokta yoğunluğunda sahip sistemler kaotik özellikli sistemler olarak adlandırılmaktadır. Kaotik sistemler geri beslemeli sistemlerdir yani çıktı fonksiyonu döngüde bir sonraki adım için girdi olarak kullanılmaktadır. Girdi değişkeninin doğrusal olmaması sebebiyle, çıktı fonksiyonu girdi değişkeninden bağımsız olarak gerçekleşmektedir. Sistemin başlangıç koşulları ve değişkenler arası ilişki kaotik sistemlerde sistemin davranışları açısından çok büyük bir öneme sahiptir. Kaotik sistemlerin oldukça karmaşık bir yapıya sahip olmasına rağmen aslında sistem kendi içinde bir düzene sahiptir. Bu tür kaotik sistemler deterministik kaos olarak da bilinmektedir. Kaotik sistemlerin bir diğer türü ise davranışı bilinemeyen ve hesaplanamayan rastlantısal kaos kavramıdır. Bu tür kaos sistemlerini davranışlarının seyri bilinemez ve tahmin edilemez. Ancak kriptolojik uygulamalarda deterministik kaos kavramı ile ilgilenilmektedir.

Kriptolojik uygulamalarda kullanılan deterministik yapılar sistemin tahmin edilebilir olduğu anlamına gelmez. Ayrık kaotik sistemler döngüsel yani iteratif bir yapıyla kaotik haritaları oluşturmaktadır. Yani, kaos tabanlı sistemlerde girdiler tümüyle değerlendirildikten sonra sistem nihai davranışını sergiler [52].

Kaotik sistemlerin başlangıç koşullarına duyarlı olması, sistemdeki her bir noktanın tepkisinin farklı olması anlamına gelmektedir. Sistem başlangıç koşullarında meydana gelecek çok küçük değişiklikler sistem cevabının tamamen farklı olacağı anlamına gelmektedir. Dinamik davranışlar sergileyen kaotik sistemlerin yörüngelerini tahmin etmek oldukça güçtür. Başlangıç koşullarından bağımsız olarak kontrol parametreleri uygun değilse sistem kaotik davranışlar sergileyemecektir ve sistem belirli bir süre sonra birbirine çok yakın davranışlar sergilemeye başlayacaktır.

Kaotik sistemler davranışları belirli bir nokta veya bölge ile sınırlı olduklarında kaotik özellik göstermezler. Bu durum ise sistemi tahmin edilebilir kılmaktadır. Benzer başlangıç koşulları çıktının öngörülebilirlik seviyesini artırmaktadır. Uygun kontrol parametreleri altında kaotik sistemler tamamen kararsız bir davranış sergilemektedirler. Bu davranışları sayesinde başlangıç koşulları birbirlerine çok yakın olsa dahi sistem çıktıları birbirinden tamamen farklı olmasını sağlamaktadır. Bu özellik kaotik sitemlerin kriptolojik uygulamalarda kullanılmasının başlıca sebebidir [50].

Zamanla kaotik bir sistem tanım aralığında tüm değerleri alması topolojik geçirgenlik kavramıyla ifade edilmektedir. Sistemin ait olduğu tüm alt bölgelerdeki değerleri alması, sistem davranışının düzensiz olduğunun bir göstergesidir. Düzensiz bir sistem de tahmin edilemezliğin kilit noktası olarak nitelendirilebilir. Kaotik sistemlerde kontrol değişkenine bağlı olarak sistem yörüngesinin yoğunluk seviyesi değişmektedir. Yani sistemlerin kaotik özellik gösterebilmesi için kontrol değişkeni hayati öneme sahiptir diyebiliriz.
Şekil 3.1'de kaotik bir sistemin temel çalışma yapısı görülmektedir.



Şekil 3.1. Kaotik sistem çalışma prensibi

Kaotik sistemin cevabı olarak adlandırabileceğimiz yörünge, sistem fonksiyonuna bağlı bir kümedir. Sistemdeki noktaların belirli bir periyotta belirli bir düzene sahip olma eğilimi periyodik nokta yoğunluğudur. Sistem içerisindeki herhangi iki nokta ne kadar yakın olursa olsun mutlaka en az bir periyodik yörüngesi mevcuttur. Bir sistem başlangıç koşullarına duyarlı olup, topolojik geçirgenliğe ve periyodik yoğunluğa sahip değilse kaotik davranışlar sergileyemez. Bir sistemin kaotik bir sistem olarak adlandırılabilmesi için başlangıç koşullarına duyarlılık, topolojik geçirgenlik ve periyodik nokta yoğunluğuna sahip olma özelliklerinin hepsini bir arada bulundurması zorundadır.

Şifreleme de yüksek güvenlik seviyesi sağlayan kaos tabanlı şifrelemenin temelleri 1989 yılına dayanmaktadır. O günden itibaren kaos tabanlı bir çok çalışma gerçekleştirilmiştir. Matthews, 1989'da tek seferlik bir anahtar sisteminin yerine kriptografide kullanılmak üzere kaotik rasgele sayı dizileri üretmeyi önerdi [53]. Bir yıl sonra Bianco ve arkadaşları şifreleme sistemleri için bir lojistik harita önerdi [54]. 1998'de Fridrich, daha fazla karmaşıklık için iki boyutlu kaotik haritalara dayalı bir kripto sistem önerdi [55]. Pareek ve arkadaşları 2006'da kaotik bir lojistik haritaya dayalı bir görüntü şifreleme algoritması önerdi [56]. Üç yıl sonra, Liu ve arkadaşları birleştirilmiş kaotik lojistik haritalarla anahtar akışı üretecini önerdi [57]. 2016'da El Assad ve Farajallah, [58] 2D kedi haritasının yeni bir formülasyonunu önerdiler. 2019 yılında Asgari ve arkadaşları [59] görüntü kripto analizine karşı yüksek direnç için bir eliptik eğrinin kullanıldığını buldu.

Babu ve arkadaşları 2020'de güvenli bir kuvvet algoritması, DNA dizi kodlaması, Arnold Cat haritası RSA algoritması ve kaotik permütasyon teknikleri kullanarak yeni bir çoklu görüntü şifreleme çerçeve formatı önermektedir [60]. Son zamanlarda, araştırmacılar güvenli görüntü şifreleme için yeni kriptografik uygulamalar geliştirdiler. Örneğin Muñoz, 2021'de q-deforme edilmiş lojistik haritayı kullanarak görüntü şifrelemeyi önerdi [61].

3.2. Önerilen Algoritma ve Geliştirilen Kullanıcı Arayüzü

Bu bölümde ilk olarak önerilen lojistik harita hakkında bilgiler verilmiş daha sonra geliştirilen kullanıcı arayüzü hakkında detaylar aktarılmıştır.

3.2.1. Önerilen algoritma

Görüntü şifreleme algoritmalarının güvenliğini sağlamak ve verileri saldırganlar tarafından ulaşılması zor duruma getirmek geliştirilen algoritmalar için hayati öneme sahiptir. Sözde rastgele sayı üreteçleri ile üretilen maske görüntüsü kullanılarak güvenli bir şifreleme işlemi gerçekleştirebilmek için maske görüntüsünde kullanılan sayılar istatistiksel olarak olabildiğince eşit dağılıma sahip olmalıdır.

Sayıların istatistiksel olarak güvenilirliğini test edebilmek için ortalama, varyans ve standart sapma değerleri bulunmaktadır. Sayıları istatistiksel olarak daha güvenli olarak nitelendirebilmemiz için varyans ve standart sapma değeri büyük olmalı, ortalama değeri ise 0 ile 256 arasında değerler alabilen piksel değerlerinin ortalaması olan 128 değerine olabildiğince yakın olmalıdır. Eş. 3.1, Eş. 3.2 ve Eş. 3.3'de ortalama varyans ve standart sapma formülleri görülmektedir.

$$\overline{X} = \frac{1}{n}\sum_{i=0}^{n} X_i \tag{3.1}$$

$$\sigma^2 = \frac{1}{n}\sum_{i=0}^{n}\left(X_i - \overline{X}\right)^2 \tag{3.2}$$

$$SS = \sqrt{\sigma^2} \tag{3.3}$$

Eşitliklerde $\overline{X}$ ortalama değeri, σ^2 varyans değerini SS standart sapma değerini, n ise dizide kullanılan sayı adedini ifade etmektedir.

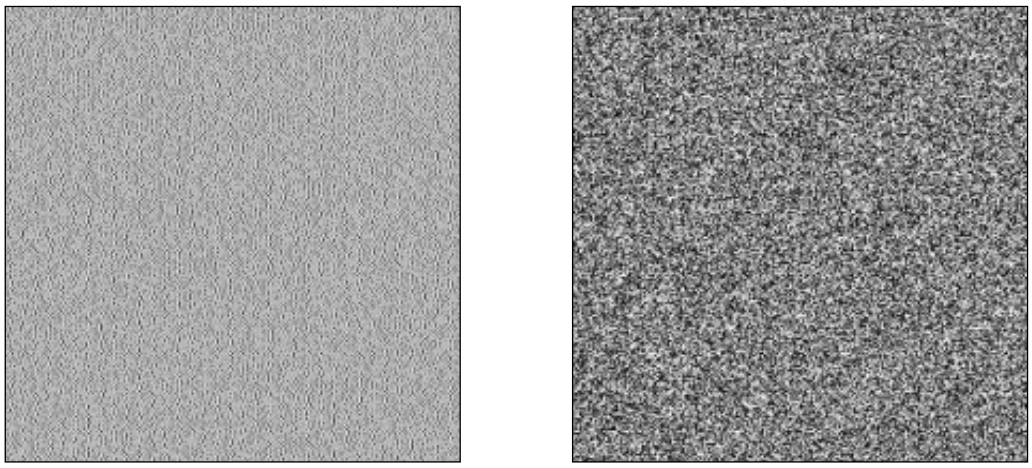
Lojistik harita ve önerilen lojistik harita ile oluşturulan sayıların ortalaması, varyansı ve standart sapması Çizelge 3.1'de görülmektedir.

Çizelge 3.1. Klasik lojistik harita ve önerilen lojistik harita ile oluşturulan sayıların ortalama, varyans ve standart sapma değerleri

	Klasik Lojistik Harita	Önerilen Lojistik harita
Ortalama	153	118
Varyans	5596,35	5656,79
Standart Sapma	74,80	75,21

Çizelge 3.1'de görüldüğü gibi önerilen lojistik harita ile oluşturulan sayıların varyans ve standart sapma değerleri klasik lojistik haritaya göre daha yüksek, ortalama değeri ise 128 değerine daha yakındır. Bu değerler önerilen lojistik haritanın klasik lojistik haritaya göre istatistiksel olarak daha güvenli olduğunu göstermektedir.

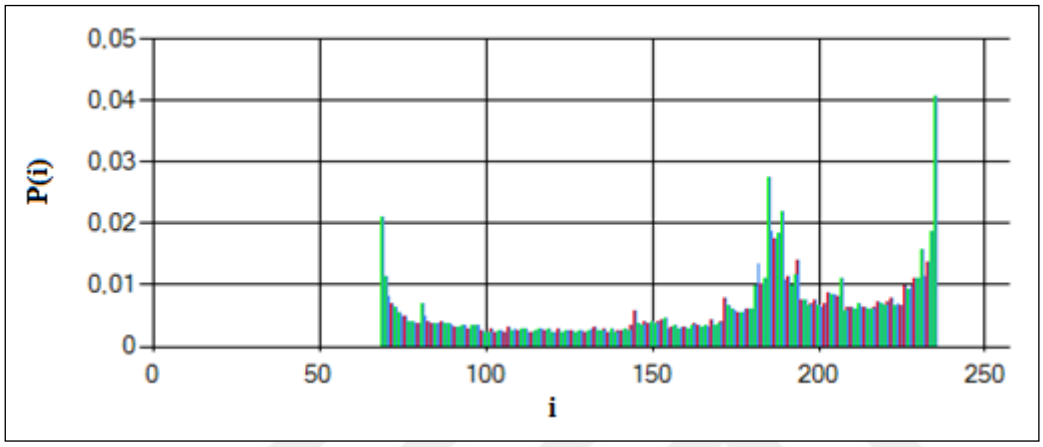
Rastgele sayı üretme penceresinde şifreleme işleminde kullanılan maske görüntü ile histogram analizi uygulanabilmektedir. Şekil 3.2'de maske görüntüler görülmektedir.



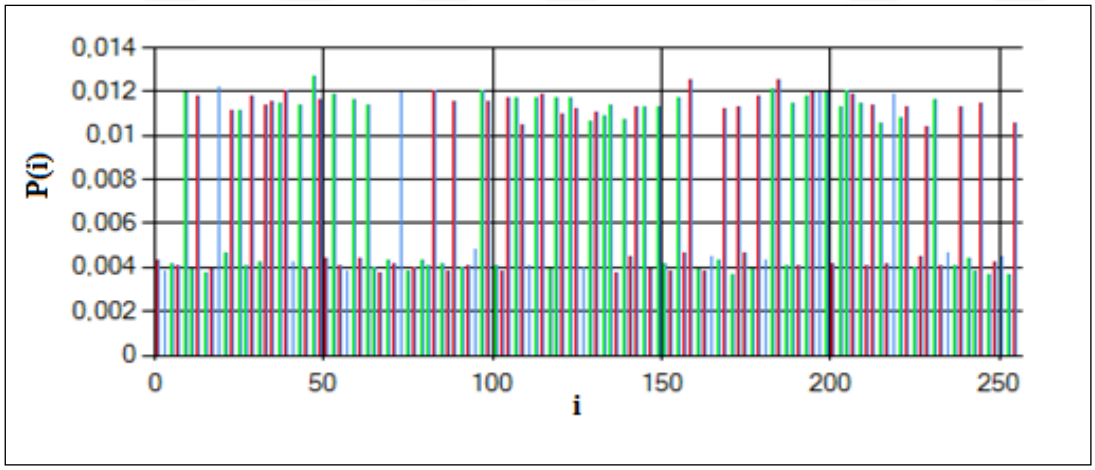
(a) (b)

Şekil 3.2. Maske görüntü (a) klasik lojistik harita ile oluşturulan, (b) önerilen lojistik harita ile oluşturulan

Şekil 3.3'te oluşturulan maske görüntülerin dağılımı olan histogram grafikleri görülmektedir. Güçlü bir sistemde kullanılacak görüntünün histogram grafiğinin olabildiğince eşit dağılımda olması gerekmektedir. Klasik lojistik harita ile oluşturulan grafikte yaklaşık 0 ve 70 değerleri arasında hiç sayı oluşmazken, önerilen lojistik harita ile oluşturulan grafikte sayılar neredeyse tüm aralıkta eşit dağılım sergilemektedir. Bu şifreleme sistemi için uygun olduğunun bir göstergesidir.



(a)



(b)

Şekil 3.3. Maske görüntünün histogram grafiği (a) klasik lojistik harita ile oluşturulan, (b) önerilen lojistik harita ile oluşturulan

Klasik lojistik harita ve önerilen lojistik harita temelde Eş. 3.4'de görülen lojistik harita fonksiyonu ile hesaplanmaktadır.

$$X_{n+1} = \mu . X_n . (1 - X_n) \tag{3.4}$$

Eş. 3.4'de bulunan klasik lojistik harita ile maske görüntü oluşturmak için kullanılan kod bloğu Şekil 3.4 a'da, önerilen maske görüntüyü oluşturmak için kullanılan kod bloğu Şekil 3.4 b'de görülmektedir.

```
for (j = 0; j < bmp1.Height; j++)
{
    for (i = 0; i < bmp1.Width; i++)
    {
        p9 = bmp1.GetPixel(i, j);
        x = mu * x1 * (1 - x1);
        z = x * 255;
        p9 = Color.FromArgb((int)z, (int)z, (int)z);
        bmp2.SetPixel(i, j, p9);
        Maske.SetPixel(i, j, p9);
        x1 = x;
    }
}
return bmp2;
```

(a)

```
for (j = 0; j < bmp1.Height; j++)
{
    for (i = 0; i < bmp1.Width; i++)
    {   p9 = bmp1.GetPixel(i, j);
        x = mu * x1 * (1 - x1);
        y = (ulong)(x * ulong.MaxValue);
        string Rstr = Decimaltobin64(y);
        char[] Ra = Rstr.ToCharArray();
        for (k = 0; k < Ra.Length; k++){keys[k] = Ra[k];}
        key[0] = keys[0];
        key[1] = keys[8];
        key[2] = keys[16];
        key[3] = keys[24];
        key[4] = keys[32];
        key[5] = keys[40];
        key[6] = keys[48];
        key[7] = keys[56];
        string bilR = new string(key);
        q1 = int.Parse(bilR);
        q1 = q1 & 255;
        p9 = Color.FromArgb((int)q1, (int)q1, (int)q1);
        bmp2.SetPixel(i, j, p9);
        Maske.SetPixel(i, j, p9);
        x1 = x;
    }
}
```

(b)

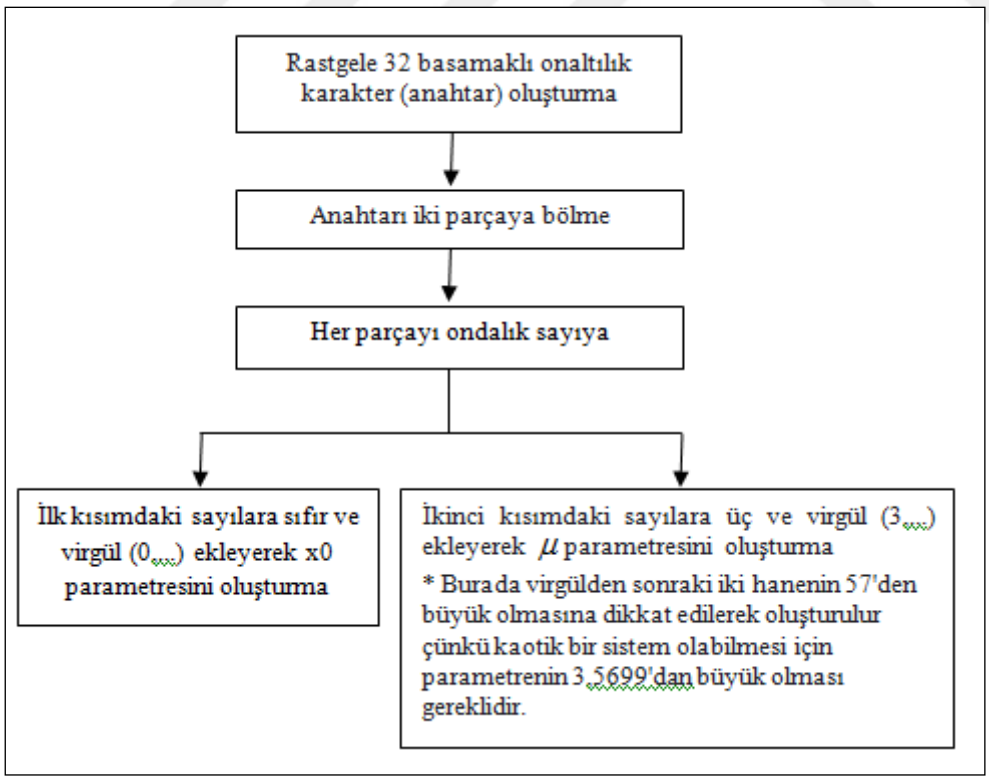
Şekil 3.4. Kod bloğu (a) klasik lojistik harita, (b) önerilen lojistik harita

Klasik lojistik harita oluşturmak için üretilen sayılar Şekil 3.3 a'daki histogram grafiğinde de görüldüğü üzere eşit dağılıma sahip değildir ve bu bize şifreleme algoritmasının

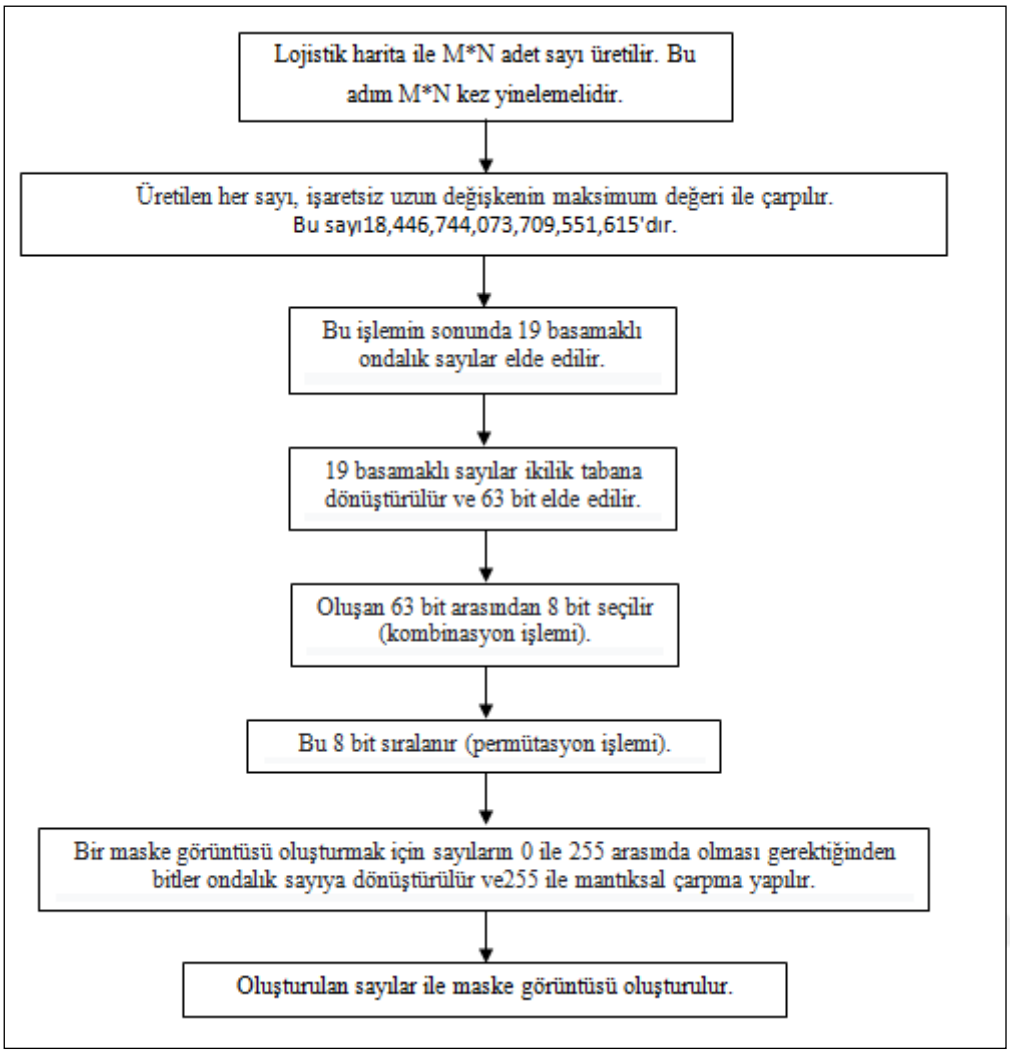
istatistiksel olarak zayıf olduğunu göstermektedir. Geliştirilen algoritma bu zayıflığın üstesinden gelebilmek için maske görüntüsünü oluşturacak sayıların üretiminin her bir döngüsünde permütasyon ve kombinasyon işlemleri kullanarak sayıların istatistiksel olarak eşit dağılımını sağlayarak algoritmayı çok daha güvenli hale getirmektedir.

Geliştirilen algoritma ile şifreleme işlemi için öncelikle Şekil 3.2'de gösterildiği üzere yazılım tarafından zamana bağlı rastgele olarak üretilen 32 basamaklı (128 bit) simetrik anahtar kullanılarak maske görüntü oluşturmak için kullanılacak başlangıç parametreleri elde edilir. Daha sonra Şekil 3.3'de bulunan adımlar sırasıyla uygulanarak permütasyon ve kombinasyon işlemleri ile istatistiksel olarak güvenliği artırılmış maske görüntüsü elde edilir. Şekil 3.5'te düz metin görüntüsü, maske görüntüsü ve maske tabanlı görüntü şifreleme işlemleri için daha uygun olan RC4 akış şifrelemesine benzerlik gösteren XOR (özel veya) operatörü kullanılarak oluşturulan şifreleme işleminin adımları görülmektedir.

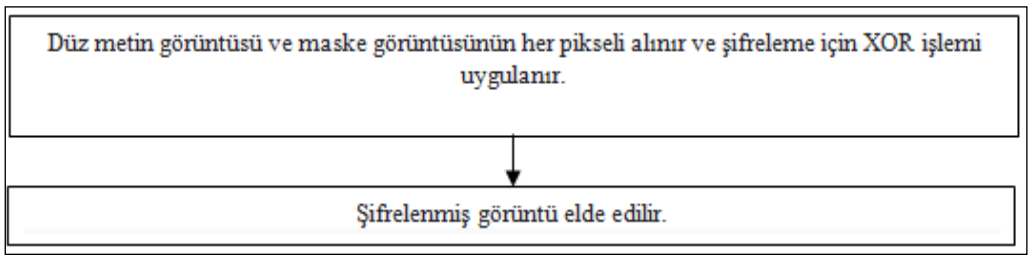
Alıcı tarafında şifre çözme işlemi şifreli resim ve simetrik anahtar kullanılarak Şekil 3.6 ve Şekil 3.7'de bulunan adımların tekrar edilmesiyle gerçekleştirilir.



Şekil 3.5. Anahtardan lojistik haritanın başlangıç değerlerini elde etme adımları



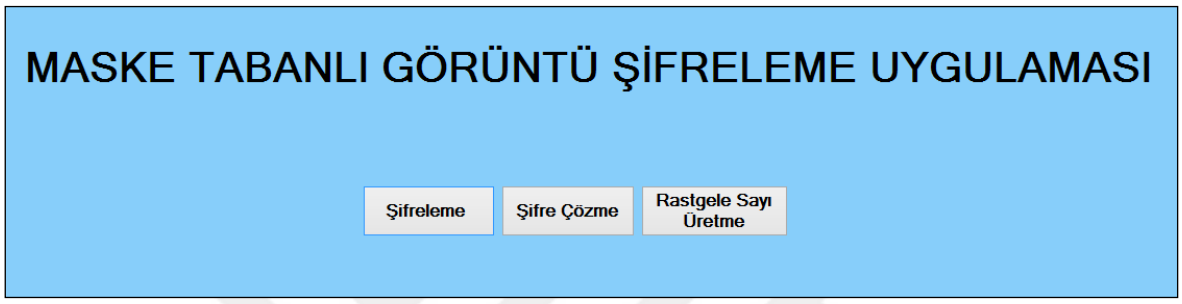
Şekil 3.6. Önerilen lojistik haritayı kullanarak maske görüntü elde etme adımları



Şekil 3.7. Düz metin görüntüsü ve maske görüntü ile şifreleme adımları

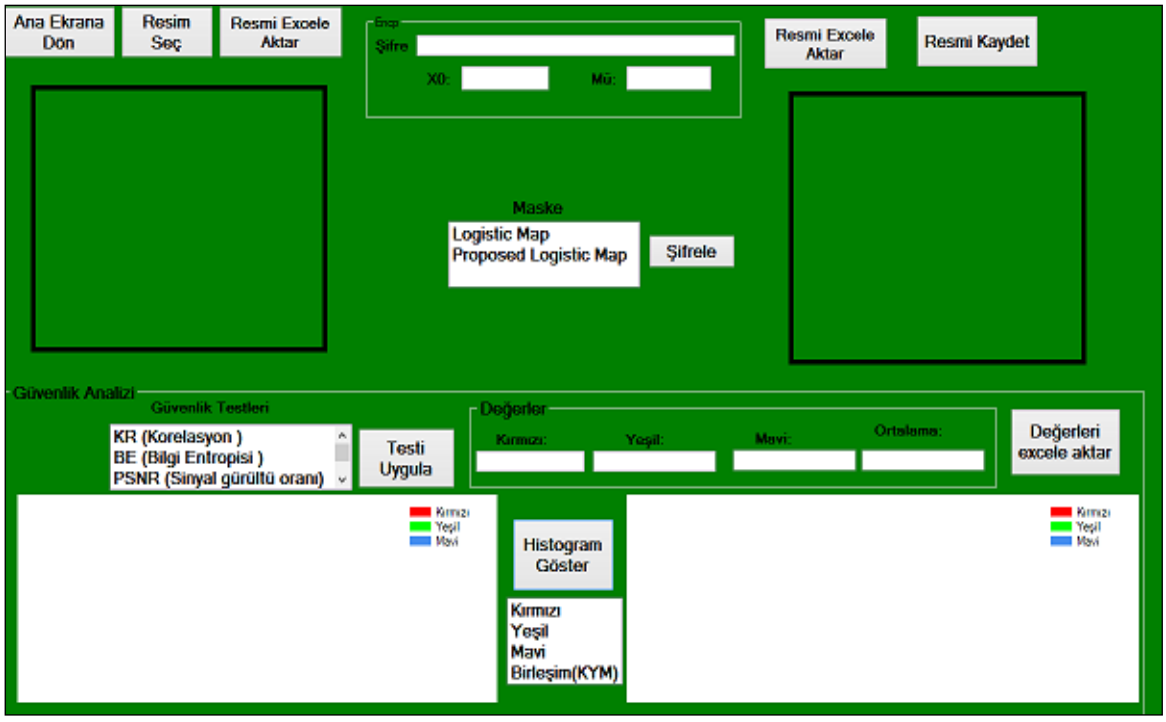
3.2.2. Geliştirilen kullanıcı arayüzü

Geliştirilen kullanıcı arayüzü Microsoft visual studio C# uygulaması ile geliştirilmiştir. Geliştirilen uygulamanın başlangıç sayfası 3 menüden oluşmaktadır. Bunlar şifreleme, şifre çözme ve lojistik harita oluşturmak için sayılar üretme ve üretilen rastgele sayılarının testlerinin gerçekleştirilebileceği rastgele sayı üretme menüleridir. Şekil 3.8'de geliştirilen kullanıcı arayüz sayfası görülmektedir.



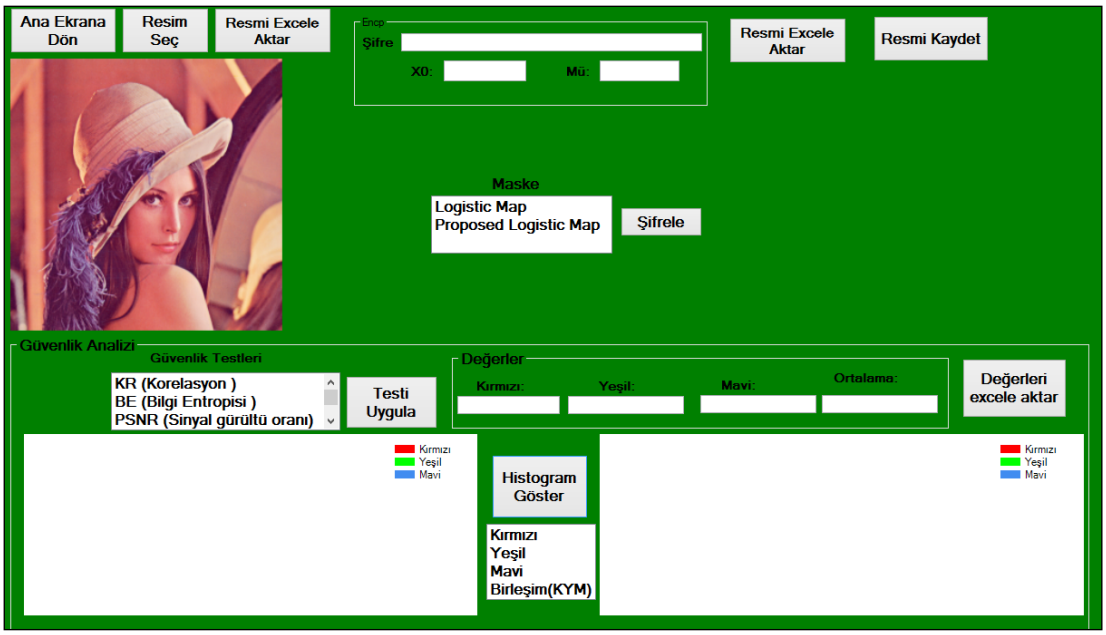
Şekil 3.8. Geliştirilen kullanıcı arayüz sayfası

Kullanıcı arayüz sayfasında resim şifreleme işlemi için şifreleme butonuna basılmalıdır. Şifreleme butonuna basıldıktan sonra açılan şifreleme penceresi Şekil 3.9'da görülmektedir.



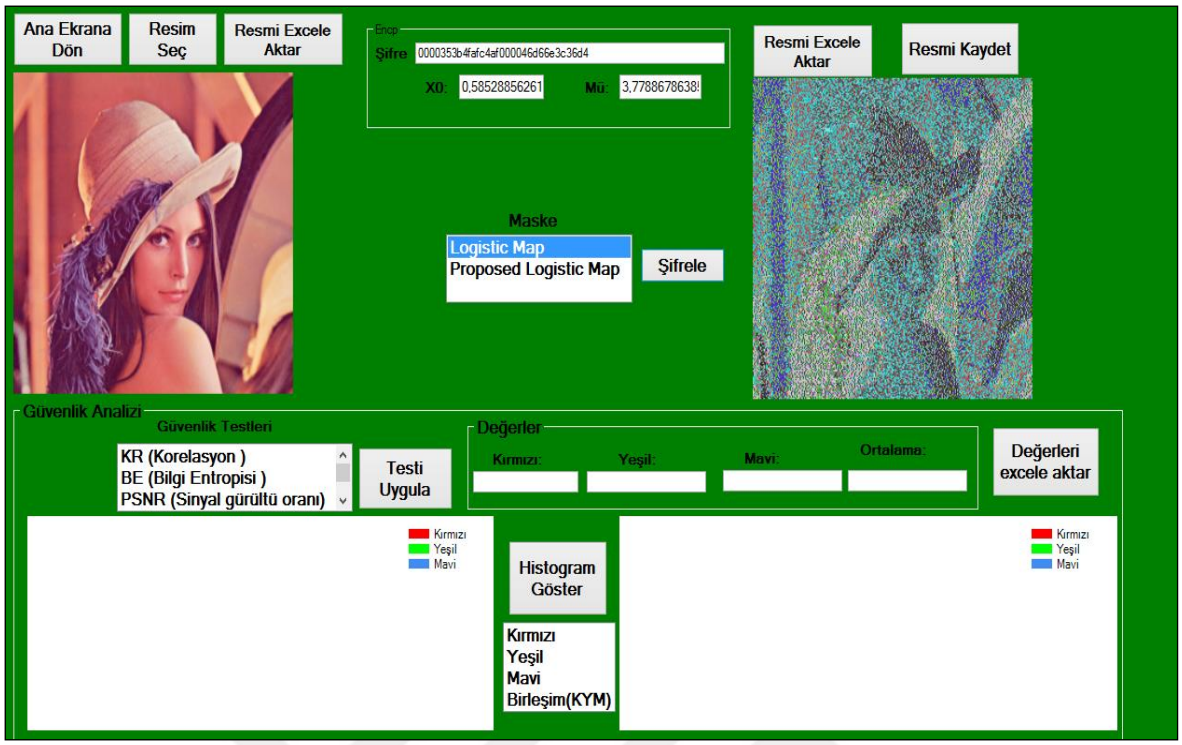
Şekil 3.9. Şifreleme arayüz sayfası

Bu pencerenin üst kısımda resim şifreleme işlemleri alanı, alt kısımda ise şifrelenmiş resme güvenlik testleri uygulanabilecek alanlar bulunmaktadır. Şifreleme işlemini gerçekleştirebilmek için öncelikle şifrelenecek görüntü "resim seç" butonu ile bilgisayardan seçilmeli ve sol tarafta bulunan siyah çerçeveli alana yüklenmelidir. Şekil 3.10'da resim seçilmiş arayüz görülmektedir.

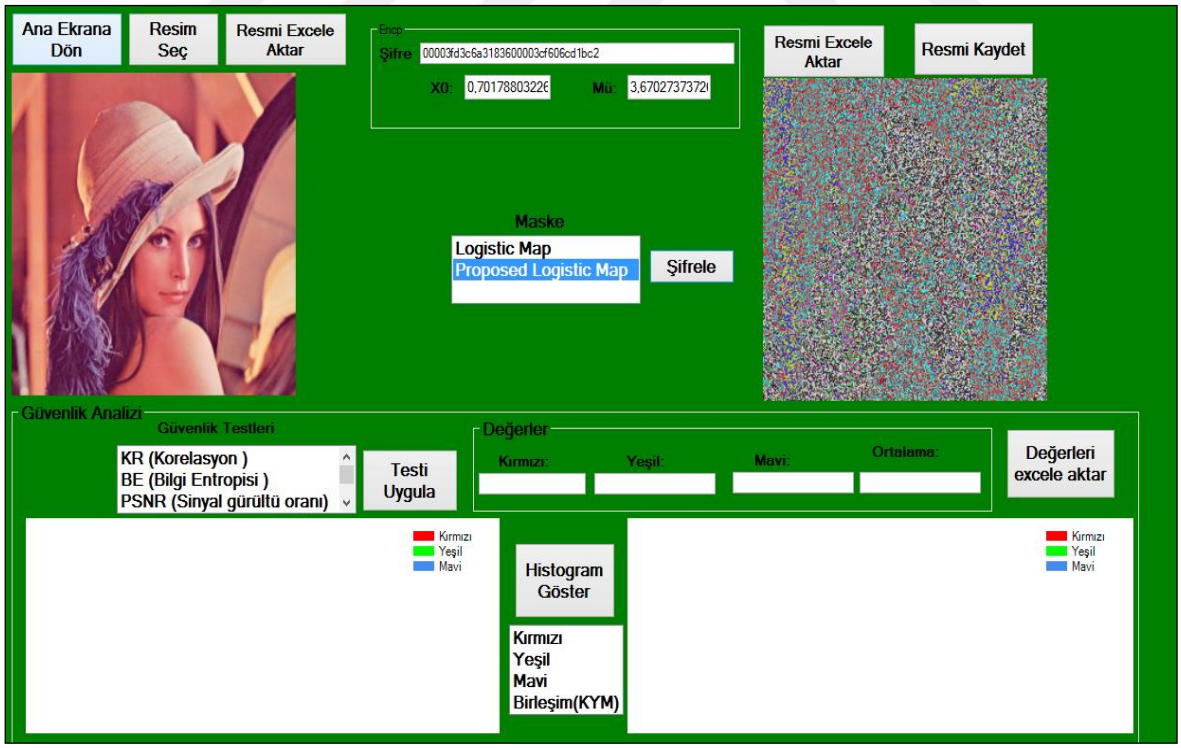


Şekil 3.10. Resim seçilmiş şifreleme arayüz sayfası

Resim seçme işlemini gerçekleştirdikten sonra şifreleme için maske türü seçilmeli ve ardından "şifrele" butonuna basılmalıdır. Bu işlem ile paralel olarak arka planda sistem tarafından 128 bit şifreleme anahtarı olarak kullanılacak şifre oluşturulur ve bu anahtar şifrelemede kullanılacak maske görüntü için başlangıç parametreleri olan X_0 ve μ değerlerini oluşturur. Şekil 3.11'de lojistik harita ile şifreleme işlemi gerçekleştirilmiş arayüz ve Şekil 3.12'de önerilen lojistik harita ile şifreleme işlemi gerçekleştirilmiş arayüz görülmektedir. Ekranın sağ ve sol kısımlarında bulunan "Resmi excele aktar" butonu ile orijinal ve şifrelendikten sonraki resimlerin piksel değerleri excel uygulamasında görülmektedir. Ayrıca " Resmi kaydet" butonu ile şifrelenen resim bilgisayara kayıt edilebilmektedir.

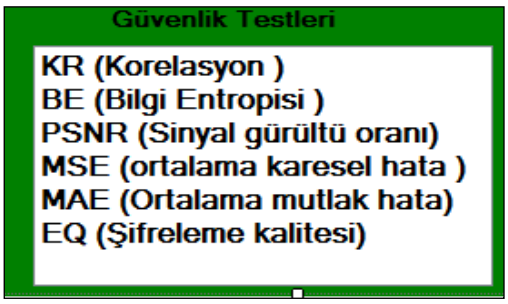


Şekil 3.11. Lojistik harita ile şifreleme gerçekleştirilmiş arayüz sayfası



Şekil 3.12. Önerilen lojistik harita ile şifreleme gerçekleştirilmiş arayüz sayfası

Şifreleme penceresinin alt kısmında bulunan güvenlik analizi bölümü ile şifrelenen resme uygulanabilecek güvenlik testleri yer almaktadır. Şekil 3.13'te Uygulanabilecek güvenlik testleri görülmektedir.



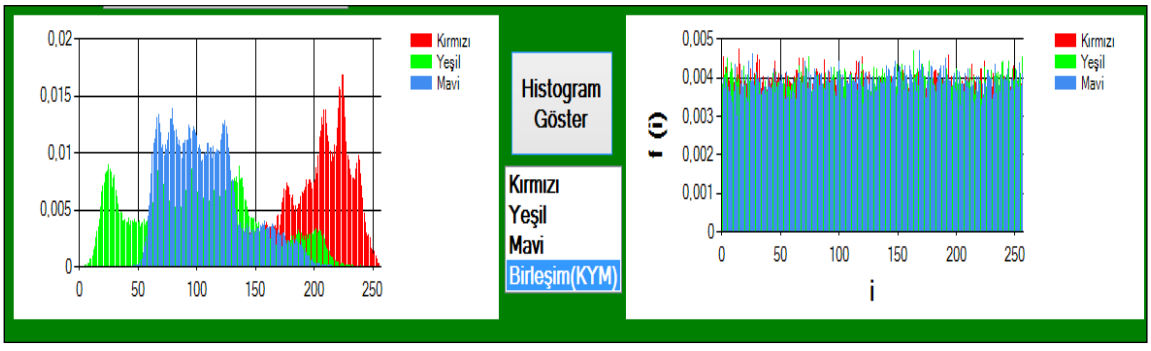
Şekil 3.13. Güvenlik testleri

Uygulanacak güvenlik testi seçildikten sonra "Testi uygula" butonu seçilen güvenlik analizi testi uygulanır. Resmin kırmızı, yeşil, mavi kanalları ve bunların ortalaması olan değerler Şekil 3.14'te görülmektedir.



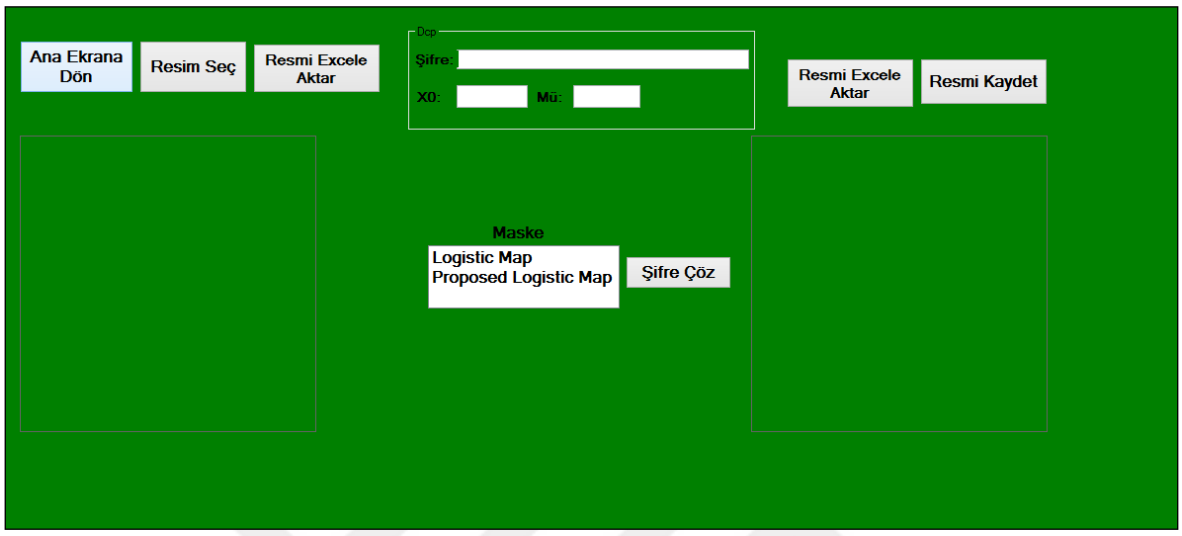
Şekil 3.14. Örnek güvenlik analizi testi

Şifreleme ekranının en alt orta kısmında bulunan "Histogram göster" butonu ile orijinal ve şifreli görüntünün kırmızı, yeşil, mavi kanalları ve tüm kanalları aynı anda görme seçenekleri ile 2 resmin histogram grafikleri karşılaştırmalı olarak görülebilmektedir. Şekil 3.15'te örnek histogram görüntüsü görülmektedir.



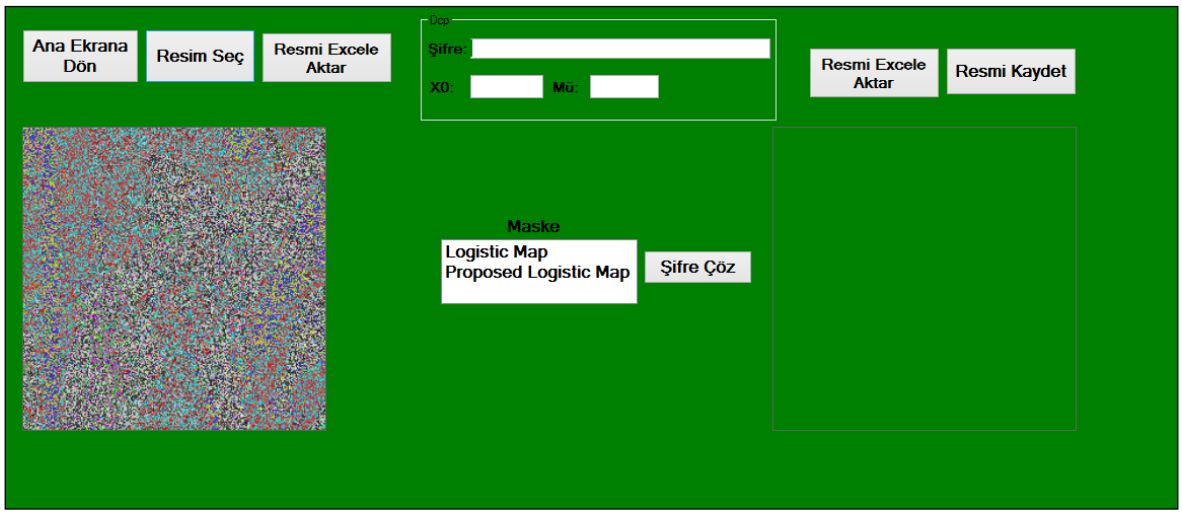
Şekil 3.15. Örnek histogram görüntüsü

Şifrelenmiş görüntünün alıcı tarafında şifre çözme işleminin gerçekleştirilmesi için ana sayfada bulunan "Şifre Çözme" butonu ile şifre çözme penceresine geçiş yapılmalıdır. Şifre çözme penceresi Şekil 3.16'da görülmektedir.



Şekil 3.16. Şifre çözme penceresi

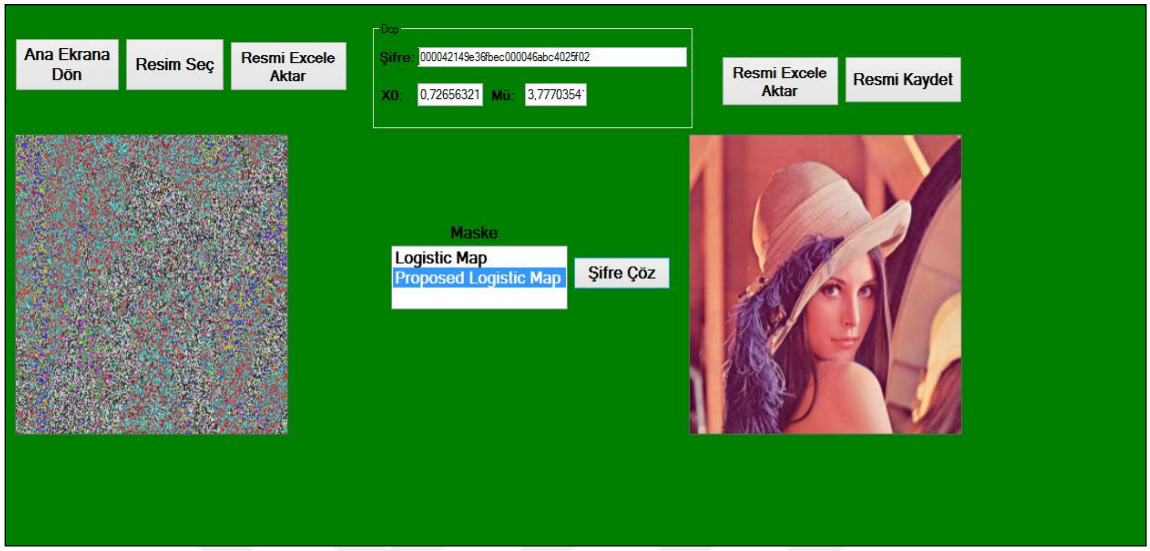
Şifre çözme işleme için şifreli görüntü "Resim seç" butonu ile seçilerek soldaki çerçeveye yüklenir. Şekil 3.17'de şifreli resim yüklenmiş arayüz görülmektedir.



Şekil 3.17. Şifreli resim yüklenmiş arayüz görüntüsü

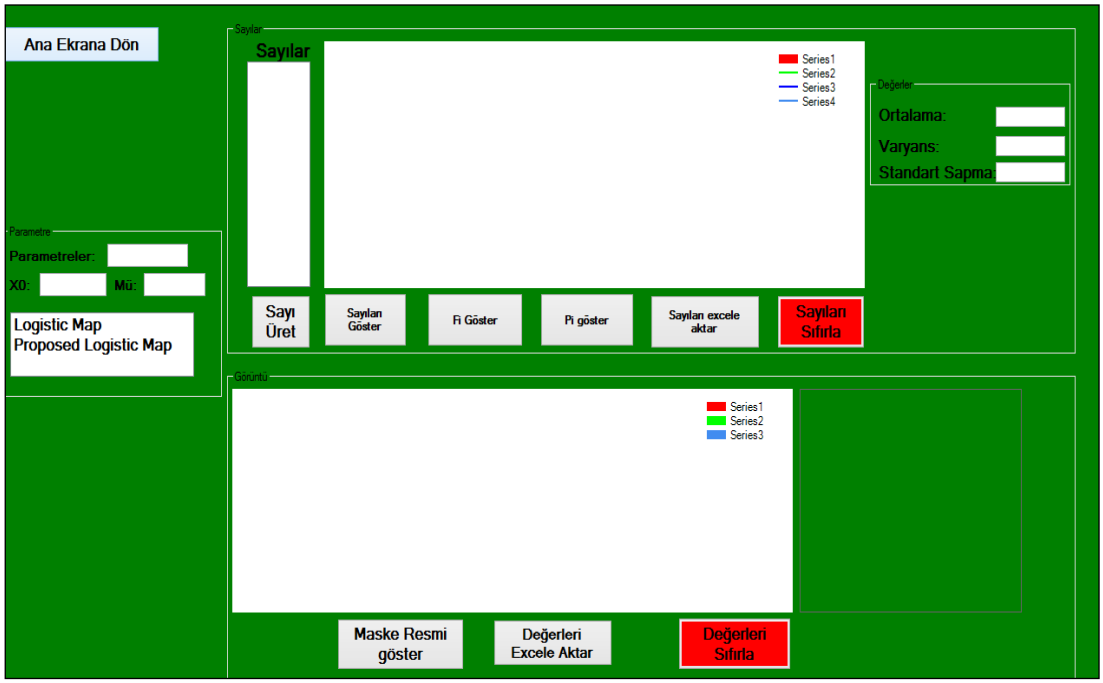
Şifreli görüntüyü yükledikten sonra şifre kısmına şifreleme işlemi için kullanılan simetrik anahtar şifre yazılmalı ve maske türü seçildikten sonra " Şifre çöz" butonuna basıldıktan

sonra şifresi çözülmüş resim elde edilmektedir. Şekil 3.18'de şifresi çözülmüş resim görülmektedir.



Şekil 3.18. Şifresi çözülmüş resim arayüz görüntüsü

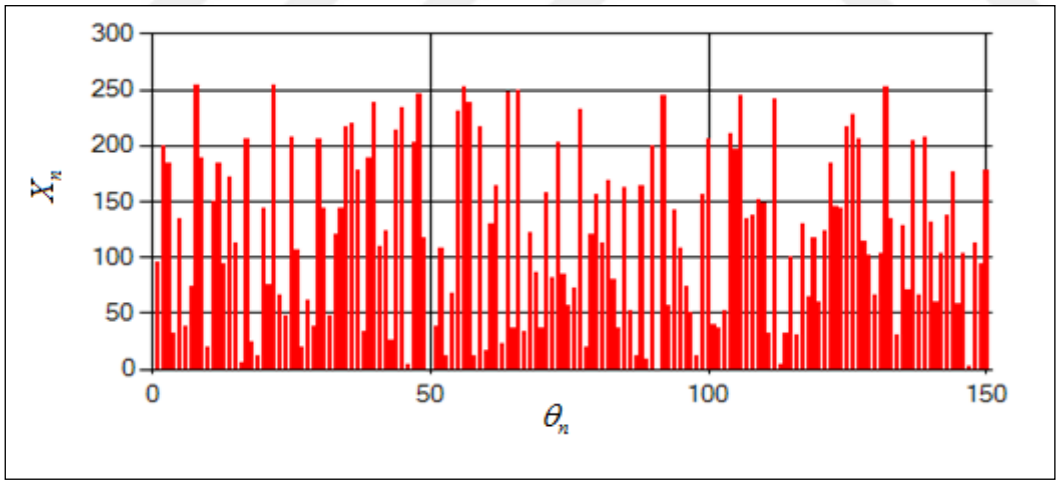
Şifreleme işleminde kullanılacak maske resmi için oluşturulan sayılar ve bunlarla ilgili testlerin gerçekleştirilebileceği rastgele sayı üretme ekranına geçiş yapabilmek için ana sayfada bulunan "Rastgele sayı üretme" butonu ile rastgele sayı üretme penceresine geçiş yapılmalıdır. Rastgele sayı üretme penceresi Şekil 3.19'da görülmektedir.



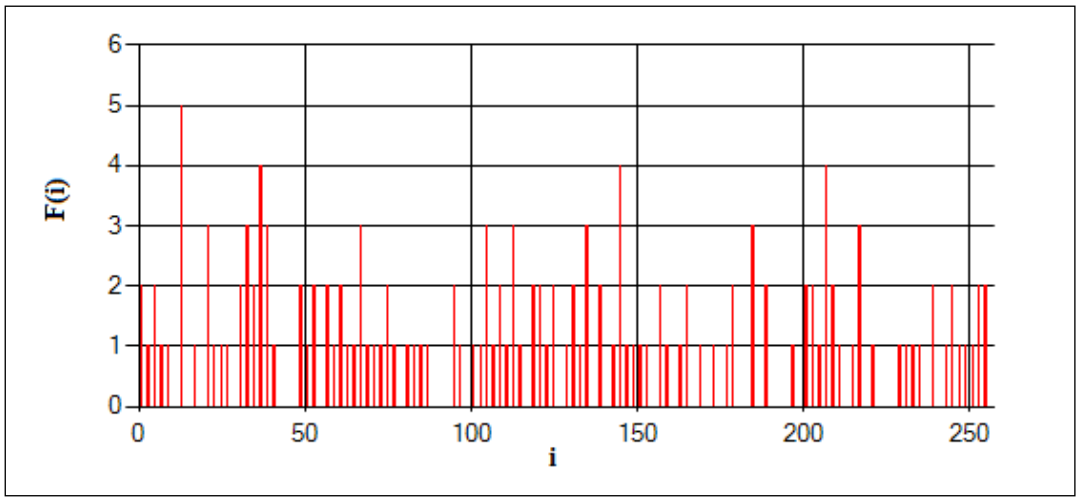
Şekil 3.19. Rastgele sayı üretme penceresi arayüz görüntüsü

Rastgele sayı üretme işleminin gerçekleştirilebilmesi için X_0 ve μ parametreleri gerekmektedir. Bu parametreler parametre alanına yazılan 8 basamaklı sayı ile oluşturulmaktadır. Burada, parametrenin 5. basamağının (μ değerinin virgülden sonraki ilk basamağı) 6 veya 6'dan büyük olmasına dikkat edilmelidir çünkü lojistik haritanın kaotik döngüye girebilmesi için μ parametresinin 3,5699'dan büyük olması gerekmektedir.

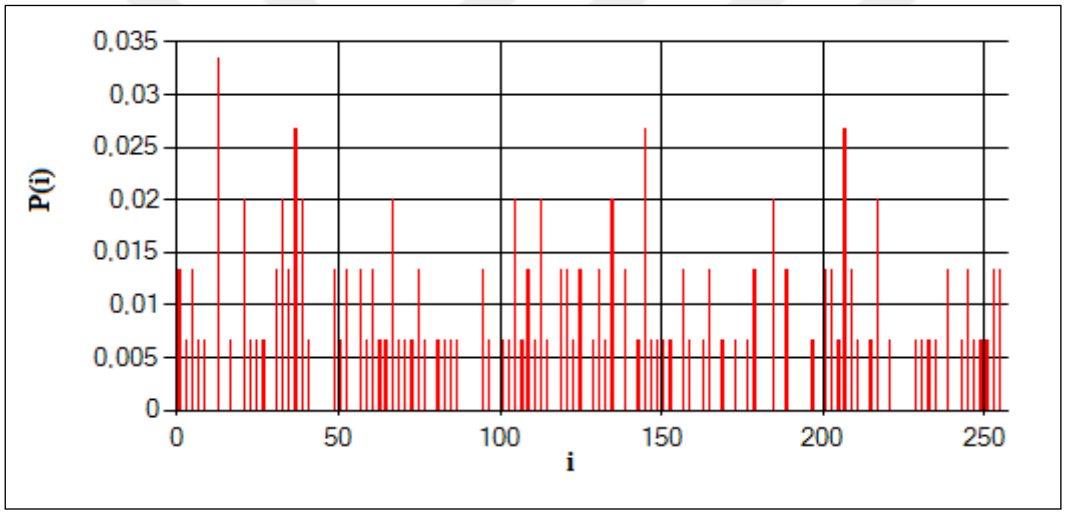
8 basamaklı parametre girilip ve istenilen harita türü seçildikten sonra "Sayı üret" butonu ile liste halinde sayılar üretilmektedir. "Sayı göster" butonu ile oluşturulan sayılar grafik olarak gösterilmekte, "Fi göster" butonu ile her bir piksel değerinde oluşturulan sayı adetleri grafiği, "Pi göster" butonu ile her bir piksel değerinde oluşturulan sayı adetlerinin yüzdesel dağılım grafiği görülmektedir. "Sayıları excele aktar" butonu ile oluşturulan sayılar excel uygulamasına aktarılmaktadır. Şekil 3.20, Şekil 3.21 ve Şekil 3.22'de sırasıyla, oluşturulan sayıların grafiği, Fi değerlerinin grafiği ve Pi değerlerinin grafiği görülmektedir.



Şekil 3.20. Önerilen lojistik harita ile üretilen sayıların grafiğinin ekran görüntüsü



Şekil 3.21. Önerilen lojistik harita ile üretilen sayıların Fi grafiğinin ekran görüntüsü



Şekil 3.22. Önerilen lojistik harita ile üretilen sayıların Pi grafiğinin ekran görüntüsü

4. DENEYSEL SONUÇLAR VEGÜVENLİK ANALİZLER

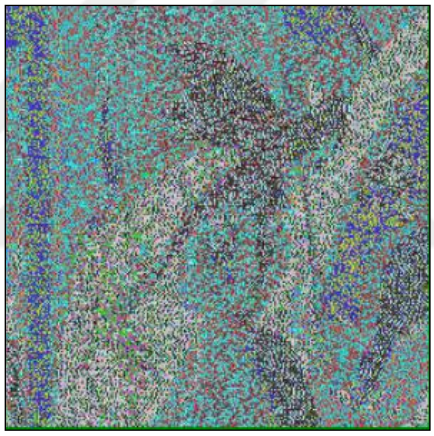
Bu bölümde ilk olarak geliştirilen arayüz kullanılarak örnek resimlerin şifreleme işlemleri gerçekleştirilmiş daha sonra şifrelenen bu resimlere güvenlik testleri uygulanmıştır.

4.1. Deneysel Sonuçlar

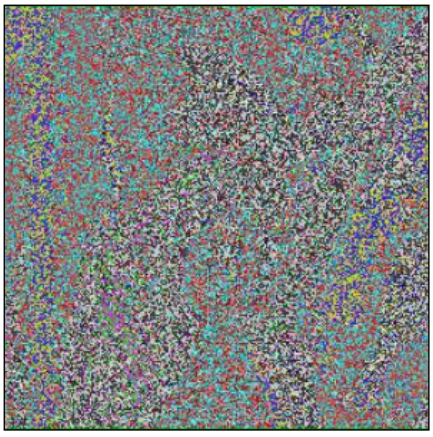
Bu bölüme kadar çoğunluğu genellikle görüntü şifreleme uygulamaları literatüründe kullanılan sırasıyla Lena, biberler, papağan, kuzey ışıkları, Gazi üniversitesi rektörlük binası, meyveler ve çiçek resimlerinin şifreleme işlemi gerçekleştirilmiştir. Şekil 4.1'den Şekil 4.7'ye bu resimlerin orijinal halleri, klasik lojistik harita ile şifrelenmiş hali ve önerilen lojistik harita ile şifrelenmiş halleri görülmektedir.



(a)



(b)

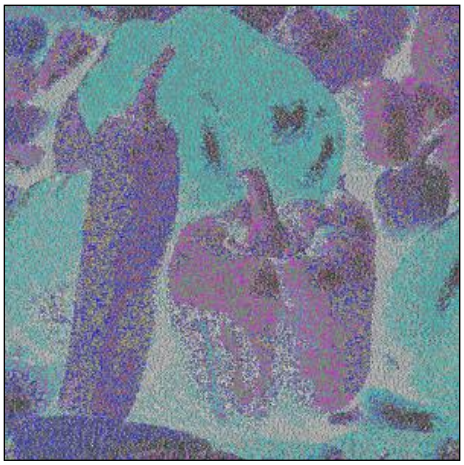


(c)

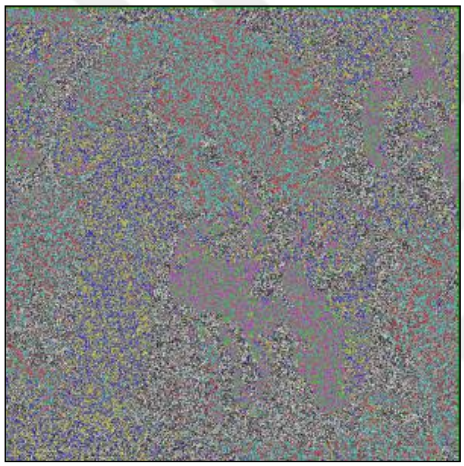
Şekil 4.1. Lena (a) orijinal görüntüsü, (b) lojistik harita ile şifrelenmiş şekli, (c) önerilen lojistik harita ile şifrelenmiş şekli



(a)



(b)

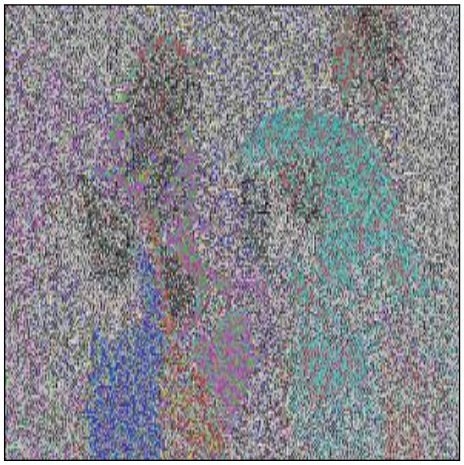


(c)

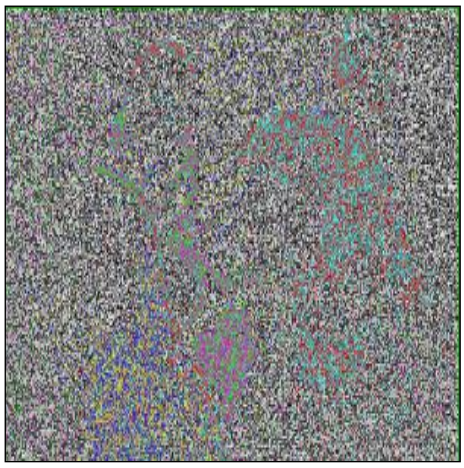
Şekil 4.2. Biberler (a) orijinal görüntüsü, (b) lojistik harita ile şifrelenmiş şekli, (c) önerilen lojistik harita ile şifrelenmiş şekli



(a)



(b)

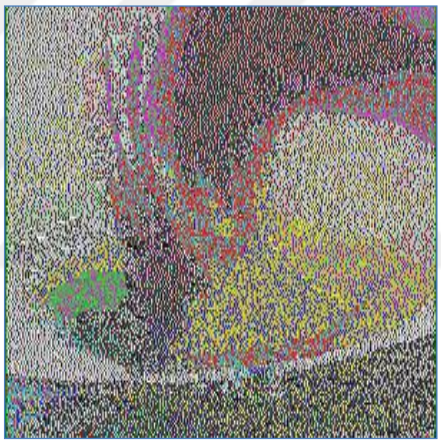


(c)

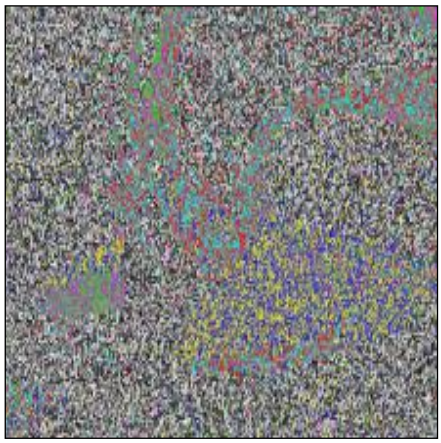
Şekil 4.3. Papağan (a) orijinal görüntüsü, (b) lojistik harita ile şifrelenmiş şekli, (c) önerilen lojistik harita ile şifrelenmiş şekli



(a)



(b)

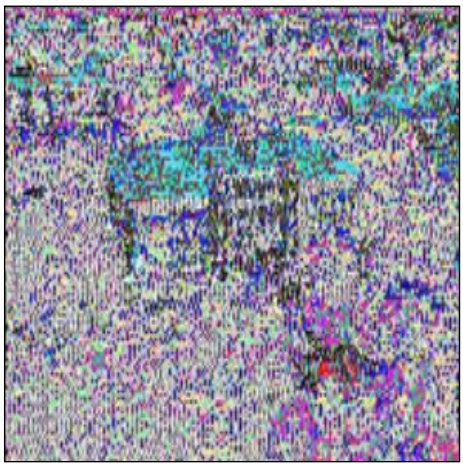


(c)

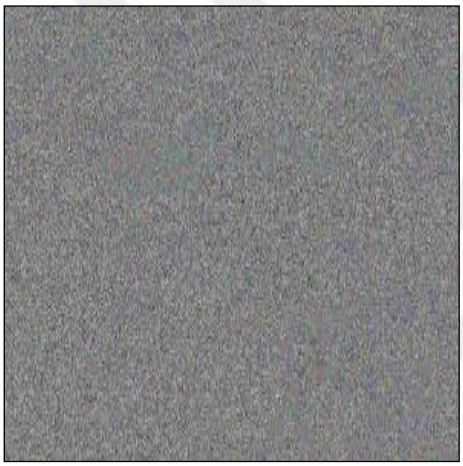
Şekil 4.4. Kuzey ışıkları (a) orijinal görüntüsü, (b) lojistik harita ile şifrelenmiş şekli, (c) önerilen lojistik harita ile şifrelenmiş şekli



(a)



(b)

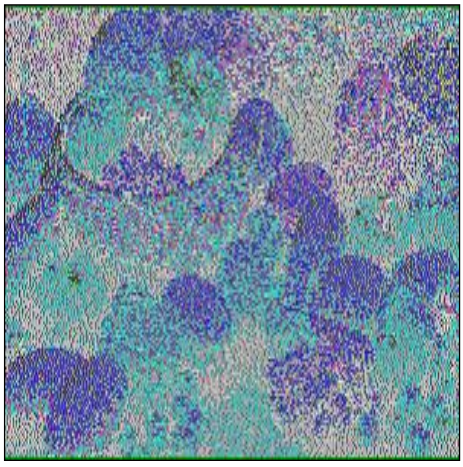


(c)

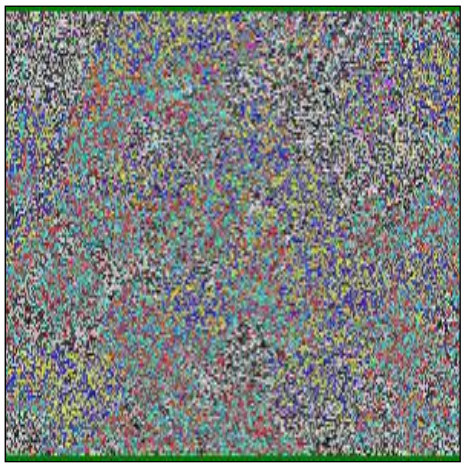
Şekil 4.5. Gazi Üniversitesi rektörlük binası (a) orijinal görüntüsü, (b) lojistik harita ile şifrelenmiş şekli, (c) önerilen lojistik harita ile şifrelenmiş şekli



(a)



(b)

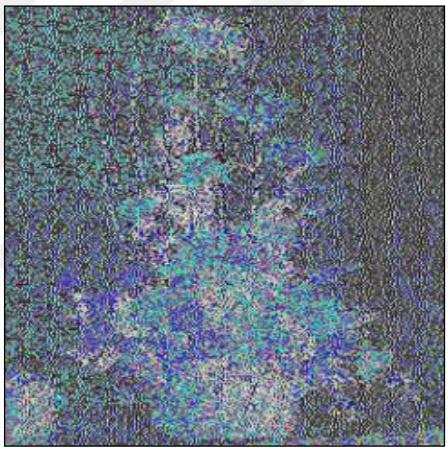


(c)

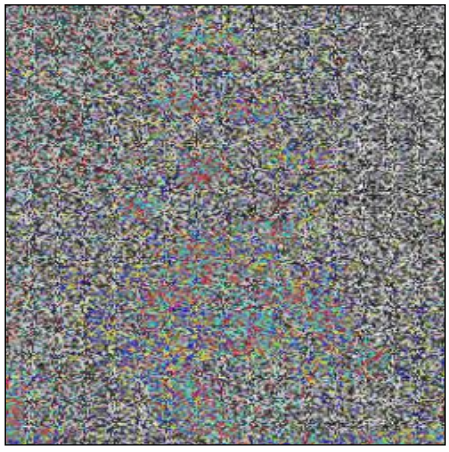
Şekil 4.6. Meyveler (a) orijinal görüntüsü, (b) lojistik harita ile şifrelenmiş şekli, (c) önerilen lojistik harita ile şifrelenmiş şekli



(a)



(b)



(c)

Şekil 4.7. Çiçek (a) orijinal görüntüsü, (b) lojistik harita ile şifrelenmiş şekli, (c) önerilen lojistik harita ile şifrelenmiş şekli

4.2. Güvenlik analizleri

İyi bir şifreleme sistemi saldırılara karşı dayanıklı olmalıdır. Bu bölümde önerilen modelin etkinliğini göstermek için önerilen yönteme farklı testler uygulanmıştır. Bu testler; anahtar uzay analizi, histogram analizi, korelasyon analizi, bilgi entropisi analizi, sinyal gürültü oranı analizi, ortalama karesel hata analizi, ortalama mutlak hata analizi ve şifreleme kalitesi analizidir. Kaba kuvvet saldırılarına karşı direnç sağlamak için anahtar uzay analizi yapılmıştır. Piksellerin renk yoğunluğu değerinin neredeyse eşit dağılımına sahip olduğunu doğrulamak için histogram analizi yapılır. İstatistiksel saldırılara karşı dayanıklı olması için korelasyon analizi uygulanmaktadır. Bilgi entropisi, şifrelenmiş görüntüde piksellerin rastgele dağılımının bir ölçüsüdür. Sinyal gürültü oranı, şifrelenmiş görüntüye saldırıdan sonra şifresi çözülen görüntünün kalitesini ölçmek için kullanılır. Ortalama karesel hata ile iki görüntü arasındaki ortalama hata hesaplanmaktadır.Orijinal ve şifreli görüntü arasındaki değişimi göstermek için ortalama mutlak hata analizi yapılır.Şifreleme kalitesi, orijinal görüntü ile şifrelenmiş görüntü arasındaki piksel değerlerindeki toplam değişimi ifade etmektedir.

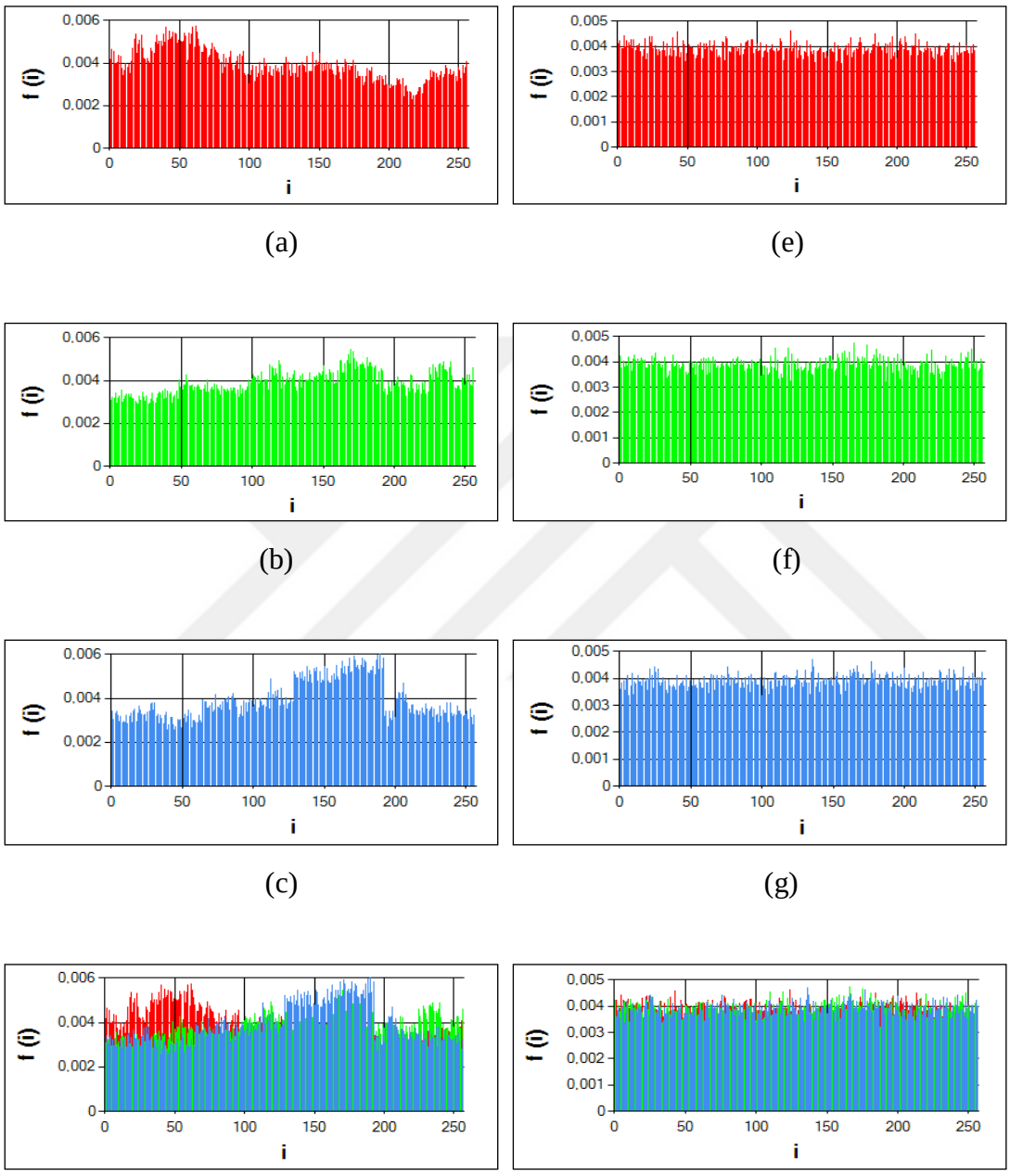
4.2.1. Anahtar uzayı analizi

Güçlü bir şifreleme sisteminin güvenliği gizli anahtarlara bağlıdır. Anahtar boyutu kaba kuvvet saldırısını imkânsız kılacak kadar büyük olmalıdır. Önerilen görüntü şifremizde gizli anahtarın 2^{128} farklı kombinasyonu vardır. Bu 128 bitlik bir şifreleme anahtarı kullanıldığını göstermektedir. Şifrelemede kullanılan maske için başlangıç parametreleri bu anahtar kullanılarak elde edilir. 128 bitlik anahtarın ilk 64 biti X_0, son 64 biti μ parametresini oluşturmak için kullanılır. 128 bitlik bu uzun sayılabilecek anahtar boyutu bir saldırı durumunda şifrenin çözülmesinin zor olacağını gösterir.

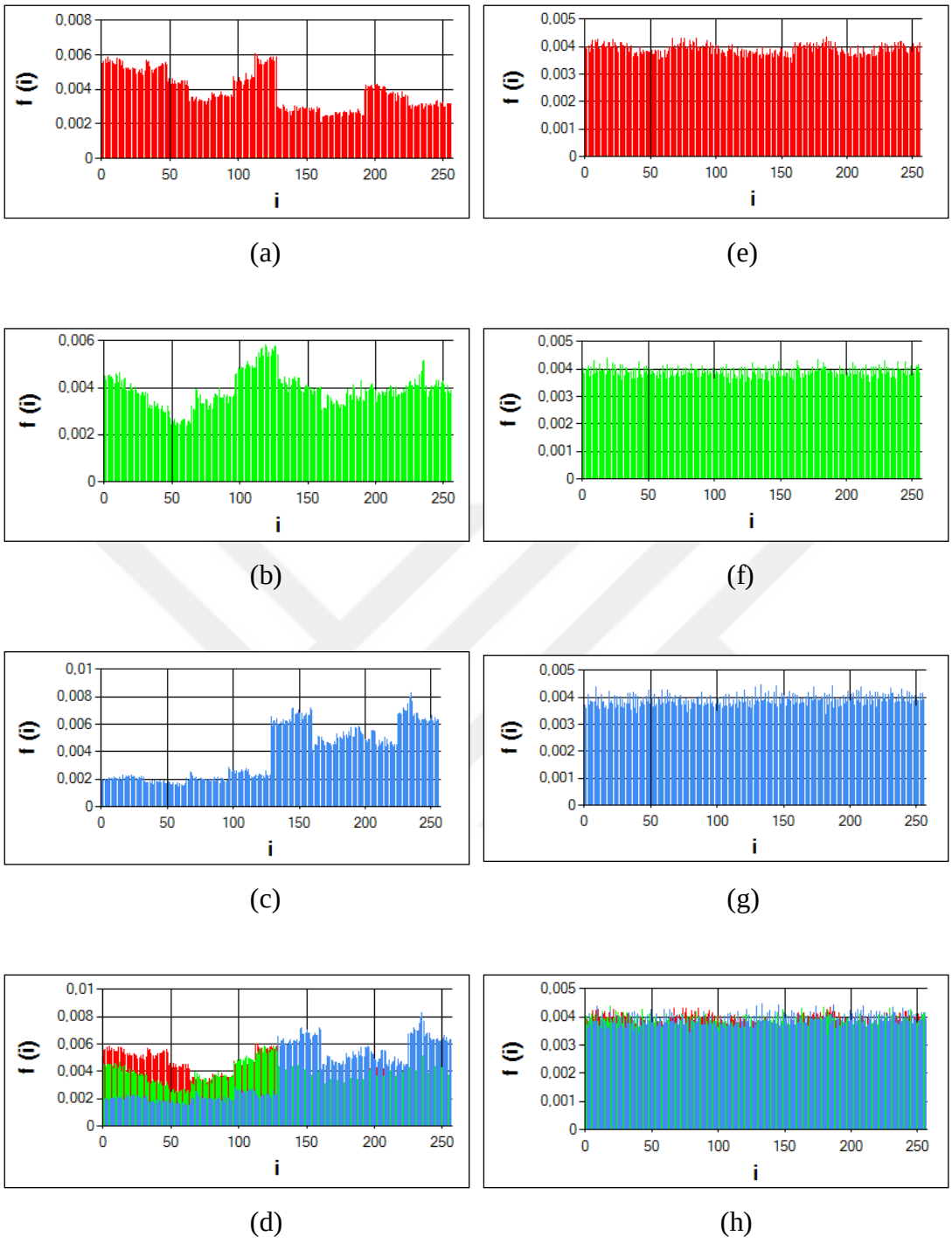
4.2.2. Histogram analizi

Histogram analizi şifrelenecek görüntü ve şifreli görüntünün renk dağılımını içerir. Bir görüntünün histogram grafiği her bir renk yoğunluğundaki piksel sayısının grafiği çizilerek oluşturulur. İdeal şifreleme sisteminde renk yoğunluğu değerleri neredeyse eşit değere sahip olmalıdır. Şekil 4.8'den Şekil 4.14'e Lena, biberler, papağan, kuzey ışıkları, Gazi üniversitesi rektörlük binası, meyveler ve çiçek resimlerinin klasik lojistik harita ve önerilen lojistik harita ile şifrelenmiş hallerinin kırmızı, yeşil, mavi ve hepsinin bir arada

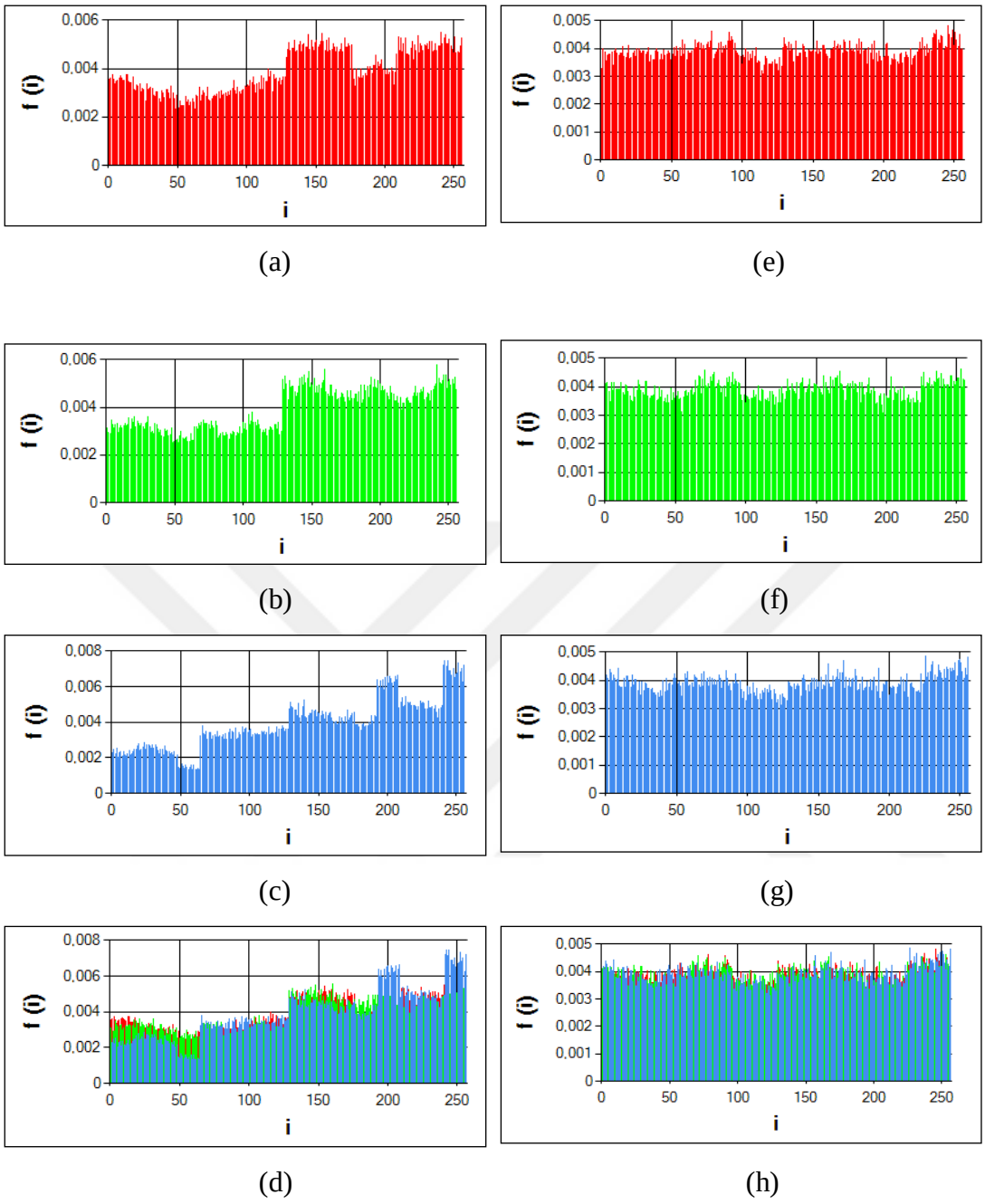
verildiği histogram grafiklerini görülmektedir. Önerilen lojistik harita ile oluşturulan tüm histogram grafiklerinde, güçlü bir şifreleme için önemli bir nokta olan renk yoğunluğu değerlerinin neredeyse eşit dağılıma sahip olduğu görülmektedir.



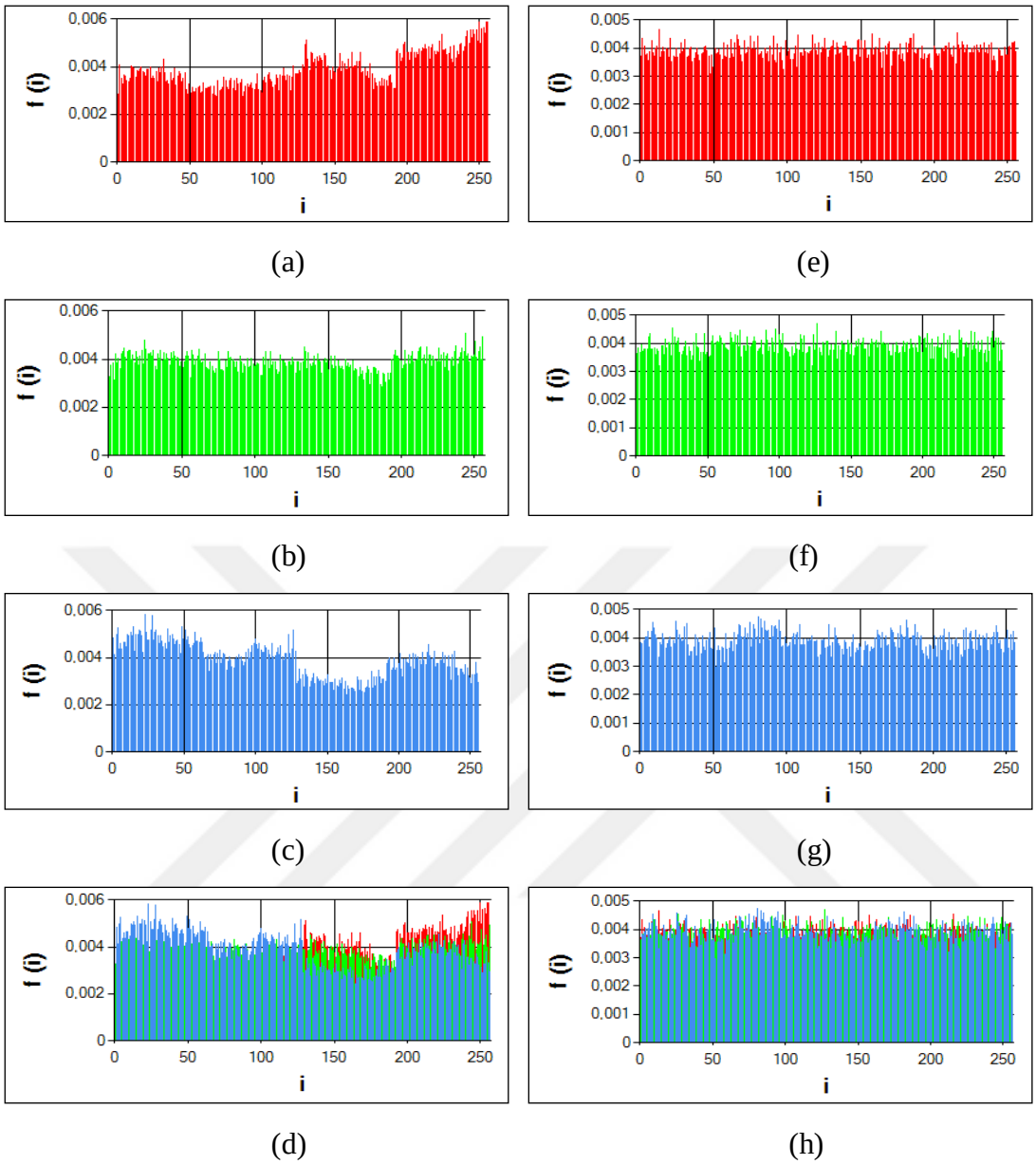
Şekil 4.8. Lena görüntüsünün klasik lojistik harita ile şifrelenmiş halinin histogram analizi (a) kırmızı kanal, (b) yeşil kanal, (c) mavi kanal, (d) tüm kanallar; önerilen lojistik harita ile şifrelenmiş görüntünün histogram analizi (e) kırmızı kanal, (f) yeşil kanal, (g) mavi kanal, (h) tüm kanallar



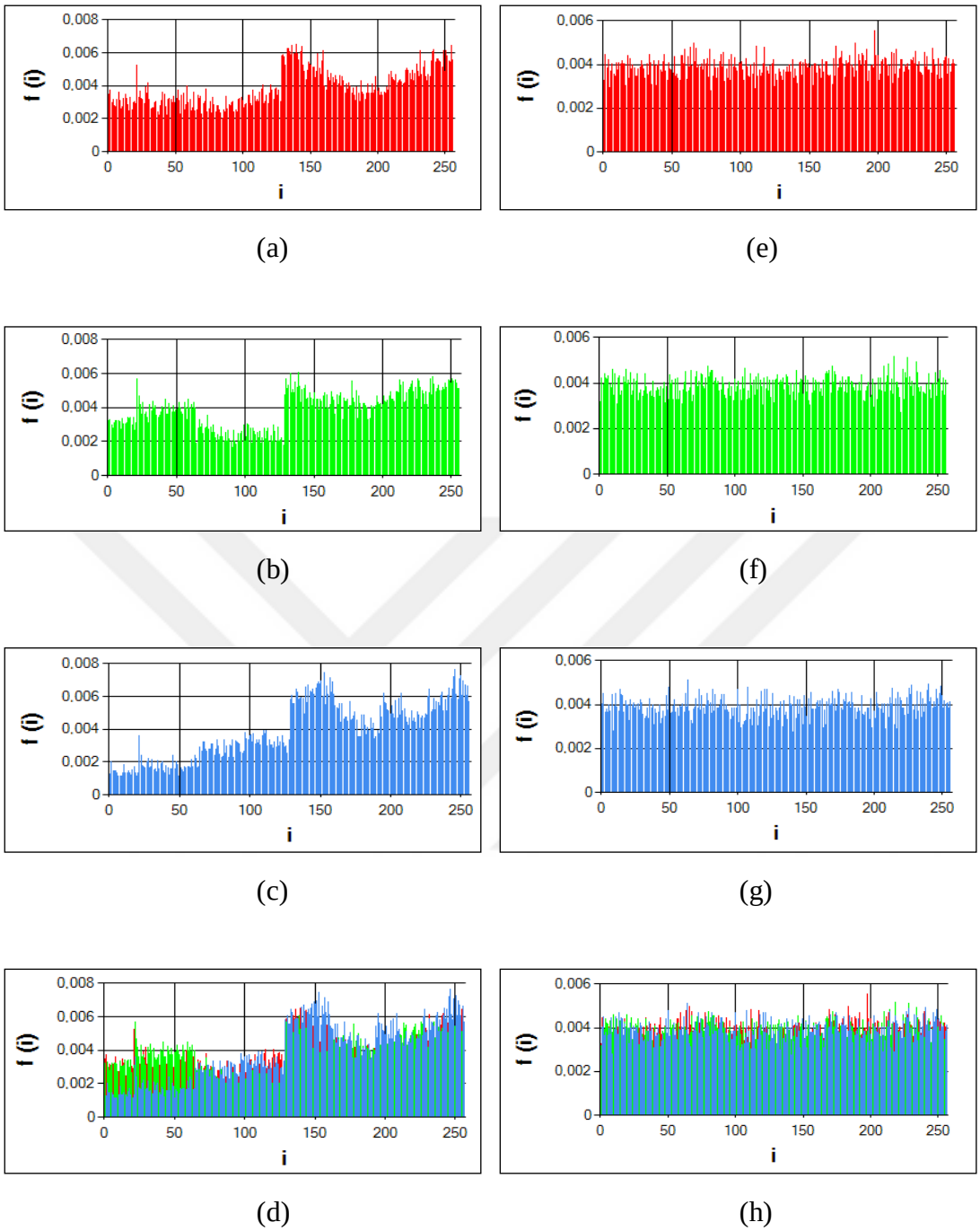
Şekil 4.9. Biberler görüntüsünün klasik lojistik harita ile şifrelenmiş halinin histogram analizi (a) kırmızı kanal, (b) yeşil kanal, (c) mavi kanal, (d) tüm kanallar; önerilen lojistik harita ile şifrelenmiş görüntünün histogram analizi (e) kırmızı kanal, (f) yeşil kanal, (g) mavi kanal, (h) tüm kanallar



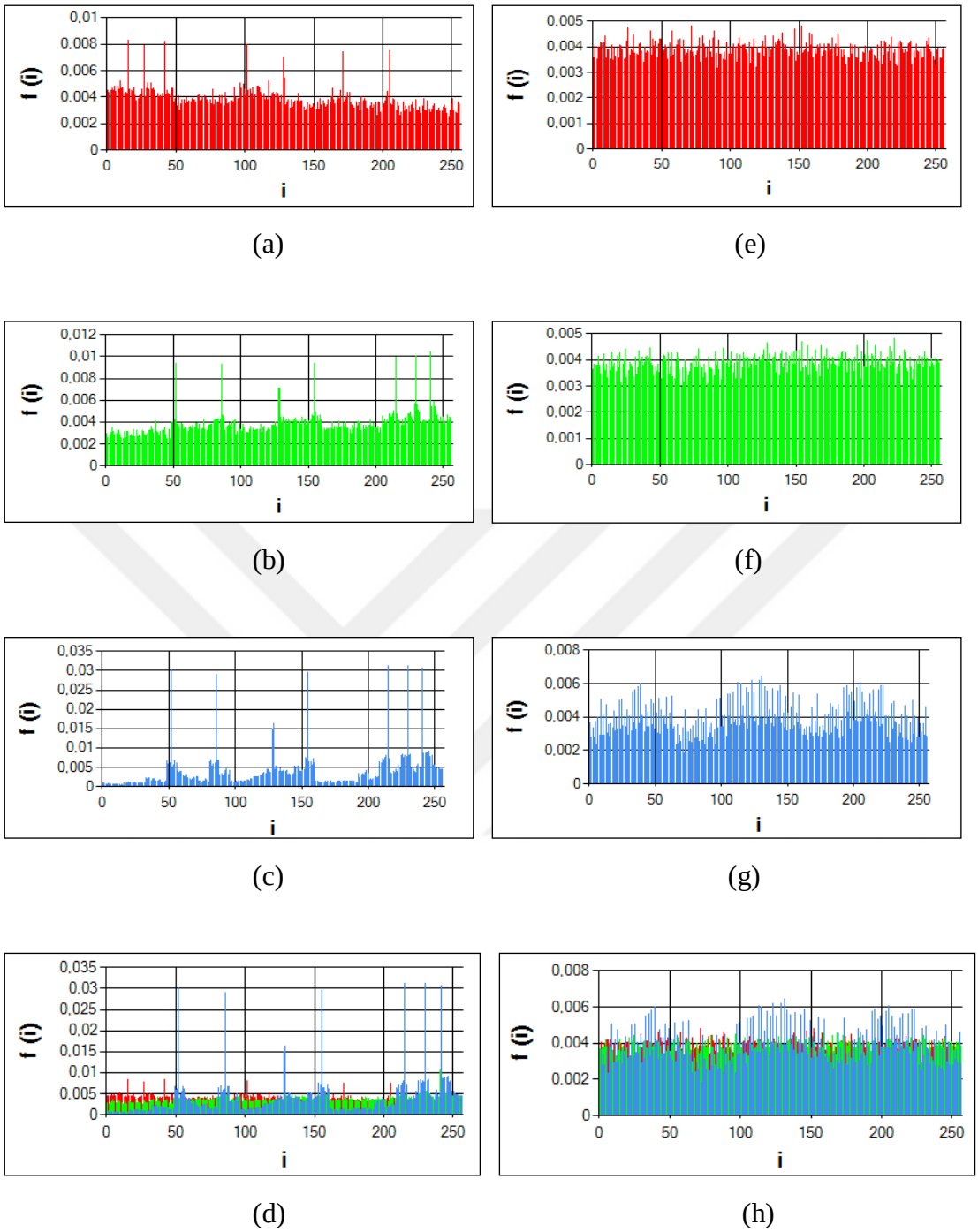
Şekil 4.10. Papağan görüntüsünün klasik lojistik harita ile şifrelenmiş halinin histogram analizi (a) kırmızı kanal, (b) yeşil kanal, (c) mavi kanal, (d) tüm kanallar; önerilen lojistik harita ile şifrelenmiş görüntünün histogram analizi (e) kırmızı kanal, (f) yeşil kanal, (g) mavi kanal, (h) tüm kanallar



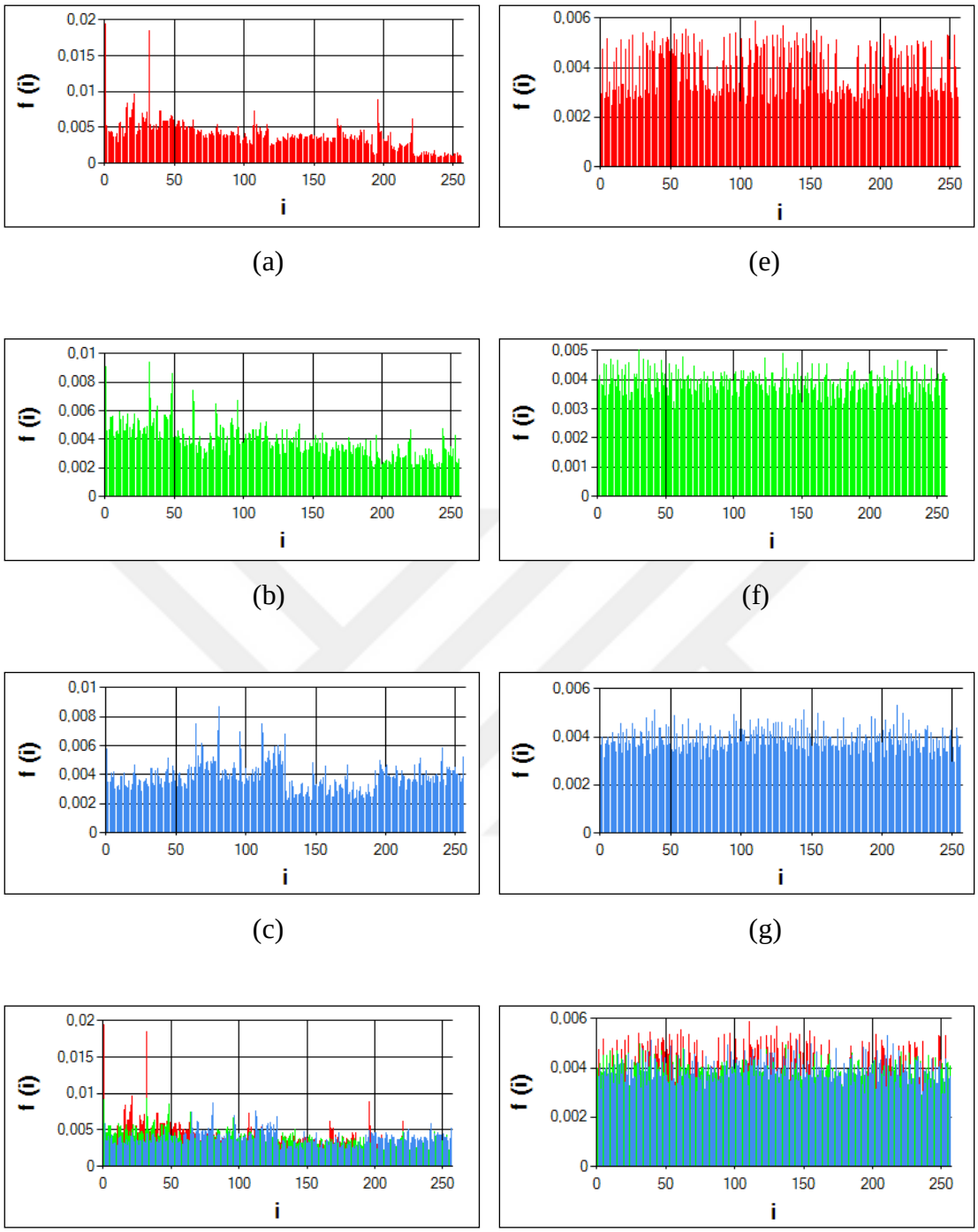
Şekil 4.11. Kuzey ışıkları görüntüsünün klasik lojistik harita ile şifrelenmiş halinin histogram analizi (a) kırmızı kanal, (b) yeşil kanal, (c) mavi kanal, (d) tüm kanallar; önerilen lojistik harita ile şifrelenmiş görüntünün histogram analizi (e) kırmızı kanal, (f) yeşil kanal, (g) mavi kanal, (h) tüm kanallar



Şekil 4.12. Gazi Üniversitesi rektörlük binası görüntüsünün klasik lojistik harita ile şifrelenmiş halinin histogram analizi (a) kırmızı kanal, (b) yeşil kanal, (c) mavi kanal, (d) tüm kanallar; önerilen lojistik harita ile şifrelenmiş görüntünün histogram analizi (e) kırmızı kanal, (f) yeşil kanal, (g) mavi kanal, (h) tüm kanallar



Şekil 4.13. Meyveler görüntüsünün klasik lojistik harita ile şifrelenmiş halinin histogram analizi (a) kırmızı kanal, (b) yeşil kanal, (c) mavi kanal, (d) tüm kanallar; önerilen lojistik harita ile şifrelenmiş görüntünün histogram analizi (e) kırmızı kanal, (f) yeşil kanal, (g) mavi kanal, (h) tüm kanallar



Şekil 4.14. Çiçek görüntüsünün klasik lojistik harita ile şifrelenmiş halinin histogram analizi (a) kırmızı kanal, (b) yeşil kanal, (c) mavi kanal, (d) tüm kanallar; önerilen lojistik harita ile şifrelenmiş görüntünün histogram analizi (e) kırmızı kanal, (f) yeşil kanal, (g) mavi kanal, (h) tüm kanallar

4.2.3. Korelasyon (KR)

Resmin komşu pikselleri arasındaki değerler benzerdir. Şifrelenmiş görüntüye istatistiksel saldırılara karşı dayanıklı olması için komşu pikseller arasındaki bağlantı minimum olmalıdır. Korelasyon, Eş. 4.1.deki formülle hesaplanır.

$$KR = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{4.1}$$

Korelasyon değeri -1 ile +1 arasında değerler alabilir. Değerin pozitif olması iki görüntü arasında pozitif bir ilişkinin olduğunu, negatif bir değer olması ise negatif bir ilişkinin olduğunu gösterir. Algoritmanın saldırılara karşı dirençli olması için yaklaşık sıfır olması gerekir. Çizelge 4.1'de görüldüğü gibi önerilen harita korelasyon değerleri klasik lojistik harita değerine göre sıfıra daha yakın değerler almıştır. Bu önerilen algoritmanın daha güçlü olduğunun bir göstergesidir.

Çizelge 4.1. Klasik lojistik harita ve önerilen lojistik harita ile şifrelenmiş görüntülerin korelasyon değerleri

	Klasik Lojistik Harita				Önerilen Lojistik harita			
Resim	Kırmızı	Yeşil	Mavi	Ortalama	Kırmızı	Yeşil	Mavi	Ortalama
Lena	-0,1123	-0,2319	-0,2063	-0,1835	-0,0076	-0,0298	-0,0287	-0,0220
Biberler	-0,2535	-0,3958	-0,4468	-0,3653	-0,0088	-0,0196	-0,0279	-0,0188
Papağan	-0,3699	-0,3226	-0,3915	-0,3613	-0,0086	-0,0025	-0,0089	-0,0067
Kuzey ışıkları	-0,3112	-0,3521	-0,3479	-0,3371	-0,0069	-0,0070	-0,0054	-0,0064
Gazi Üniv.	-0,3986	-0,3099	-0,4221	-0,3769	-0,0073	-0,0006	-0,0175	-0,0085
Meyveler	-0,1879	-0,2583	-0,3572	-0,3572	-0,0047	-0,0064	-0,0074	-0,0062
Çiçek	-0,2352	-0,3178	-0,4367	-0,3299	-0,0190	-0,0181	-0,0275	-0,0215

4.2.4. Bilgi entropisi analizi (BE)

Şifrelenmiş görüntüde piksellerin rastgele dağılımın bir ölçüsü olan bilgi entropisi BE Eş. 4.2'deki formül ile hesaplanmaktadır.

$$BE = \sum_{i=0}^{2^n-1} p(i) \log_2 \frac{1}{p(i)} \tag{4.2}$$

Burada $p(i)$ her bir pikselin görüntü içinde olma olasılığını temsil etmektedir. BE değeri 8'e yaklaştıkça piksellerin rastgeleliği artmakta ve algoritma daha güvenli hale geldiği değerlendirilmektedir. Çizelge 4.2'de önerilen lojistik harita BE değerlerinin 8'e daha yakın

olduğu görülmektedir. Bu sonuçlar önerilen algoritmanın daha güvenli olduğunu göstermektedir.

Çizelge 4.2. Klasik lojistik harita ve önerilen lojistik harita ile şifrelenmiş görüntülerin bilgi entropisi değerleri

	Klasik Lojistik Harita				Önerilen Lojistik harita			
Resim	Kırmızı	Yeşil	Mavi	Ortalama	Kırmızı	Yeşil	Mavi	Ortalama
Lena	7,9795	7,9881	7,9636	7,9771	7,9969	7,9973	7,9964	7,9968
Biberler	7,97745	7,9877	7,9127	7,959286	7,9966	7,9967	7,9966	7,9967
Papağan	7,9221	7,9259	7,8325	7,8935	7,9980	7,9979	7,9977	7,9979
Kuzey ışıkları	7,9838	7,9962	7,9882	7,9894	7,9961	7,9971	7,9966	7,9966
Gazi Üniv.	7,9618	7,9561	7,8741	7,9307	7,9907	7,9914	7,9914	7,9912
Meyveler	7,9888	7,9830	7,8129	7,9283	7,9955	7,9953	7,9728	7,9879
Çiçek	7,7988	7,9244	7,9445	7,8892	7,9544	7,9923	7,9900	7,9789

4.2.5. Sinyal gürültü oranı (PSNR) ve ortalama karesel hata (MSE) analizi

PSNR, şifrelenmiş görüntüye saldırıdan sonra şifresi çözülen görüntünün kalitesini ölçmek için kullanılır. PSNR değeri ne kadar büyükse şifreli görüntü orijinal görüntüye o kadar yakın demektir ve iyi bir şifreleme sisteminde PSNR değeri oldukça küçük olmalıdır PSNR Eş. 2.13'deki MSE Eş. 2.14'dekiformül ile hesaplanmaktadır.

$$PSNR = 10\,x\log\left(\frac{I_{MAX}}{MSE}\right)(dB) \tag{4.3}$$

$$MSE = \frac{1}{M\,x\,N}\sum_{i=1}^{m}\sum_{i=1}^{n}|C(i,j)-P(i,j)|^2 \tag{4.4}$$

Burada $C(i,j)$ şifreli görüntünün piksel değerlerini ve $P(i,j)$ orijinal görüntünün piksel değerlerini ve I_{MAX} görüntünün maksimum piksel değerini temsil etmektedir.

Güvenli bir sistemde PSNR değeri 8,3875'den küçük olmalıdır. MSE ile iki görüntü arasındaki ortalama hata hesaplanmaktadır. MSE değeri şifreleme sisteminin kalitesi için kritik bir değerdir ve büyük MSE değeri güçlü bir şifreleme sistemi anlamına gelmektedir. MSE değerinin güvenlik ölçütü olarak 9555 ve üzerindeki değerler üzerindeki değerler güvenli olarak kabul edilmektedir. Çizelge 4.3'de PSNR değerini 8,3875'den küçük ve Çizelge 4.4'de MSE değerini 9555 büyük olması önerilen lojistik haritanın güvenli olduğunu göstermektedir.

Çizelge 4.3. Klasik lojistik harita ve önerilen lojistik harita ile şifrelenmiş görüntülerin sinyal gürültü oranı değerleri

	Klasik Lojistik Harita				Önerilen Lojistik harita			
Resim	Kırmızı	Yeşil	Mavi	Ortalama	Kırmızı	Yeşil	Mavi	Ortalama
Lena	7,1728	8,1528	9,7480	8,3579	7,4531	8,24272	9,3801	8,3586
Biberler	8,1230	6,3144	6,4126	6,9500	9,0612	7,6434	7,6957	8,1334
Papağan	6,7654	7,1352	5,7050	6,5352	8,3781	8,6703	7,3592	8,1358
Kuzey ışıkları	7,2418	6,8919	7,5332	7,2225	8,4453	8,1185	8,6214	8,3951
Gazi Üniv.	6,4245	7,4964	5,6987	6,5398	7,9162	8,7787	7,3395	8,0114
Meyveler	6,8801	6,7026	4,3898	5,9908	7,6618	7,5358	5,5744	6,9240
Çiçek	4,8860	6,3185	6,5589	5,9211	6,2754	7,5290	7,7174	7,1739

Çizelge 4.4. Klasik lojistik harita ve önerilen lojistik harita ile şifrelenmiş görüntülerin ortalama karesel hata değerleri

	Klasik Lojistik Harita				Önerilen Lojistik harita			
Resim	Kırmızı	Yeşil	Mavi	Ortalama	Kırmızı	Yeşil	Mavi	Ortalama
Lena	12468,0	9949,3	6890,8	9769,4	11908,5	10095,1	7999,5	10001,0
Biberler	10017,9	15192,6	14853,1	13354,6	8071,5	11187,6	11053,7	10104,3
Papağan	13694,0	12576,4	17481,2	14583,9	9446,4	8831,8	11944,1	10074,1
Kuzey ışıkları	12271,3	13301,1	11473,5	12348,6	9301,3	16028,2	8931,6	9620,4
Gazi Üniv.	14812,5	11572,6	17506,9	14630,7	10506,5	8613,9	11998,5	10373,0
Meyveler	13337,2	13893,7	23664,5	16965,1	11140,2	11468,0	18014,87	13541,0
Çiçek	21109,5	15178,2	14360,9	16882,9	15329,8	11486,2	10998,5	12604,8

4.2.6. Ortalama mutlak hata analizi (MAE)

Ortalama mutlak hata analizi orijinal ve şifreli görüntü arasındaki değişimi gösteren bir analiz yöntemidir. MAE Eş. 2.15'deki formül ile hesaplanmaktadır.

$$MAE = \frac{1}{M\,x\,N} \sum_{i=1}^{m} \sum_{i=1}^{n} | C(i,j) - P(i,j) | \tag{4.5}$$

Burada $C(i,j)$ şifreli görüntünün piksel değerlerini ve $P(i,j)$ orijinal görüntünün piksel değerlerini temsil etmektedir. Güvenlik ve performans kriteri olarak MAE değerinin genellikle

80 ve üzerinde olması şifreleme sisteminin güvenli bir sistem olduğu kabul edilmektedir. Çizelge 4.5'de MAE değerinin 80'den büyük olması önerilen lojistik haritanın güvenli olduğunu göstermektedir.

Çizelge 4.5. Klasik lojistik harita ve önerilen lojistik harita ile şifrelenmiş görüntülerin ortalama mutlak hata değerleri

	Klasik Lojistik Harita				Önerilen Lojistik harita			
Resim	Kırmızı	Yeşil	Mavi	Ortalama	Kırmızı	Yeşil	Mavi	Ortalama
Lena	92,8	82,5	70,6	82,0	88,3	81,3	73,1	80,9
Biberler	87,4	108,0	106,4	100,6	74,3	86,4	85,9	82,5
Papağan	105,1	100,6	120,0	108,6	79,5	77,1	89,3	82,0
Kuzey ışıkları	96,5	100,2	92,9	96,6	80,1	82,8	78,6	80,5
Gazi Üniv.	108,5	95,5	119,0	107,6	83,7	76,4	89,6	83,2
Meyveler	95,8	98,1	134,2	109,3	86,2	87,6	113,2	95,7
Çiçek	128,7	107,5	103,5	113,2	103,3	87,8	86,0	92,3

4.2.7. Şifreleme kalitesi analizi (EQ)

Orijinal görüntü ile şifrelenmiş görüntü arasındaki piksel değerlerindeki toplam değişim şifreleme kalitesi olarak ifade edilmektedir. EQ Eş. 2.16'daki formül ile hesaplanmaktadır.

$$EQ = \frac{1}{256}\sum_{i=0}^{255}\left(H_L(C) - H_L(P)\right)^2 \quad (4.6)$$

Burada $H_L(C)$ şifreli görüntüde her bir pikselin oluşma sayısı ve $H_L(P)$ orijinal görüntüde her bir pikselin oluşma sayısını temsil etmektedir. EQ değerinin güvenlik ölçütü olarak 210'dan büyük olması gerektiği kabul edilmektedir. Çizelge 4.6'de önerilen lojistik harita EQ değerlerinin 210'dan büyük olduğu görülmektedir. Bu sonuçlar önerilen algoritmanın daha güvenli olduğunu göstermektedir.

Çizelge 4.6. Klasik lojistik harita ve önerilen lojistik harita ile şifrelenmiş görüntülerin şifreleme kalitesi değerleri

	Klasik Lojistik Harita				Önerilen Lojistik harita			
Resim	Kırmızı	Yeşil	Mavi	Ortalama	Kırmızı	Yeşil	Mavi	Ortalama
Lena	228,2	158,4	261,4	216,0	220,0	151,0	259,2	210,1
Biberler	225,5	152,4	275,3	217,7	199,6	199,5	247,5	215,5
Papağan	337,6	365,3	485,8	396,3	264,3	282,8	375,2	307,5
Kuzey ışıkları	132,3	62,5	117,5	104,1	249,4	191,5	240,0	227,0
Gazi Üniv.	75,6	87,7	121,6	95,0	202,5	215,9	239,2	219,2
Meyveler	77,9	86,0	303,6	155,9	168,0	172,2	375,1	238,4
Çiçek	442,8	443,4	432,4	439,5	432,8	450,4	445,9	443,0

5. SONUÇ VEÖNERİLER

İnsanlık tarihinin gelişimiyle birlikte kişiler arası iletişimde geçmişten günümüze hızlı bir ilerleyiş sergilemiştir. Günümüzde kişiler arası iletişiminin dijital ortama evrilmesiyle belki konunun en hayati noktası olarak adlandırabileceğimiz güvenlik sorunları çok çeşitli sorunlara yol açabilmektedir. Güvenlik ihtiyacı insanlık tarihi boyunca ihtiyaç duyulan en hayati ihtiyaçlardan biri konumunda bulunmaktadır. Bilgi güvenliğinin sağlanması, kişilerden kurumlara kadar çok geniş bir kitle için hayati öneme sahiptir. Kurumlar için özellikle askeri alanda ve kamu güvenliğinin sağlanması için, bireyler için günümüzde belki de en değerli hazine olarak adlandırabileceğimiz kişisel verilerimizin korunması için önemli bir noktadır. Güvenlik ihtiyaçlarını gidermek için geçmişten günümüze birçok farklı şifreleme uygulaması geliştirilmektedir. Geliştirilen şifreleme algoritmaları içinde bulunan somut olaya göre birbirinden farklılıklar gösterebilmektedir. Geliştirilen tüm algoritmaların çeşitli avantaj ve dezavantajları bulunmaktadır. Bu noktada önemli olan ihtiyaca göre en verimli şifreleme algoritmasını oluşturabilmektir.

Bu tez çalışmasında, permütasyon ve kombinasyon işlemleri ile istatistiksel olarak rastgeleliği artırılmış kaotik lojistik harita ve RC4 şifreleme yöntemine benzer, XOR şifrelemesine dayanan yeni bir görüntü şifreleme ve şifre çözme yöntemi tasarlanmış ve sunulmuştur. Klasik lojistik harita kaotik özellik gösterme bakımından yetersiz olduğu yapılan testler sonucunda görülmüştür ve lojistik harita algoritması üzerinde geliştirmeler yapılmıştır. Yapılan geliştirmelerden sonraki analizlerde hem oluşturulan sayı dizisi hem de maske oluşturup şifreleme işlemi sonrasında yapılan analizlerin sonucunda görülmüştür ki, geliştirilen algoritma klasik lojistik haritaya göre çok daha iyi sonuçlar vermiştir. Bir sahte rastgele sayı üreteç algoritması olan lojistik harita kullanılarak oluşturulan sayılar, istatistiksel olarak güvenilirliğini test edebilmek adına ortalama, varyans ve standart sapma değerlerine bakılmıştır. Oluşturulan sayı dizisini güvenli olarak nitelendirebilmemiz ve kriptolojik uygulamalarda kullanabilmemiz için, varyans ve standart sapma değeri büyük olmalı, ortalama değeri ise 0 ile 256 arasında değerler alabilen piksel değerlerinin ortalaması olan 128 değerine olabildiğince yakın olmalı ve sayılar kullanılarak oluşturulan histogram grafiğinde sayıların neredeyse tüm aralıkta eşit dağılım sergilemelidir. Yapılan testler sonucunda önerilen lojistik harita ile oluşturulan sayıların varyans ve standart sapma değerleri klasik lojistik haritaya göre daha yüksek, ortalama değeri ise 128 değerine daha

yakın ve histogram grafiğinin neredeyse tüm aralıkta eşit dağılım sergilediği görülmüştür. Bu şifreleme sistemi için uygun olduğunun bir göstergesidir.

Kriptolojik uygulamalar geliştirirken karşılaşılan temel problemlerden biri de güvenliği artırırken uygulama hızının düşmesidir. Görüntü gibi yüksek boyutlardaki verileri şifrelemek çok daha fazla zaman gerektirir. Görüntü şifreleme işleminin hızlı bir şekilde gerçekleştirilmesi oldukça önemlidir. Hızlı bir görüntü şifreleme işlemi için asimetrik şifreleme yöntemleri yerine kaosa dayalı güvenli şifreleme yöntemleri ve daha az zaman gerektiren simetrik metotlar tercih edilir. Geliştirilen algoritmada da şifreleme metodu olarak simetrik RC4 şifreleme yöntemine benzer, XOR şifrelemesi kullanılmıştır. Bu sayede Kaotik lojistik harita kullanılarak güvenlik sorunu, simetrik bir algoritma tercih edilerek, şifreleme sistemlerinin iki ana problemi olan hız ve güvenlik sorununa çözüm bulunmuştur.

Permütasyon ve kombinasyon işlemleri ile istatistiksel olarak rastgeleliği artırılmış kaotik lojistik harita ile şifreleme işlemi gerçekleştirildikten sonra şifreleme işlemini test etmek için; anahtar uzay, histogram analizi, korelasyon analizi, bilgi entropisi analizi, sinyal gürültü oranı ve ortalama karesel hata analizi, ortalama mutlak hata analizi ve şifreleme kalitesi analizi gerçekleştirilmiştir. Yapılan analizler sonucunda piksellerin renk yoğunluğu değerinin nerdeyse eşit dağılıma sahip olduğu, korelasyon değerinin yaklaşık 0 olduğu, bilgi entropisi değerinin 8'e daha yakın olduğu, sinyal gürültü oranının 8,3875'den küçük olduğu, ortalama karesel hata değerinin 9555'den büyük olduğu, ortalama mutlak hata değerinin 80'den büyük olduğu, şifreleme kalitesi değerinin 210'dan büyük olduğu görülmüştür. Yapılan tüm istatistiksel ve şifreleme analizlerinde geliştirilen algoritmanın hızlı, sağlam ve tamamen güvenli görüntü şifreleme yöntemi olduğu görülmüştür.

İlerleyen dönemde bu tez üzerinden devam eden çalışmalarda, hız problemine daha iyi çözümler bulunduğu durumlarda, uygulamanın güvenliği artırmak için geliştirilen uygulama da kullanılan tek boyutlu maskenin boyutu artırılabilir. Uygulamaya farklı bir bakış açısı getirmek amacıyla permütasyon ve kombinasyon yöntemlerinden farklı istatistiksel veya matematiksel işlem ve/veya operatörler kullanılabilir. Uygulama da kullanılan permütasyon ve kombinasyon yöntemleri farklı bir sahte rastgele sayı üretici olan haritalar da kullanılarak uygulama geliştirme analizi yapılabilir.

KAYNAKLAR

1. Sağıroğlu, Ş. ve Alkan, M. (2018). *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık.* Ankara: Grafiker Yayınları, 49-83.

2. Yeşilbaş, E. (2016). *Cebirsel kriptoloji yöntemleri ve bazı uygulamaları*. Yayımlanmamış Yüksek Lisans Tezi, Recep Tayyip Erdoğan Üniversitesi, Fen Bilimleri Enstitüsü, Rize.

3. Obaid, Z., Sabonchi, A., ve Akay, B. (2016). Klasik kriptoloji yöntemlerinin karşılaştırılması. *Engineering Sciences*, 11(4), 100-108.

4. Türk, S., ve Şamlı, R. (2020). Yapay sinir ağları ile klasik kriptografi algoritmalarının şifreli veriler üzerinden sınıflandırılması, *Uludağ University Journel of The Faculty of Engineering*, 25(2), 651-664.

5. Rachmawati, D., Budiman, M. A., and Aulya, L. (2018, February). Three-pass protocol scheme for bitmap image security by using vernam cipher algorithm. *In IOP Conference Series: Materials Science and Engineering*, 308(1).

6. Touil, H., El Akkad, N., and Satori, K. (2020, June). Text Encryption: Hybrid cryptographic method using Vigenere and Hill Ciphers. *In 2020 International Conference on Intelligent Systems and Computer Vision (ISCV)* (pp. 1-6). IEEE.

7. Zeebaree, S. R. (2020). DES encryption and decryption algorithm implementation based on FPGA. *Indoneian Journal Electrical Engineering Computer Science,*18(2), 774-781.

8. Yang, C. H., and Chien, Y. S. (2020). FPGA Implementation and Design of a Hybrid Chaos-AES Color Image Encryption Algorithm. *Symmetry,* 12(2), 189.

9. Jiao, K., Ye, G., Dong, Y., Huang, X., and He, J. (2020). Image encryption scheme based on a generalized arnold map and rsa algorithm. *Security and Communication Networks,* 2020.

10. Jindal, P., and Singh, B. (2015). RC4 encryption-A literature survey. Procedia Comp*uter Science,* 46, 697-705.

11. Zhang, Y. (2018). The unified image encryption algorithm based on chaos and cubic S-Box. *Information Sciences,* 450, 361-377.

12. Oğraş, H. (2017). *Kaos tabanlı bir görüntü şifreleme algoritması ve donanımsal ortamda gerçekleştirilmesi.* Doktora Tezi, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elazığ.

13. İkikat, F.Y.(2019). *Renk uzayı dönüşümü ve Lorenz haritaları ile yeni bir görüntü şifreleme algoritması.*Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

14. Güleryüz, H.İ. (2014). *Gri seviye görüntülerde kriptografik uygulamalar. Yüksek Lisans Tezi, Fırat Üniversitesi* , Fen Bilimleri Enstitüsü, Elazığ.

15. Yıldırım, H. M.(2014). Bilgi güvenliği ve kriptoloji. *Uluslararası Adli Bilişim Sempozyumu*, Ankara.

16. Paar, C.(2010).*Understanding Cryptography*.Bochum:Springer, 1-29.

17. Yayık, A.(2013). *Yapay sinir ağı ile kriptoloji uygulamaları.* Yüksek Lisans Tezi, Mustafa Kemal Üniversitesi , Fen Bilimleri Enstitüsü, Hatay.

18. Kodaz, H., ve Botsalı, F. M. (2010). Simetrik ve asimetrik şifreleme algoritmalarının karşılaştırılması. *Selçuk Teknik Dergisi*, 9(1).

19. Obaid, Z. (2016).*Kriptoloji yöntemlerinin karşılaştırılması.* Yüksek Lisans Tezi. Kayseri Erciyes Üniversitesi, Fen Bilimleri Enstitüsü, Kayseri.

20. Topaloğlu, N.,Calp, M. H., ve Türk, B. (2016). Bilgi güvenliği kapsamında yeni bir veri şifreleme algoritması tasarımı ve gerçekleştirilmesi. *Bilişim Teknolojileri Dergisi*, 9(3), 291.

21. Türker, İ. (2018).*BB84 yyöntemi kullanılarak kuantum şifreleme benzetim ortamı geliştirilmesi*. Yüksek Lisans Tezi. Harran Üniversitesi, Fen Bilimleri Enstitüsü, Şanlıurfa.

22. Beşkirli, A., Özdemir, D., ve Beşkirli, M. (2019). Şifreleme yöntemleri ve RSA algoritması üzerine bir inceleme. *Avrupa Bilim ve Teknoloji Dergisi*, özel sayı, 284-291.

23. Çakır, B. (2012).*Akış şifreleme algoritmalarının karşılaştırmalı olarak incelenmesi.* Yüksek Lisans Tezi, Hacettepe Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

24. Yasin, E.T. (2017).*Image encryption based on haar wavelet transformation and RC4 algorithm.* Yüksek Lisans Tezi, Yüzüncü Yıl Üniversitesi , Fen Bilimleri Enstitüsü, Van.

25. Atalay, N. S., Doğan, Ş., Tuncer, T., ve Akbal, E. (2019). İmge şifreleme yöntem ve algoritmaları. *Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi*, 10(3), 815-831.

26. Şahin, F. (2015). Modern blok şifreleme algoritmaları. *İstanbul Aydın Üniversitesi Dergisi*, 7(26), 23-40.

27. Şahin, A., Buluş, E., ve Sakallı, M. T.(2014). Modern blok şifreleme algoritmalarının gücünün incelenmesi. *IDEA*, 8, 8.

28. Karakoç, F. (2008).*Kripto analizde melez bir yöntem: çakışma saldırısı.* Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi , Fen Bilimleri Enstitüsü, İstanbul.

29. Yerlikaya, T.,ve Aslanyürek, C. (2019). RSA algoritmasının şifreleme hızını arttıran algoritmalar ve performansları. *DÜMF Mühendislik Dergisi*, 10(3), 853-862.

30. Yücelen, A. M., Baykal, A., ve Coşkun, C.(2017). Kriptolojide eliptik eğri algoritmasının uygulanması. *Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi*, 8(3), 503-513.

31. Wu, X.,Wang, D., Kurths, J., and Kan, H. (2016). A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system. *Information Sciences*, 349, 137-153.

32. Şekertekin, Y. (2017). *IKEDA ve HENON Kaotik haritaları Kullanarak Görüntü Şifreleme.* Yüksek Lisans Tezi, Van Yüzüncü Yıl Üniversitesi, Fen Bilimleri Enstitüsü, Van.

33. Wu, X., Wang, D., Kurths, J., and Kan, H. (2016). A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system. *Information Sciences*, 349, 137-153.

34. Sakal, H. (2016). *Görüntü şifreleme teknikleri ve bir uygulama tasarımı.* Yüksek lisans Tezi, Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü, Kocaeli.

35. Arpacı, B.(2019). *Güvenli veri iletimi için değiştirilmiş chua devresi yardımıyla tasarlanan renkli görüntü şifreleme sistemi uygulaması* .Yüksek Lisans Tezi, Gazi Üniversitesi , Bilişim Enstitüsü, Ankara.

36. Liu, H.,Wang, X., and Kadir, A. (2014). Chaos-based color image encryption using one-time keys and Choquet fuzzy integral. *International Journal of Nonlinear Sciences and Numerical Simulation*, 15(1), 1-10.

37. Ma, C. W., and Ma, Y. G. (2018). Shannon information entropy in heavy-ion collisions. *Progress in Particle and Nuclear Physics*, 99, 120-158.

38. Norouzi, B., Seyedzadeh, S. M., Mirzakuchaki, S., and Mosavi, M. R. (2015). A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos. *Multimedia Tools and Applications*, 74(3), 781-811.

39. Chai, X., Gan, Z., & Zhang, M. (2017). A fast chaos-based image encryption scheme with a novel plain image-related swapping block permutation and block diffusion. *Multimedia Tools and Applications*, *76*(14), 15561-15585.

40. Wang, W., & Lu, Y. (2018, March). Analysis of the mean absolute error (MAE) and the root mean square error (RMSE) in assessing rounding model. In *IOP conference series: materials science and engineering* (Vol. 324, No. 1, p. 012049). IOP Publishing.

41. Norouzi, B., Mirzakuchaki, S., Seyedzadeh, S. M., & Mosavi, M. R. (2014). A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process. *Multimedia tools and applications*, *71*(3), 1469-1497.

42. Hanköylü, S. (2019). *Kuantum Rastgele Sayı Üreteci Tasarımı ve Uygulaması.* Yüksek Lisans Tezi, Hacettepe Üniversitesi , Fen Bilimleri Enstitüsü, Ankara.

43. Koçdoğan, A. (2015). *Fpga üzerinde hafızalı hücresel otomat yapısı ile rastgele sayı üreteci tasarımı.* Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi , Fen Bilimleri Enstitüsü, İstanbul.

44. Dereli, S. (2020). Yüksek hızlı FPGA ile yeni bir LFSR tabanlı 32-Bit kayan noktalı rastgele sayı üreteci tasarımı. *International Journal of Advances in Engineering and Pure Sciences*, 32(3), 219-228.

45. Yıldız, İ. Y. (2019). *Anahtarlı Boole geri besleme fonksiyonu olan kayan anahtar üreteçleri için gelişmiş saldırı yöntemi*. Yüksek Lisans Tezi, İstanbul Şehir Üniversitesi , Fen Bilimleri Fakültesi, İstanbul.

46. Marsaglia, G. (2003). Xorshift rngs. *Journal of Statistical Software*, 8(14), 1-6.

47. Vigna, S. (2017). Further scramblings of Marsaglia's xorshift generators. *Journal of Computational and Applied Mathematics*, 315, 175-181.

48. Taha, E., ve Turgay, K. (2020). Görüntü Şifreleme için trivium-doğrusal eşlenik üreteci tabanlı bit üretimi. *Fırat Üniversitesi Mühendislik Bilimleri Dergisi*, 32(1), 287-294.

49. Zhang, C. (2010). Period three begins. *Mathematics Magazine*, 83(4), 295-297.

50. Wang, L., and Cheng, H. (2019). Pseudo-random number generator based on logistic chaotic system. *Entropy*, 21(10), 960.

51. Werndl, C. (2020). What are the new implications of chaos for unpredictability?. *The British Journal for the Philosophy of Science*, 60(2009), 195–220.

52. Keleş, C. (2012). *Kaotik haritalar kullanarak görüntü şifreleme.* Doctoral dissertation, Karadeniz Teknik Üniversitesi, Trabzon.

53. Xu, L., Gou, X., Li, Z. and Li, J., A novel chaotic image encryption algorithm using block scramblingand dynamic index based diffusion. *Optics and Lasers in Engineering,* (2017) 91 41-52.

54. Bianco, M. E., & Reed, D. A. (1991). U.S. Patent No. 5,048,086. Washington, DC: U.S. Patent and Trademark Office.

55. Fridrich, J., Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and chaos,* 8(06), 1259-1284.

56. Pareek, N. K., Patidar, V. & Sud, K. K., Image encryption using chaotic logistic map. *Image and vision computing,* 24 (2006), 926-934.

57. Liu, S., Sun, J., Xu, Z., An improved image encryption algorithm based on chaotic system, *Journal of Computers,* 4 (2009) 1091-1100.

58. El Assad, S. and Farajallah, M., A new chaos-based image encryption system, *Signal Processing:Image Communication,* 41 (2016) 144-157.

59. Asgari-Chenaghlu, M., Balafar, M. A., &Feizi-Derakhshi, M. R. (2019). A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation. *Signal Processing,* 157, 1-13.

60. Babu, M., Devi, G. S., Krishna, M. Y., Prasanna, M. V., &Iswarya, N. (2020). Image Encryption Using Chaotic Maps and DNA Encoding. *Jornal of Xidian University,* 14(4).

61. Muñoz-Guillermo, M. (2021). Image encryption using q-deformed logistic map. *Information Sciences*, 552, 352-364.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı :UZUN, Ali
Uyruğu :T.C.

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Yüksek lisans	Gazi Üniversitesi/Adli Bilişim	Devam ediyor
Lisans	Gazi Üniversitesi/Elektrik-Elektronik Müh.	2018
Lise	Ersin Bacaksız Anadolu Lisesi	2014

İş Deneyimi

Yıl	Yer	Görev
2021 Eylül-2022 Mart	ATEL Tek. ve Sav. A.Ş	Satış mühendisi
2022 Mart-Halen	Rekabet Kurumu	Rekabet uzman yardımcısı

Yabancı Dil

İngilizce

Tezden Üretilen Yayınlar

1. Uzun, A. ve Sayan, H. H. (Aralık, 2021). Mask Based Image Encryption Using Chaotic Logistic Map. *International Conference on Informatics and Computer Science* (pp.102-108). (Tezden üretilmiştir.)

Hobiler

Film izlemek, yürüyüş yapmak, yemek yapmak.



GAZİLİ OLMAK AYRICALIKTIR..