**BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ**

**Fen Bilimleri Enstitüsü**
**Bilgisayar Mühendisliği Anabilim Dalı**

# KAOTİK SİSTEM TABANLI GÖRÜNTÜ ŞİFRELEME

**Sefa TUNÇER**
**Yüksek Lisans Tezi**

**Tez Danışmanı**
**Doç. Dr. Cihan KARAKUZU**

**BİLECİK, 2016**

**Ref.No:10120213**

**BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ**

**Fen Bilimleri Enstitüsü**
**Bilgisayar Mühendisliği Anabilim Dalı**

# KAOTİK SİSTEM TABANLI GÖRÜNTÜ ŞİFRELEME

**Sefa TUNÇER**
**Yüksek Lisans Tezi**

**Tez Danışmanı**
**Doç. Dr. Cihan KARAKUZU**

**BİLECİK, 2016**

**BILECIK SEYH EDEBALI UNIVERSITY**

**Institute of Sciences**
**Department of Computer Engineering**

# IMAGE ENCRYPTION BASED ON CHAOTIC SYSTEM

**Sefa TUNÇER**
**Master's Thesis**

**Thesis Advisor**
**Assoc. Prof. Cihan KARAKUZU**

**BILECIK, 2016**

**BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ**

**FEN BİLİMLERİ ENSTİTÜSÜ**

**YÜKSEK LİSANS**
**JÜRİ ONAY FORMU**

Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulunun 22/06/2016 tarih ve 33 sayılı kararıyla oluşturulan jüri tarafından 14/07/2016 tarihinde tez savunma sınavı yapılan Sefa TUNÇER'in "KAOTİK SİSTEM TABANLI GÖRÜNTÜ ŞİFRELEME" başlıklı tez çalışması Bilgisayar Mühendisliği Anabilim Dalında YÜKSEK LİSANS tezi olarak oy birliği/ ~~oy çokluğu~~ ile kabul edilmiştir.

**JÜRİ**

**ÜYE**
**(TEZ DANIŞMANI) : Doç. Dr. Cihan KARAKUZU**

**ÜYE : Doç. Dr. Alpaslan DUYSAK**

**ÜYE : Yrd. Doç. Dr. Fuat KARAKAYA**

**BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI BAŞKANI:**
**Doç. Dr. Cihan KARAKUZU**

**ONAY**

Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulunun …./…./…..... tarih ve ……/…… sayılı kararı.

İMZA/ MÜHÜR

## TEŞEKKÜR

Bu tez çalışmasında asimetrik şifreleme, görüntü steganografi, kaotik sistemler, kaotik nöral ağ tabanlı görüntü şifreleme ve 3B kaotik cat map tabanlı görüntü şifreleme konuları ele alınmıştır. Ayrıca yapılan çalışmaların güvenliğini test etmek amacıyla analiz yöntemleri uygulanmıştır.

Çalışmalardan elde edilen tecrübeler ve bilgiler ışığında bilgi şifreleme ve gizleme gibi çalışmaların günümüzde önemli bir yer edindiği ve gelecekte önemini giderek artıracağı görülmektedir.

Tez çalışmamın planlanmasında, araştırılmasında, yürütülmesinde ve oluşumunda ilgi ve desteğini esirgemeyen, engin bilgi ve tecrübelerinden yararlandığım, yönlendirme ve bilgilendirmeleriyle çalışmamı bilimsel temeller ışığında şekillendiren sayın hocam Doç. Dr. Cihan KARAKUZU ’ya sonsuz teşekkürlerimi sunarım.

Maddi ve manevi olarak desteklerini esirgemeyen anne babama ve üzerimde emeği olan herkese ayrıca teşekkürlerimi sunarım.

Sefa TUNÇER

Haziran 2016

# ÖZET

Günümüzde teknolojinin gelişmesiyle birlikte bilgiyi gizleme ve şifreleme önemli bir hale gelmiştir. Bir gizleme sanatı olan steganografi bilginin varlığının fark edilmemesini, kriptografi bilginin şifrelenerek korunmasını amaçlamaktadır. Bu çalışmada bilgi güvenliği açısından önemli olan görüntü steganografi ve kaotik sistem tabanlı görüntü şifreleme uygulamaları gerçekleştirilmiştir.

Çalışmanın başlangıç kısmında, görüntü steganografi, LSB ve L3B yöntemleri kullanılarak iki farklı şekilde gerçekleştirilmiştir. Düz metin, RSA asimetrik şifreleme algoritması ile şifrelendikten sonra görüntüye gizlenmiştir. LSB ve L3B yöntemlerinin üstünlükleri, sakıncaları ve görüntüde meydana getirdiği değişiklikler ile ilgili analizler yapılmıştır.

Çalışmanın ikinci kısmında, görüntü şifrelemede kullanılan kaotik sistemlerin iki ve üç boyutlu faz portreleri ve zaman düzleminde oluşturduğu kaotik zaman serileri incelenmiştir. Kaotik sistemlerin davranışlarının incelenmesinin ardından kaotik nöral ağ (KNA) tabanlı 24 bit RGB ve 3B KCM tabanlı gri seviye görüntü şifreleme uygulamaları gerçekleştirilmiştir. Bu algoritmalarda görüntüyü karıştırma, anahtar oluşturma vb. işlemler için 1, 2 ve 3 boyutlu kaotik sistemler kullanılmıştır. Şifreleme algoritmalarının güvenlik ve başarım analizleri yapılmıştır. KNA ve KCM tabanlı görüntü şifreleme algoritmaların yüksek başarıma sahip olduğu gözlenmiştir.

**Anahtar Kelimeler**

Görüntü steganografi; Kaotik sistemler; Kaotik tabanlı görüntü şifreleme; Kaotik nöral ağ; 3B kaotik Cat Map; Güvenlik ve başarım analizleri.

## ABSTRACT

Nowadays, information hiding and encryption has become important with the developing technology. Steganography which is an art of hiding ensures undetection of the existence of information, meanwhile cryptography aims protection by encrypting a document. In this study, image steganography, important for information security and image encryption application based on chaotic system have been performed.

In the starting part of the study, image steganography carried out with two different ways using LSB and L3B methods. A plain text is hidden into the image after it is encrypted by RSA asymmetric encryption. Analysis are performed about advantages and disadvantages of LSB and L3B methods and changes caused in the image.

In the second part of the study, two and three-dimensional phase portraits and chaotic time series of chaotic systems that is used in image encryption has been investigated. After the investigation of chaotic systems behavior, chaotic neural network based 24-bit RGB and 3D KCM based gray level image encryption applications are performed. In these algorithms, 1D, 2D and 3D chaotic systems are used for image shuffling, key generation, etc. Security and performance analysis of encryption algorithms have been performed. It is observed that image encryption algorithms based on KNA and KCM have superior performances.



**Key Words**

Image steganography; Chaotic systems; Image encryption based on chaotic; Chaotic neural network, 3D chaotic Cat Map; Security and performance analysis.

# İÇİNDEKİLER

# ŞEKİLLER DİZİNİ

**Sayfa No**

# ÇİZELGELER DİZİNİ

**Sayfa No**

# SİMGELER VE KISALTMALAR

**Simgeler**

| | |
|---|---|
| $p$ | : RSA'da bir asal sayı |
| $q$ | : RSA'da bir asal sayı |
| $n$ | : Açık ve gizli anahtar için mod değeri |
| $\vartheta(n)$ | : Totient değeri |
| $m$ | : Düz mesaj |
| $c$ | : Şifreli mesaj |
| $f()$ | : Fonksiyon |
| $g()$ | : Fonksiyon |
| $t$ | : Zaman |
| $x_n$ | : Cat Map uygulanan görüntünün *n.* değeri |
| $x_{n+1}$ | : Cat Map uygulanan görüntünün *(n+1).* değeri |
| $a_x$ | : Cat Map parametresi |
| $x(t)$ | : x'in t. zamandaki değeri |
| $N_0$ | : İterasyon sayısı |
| arg(max) | : Bir dizi elemanın en büyüğünün indisi |
| $W_{cl}$ | : Permütasyon ağ katmanı ağırlık matrisi |
| $W_{dl}$ | : Kaotik nöral ağın ağırlık matrisi |
| $B_{cl}$ | : Kaotik nöral ağ bias vektörü |
| $A_l$ | : Kaotik nöral ağın bias matrisi |
| $B_{dl}$ | : Kaotik nöral ağın bias matrisi |
| $XOR$ | : Özel veya |
| $S$ | : Şifreli görüntü |
| $k_{xy}$ | : Korelasyon katsayısı |
| $d(x)$ | : Varyans |
| $e(x)$ | : Ortalama değer |
| $kb/s$ | : Kilobayt/saniye |
| $L_g$ | : Kaotik Logistic Map başlangıç değeri |
| $\varphi(i)$ | : Kaotik Logistic Map sayısal değeri |
| $I(i)$ | : Görüntünün i. piksel değeri |
| $E(i)$ | : Şifrelenmiş görüntünün i. piksel değeri |

$z_{100}$ : Chen kaotik sistemi 100. İterasyon değeri

**Kısaltmalar**

| | |
|---|---|
| LSB | : En anlamsız bit |
| L3B | : En anlamsız üç bit |
| YSA | : Yapay sinir ağları |
| 2B | : 2 boyutlu |
| 3B | : 3 boyutlu |
| RGB | : Kırmızı, yeşil, mavi renk tonları |
| R | : Kırmızı renk tonu |
| G | : Yeşil renk tonu |
| B | : Mavi renk tonu |
| KNA | : Kaotik nöral ağ |
| PAK | : Permütasyon ağ katmanı |
| KAK | : Kaotik ağ katmanı |
| KCM | : Kaotik Cat Map |
| JPEG | : Görüntü dosyası uzantısı (Joint Photographic Experts Group) |
| AES | : Simetrik şifreleme algoritması (Advanced Encryption Standard) |

# 1. GİRİŞ

Kriptoloji, saklanması veya gönderilmesi gereken mesajların, bilgilerin bir anahtarla belli bir sisteme göre şifrelenmesi, şifrelenen mesajın anahtarı kullanılarak alıcı tarafından deşifre edilmesidir. Kısaca şifre bilimine kriptoloji denilmektedir. Kriptografi ve kripto analiz olmak üzere iki dala ayrılır. Günümüzde teknoloji çok hızlı geliştiğinden güvenlik sorunlarını da beraberinde getirmektedir. Özel şirketler, askeri kurumlar, devlet kurumları vb. birçok birim arasındaki iletişimin güvenliğini sağlamak için kriptoloji alanındaki gelişmeler büyük önem arz etmektedir. Bu amaçla güvenlik zafiyetlerini engellemek ve bunu yaparken hızlı iletişimi de sağlamak amacıyla birçok kriptografik yöntem geliştirilmektedir.

Kriptografik algoritmalar gizlilik, bütünlük, süreklilik, kimlik denetimi, inkar edilememezlik ve izlenebilirlik gibi güvenlik protokollerinin bileşenleri haberleşmede güvenliğini sağlamak amacıyla kullanılırlar (Yıldırım, 2014). Kriptografik sistemler simetrik anahtarlı, asimetrik anahtarlı olmak üzere ikiye ayrılır, fakat anahtarsız şifreleme sistemleri de mevcuttur. Simetrik sistemlerde bir gizli anahtar mevcuttur, bu anahtarın gönderici ve alıcı tarafta bulunması gerekmektedir. Asimetrik sistemlerde gizli bir anahtara ek olarak, açık anahtar mevcuttur. Bu sistemlerde açık anahtar ve gizli anahtarın ikisi ele geçirildiğinde şifre çözme işlemini yapmak mümkündür. Bu sayede, açık anahtarın üçüncü bir şahıs tarafından ele geçirilmesi şifrelenen bilgilerin ele geçirilmesi açısından bir tehdit oluşturmamaktadır.

Asimetrik şifreleme yöntemlerinden biri olan RSA algoritması, 1978 yılında Ronald Rivest, Adi Shamir, Leonard Adleman tarafından bulunmuştur. RSA kriptosisteminde, herkes tarafından bilinen bir anahtar ve göndericinin bir yöntemle şifrelediği bir bilgi vardır. Gizli anahtarın gönderici ve alıcı tarafın her ikisinde de bulunmasına gerek yoktur. Sadece alıcı tarafta bulunması yeterlidir. Bu sistem özellikle dijital imza sistemlerinde olmak üzere gizliliğin sağlanması gereken yerlerde kullanılmaktadır. Sistemin güvenliği tamsayıları çarpanlara ayırmanın zorluğuna dayanmaktadır (Kriptolojiye Giriş Ders Notları, 2004).

Kriptoloji biliminin yanı sıra steganografi bilimi de önemli konulardan biridir. Steganografi, bir veriyi başka bir verinin içine gizleyen ve gizlenen bu verinin fark edilmesini engellemeyi amaçlayan bilim dalıdır. Latince 'steganos' ve 'graph' kelimelerinin birleşimi olan steganografi gizlenmiş yazı anlamına gelir. Steganografi var olan bilgiyi değiştirmeden gizlenerek başka bir verinin içinde istenen noktaya ulaştırmayı amaçlar, kriptografi veriyi şifreleyerek istenen noktaya ulaştırmayı amaçlar. Steganografinin aksine kriptografide verinin şifreli olduğunun fark edilmesi bir önem teşkil etmemektedir.

Steganografide gizli mesajın saklandığı veriye örtü verisi denilmektedir. Örtü verisi, gizli mesajın içine gömülmesiyle fark edilemeyecek miktarda bozulur. Bu açıdan bakıldığında steganografi ile karıştırılan yöntemlerden biri de sayısal damgalamadır. Steganografinin aksine, sayısal damgalama uygulamalarında örtü verisi genelde bozulmaz ve örtü verisinin bir parçası olarak saklanır (Kurtuldu ve Arıca, 2009). Steganografi, dilbilim ve teknik olmak üzere ikiye ayrılmaktadır. Dilbilim steganografide taşıyıcı birim bir metindir. Teknik steganografide ise görünmez mürekkep, gizli yerler ve bilgisayar tabanlı yöntemler bulunmaktadır. Burada çalışma için önem teşkil eden kısım bilgisayar tabanlı olan yöntemlerdir. Bunlar metin, ses ve görüntü dosyalarına veri gizleme yöntemleridir. Gizlenecek olan veri sayısal olarak ifade edilebilen metin, ses, görüntü, video vb. olabilmektedir (Badem ve Güneş, 2011).

Steganografide en basit yöntemlerden biri en anlamsız bite gizleme (LSB) yöntemidir. 24 bitlik görüntü kırmızı, yeşil ve mavi renk tonlarının karışımından meydana gelmektedir. Böyle bir görüntüye gizleme yapılacağı düşünüldüğünde 3 bayttan oluşan her piksele 3 bit veri gizlenebilmektedir. Yani 1 bayt (8 bit) veri içine LSB yöntemi ile 1 bit veri gizlenebilmektedir. Piksellere gizlenen veri boyutu artırılırsa fark edilir derecede bozulmalara yol açacaktır ve güvenlik açısından zafiyet oluşturacaktır.

Literatürde görüntü steganografi yöntemlerinden en çok kullanılanı LSB yöntemidir. Bu yüzden bu yönteme karşı yapılan ataklar oldukça fazladır. Görüntüye gizlenen bit sayısını tespit etmek ve bir görüntüye gömülebilecek bilgi boyutunu artırabilmek amacıyla yapılan çeşitli analizler mevcuttur (Chandramouli ve Memon 2001; Thangadurai ve Devi, 2014).

Kaos teorisi sonuçları tahmin edilemeyen sistemleri açıklayan bilimsel bir ilkedir. Genel anlamda 1980'li yıllarda araştırılmıştır. Bir sigara dumanının havada yaptığı şekiller düzensiz ve bağımsız değildir. Sigaranın bu dinamikleri ortamdaki birçok etkene ve parametreye bağlıdır. Ancak bu parametre ve bilgiler çok fazladır ve bunları inceleyip net olarak bir kanıya varmak imkansızdır. Sigara dumanının şeklini bulunulan ortamdaki rüzgar, sıcaklık, basınç gibi fiziksel büyüklükler etkileyebilir ve bu faktörlerin birbirine bağlı olabileceği de hesaba katıldığında durum tahmin edilemeyen bir hale gelir (Bodur, 15.03.2016; Wikipedia, 15.03.2016).

Kaosun aslında hayatın her safhasında yer aldığı ve zincirleme olarak hayatta var olan tüm olguların birbirini zincirleme etkilediği düşünülmektedir. İlk olarak 1963 yılında hava durumu deterministik periyodik olmayan akışlarla ifade edilmeye çalışılmıştır (Lorenz, 1963). Bu hesaplarda ilk olarak 0,506127 ondalık sayısı kullanılmıştır ve daha sonra 0,506 sayısı sisteme giriş olarak verilmiştir. Seçilen bu iki sayı arasında binde bir oranında bir fark olmasına rağmen elde edilen sonuçlar arasında çok büyük farklılık meydana gelmiştir. 1972 yılında kaotik sistemlerin ortaya çıkmasında etkili olan Edward Lorenz'in ortaya attığı kelebek etkisi teorisine göre Afrika'da kanat çırpan bir kelebeğin, Amerika'da fırtına oluşturabileceği belirtilmiştir. Kelebek etkisi, bir sistemdeki başlangıç verilerinin çok küçük miktardaki değişimi sonucu, tahmin edilemeyen ve çok büyük değişikliklerin meydana gelmesi olarak tanımlanmıştır (Gizli İlimler Kütüphanesi, 20.02.2016).

Kaotik sistemlerin belirli bir frekans aralığında bulunduğu ve bu sınırlar içerisinde hareketlerinin belirlenemez olduğu Lorenz tarafından saptanmıştır. Kaotik sistemleri, belirli bir alana çeken bu yapılara kaotik çekerler adı verilmektedir. Bu çekerlere bakıldığında bu çekerleri meydana getiren eğrilerin, belirli sayıdaki parametreler dizisinin, zaman düzleminde hiçbir zaman iki kez aynı rotayı izlemediği ve bu rotalar arasında kesinlikle küçük de olsa bir farklılık olduğu görülmüştür. Çekerlerin oluşturduğu eğrilerin bu özelliğinden dolayı fraktal yapıda olduğu söylenebilir (Bodur, 15.03.2016).

Kaotik sistemler görüntü şifreleme uygulamalarında oldukça yoğun kullanılmaktadır. Bilinen kaotik sistemlerin kullanıldığı (Bigdeli, vd. 2012) ve (Chen, vd., 2004) 'de başarım ve güvenlik bakımından oldukça iyi sonuçlar elde edildiği

görülmektedir. Ayrıca birden fazla kaotik sistem kullanılması, bu sistemlerin başlangıç değerlerine hassas bağlılığı ve şifrelemede kullanılan parametrelerin fazla olması güvenlik seviyesini oldukça artırmaktadır. Bu sayede şifrelenen görüntünün istenmeyen şahıslar tarafından ele geçirilmesi, şifrelemede kullanılan parametreleri bilmediği takdirde, neredeyse imkansız hale gelmektedir.

Kaotik sistemler, ayrık zamanlı ve sürekli zamanlı olmak üzere ikiye ayrılmaktadır. Diferansiyel denklemlerden meydana gelen kaotik sistemlerin boyutu, yani denklem sayısı arttıkça, parametrelerin ve başlangıç değerlerinin sayısı da artmaktadır (Akgül, 2015; Dalkıran ve Danışman, 2010). Artan parametre ve başlangıç değerlerine bağlı olarak bilinmeyen değişken sayısını da artıracaktır. Şifreleme ve şifre çözme işlemlerinde kullanılan kaotik sistemlerde bilinmeyen değerlerin fazla olması üçüncü bir şahıs tarafından anahtarın veya şifrelenen bilgilerin ele geçirilmesini çok zor hale getirecektir. Ayrıca, parametreler ve başlangıç değerlerinin algoritmada kullanıldığı yerler de önemlidir. Denklem sayısı şifrelemede karıştırma ve yayılma özelliklerini artırır, fakat şifreleme hızını negatif yönde etkileyebilir (Akgül, 2015). Ayrıca Akgül (2015), veri güvenliği ve kriptoloji gibi alanlarda yeni olan karmaşık kaotik sistemlerin kullanılmasının çok daha önemli olduğunu vurgulamaktadır.

Görüntü şifrelemede kaotik sistemlerin kullanılması, sağladığı bazı üstünlüklerden ve analiz yöntemlerine karşı gösterdiği yüksek dayanıklılıktan kaynaklanmaktadır. Bu analizler anahtar güvenliği, histogram analizi, anahtar hassaslığı, görüntüdeki bitişik piksellerin birbiri ile olan ilişki katsayısı, bilginin düzensizlik analizi, şifreleme ve şifre çözme hızıdır. Bu sayede, yapılan her analize karşı doğrudan daha başarılı olduğu söylenemese de, genel anlamda kullanılan geleneksel simetrik ve asimetrik şifreleme algoritmalarına karşı üstünlük sağladığı görülmektedir.

YSA, insan beyninin yapısı temel alınarak modellenen biyolojik ağların ilkel modelleri olarak tanımlanabilir. YSA 1943 yılında gelişmeye başlamıştır. Bu tarihte ilk sinir hücresi modeli McCulloch ve Pitts tarafından geliştirilmiştir. Gerçekte fiziksel sistemlerin doğrusal olmayan davranışlar sergilemesi, fizik kurallarını kullanarak bu sistemleri modellemeyi mümkün kılmamaktadır. YSA, doğrusal olmayan bir modeli sınırlı sayıdaki örneklerden öğrenebilir ve genellikle başarılı sonuçlar verir (Karakuzu,

2016). Bu çalışmada YSA, kaotik nöral ağ tabanlı görüntü şifreleme ve şifre çözme kısmında kullanılmıştır. Kaotik nöral ağ ile YSA benzerdir, fakat birbirinden farklı yapıdadırlar. Kaotik nöral ağ yapısında iterasyon vardır ve giriş değerleri her iterasyonda değişmektedir, fakat YSA'daki gibi ağırlık güncelleme mevcut değildir. Çalışmada kullanılan ağırlıklar, kaotik sistemler kullanılarak üretilen anahtar ile belirlenmektedir ve tüm iterasyonlarda sabittir. Dalkıran ve Danışman (2010), kriptoloji açısından kaotik sistemlerin senkronizasyonu ve parametrelerinin az olması gibi özelliklerinin ciddi sorunlara sebep olacağını belirtmişlerdir. YSA'da bulunan deneyimlere bağlı öğrenme, az bir veriden genelleme yapabilme, girişler ve çıkışlar arasında doğrusal olmayan bir ilişki olması gibi özellikler kaotik sistemlerin bu sakıncasını ortadan kaldırmaya yöneliktir (Karakuzu, 2016; Çayıroğlu, 2016). Bizim çalışmamızda bu eksiklikler kullanılan kaotik sistemlerin sayısını artırarak giderilmeye çalışılmıştır. Bu tez çalışmasında birden fazla sürekli zamanlı ve ayrık zamanlı kaotik sistem kullanılmıştır. Şifreleme anahtarı kaotik sistemlere giriş olarak uygulandığından, parametre sayısının fazla olması anahtar boyutunu da aynı oranda artıracaktır. Anahtar şifrelemede kullanılan en önemli unsurlardan biri olması nedeniyle, boyutunun artmasıyla birlikte yapılan saldırılara karşı daha güçlü bir algoritma elde edilecektir.

Bu tezde, öncelikle asimetrik şifreleme algoritmasıyla şifrelenen bir metnin görüntü dosyasına gizlenmesi, yani görüntü steganografi uygulaması gerçekleştirilmiştir. Öncelikle metinsel bir veri RSA asimetrik şifreleme algoritması ile şifrelenmiştir. Ardından şifrelenen bu metin görüntü dosyasına LSB veya L3B yöntemlerinden biri tercih edilerek gizlenmiştir. Gizli metnin bulunduğu stego görüntünün renk tonlarında meydana gelen değişikliklerin insan gözüyle fark edilebilirliği ve histogram değerleri incelenmiştir. Görüntü steganografi yöntemlerinin üstünlükleri ve sakıncaları, görüntü dosyasında gizli olan verinin fark edilebilirliği gibi unsurlar tartışılmıştır.

Ardından görüntü şifrelemede kullanılacak olan kaotik sistemlerin çalışma yapıları incelenmiştir. Ayrık zamanlı ve sürekli zamanlı olarak ayrılan bu sistemler doğru yerde kullanıldığında büyük avantajlar sağlamaktadır. Saldırılara karşı daha güçlü olan sürekli zamanlı sistemler daha çok tercih edilmektedir. Güçlü olmasının sebebi parametrelerinin ve başlangıç değerlerinin fazla olmasından kaynaklanmaktadır.

Ürettiği değerler incelenerek kullanılması gereken yerlere göre düzenlenen kaotik sistemler görüntü şifreleme algoritmalarında kullanılmıştır. Şifreleme adımlarının neredeyse tamamına dahil edilen kaotik sistemler görüntüyü karıştırma, sınırlı bir alanda rasgele sayı üretme ve anahtar üretme gibi işlemlerde kullanılmıştır. Şifrelenen görüntülerin orijinal hallerini elde etmek amacıyla şifre çözme algoritmaları oluşturulmuştur. Bu algoritmalarda kaotik sistemlerin yapısında ve ürettiği değerlerde herhangi bir değişiklik yapılmadan, uygulanan matematiksel işlemlerin tersi alınarak orijinal görüntüler elde edilmişlerdir. Ayrıca algoritmaların başarım ölçütlerini belirlemek amacıyla şifrelenen görüntüler çeşitli analiz yöntemleri ile güvenlik kontrollerinden geçirilmiştir.

Tent Map, 2B Cat Map ve 3B Cat Map sistemleri ayrık zamanlı kaotik sistemlerdir. Ayrık zamanlı kaotik sistemler genellikle tek boyutludur, fakat iki boyutlu olan 2B cat map ve üç boyutlu olan 3B Cat Map sistemleri de kullanılmıştır (Chen, vd., 2004). Lorenz, Chua, Lü ve Chen kaotik sistemleri üç boyutlu sürekli zamanlı kaotik sistemlerdir. 3B Cat Map ile kıyaslandıklarında başlangıç değerleri ve parametre sayısının daha fazla olması sebebiyle sürekli zamanlı kaotik sistemler daha güçlüdür. Fakat bu kaotik sistemlerin kullanıldıkları algoritmada hangi amaca hizmet ettikleri de önemli olduğundan direk bir kıyaslama yapılması uygun değildir.

Kaotik sistemlerin ardından, kaotik nöral ağ tabanlı görüntü şifreleme ve şifre çözme aşamasına geçilmektedir. Bu aşamada Bigdeli, vd. (2012) kullandığı görüntü şifreleme algoritması gerçekleştirilmeye çalışılmıştır, fakat uygulanan işlemler birebir aynı değildir. Bu algoritma ile bir RGB görüntüsü nöral bir yapı kullanarak şifrelenmiştir. Kaotik sistemlere bağlı bir şifreleme anahtarı oluşturulmuştur ve bu anahtar ile nöral ağda bulunan ağırlık değerleri elde edilmiştir. Şifrelenecek olan görüntü nöral ağa giriş olarak verilmiştir. Kaotik sistemlerin ürettiği değerler nöral ağın her aşamasında oluşan çıkışlarla matematiksel işlemlere tabi tutulmuştur.

Son olarak 3B kaotik Cat Map tabanlı simetrik görüntü şifreleme yöntemi kullanılarak gri seviye görüntüler şifrelenmiştir. Bu aşamada Chen, vd. (2004) kullandığı görüntü şifreleme algoritması gerçekleştirilmeye çalışılmıştır. Algoritmalar birebir aynı olmasa da benzerdir. Bu bölüm şifreleme algoritması, şifre çözme algoritması, güvenlik ve başarım analizlerinden meydana gelmektedir. Şifreleme

algoritması haritanın ayrıklaştırılması, yayılma süreci ve anahtar şeması aşamalarından oluşmaktadır. Kaotik sistemler algoritmanın tüm adımlarında kullanılmaktadır. Bu tez çalışmasının omurgası olan görüntü şifreleme kısmının kapsamı ile ilgili görülen literatür çalışmaları aşağıda kısaca özetlenmiştir.

Prusty ve arkadaşları (2013), Arnold Cat Map kaotik sistemini kullanarak görüntüyü karıştırmış ve Henon Map'ı kullanarak anahtar ve rasgele sayılar üretip görüntü şifreleme yapmışlardır. Farklı formatlardaki görüntüleri şifreleyerek başarılı sonuçlar elde etmişlerdir.

Li ve arkadaşları (2015), Tent Map ve Lorenz kaotik sistemlerini kullanarak görüntü şifreleme uygulaması gerçekleştirmişlerdir. 256 bitten daha büyük anahtar genişliği, rasgelelik özelliği, histogram ve korelasyon testlerinden başarıyla geçmesi bakımından güvenli ve başarılı bir şifrelemedir.

Liu ve Wang (2013), aynı boyutlardaki üç farklı görüntüdeki R, G ve B değerlerini sırasıyla birleştirerek şifreleme ve deşifreleme gerçekleştirmiştir. Şifrelemede anahtar için SHA-256 hash fonksiyonunu ve rasgele sayı üretmek amacıyla Lorenz kaotik sistemini kullanmışlardır.

Wang ve arkadaşları (2009), görüntü şifrelemede her iterasyonda farklı kontrol parametreleri üreterek daha güçlü bir algoritma elde etmeyi amaçlamışlardır. Bu sayede görüntü her aşamada farklı anahtar ile şifrelenmiş, hız ve güvenlik bakımından oldukça iyi sonuçlar elde edilmiştir.

Wong ve arkadaşları (2008), kaotik Standart Map'i kullanarak basit ekleme ve değiştirme işlemlerine bağlı bir görüntü şifreleme uygulaması yapmışlardır. Bu kaotik tabanlı şifreleme algoritmasını hıza dayalı geliştirmeye çalışmışlardır ve sonuç olarak 512x512 boyutlarında gri tonlamalı bir görüntüyü 100 milisaniyenin altında şifrelemeyi başarmışlardır.

Zeghid ve arkadaşları (2007), literatürde daha çok metin şifrelemede kullanılan AES algoritmasını görüntü şifrelemede kullanmışlardır. AES algoritmasını görüntü şifrelemedeki eksik yanlarını gidermek amacıyla bir anahtar üreteci kullanarak yeniden

düzenlemişlerdir. Böylece anahtar genişliği, histogram analizi, korelasyon katsayısı ve entropi analizi gibi testlerde daha güçlü bir algoritma elde etmişlerdir.

Xiao ve arkadaşları (2009), Arnold Cat Map ve Chen kaotik sistemlerini kullanarak gri tonlamalı görüntü şifreleme algoritması geliştirmişlerdir. Güvenlik testlerinden elde edilen sonuçlara bakılarak başarılı olduğu görülmektedir. Bu tez çalışmasında Xiao ve arkadaşlarının (2009) kullandığı şifreleme algoritmasına benzer matematiksel işlemler KNA tabanlı görüntü şifrelemede kullanılmıştır.

Hongjun ve Xingyuan (2010), görüntü şifrelemede Chebyshev Map kaotik sistemini kullanarak görüntüde herhangi bir sebepten dolayı oluşan gürültülere karşı güçlendirilmiş bir algoritma geliştirmişlerdir. Şifreli görüntüde oluşan gürültüye karşı en az kayıpla orijinal görüntüyü elde etmişlerdir.

Bu tezde yapılan görüntü şifrelemede karıştırma, yayılma, anahtar ve rasgele sayı üretimi gibi süreçler yukarıda özetlenen literatürde geçen kaotik tabanlı görüntü şifreleme algoritmalarına benzer yapıdadır. Algoritmalardaki karıştırma süreci genellikle Cat Map kullanılarak, yayılma süreci, anahtar ve rasgele sayı üretimi gibi süreçler ise genellikle 3 boyutlu ayrık zamanlı kaotik sistemler kullanılarak gerçekleştirilmiştir. Literatürde bulunan kaotik tabanlı sistemlerin anahtar hassasiyetinin $10^{-14}$ seviyelerinde olduğu görülmüştür. Genellikle şifrelenen görüntüler 24 bit veya gri tonlamalı görüntülerdir. İncelenen algoritmalarda başarımı ölçmek amacıyla anahtar genişliği, histogram analizi, anahtar hassaslığı, korelasyon katsayısı analizi, bilgi entropi analizi ve hız analizi gibi testler yapıldığı görülmüştür. Bu çalışmada da aynı testler başarılı bir şekilde uygulanmıştır.

# 2. GÖRÜNTÜ STEGANOGRAFİ

Görüntü steganografi, bir bilginin herhangi bir görüntü içerisine gizlenmesi yöntemidir. Steganografide bilgi, veri iletişimi boyunca değiştirilemez ve veri bütünlüğü sağlanır. Başka bir ifadeyle, görüntü piksellerinin RGB (kırmızı, yeşil, mavi) değerlerinin değiştirilmesi işlemidir (Thangadurai ve Devi, 2014). Stego görüntü, örtü görüntüsü ile gizlenecek metnin birleşiminden meydana gelir.

Görüntü steganografiye ait bileşenler şunlardır; gönderilecek olan mesaj, içine veri gömülecek olan örtü verisi, gönderici ve alıcı tarafta bulunması gereken anahtar, gömülmüş veriyi/mesajı içeren stego, çıktı olarak stegoyu üreten bir steganografik fonksiyon ve çıktı olarak gömülü veriyi üreten ters fonksiyondur (Laskar ve Hemachandran, 2012).

Bu çalışmada, görüntüye veri gizleme iki farklı şekilde yapılmıştır. İlk yöntem en anlamsız bit (LSB) yöntemi, diğeri ise görüntü piksellerinin son üç bitine gizleme yöntemidir. Görüntüye gizleme işlemi yapılmadan önce veri asimetrik anahtarlı şifreleme yöntemi ile şifrelenmiştir.

## 2.1. RSA Algoritması ile Veriyi Şifreleme

Düz metin RSA algoritması ile şifrelenip, ardından herhangi bir iletişim kanalıyla gönderilecek veya saklanacaktır. RSA, en popüler asimetrik şifreleme algoritmasıdır. Tamsayıları çarpanlara ayırmanın algoritmik zorluğuna dayanmaktadır. Anahtar üretme aşamasında seçilen asal sayının büyüklüğüne göre güvenliği artmaktadır. Anahtar üretimi, şifreleme ve şifre çözme olmak üzere üç aşamadan oluşmaktadır (Yerlikaya, vd., 2007; Nabiyev ve Günay, 2010).

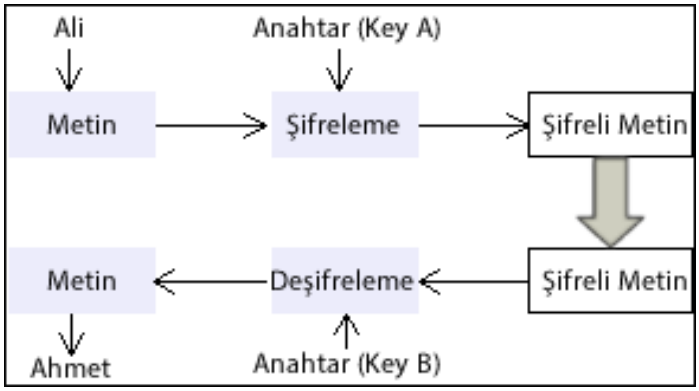
### 2.1.1. RSA şifreleme algoritması

RSA' da gizli ve açık anahtar olmak üzere iki anahtar üretilmektedir. Açık anahtar düz metnin şifrelenmesi aşamasında kullanılır. Şifre çözme işlemi gizli anahtar olmadan yapılamayacağı için açık anahtarın herhangi bir şekilde ele geçirilmesi büyük bir problem oluşturmamaktadır. RSA şifreleme adımları aşağıdaki gibidir:

- 2 adet asal sayı seçilir. ($p$ ve $q$)

- Açık ve gizli anahtar için mod değeri belirlenir. $n = p.q$
- $\vartheta(n) = (p-1)(q-1)$ totient değeri hesaplanır.
- $1 < e < \vartheta(n)$ aralığında bir e tamsayısı üretilir. $\vartheta(n)$ ve e aralarında asal olmalıdır (Nabiyev ve Günay, 2010).
- $d.e = 1 \ mod(\vartheta(n))$'e bağlı olarak $d$ tamsayısı belirlenir. $d$, gizli anahtarın üssüdür ve genişletilmiş Öklid algoritması ile elde edilir.
- Mesaj, tersinir $m$ tamsayısı olarak belirlenir. ($0<m<n$)
- Şifreli mesaj $c = m^e mod(n)$ olarak hesaplanır.
- $m = c^d \ mod(n)$ işlemi ile şifrelenen mesaj çözülür. Yani $m$'nin tersi şifreli mesaj olmaktadır (Nabiyev ve Günay, 2010).

Yukarıdaki adımları izleyerek şifreleme işlemi gerçekleştirildikten sonra görüntüye gizleme aşamasına geçilir. Simetrik şifrelemede gizli tutulması gereken bir anahtar olması sebebiyle güvenlik sorunları meydana gelmektedir. Asimetrik şifrelemede bunu ortadan kaldırmak amacıyla şifreleme ve şifre çözme işlemleri için farklı anahtarlar (Şekil 2.1) kullanılmaktadır (Selvi, vd., 2012). Yapılan şifrelemede herkes tarafından bilinen bir açık anahtar vardır. Ancak şifre çözme işlemi gizli anahtarla yapıldığından asimetrik şifreleme olarak adlandırılmıştır.




**Şekil 2.1.** Asimetrik şifreleme yapısı.

Şifrelemede kullanılan anahtara bağlı olarak şifre çözme anahtarının elde edilmesinin çok zor olması gerekmektedir. Asimetrik şifreleme algoritmaları özellikle çok kullanıcılı sistemlerde büyük avantajlar sağlamaktadır. Ayrıca dijital imza ve kimlik denetimi uygulamalarında kullanılmaktadır (Selvi, vd., 2012).

Asimetrik şifreleme algoritmaları içerisinde bulunan sayıların basamak sayısının çok fazla olması ve bu sayılarla cebirsel işlemlerin yapılmasından dolayı yavaş çalışmaktadır. Bu bir dezavantaj olarak nitelendirilebilir. Kriptoloji alanında yeni çalışmalar yapılarak bu dezavantaj ortadan kaldırılmaya çalışılmaktadır (Karpinskyy ve Kinakh, 2003). Asimetrik şifreleme yöntemlerinde ters şifreleme fonksiyonlarının kullanılması sebebiyle çözülmesi zordur (Selvi, vd., 2012).

RSA, tam sayıları çarpanlara ayırmanın algoritmik zorluğuna dayanan en popüler asimetrik şifreleme yöntemidir. Anahtar oluşturma işleminde büyük asal sayılar seçilerek algoritma daha zor hale getirilmiştir (Guo, vd., 2014). RSA algoritması anahtar üretimi, şifreleme ve şifre çözme aşamalarından oluşur (Nabiyev ve Günay, 2010; Guo, vd., 2014).

RSA algoritması ile yapılan şifrelemede düz metin boyutu, şifreli metin boyutu ve şifreleme süresi Çizelge 2.1'de verilmiştir. Bu sonuçların elde edildiği bilgisayar 2.2 GHz işlemci ve 4 GB RAM özelliklerine sahiptir.

**Çizelge 2.1.** RSA şifreleme sonuçları.

| Düz metin (Bayt) | Şifreli Metin (Bayt) | Şifreleme Süresi (Saniye) |
|---|---|---|
| 4726 | 21100 | 0.018 |
| 13573 | 60601 | 0.40 |
| 48092 | 214579 | 4.594 |

## 2.2. Şifreli Veriyi Görüntü Dosyasına Gizleme

RSA algoritması ile şifrelenen veri görüntü dosyasına en anlamsız bite gizleme ve en anlamsız 3 bite gizleme yöntemlerini kullanarak gizlenmiştir. Amaç görüntülerde meydana gelen değişiklikleri incelemektir.

### 2.2.1. En anlamsız bite gizleme yöntemi (LSB)

Bilgiyi görüntüye gizleme yaklaşımlarının en basiti LSB yöntemidir. Bu yöntemde, görüntüdeki piksel değerlerinin sadece son biti değiştirilir. Yöntemi

uyguladıktan sonra renk tonlarında meydana gelen değişiklik çok küçük olduğundan görüntüde oluşan değişiklikleri insan gözüyle fark etmek neredeyse imkansızdır (Karim, vd., 2011).

'A' karakterinin ASCII tablosundaki ikili değeri 01000001'dir ve diğer alfabetik karakterler de benzer ikilik değerlere sahiptir. Bundan dolayı eğer bir karakteri gizlemek istiyorsak sekiz bitlik alana ihtiyacımız olmaktadır (Dagar, 2013). Bu çalışmada, gizleme işlemi 24 bit görüntülere uygulanmıştır. Bir veriyi herhangi bir görüntüye gizleme adımları aşağıda belirtilmektedir.

- Şifreli metnin ASCII değerleri elde edilir. Metnin her harfi onluk sistemden ikilik sisteme dönüştürülür.
- Görüntüdeki her pikselin RGB değerleri belirlenir.
- Her bir pikseldeki RGB değerlerine veri gizlenir. Renk tonlarında maksimum 3 bitlik bir değişim meydana gelir.
- Aşağıda LSB yöntemiyle veri gizleme işlemi açıklanmıştır. Gizlenecek veri "01001001" ve görüntünün ilk 8 pikselindeki kırmızı (R) değerlerinin ilk durumu ve gizleme işlemi yapıldıktan sonraki durumu Çizelge 2.2'deki gibi olmaktadır.

**Çizelge 2.2.** LSB'de veri gizlendikten sonra R değerleri.

| Piksel | Önce (Kırmızı değerleri) | Sonra (Kırmızı değerleri) |
|---|---|---|
| 1 | 1111001**1** | 1111001**0** |
| 2 | 1001011**1** | 1001011**1** |
| 3 | 1001000**1** | 1001000**0** |
| 4 | 1001000**0** | 1001000**0** |
| 5 | 0001101**1** | 0001101**1** |
| 6 | 1001010**0** | 1001010**0** |
| 7 | 0001111**1** | 0001111**0** |
| 8 | 0001000**0** | 0001000**1** |

Sonra adlı sütunda bulunan koyu renkli LSB bit değerleri sırasıyla gizlenecek karakterin bit değerleridir. Veri, görüntünün kırmızı değerlerinin tamamına

gizlendikten sonra sırasıyla yeşil (G) ve mavi (B) değerlerine de gizlenmektedir. 256x256 olan 24 bitlik bir görüntüye 256x256x3 bit veri gizlenebilir. Bu da yaklaşık 24576 karakteri ifade etmektedir.


**Şekil 2.2.** L3B steganografi (a) Orijinal görüntü (b) Stego görüntü.

256x256 boyutlarındaki orijinal görüntü ve yaklaşık 22000 karakter (yaklaşık 3000 kelime) gizlenen stego görüntü Şekil 2.2'de görülmektedir. İki görüntü arasındaki fark insan gözüyle fark edilememektedir, yani neredeyse imkansızdır. LSB yöntemi ile veri gizlemede görüntünün renk tonlarında çok fazla değişiklik meydana gelmemektedir.

### 2.2.2. Son üç bite gizleme yöntemi (L3B)

Son 3 LSB bite gizlenen verinin elde edilmesi bakımından 1 bit LSB yöntemine göre daha zordur. 1 bit L3B yönteminde gizlenen veriyi elde etmek için geliştirilmiş bazı saldırılar mevcuttur. L3B yöntemi ile veriyi görüntüye gizleme adımları aşağıda belirtilmektedir.

- Şifreli metnin ASCII değerleri elde edilir. Metnin her harfi onluk sistemden ikilik sisteme dönüştürülür.
- Görüntüdeki her pikselin RGB değerleri belirlenir ve LSB yönteminden farklı olarak onluk sistemden ikilik sisteme dönüştürülür.
- Her bir pikseldeki R, G ve B değerlerine 3'er bit olmak üzere toplam 9 bit veri

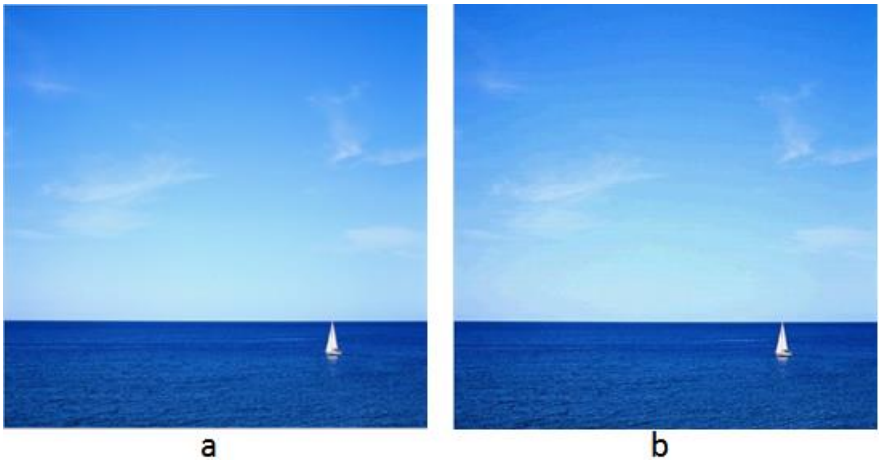
gizlenir. Bu işlemlerden sonra RGB değerlerinin son 3 biti değiştirilmiş olur.

Gizlenecek 3 karakterin ASCII kodu (24 bit) “000 110 010 100 101 001 000 111”, görüntünün ilk 8 pikselindeki R değerleri ve L3B yöntemiyle veri gizlendikten sonraki durumu Çizelge 2.3’de gösterilmiştir.

**Çizelge 2.3.** L3B’de veri gizlendikten sonra R değerleri.

| Piksel | Veri gizlenmeden önce (Kırmızı değerleri) | Veri gizlendikten sonra (Kırmızı değerleri) |
|---|---|---|
| 1 | 11110**011** | 11110**000** |
| 2 | 10010**111** | 10010**110** |
| 3 | 10010**001** | 10010**010** |
| 4 | 10010**000** | 10010**100** |
| 5 | 00011**011** | 00011**101** |
| 6 | 10010**100** | 10010**001** |
| 7 | 00011**111** | 00011**000** |
| 8 | 00010**000** | 00010**111** |

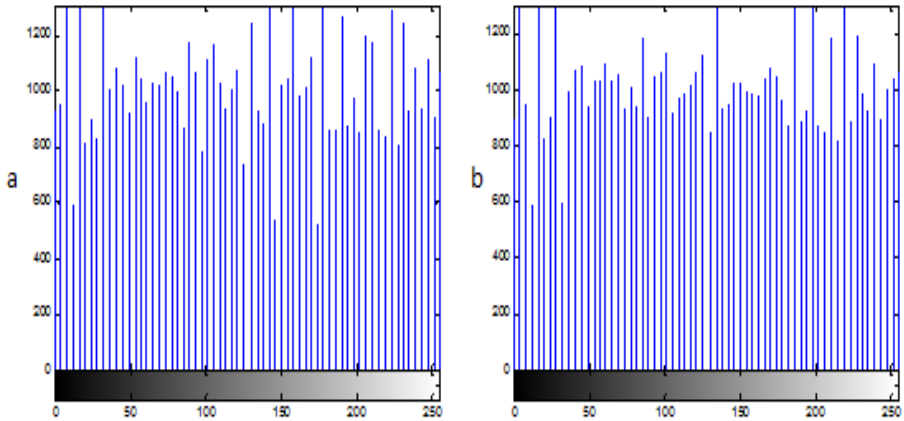
24 bit veri 3 parçaya bölünür. Her pikselin R değerlerine Çizelge 2.3’de görüldüğü gibi 3 bit veri gizlenir. *Veri gizlendikten sonra* sütununun son 3 biti sırasıyla gizlenen verileri temsil etmektedir. Bitlerin değişimi *Veri gizlenmeden önce* ve *Veri gizlendikten sonra* sütunlarının arasındaki değişime bakılarak kıyaslanabilir. LSB’ye benzer şekilde veri R değerlerine gizlendikten sonra G ve B değerlerine de sırasıyla gizlenir. 512x512 boyutlarındaki bir görüntü dosyasına her piksele 9 bit veri gizlenerek 512x512x9 bit veri, yani 294912 karakter gizlenebilmektedir. Kayıpları önlemek amacıyla veri boyutunu daha önceden belirlemek gerekmektedir. L3B yöntemiyle veri gizleme işlemi yapıldıktan sonra değişimleri analiz edebilmek için renk tonu değerleri birbirine yakın olan Şekil 2.3’deki görüntü seçilmiştir. 256x256’lık görüntüye yaklaşık 22000 karakter (yaklaşık 3000 kelime) gizlenmiştir. LSB’nin aksine dikkatle bakıldığında renk tonlarında oluşan değişimler L3B’de fark edilebilmektedir.



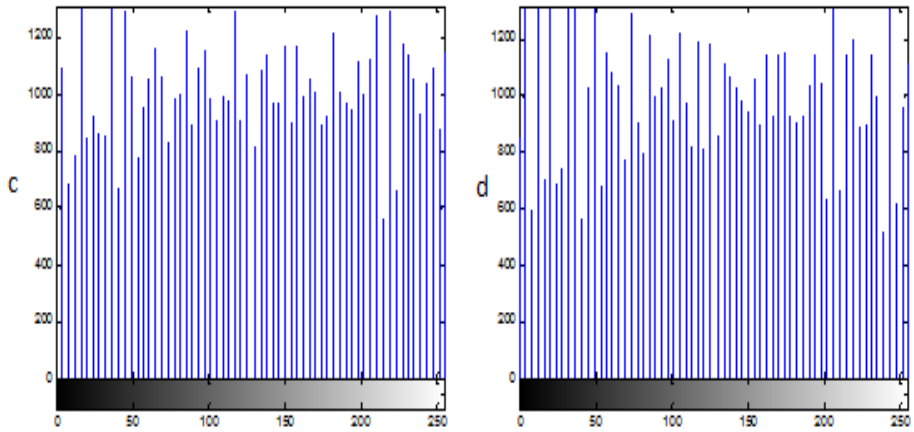

**Şekil 2.3.** L3B steganografi (a) Orijinal görüntü (b) Stego görüntü.

## 2.3. Görüntülerin Histogram Değerleri

LSB yöntemi ile gizleme yapılan Lena'ya ait orijinal ve veri gömülü görüntünün histogram eğrileri Şekil 2.4'de verilmiştir. Aynı şekilde L3B yöntemi ile gizleme yapılan gökyüzüne ait orijinal ve veri gömülü görüntünün histogramları da Şekil 2.5'de verilmiştir. Oluşan bu histogramlarda orijinal görüntü ile veri gömülü görüntü arasındaki fark anlaşılabilmektedir. L3B yönteminde histogramlardaki farklılık, belli değerlerdeki artış-azalış, LSB'ye göre bariz bir şekilde görülebilmektedir. Buradaki önemli nokta histogram eğrisinin belli bir alana yığılmasını önlemektir.




**Şekil 2.4.** Kırmızı değerleri histogramı a) Orijinal Lena b) Veri gömülü Lena.




**Şekil 2.5.** Kırmızı değerleri histogramı c) Orijinal gökyüzü d) Veri gömülü gökyüzü.

LSB yönteminde orijinal görüntü ile stego görüntü arasında oluşan farklılık çok az olmaktadır. Bunun sebebi görüntüdeki her pikselin 0-255 aralığındaki RGB değerinde meydana gelen artış-azalış miktarının çok az olması veya bu değerlerde hiç değişiklik olmamasıdır. İki görüntü birbiri ile hemen hemen aynıdır. Mevcut LSB gizleme yöntemiyle yapılan uygulamada R değerlerinde meydana gelen değişim ve aralarındaki renk tonu farkı Çizelge 2.4'de görülmektedir. Benzer şekilde, mevcut L3B gizleme yöntemiyle yapılan uygulamada R değerlerinde meydana gelen değişim ve aralarındaki renk tonu farkı da görülmektedir.

**Çizelge 2.4.** LSB ve L3B steganografi sonucu görüntü piksellerindeki değişiklik.

| Pikseller | Önce (R değeri) | Sonra (LSB) (R değeri) | Fark (LSB) | Sonra (L3B) (R değeri) | Fark (L3B) |
|---|---|---|---|---|---|
| 1 | 243 | 242 | 1 | 240 | 3 |
| 2 | 151 | 151 | 0 | 150 | 1 |
| 3 | 145 | 144 | 1 | 146 | 1 |
| 4 | 144 | 144 | 0 | 148 | 4 |
| 5 | 25 | 25 | 0 | 27 | 2 |
| 6 | 148 | 148 | 0 | 145 | 3 |
| 7 | 31 | 30 | 1 | 24 | 7 |
| 8 | 16 | 17 | 1 | 23 | 7 |

Çizelge 2.4'de elde edilen sonuçlara göre, L3B yönteminde stego görüntü ve orijinal görüntü arasındaki renk tonu farklılığı LSB yönteminden daha büyük olmaktadır. Eğer aradaki renk tonu farkı onluk sistemde dörtten büyük ise insan gözü

ile dikkatle bakıldığında algılanabilmektedir. Dört veya dörtten küçük olduğunda değişimin farkına varılamamaktadır. Buna ilaveten renk tonu farkı 7'den büyük ise açık bir şekilde renk değişimi görülmektedir.

Sonuç olarak, LSB steganografi yönteminde gizlenen verinin varlığını bilmek zordur, fakat L3B steganografi yönteminde gizlenen verinin varlığını bilmek daha kolaydır. Renk değişimi kolayca fark edildiğinden dolayı, ikinci yöntemde düşük renk yoğunluğuna sahip görüntüler seçilmemelidir. Ayrıca bilinen ve sürekli kullanılan görüntüler tercih edilmemelidir. Kullanılan steganografi ve kriptografi yöntemleri sayesinde verinin güvenli bir şekilde saklanabilir veya iletilebilir hale geldiği görülmüştür.

# 3. KAOTİK SİSTEMLER

Kaos, başlangıç koşullarına aşırı duyarlı ve gürültü gibi bir güç spektrumuna sahip, düzensizliğin düzenli hali şeklinde tanımlanabilir. Kaosu ilk defa 20. yüzyılın başlarında Fransız filozof Henry Poincare, karmaşık bir sistemin kararlılığı ile ilgili astronomi alanında çalışmalarda kullanmıştır. Günümüzde mühendislik, tıp, bilişim, meteoroloji, ekonomi, kimya, görüntü işleme, bulanık mantık, optimizasyon, haberleşme, mekatronik gibi birçok alanda kullanılmaktadır. Ayrık zamanlı sistemlerde değişimler fark denklemleri veya tekrarlama kullanılarak çözülür. Ayrık zamanda elde edilen sonuçların gösterilmesinin matematiksel yolu veya herhangi bir işlemin üst üste tekrar edilmesi tekrarlama olarak kabul edilir. Sürekli zamanlı sistemlerde türevsel denklemler kullanılarak matematiksel işlemler gerçekleştirilir (Pamuk, 2013). Kaotik sistemler, sınırsız sayıda değişik periyodik salınımlar içeren, genlik ve frekansları tespit edilemeyen doğrusal olmayan bir davranış türü sergilerler. Ancak bu dinamikler kaotik işaretler içeren sınırlı bir alanda gerçekleşir. Bu işaretlere bağlı olarak, dinamik sistemin şimdiki durumu, geçmiş durumu ve olası durumların kümesi de bilinmektedir (Akgül, 2015). Kaotik sistemlerin özellikleri aşağıda verilmiştir.

- Zaman boyutunda düzensiz hareket eder.
- Başlangıç şartlarına hassas bağımlıdır.
- Sınırsız sayıda periyodik salınım içerir. Rasgele değildirler.
- Genliği ve frekansı belirsizdir.
- Sınırlı bir alanda değişen işaretler içerir (Akgül, 2015; Orhan, 2013).

Kaotik sistem senkronizasyonu fizik, iletişim güvenliği, yapay sinir ağları, bulanık mantık vb. potansiyel uygulamalar için doğrusal olmayan bilim konularında kritik unsurlardan biridir (Stork, 2011).

Kaotik sistemler ayrık zamanlı ve sürekli zamanlı olmak üzere ikiye ayrılmaktadır. Sürekli zamanlı kaotik bir sistem en az üç denkleme sahiptir ve üç boyutludur. Ayrık zamanlı bir kaotik sistem ise genellikle tek boyutludur ve tek denklemden oluşmaktadır. Ayrık zamanlı kaotik sistem, sürekli zamanlı kaotik sistem ile karşılaştırıldığında iletişimde yüksek frekans verimliliği ve güvenliği sağlamaktadır (Orhan, 2013; Zheng, vd., 2009).

### 3.1. Ayrık Zamanlı Kaotik Sistemler

Ayrık zamanlı kaotik sistemler, eğrisel bir fonksiyonun iteratif sonuçlarından meydana gelen ve genellikle geri besleme özelliği gösteren dizilerden oluşan bir yapıdır. Böyle bir sistemin en basit hali Eşitlik 3.1'deki fonksiyon ile ifade edilebilir.

$$x_{n+1} = f(x_n) \tag{3.1}$$

Kaotik fonksiyonu elde etmek için, başlangıç koşullarına yüksek duyarlılıkla bağlı oluşan $x_n$ değerlerinin periyodik olmaması ve birbirinden çok farklı olması gerekmektedir. Ayrık zamanlı kaotik sistemeler bir boyutlu basit bir denklem ile ifade edilebilmektedir (Özdemir, 2008). Bunun dışında iki boyutlu ve üç boyutlu ayrık zamanlı kaotik sistemler de mevcuttur. Literatürde tek boyutlu olmayan ve basit yapıda olan bu sistemlere rastlamak mümkündür (Stork, 2011).

En çok kullanılan tek boyutlu kaotik sistemlerin başında *Logistic Map* gelmektedir (Oğraş ve Turk, 2012). Tek boyutlu ayrık zamanlı kaotik sistemlere *Logistic Map, Tent Map, Cubic Map, Gauss Map, Gaussian White Chaotic Map* örnek olarak verilebilir.

İki boyutlu kaotik sistemler iki farklı denklem ile ifade edilmektedir. En çok kullanılan iki boyutlu ayrık zamanlı kaotik sistemlerin başında *Arnold's Cat Map* gelmektedir (Prusty, vd., 2013). Literatürde *Arnold's Cat Map*'e ek olarak *Delayed Logistic Map, Henon Map, Lozi Map, Tinkerball Map, Burgers Map* gibi iki boyutlu kaotik sistemler mevcuttur.

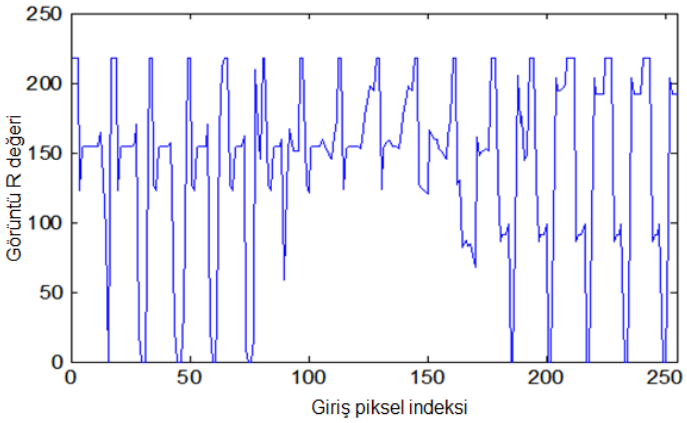
#### 3.1.1. Tent Map kaotik sistemi

Tek boyutlu ayrık zamanlı kaotik Tent Map sistemi Eşitlik 3.2'de, tersi ise ($f^{-1}$) Eşitlik 3.3'deki denklem ifade edilir (Bigdeli, vd, 2012; Masuda ve Aihara, 2002).

$$f(a,x) = \begin{cases} \left\lceil \frac{M}{a} x \right\rceil, & 0 \le x \le a \\ \left\lfloor \frac{M}{M-a} (M-x) \right\rfloor + 1, & a < x \le M \end{cases} \tag{3.2}$$

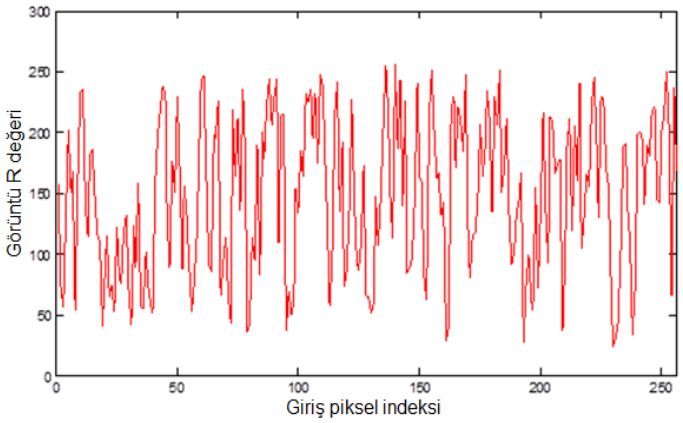
$$f^{-1}(a,y)=\begin{cases}\lfloor ay/M \rfloor, & \left(\left\lfloor \frac{ay}{M}\right\rfloor-\left\lceil \frac{ay}{M}\right\rceil=-1\ ve\ \frac{\left\lfloor \frac{ay}{M}\right\rfloor}{a}>-\left\lceil\left(\frac{a}{S}-1\right)y\right\rceil\right)veya\left\lfloor \frac{ay}{M}\right\rfloor-\left\lceil \frac{ay}{M}\right\rceil=0 \\ \left\lceil\left(\frac{a}{M}-1\right)y+S\right\rceil, & \left\lfloor \frac{ay}{M}\right\rfloor-\left\lceil \frac{ay}{M}\right\rceil=-1\ ve\ \frac{\left\lfloor \frac{ay}{M}\right\rfloor}{a}\leq-\left\lceil\left(\frac{a}{M}-1\right)y\right\rceil\end{cases} \tag{3.3}$$

Fonksiyondaki $a$ değeri kullanıcı tarafından belirlenen ($a \in [1, M]$) bir tamsayı, $\lfloor x \rfloor$ ve $\lceil x \rceil$ değerleri ise sırasıyla $x$'in alt ve üst sınır değerlerini ifade etmektedir. $M$ değeri genelde düz metne göre seçilir ve 8 bit bir görüntü için $M = 256$'dır. Ayrık Tent Map birebir eşleştirme yapmaktadır. Tent Map'in etkisini zaman düzleminde göstermek için bir görüntünün $16 \times 16$'lık bir kısmı seçilir ve ardından Tent Map kaotik sistemine giriş olarak uygulanır. Girişler ve çıkışlar zaman düzleminde Şekil 3.1'de görülmektedir. Bu sistemin girişleri yarı periyodik bir davranışa sahip iken, Tent Map sisteminin çıkışlarına bakılarak kaotik davranış gösterdiği söylenebilir.




**Şekil 3.1.** Bir görüntünün 16x16 kesiti.

Şekil 3.1'de görülen değerler bir görüntünün 16x16'lık bir kesitine aittir. Görüntüye ait bu kesit Tent Map sistemine giriş olarak uygulanmıştır. Girişe bağlı elde edilen çıkışlar Şekil 3.2'deki gibi oluşmuştur.




**Şekil 3.2.** Tent Map uygulanmış görüntü.

Şekil 3.1 ve Şekil 3.2 incelendiğinde girişler ile çıkışlar arasında herhangi bir benzerlik ve periyodiklik yoktur. Tent Map kaotik sisteminin herhangi bir görüntüye uygulandığında birbiri ile ilişkili olmayan piksel değerleri üreteceği açıkça görülmektedir. Ayrıca Şekil 3.2'de elde edilen değerlerin Tent Map işlemine göre tersi alındığında Baboon görüntüsünün $16 \times 16$ kesitine ait orijinal değerler elde edilmektedir. Giriş ve çıkışlar piksel değerlerinin değişimi açısından incelendiğinde başarım oranının yüksek olduğu görülmektedir.

### 3.1.2. 2B Cat Map kaotik sistemi

Görüntü şifreleme permütasyon evresinde genellikle iki boyutlu üç tip kaotik harita kullanılmaktadır. Bunlar *Standart Map, Cat Map* ve *Genelleştirilmiş Baker Map* haritalarıdır (Bigdeli, vd, 2012). Cat Map literatürde en yaygın kullanılan haritadır. $N \times N$ boyutlu bir gri seviye görüntü ve bu görüntüye ait piksel değerlerinin koordinatları $C = \{(x, y) \mid x, y = 1, 2, \dots, N\}$ olarak belirlenirse Cat Map aşağıdaki gibi tanımlanır (Xiao, vd., 2009).

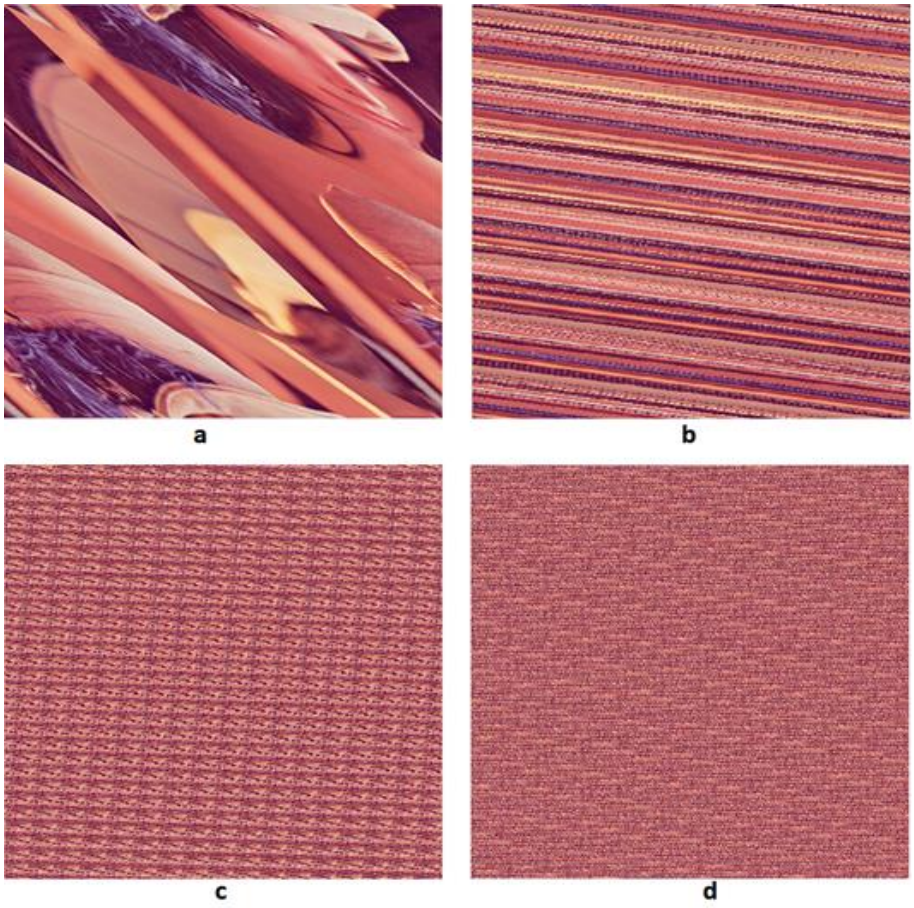
$$\begin{pmatrix} x' \\ y' \end{pmatrix} = Q \begin{pmatrix} x \\ y \end{pmatrix} mod(N) = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} mod(N) \tag{3.4}$$

Yukarıdaki denklemde Cat Map kontrol parametreleri olan $p$ ve $q$ pozitif tamsayılardır. $(x, y)$ ve $(x', y')$ değerleri ise sırasıyla koordinat değerlerinin orijinal ve yeni pozisyonlarıdır. Burada $\det(Q) = 1$ olduğundan alan korunur, yani herhangi bir

koordinat birbiriyle çakışmaz ve herhangi bir kayıp meydana gelmez (Bigdeli, vd, 2012).

**Şekil 3.3.** Orijinal Lena görüntüsü 512x512.

2B Cat Map, sınırları belirli bir alanda sürekli farklı koordinat değerleri üreterek görüntüdeki piksellerin yerlerinin değişimini sağlamaktadır. Şekil 3.3'deki Lena görüntüsü 2B Cat Map sistemine giriş olarak uygulandığında Şekil 3.4'deki gibi farklı şekillerde görüntü pikselleri karıştırılabilmektedir. Görüntü piksellerinin karışımındaki farklılık 2B Cat Map sisteminde bulunan $p$ ve $q$ parametrelerinden kaynaklanmaktadır. Şekil 3.4'de elde edilen görüntülerde $p = 1$ ve $q = 1$ seçildiğinde (a) görüntüsü, $p = 5$ ve $q = 7$ seçildiğinde (b) görüntüsü, $p = 22$ ve $q = 30$ seçildiğinde (c) görüntüsü, $p = 401$ ve $q = 401$ seçildiğinde (d) görüntüsü elde edilmektedir. Bu değerlerin değişiminden de anlaşılacağı üzere $p$ ve $q$ değerleri artırıldıkça görüntüdeki pikseller daha homojen karışmaktadır.




**Şekil 3.4.** Lena görüntüsüne Cat Map uygulama (a) p=1, q=1 (b) p=5, q=7 (c) p=22, q=30 (d) p=401, q=401.

Piksellerin koordinatlarının değişmesi, görüntü şifreleme işlemlerinde büyük kolaylık sağlamaktadır. Orijinal görüntüde bulunan bitişik piksel değerleri birbirine çok yakın olacağından, bu kısımlar şifrelendiğinde birbirine yakın değerler oluşturabilmektedir. Fakat 2B Cat Map uygulanan görüntüde bitişik piksel değerleri farklılaşacaktır. Bu sayede daha sağlam bir şifreleme yapılabilecektir.

### 3.1.3. 3B Cat Map kaotik sistemi

Üç boyutlu Cat Map, iki boyutlu Cat Map sisteminin genişletilmiş halidir. 2B Cat Map $p$ ve $q$ kontrol parametreleri ile Eşitlik 3.4'deki gibi tanımlanmıştır. Bu harita Eşitlik 3.5, 3.6 ve 3.7 haritaları göz önünde bulundurularak üç boyutlu üç harita olarak genişletilmiştir. Eşitlik 3.5'de $z_n$ sabitlenerek $x - y$ düzleminde, Eşitlik 3.6'da

$x_n$ sabitlenerek $y-z$ düzleminde, Eşitlik 3.7'de $y_n$ sabitlenerek $x-z$ düzleminde 2B Cat Map uygulanır.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a_z & 0 \\ b_z & a_z b_z + 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} mod 1, \tag{3.5}$$

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & a_x \\ 0 & b_x & a_x b_x + 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} mod 1, \tag{3.6}$$

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 0 & a_y \\ 0 & 1 & 0 \\ b_y & 0 & a_y b_y + 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} mod 1, \tag{3.7}$$

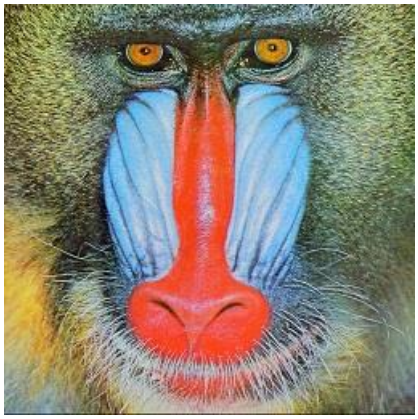
Chen ve arkadaşları (2004) bu üç haritayı birleştirilerek üç boyutlu Cat Map'i Eşitlik 3.8'deki gibi elde etmişlerdir.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = C \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} mod 1 \tag{3.8}$$

$$C = \begin{bmatrix} 1 + a_x a_z b_y & a_z & a_y + a_x a_z + a_x a_y a_z b_y \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 & a_y a_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x a_y b_y + a_x \\ a_x b_x b_y + b_y & b_x & a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{bmatrix} \tag{3.9}$$

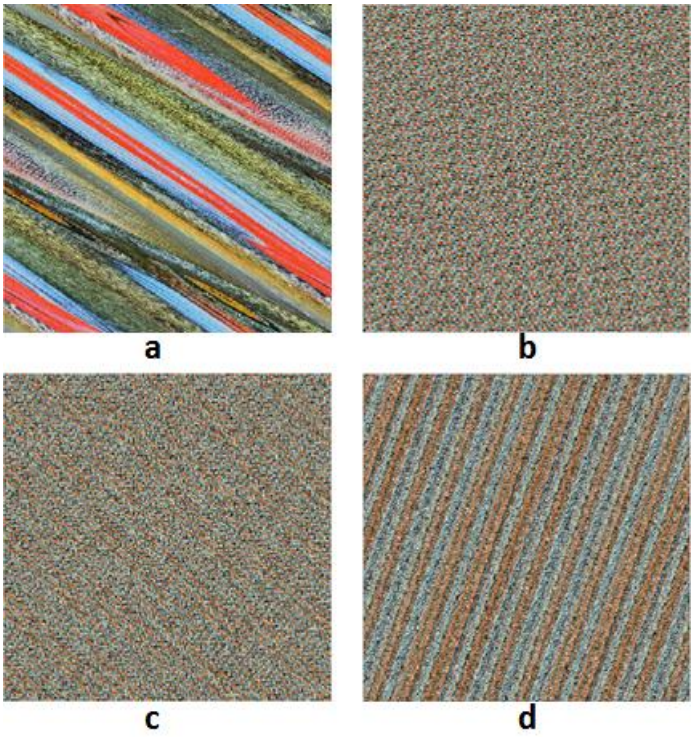
Özel bir durum olarak, $a_x = b_x = a_y = b_y = a_z = b_z = 1$ olarak belirlendiğinde orijinal 2B Cat Map'in yayılımı Eşitlik 3.11'deki gibi olur.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = C \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} mod(N) \ , \ C = \begin{bmatrix} 2 & 1 & 3 \\ 3 & 2 & 5 \\ 2 & 1 & 4 \end{bmatrix} \tag{3.11}$$



**Şekil 3.5.** Orijinal 256x256 Baboon görüntüsü.

3B Cat Map, 2B Cat Map gibi sınırları belirli bir alanda sürekli farklı koordinat değerleri üreterek görüntüdeki piksellerin yerlerinin değişimini sağlamaktadır. Şekil 3.5'deki Baboon görüntüsü 3B Cat Map sistemine giriş olarak uygulandığında Şekil 3.6'daki gibi farklı şekillerde görüntü pikselleri karıştırılabilmektedir. Görüntü piksellerinin karışımındaki farklılık 3B Cat Map sisteminde bulunan $a_x, a_y, a_z, b_x, b_y, b_z$ parametrelerinden kaynaklanmaktadır. Şekil 3.6'da elde edilen görüntülerde bu değerler sırasıyla $1, 1, 1, 1, 1, 1$ seçildiğinde (a) görüntüsü, 3,4,5,6,7,8 seçildiğinde (b) görüntüsü, 11,12,13,14,15,16 seçildiğinde (c) görüntüsü, seçildiğinde 58,59,60,61,62,63 (d) görüntüsü elde edilmektedir. Tüm parametreler 0 yapıldığında birim matris elde edildiğinden görüntüde herhangi bir değişiklik meydana gelmemektedir. Parametrelerin büyük olması görüntüdeki karışıklığı artırmaktadır. Ancak parametreler şifrelenecek üç boyutlu görüntünün boyutunun bir kenar boyutunu aşmayacak şekilde belirlenmelidir.




**Şekil 3.6.** Baboon görüntüsüne 3B Cat Map uygulama.

### 3.2. Sürekli Zamanlı Kaotik Sistemler

Sürekli zamanlı kaotik sistemler en az üç boyutludur. Bir sürekli zamanlı kaotik sistemin oluşması için en az üç denklem gereklidir ve genellikle adi diferansiyel denklemleri ile oluşmaktadır. Bu denklemler aşağıdaki gibi ifade edilmektedir.

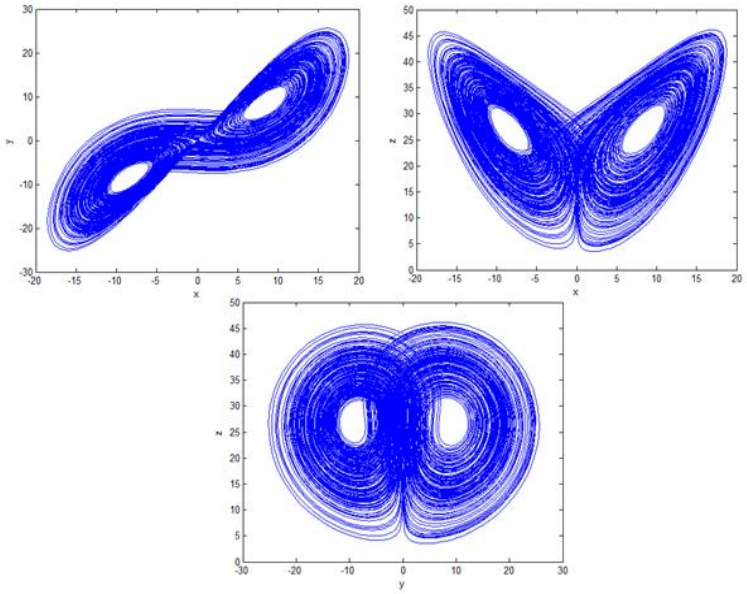
$$f(y', y'', \dots, y^n, y) = f(x) \tag{3.12}$$

Denklemde *n* sistemin derecesini belirtir ve sürekli zamanlı kaotik sistemlerde değeri en az üç olmalıdır (Wikipedia, 19.05.2016). Literatürde bulunan sürekli zamanlı kaotik sistemlerden olan Lorenz en yaygın kullanılanlardan biridir (Wikipedia, 19.05.2016). Bunun dışında Chua, Chen, Moore-Spiegel, Van Der Pol gibi sistemler sürekli zamanlı kaotik sistemlerdir (Akgül, 2015). Lorenz spektrumu geniş bir frekans bölgesinde periyodik olmayan salınımlar ürettiğinden literatürde kriptosistemlerde ve haberleşmede oldukça yoğun kullanılmaktadır (Sevinç, 2003).

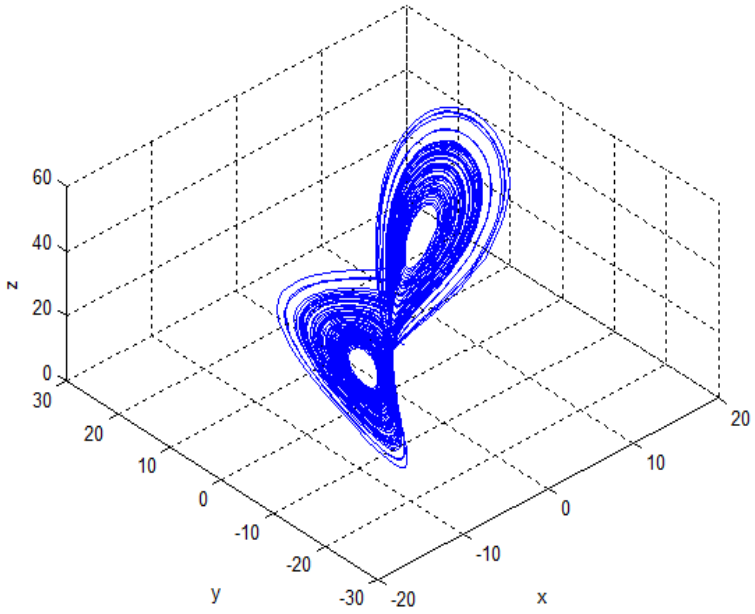
### 3.2.1. Lorenz kaotik sistemi

Lorenz kaotik sistemi iki boyutlu akışkan konveksiyonu modeli olarak 1962-63 yıllarında Lorenz tarafından geliştirilmiştir (Lorenz, 1963; Gonzalez, vd., 1999). $a$, $b$ ve $c$ sistemin sabit parametreleri olarak ele alınırsa kaotik Lorenz sisteminin dinamikleri Eşitlik 3.13 ile ifade edilir. $a = 10$, $b = 8/3$, $c = 28$ olduğunda sistem kaotik davranış göstermektedir (Li ve Yin, 2009). Lorenz kaotik sisteminin durum uzayı yörüngeleri Şekil 3.7'de görüldüğü gibi oluşmaktadır. Bu faz portrelerine ait grafik üç boyutlu oluşturulduğunda x, y ve z eksenlerindeki görünümü Şekil 3.8'deki gibi olmaktadır.

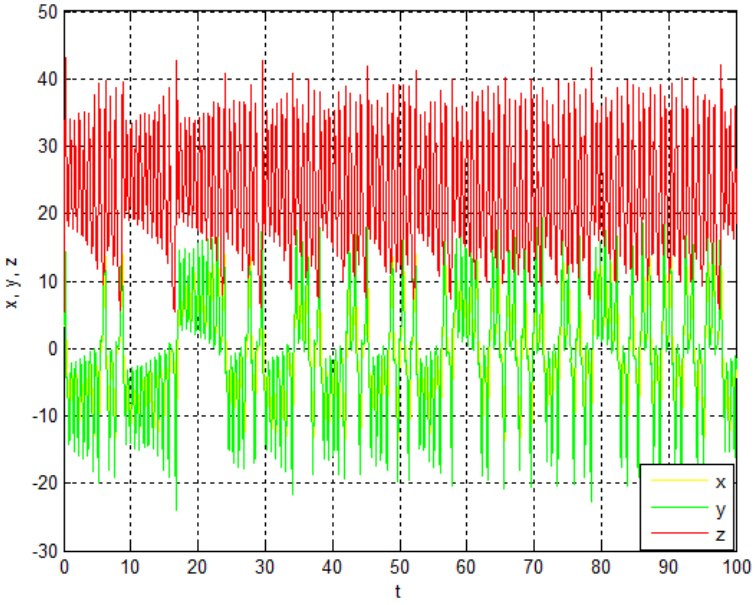
$$\begin{cases} x'(t) = a(y(t) - x(t)) \\ y'(t) = -x(t)z(t) + cy(t) \\ z'(t) = x(t)y(t) - bz(t) \end{cases} \tag{3.13}$$



**Şekil 3.7.** Lorenz sistemine ait x-y, x-z, y-z fazları.




**Şekil 3.8.** Lorenz kaotik sistemi üç boyutlu grafiği.




**Şekil 3.9.** Lorenz sistemi kaotik zaman serisi

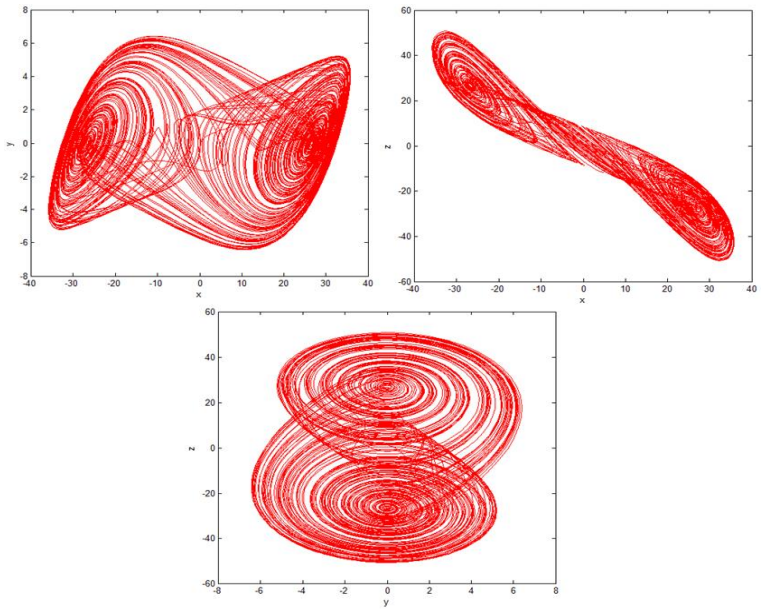
Lorenz sistemi için belirtilen parametrelere bağlı olarak elde edilen kaotik zaman serisi Şekil 3.9'da görüldüğü gibi olmaktadır.

### 3.2.2. Chua kaotik sistemi

Chua kaotik sistem modeli Eşitlik 3.14 ile ifade edilir. Eşitliklerde $a$, $b$ sabit parametreler ve $f(x(t)) = 2x(t) - x(t)/7$ 'dir.

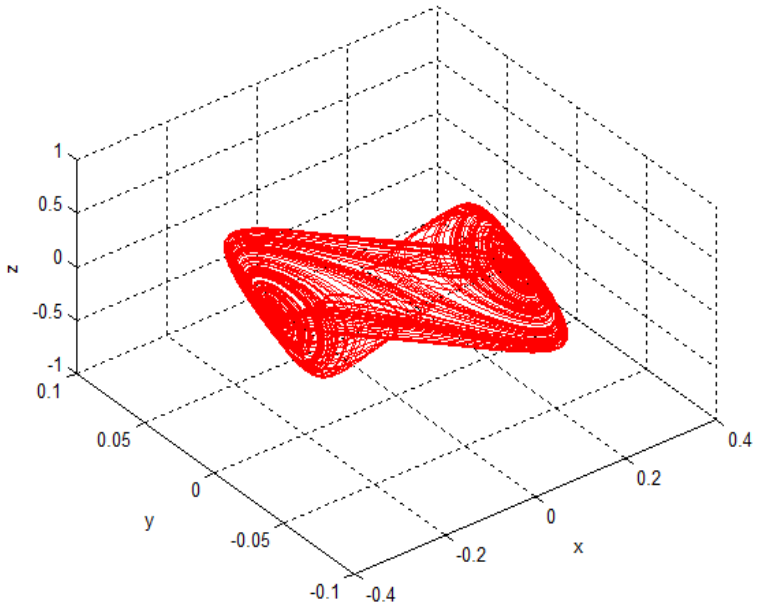
$$\begin{cases} x'(t) = a(y(t) - f(x(t))) \\ y'(t) = x(t) - y(t) + z(t) \\ z'(t) = -by(t) \end{cases} \tag{3.14}$$

a=10, b=100/7 seçildiğinde sistem kaotik davranış göstermektedir (Botmart ve Niamsup, 2007). Lorenz sisteminde üç adet sabit parametre mevcut iken Chua sisteminde iki adet sabit parametre vardır. Chua kaotik sisteminin durum uzayı yörüngeleri Şekil 3.10'da görüldüğü gibi oluşmaktadır.

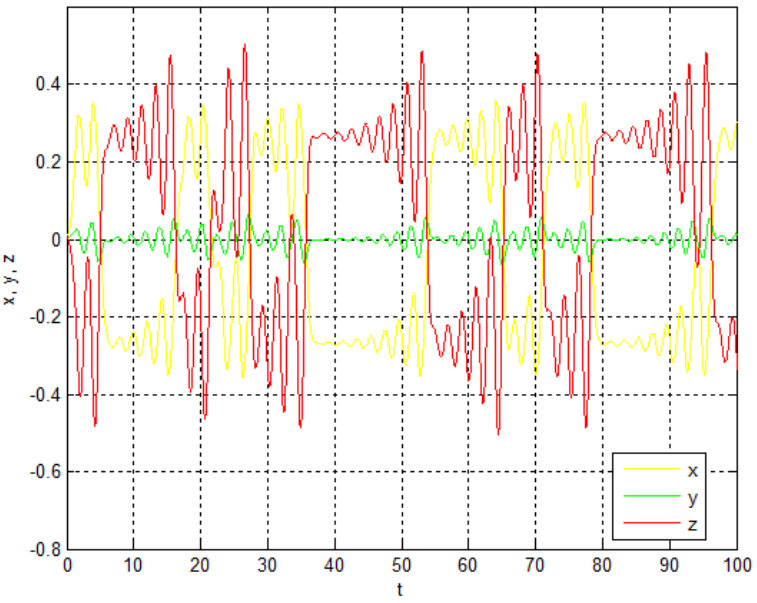


**Şekil 3.10.** Chua sistemine ait x-y, x-z, y-z fazları.

Bu faz portrelerine ait grafik üç boyutlu oluşturulduğunda x, y ve z eksenlerindeki görünümü Şekil 3.11'de, kaotik zaman serisi ise Şekil 3.12'de görüldüğü gibi olmaktadır.




**Şekil 3.11.** Chua kaotik sistemi üç boyutlu grafiği.



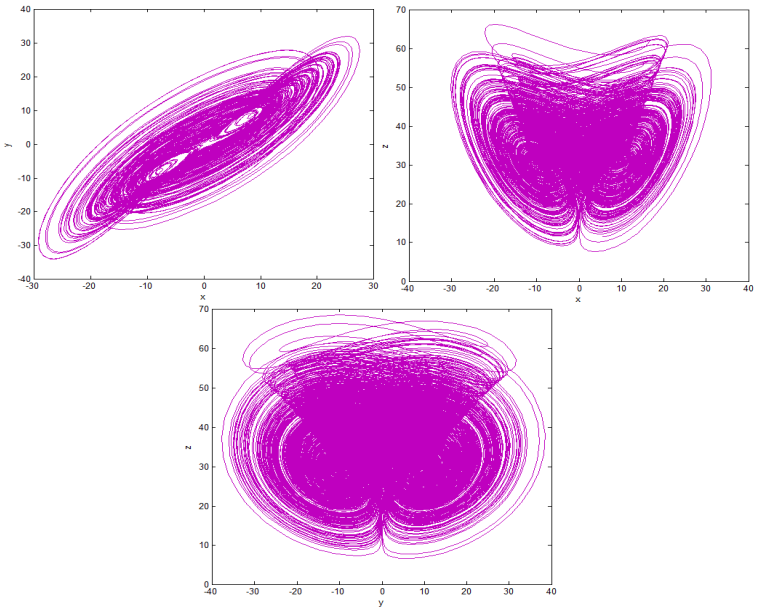

**Şekil 3.12.** Chua sistemi kaotik zaman serisi.

### 3.2.3. Lü kaotik sistemi

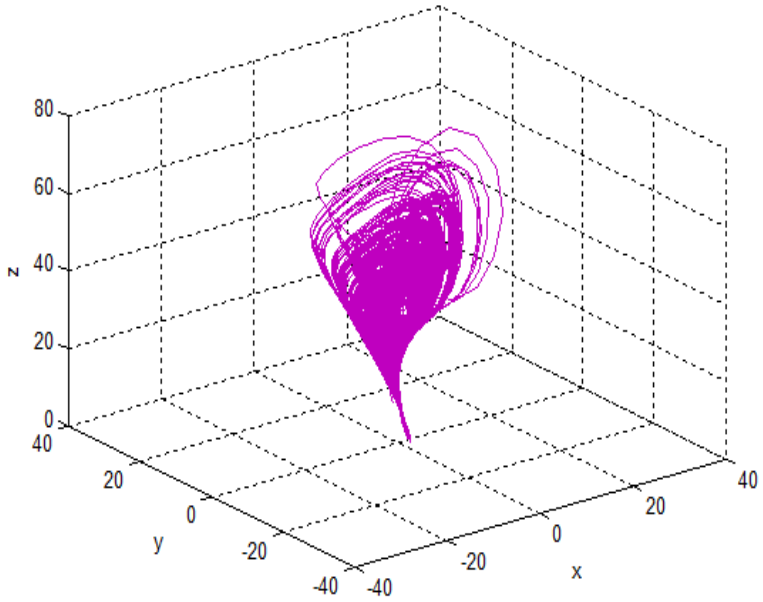
Lü kaotik sistem modeli aşağıdaki eşitlikle ifade edilir. Eşitliklerde $a$, $b$ ve $c$ sabit parametrelerdir.

$$\begin{cases} x'(t) = a(y(t) - x(t)) \\ y'(t) = -x(t)z(t) + cx(t) \\ z'(t) = x(t)y(t) - bz(t) \end{cases} \tag{3.15}$$

$a = 36, b = 3$ ve $c = 20$ olduğunda sistem kaotik davranış göstermektedir (Lü, vd., 2002). Lü kaotik sisteminin durum uzayı yörüngeleri Şekil 3.13'de görüldüğü gibi oluşmaktadır. Bu faz portrelerine ait grafik üç boyutlu oluşturulduğunda x, y ve z eksenlerindeki görünümü Şekil 3.14'deki gibi olmaktadır.

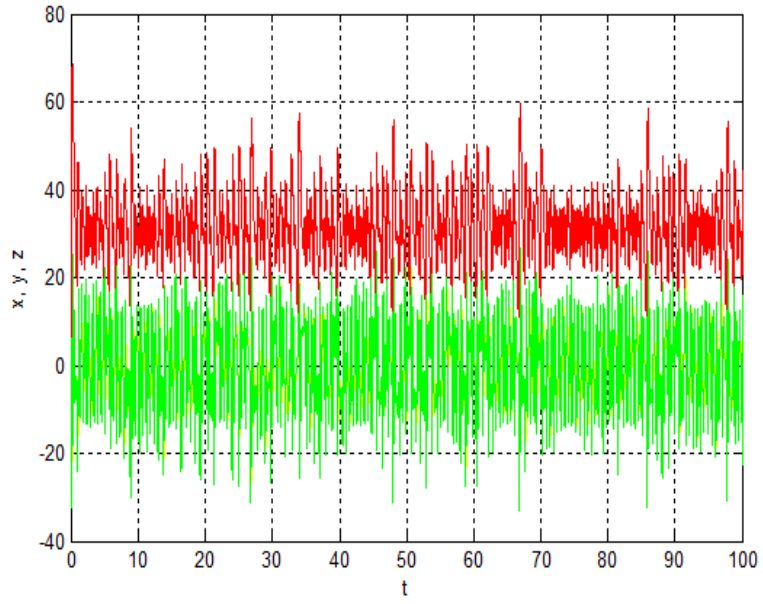


**Şekil 3.13.** Lü sistemine ait x-y, x-z, y-z fazları.




**Şekil 3.14.** Lü kaotik sistemi üç boyutlu grafiği.

Lü sistemi için belirtilen parametrelere bağlı olarak elde edilen kaotik zaman serisi Şekil 3.15'de görüldüğü gibi olmaktadır.



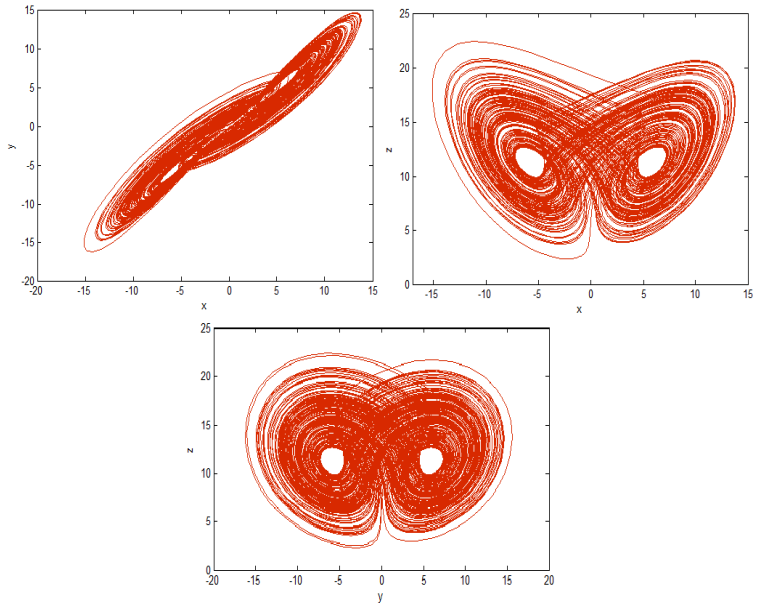

**Şekil 3.15.** Lü sistemi kaotik zaman serisi.

### 3.2.4. Chen kaotik sistemi

Chen kaotik sistem modeli aşağıdaki Eşitlik 3.16 ile ifade edilir.

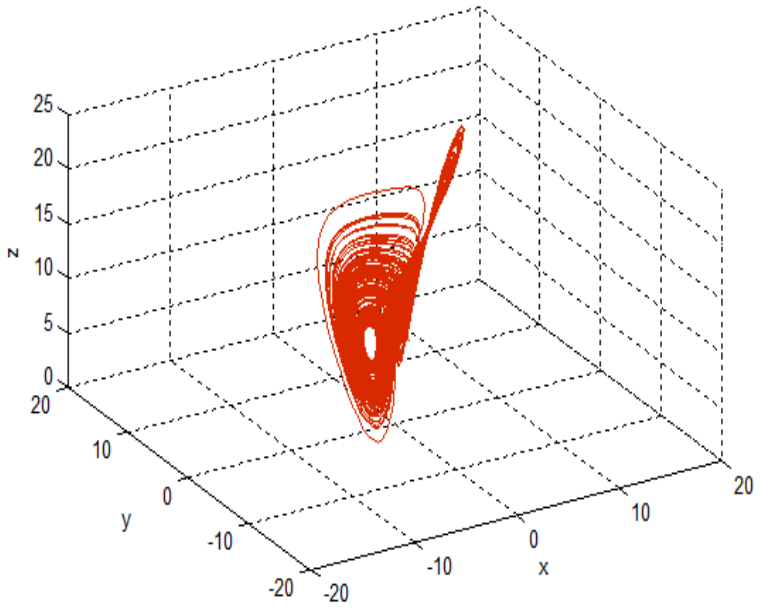
$$\begin{cases} x'(t) = a(y(t) - x(t)) \\ y'(t) = (c-a)x(t) - x(t)z(t) + cy(t) \\ z'(t) = x(t)y(t) - bz(t) \end{cases} \tag{3.16}$$

Eşitliklerde $a, b$ ve $c$ sabit parametrelerdir. $a = 35, b = 3$ ve $c \in [20,28.4]$ olduğunda sistem kaotik davranış göstermektedir (Xiao, vd., 2009; Chen ve Ueta, 1999). Simülasyon sonuçlarına göre sistem yörüngesi $c$ parametresine karşı aşırı hassastır, dolayısıyla bir şifreleme anahtarı üretildiğinde $c$ değeri ile kontrol edilebilir. Chen kaotik sisteminin durum uzayı yörüngeleri Şekil 3.16'da görüldüğü gibi oluşmaktadır.

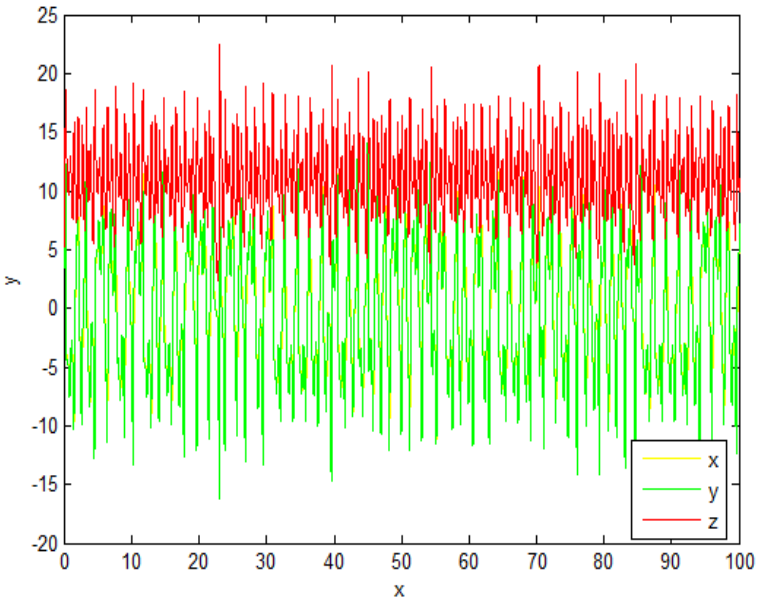



**Şekil 3.16.** Chen sistemine ait x-y, x-z, y-z fazları.

Bu faz portrelerine ait grafik üç boyutlu oluşturulduğunda x, y ve z eksenlerindeki görünümü Şekil 3.17'deki gibi olmaktadır. Chen sistemi için belirtilen parametrelere bağlı olarak elde edilen kaotik zaman serisi Şekil 3.18'de görüldüğü gibi olmaktadır.




**Şekil 3.17.** Chen kaotik sistemi üç boyutlu grafiği.



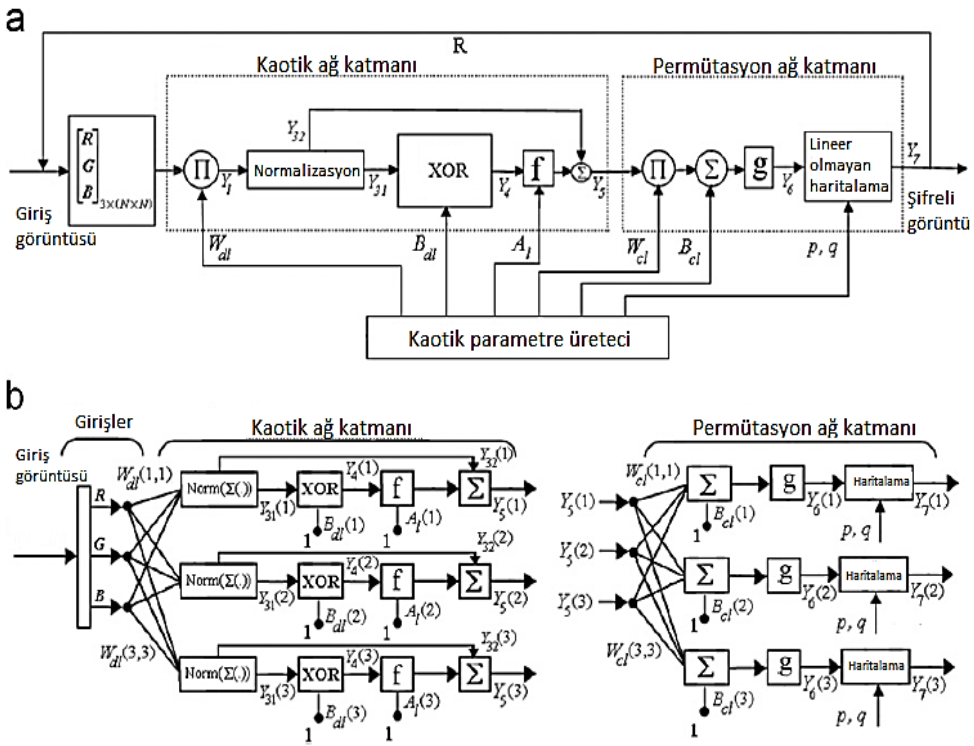

**Şekil 3.18.** Chen sistemi kaotik zaman serisi.

# 4. KAOTİK NÖRAL AĞ TABANLI GÖRÜNTÜ ŞİFRELEME

KNA tabanlı görüntü şifreleme (Bigdeli, vd., 2012)'de verilen algoritma ile gerçekleştirilmiştir. Bu çalışma KNA tabanlı görüntü şifreleme algoritması, şifre çözme algoritması ve algoritmanın güvenlik ve başarım analizleri bölümlerinden meydana gelmektedir.

## 4.1. Şifreleme Algoritması

Şifreleme algoritması, kaotik anahtar üretim bloğu, kaotik ağ katmanı (KAK) ve permütasyon ağ katmanından (PAK) oluşan üç ayrı öbek içermektedir. Şekil 4.1'de bu şifreleme yönteminin öbek yapısı görülmektedir. İkinci ve üçüncü katmanlar 3 giriş 3 çıkış ve 3'er nörondan meydana gelmektedir. Kaotik anahtar üretim bloğu bu katmanlara uygun ağırlık ve eşik (bias) değerleri üreterek ağı desteklemektedir.

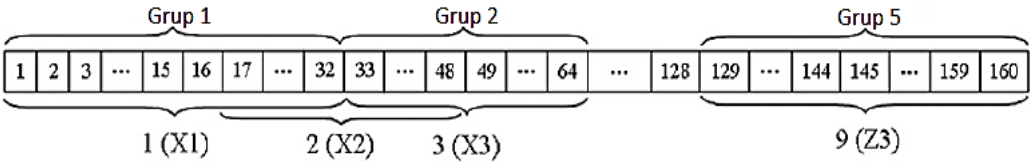



**Şekil 4.1.** Şifreleme süreci (a) öbek şeması, (b) ağ şeması (Bigdeli, vd., 2012).

Giriş görüntüsünün RGB bileşenleri KAK'ın girişine uygulanır. Girdilerin doğrusal kombinasyonu bir doğrusal ve bir de eğrisel aşamadan geçirilir. Bunlar

doğrusal normalizasyon ve bit bazında özel veya işlemleridir. Ardından aktivasyon fonksiyonu olan kaotik Tent Map bloğuna girilir. Bu katmanın çıkışı PAK'a giriş olarak verilen dağınık (karışık) bir bilgidir. Bu katmanda permütasyon, bilginin karıştırılması, iki adımda gerçekleşir. İlk adımda gizli veriye doğrusal bir permütasyon uygulanır. Permütasyon matrisi kaotik anahtar üretim bloğu tarafından üretilir. Daha sonra dağınık diziler 2B Cat Map (Bkz. Eşitlik 3.4) permütasyon algoritması vasıtasıyla eğrisel (lineer olmayan) bir şekilde karıştırılır. Bu işlemler yüksek güvenlik ve daha fazla karışıklık sağlamak amacıyla birkaç kez (R kez) tekrarlanır. Şifreleme işlemi aşağıdaki adımlar takip edilerek gerçekleştirilir (Bigdeli, vd, 2012).

*Adım 1:* Algoritmada, gizli anahtar olarak kullanılmak üzere 160 bitten meydana gelen bir doğrulama kodu kullanılmaktadır. Bu bilgilere bakarak anahtar boyutunun $2^n$ olmasından dolayı $2^{160}$ olduğu görülmektedir. $n$ anahtarın bit türünden uzunluğudur. Doğrulama kodu olarak 160 bitlik bir dizi seçilir ve sonra bu dizi beş gruba bölünür. Bu beş gruptaki değerler $x_1(0), y_1(0), z_1(0), x_2(0), y_2(0), z_2(0), x_3(0), y_3(0), z_3(0)$ olarak 9 giriş parametresi olarak ayrılır. Doğrulama kodundan gizli anahtarın üretimi Şekil 4.2'de görüldüğü gibidir. Daha sonra tekrar sayısı olarak bir $R$ değeri ve tamamlayıcı gizli anahtar olarak $N_0$ değeri belirlenir.




**Şekil 4.2.** 160 bit doğrulama kodundan 9 adet anahtar üretimi (Bigdeli, vd., 2012).

*Adım 2:* Chua, Lorenz ve Lü kaotik sistemleri geçiş işlemlerinin zararlı etkisinden kurtulmak amacıyla Runge-Kutta algoritmasını kullanarak $N_0$ adım işletilir. Böylece $x_1(N_0), y_1(N_0), z_1(N_0), x_2(N_0), y_2(N_0), z_2(N_0), x_3(N_0), y_3(N_0), z_3(N_0)$ elde edilir. Adım sayısı olarak bir $k$ sayısı belirlenir ve başlangıçta $k = 1$ alınır, her adımda 1 artırılır.

*Adım 3:* $N \times N$ piksel boyutlarında bir $F$ görüntüsü seçilir. Belirlenen üç kaotik sistem $N_0$ kez iterasyondan geçirildiği için, $N_0$'a kadar olan kısım tekrar

kullanılmayacaktır. $i = (r-1) \times (N \times N) + 1, \ldots, r \times (N \times N)$ olmak üzere $N_0 + i$ için üç kaotik sistemin değerleri iteratif şekilde hesaplanır. $i = 1, 2, \ldots, r \times (N \times N)$ olmak üzere kaotik sistemin iterasyon sayısını temsil eder. Her bir iterasyonda $W_{dl}, A_l$ ve $B_{dl}$ değerleri sırasıyla Eşitlik 4.1, 4.2, 4.3, 4.4 ve 4.5 kullanılarak hesaplanır.

$$W_{dl} = \begin{bmatrix} x_1(N_0+i) & x_2(N_0+i) & x_3(N_0+i) \\ y_1(N_0+i) & y_2(N_0+i) & y_3(N_0+i) \\ z_1(N_0+i) & z_2(N_0+i) & z_3(N_0+i) \end{bmatrix} + \alpha I \tag{4.1}$$

$$a(j,i) = mod\left(\left(\left|x_j(N_0+i)\right| - floor\left(x_j(N_0+i)\right)\right) \times 10^{14}, 255\right) + 1, \ \ j = 1,2,3 \tag{4.2}$$

$$A_l(i) = [a(1,i), a(2,i), a(3,i)]^T \tag{4.3}$$

$$b(j,i) = mod\left(\left(\left|y_j(N_0+i)\right| - floor\left(y_j(N_0+i)\right)\right) \times 10^{14}, 255\right) + 1, \ \ j = 1,2,3 \tag{4.4}$$

$$B_{dl}(i) = [b(1,i), b(2,i), b(3,i)]^T \tag{4.5}$$

$W_{dl}$ KAK'ın ağırlık matrisini, $A_l$ ve $B_{dl}$ KAK'ın eşik (bias) matrislerini, $mod(x,y)$ x'in y'ye bölümünden kalanı, $floor(x)$ x değerini kendisinden daha küçük veya eşit olan tamsayıya yuvarlanmasını temsil etmektedir. $I$ matrisi 3x3 boyutlarında birim matris ve $\alpha$ parametresi $W_{dl}^{-1}$ matrisinden kaynaklanan düzenlilik problemlerini önlemek amacıyla kullanılmaktadır. Bir diğer matris olan $W_{cl}$, PAK'ın ağırlık matrisidir ve kaotik nöral ağın çıkışının üç renk bileşeninin doğrusal karışımı için kullanılır. Yani görüntünün R, G ve B bileşenlerinin pozisyonlarını değiştirmek için kullanılır. Dolayısıyla 3x3 boyutunda matrislerden meydana gelir ve her bir satır ve sütunda sadece bir adet '1' değeri bulunur. $W_{cl}$'yi belirlemek için Eşitlik 4.6, 4.7, 4.8 ve 4.9 kullanılır.

$$D_i = [x_1(N_0+i), y_2(N_0+i), z_3(N_0+i)] \tag{4.6}$$

$$w_{1,i} = \arg(\max(D_i)) \tag{4.7}$$

$$w_{2,i} = \arg(\max(D_i)) \tag{4.8}$$

$$W_{cl,i}(1,w_{1,i}) = W_{cl,i}(2,w_{2,i}) = 1 \tag{4.9}$$

Eşitlik 4.7 ve 4.8'de belirtilen $\arg(\max(D_i))$, $D_i$ vektöründeki maksimum değerin indeksini belirlemektedir. Sonra $W_{cl}$ matrisinin ilk ve ikinci satırlarının 0 olmayan terimleri belirlenir. Bu işlemlerin ardından $W_{cl}$ matrisinin her satır ve sütunda yalnız bir adet '1' olacak şekilde üçüncü satırın 0 olmayan terimi belirlenir. Bir görüntüdeki RGB değerlerinin pozisyonlarının değişimi Eşitlik 4.10'daki gibi örneklenebilir.

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} B \\ R \\ G \end{bmatrix} \tag{4.10}$$

*Adım 4:* Giriş görüntüsü *F*'nin $N \times N$ piksel olduğu varsayılır. *F* görüntüsünün RGB değerleri ile boyutu $N \times N \times 3$ olmaktadır. Giriş değerlerinin RGB bileşenlerinin $i$. pikselinin değeri $X_k = [R_k, G_k, B_k]^T$, $k = 1, \dots, (N \times N)$ şeklinde gösterilebilir. Görüntünün tüm renk bilgileri $3 \times (N \times N)$ şeklinde üç satırdan meydana gelen bir matrise dönüştürülür. *X* matrisi KAK'ın girişi olarak hesaplanır.

*Adım 5:* Gizli bilgiyi üretmek için F matrisinin her bir sütununa birkaç işlem uygulanır. İşlemler $F_k$, $k = 1, \dots, (N \times N)$ ve $i = (r-1) \times (N \times N) + 1, \dots, r \times (N \times N)$ değerlerine bağlı olarak $X_1$ (Eşitlik 4.11) elde edildikten sonra normalizasyon uygulanarak (Eşitlik 4.12) değerler 0-255 aralığına alınır ve $X_2$ belirlenir.

$$X_{1,k} = W_{dl}(i)F(k) \tag{4.11}$$

$$X_2(k) = Normalizasyon(X_1(k)) \tag{4.12}$$

$X_2$, 0-255 aralığında belirlendikten sonra $X_3$ değeri Eşitlik 4.13'deki gibi hesaplanır. Ardından daha sonraki işlemlerde kullanılmak üzere $X_{31}$ (Eşitlik 4.14) ve $X_{32}$ (Eşitlik 4.15) değerleri de $X_3$'e bağlı olarak belirlenir.

$$X_3(k) = floor\big(X_2(k)\big) + mod(X_2(k), floor(X_2(k))) \tag{4.13}$$

$$X_{31}(k) = floor\big(X_2(k)\big) \tag{4.14}$$

$$X_{32}(k) = mod(X_2(k), floor(X_2(k))) \tag{4.15}$$

$$X_4(k) = XOR(X_{31}(k), B_{dl}(i)) \quad (4.16)$$

$$X_5(k) = f(X_4(k), A_l(i)) + X_{32}(k) \quad (4.17)$$

Özel veya (XOR) işlemi ile $X_4$ (Eşitlik 4.16) değeri belirlenir. Bu adımda XOR işlemi bit bit özel veya işleminin gerçeklemesini sağlamaktadır. Daha sonra kaotik aktivasyon fonksiyonu (Eşitlik 4.17) uygulanır. $f$ fonksiyonu kaotik Tent Map sisteminin uygulandığını ifade etmektedir.

*Adım 6:* KAK'ın çıkışı olan $3 \times (N \times N)$ boyutlarındaki $X_5$ matrisi PAK'de iki aşamada karıştırılır. İlk adımda, $X_5$'in $X_5(k), k = 1, \dots, (N \times N)$ her sütunu doğrusal bir şekilde karıştırılır.

$$X_6(k) = g(W_{cl}(i)X_6(k) + B_{cl}(i)) \quad (4.18)$$

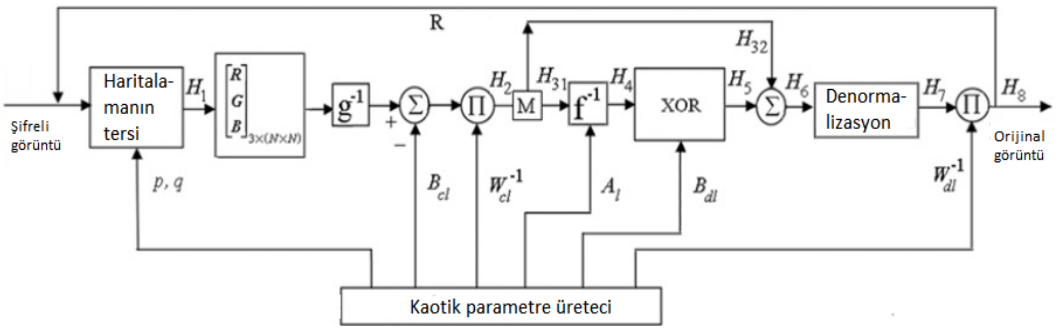
Genellikle, nöral ağ katman yapısındaki parametreler olan nöronların aktivasyon fonksiyonları, ağırlık matrisi ve bias vektörü belirlenen amaçlar doğrultusunda düzenlenir. Bu çalışmada amaç, nöral yapıyı kullanarak görüntünün kırmızı, mavi ve yeşil bileşenlerinin pozisyonlarını ve piksel değerlerini değiştirmektir. Bunun için uygun ağırlık değerleri ve bias değerleri seçilir. Bias kullanımıyla elde edilen sonuçlar görüntü piksel değerlerini doğrudan etkilediğinden $B_{cl}(i) = [0,0,0]^T$ olarak belirlenmesi uygundur. $g(x) = x$ eşitliği elde edilen sonuçların yüksek başarım oranına sahip olmasını sağlamaktadır. Ancak her zaman $g(x) = x$ olduğunda istenilen sonuçlar elde edilememektedir. Bu fonksiyon tersinir olacak şekilde değiştirilerek elde edilen R, G ve B değerlerinin histogramları istenilen şekilde elde edilebilmektedir. Ağırlık matrisi olan $W_{cl}$ de 3. adımda belirtildiği gibi hesaplanır.

*Adım 7:* Bu adımda lineer permütasyon aşamasının çıkışları karıştırılır. Bu amaçla $X_6$ matrisinin her satırı bir $N \times N$ matrisi şeklinde düzenlenir ve böylece üç çıkış $N \times N$ matrisi elde edilir. Sonra her matris 2B Cat Map permütasyon algoritması (Bkz. Eşitlik 3.4) ile karıştırılır. Lineer olmayan bir şekilde karıştırılan matrisler şifreli görüntünün kırmızı, yeşil ve mavi değerleri ve şifreli görüntü çıkışı $X_7$ olarak belirlenir.

*Adım 8:* Eğer geçerli şifreleme için son iterasyona gelinmemişse ($r < R$), $F = X_7$ yapılır. $r$ değeri 1 artırılır ve 3. adıma geri dönülür. Bu şekilde devam edilerek son iterasyonda şifreli görüntü ($F_{son}$) elde edilir ve şifreleme işlemi tamamlanmış olur.

### 4.2. Şifre Çözme Algoritması

Şifre çözme aşamasında, şifreleme işleminde yapılan işlemlerin tersi gerçekleştirilmelidir. Dolayısıyla, PAK ve KAK işlemlerinin tersi belirlenip şifreli görüntüye iteratif bir şekilde uygulanarak orijinal görüntü elde edilmeye çalışılmalıdır. Şifre çözme öbek şeması Şekil 4.3'de görülmektedir. Akış şemasına bakılarak şifre çözme süreci aşağıdaki adımlarla yapılabilir.




**Şekil 4.3.** Şifre çözme öbek şeması (Bigdeli, vd., 2012).

*Adım 1:* Şifreleme işleminde kullanılan doğrulama kodu ile gizli anahtar olan $x_1(0), y_1(0), z_1(0), x_2(0), y_2(0), z_2(0), x_3(0), y_3(0), z_3(0)$ değerleri üretilir. $N_0$ ve $R$ değerleri bilindiğine göre Chua, Lorenz ve Lü kaotik sistemleri $i = (i-1) \times (N \times N) + 1, \dots, i \times (N \times N)$ olacak şekilde iterasyon yapılır. $r = R$ ve giriş görüntüsü $S = F_{son}$, yani şifreli görüntü olur.

*Adım 2:* Şifreleme işleminde hesaplanan $W_{cl}, W_{dl}, B_{dl}, B_{cl}$ ve $A_l$ değerleri üç kaotik sistemi kullanarak $N_0 + i$, $i = (r-1) \times (N \times N) + 1, \dots, r \times (N \times N)$ için hesaplanır (Bkz. Eşitlik 4.1, 4.3, 4.5, 4.9).

*Adım 3:* $S$ şifreli görüntüsünün her bir tabakasına (R, G veya B), doğrusal olmayan permütasyonun tersi uygulanır. Elde edilen değerler $S_1$'de $3 \times (N \times N)$ matris formunda tutulur.

*Adım 4:* $S_1(k)$ ifadesi $k = 1, 2, \dots, (N \times N)$ $S_1$ matrisinin k. sütunu ve $i = (r-1) \times (N \times N) + 1, \dots, r \times (N \times N)$ olmak üzere, doğrusal permütasyonun tersi aşağıdaki gibi yapılır.

$$S_2(k) = W_{cl}^{-1}(g^{-1}\big(S_1(k)\big) - B_{cl}(i)) \tag{4.19}$$

*Adım 5:* Şifrelemede yapılan matematiksel işlemlerin tersi uygulanarak gizli bilgi sırasıyla Eşitlik 4.20, 4.21, 4.22, 4.23. 4.24, 4.25, 4.26 ve 4.27 kullanılarak elde edilir. Şifrelemede yapılan normalizasyon işleminin tersi uygulanarak denormalizasyon gerçekleştirilir.

$$S_3(k) = floor\big(S_2(k)\big) + mod\left(S_2(k), floor\big(S_2(k)\big)\right) \tag{4.20}$$

$$S_{31}(k) = floor\big(S_2(k)\big) \tag{4.21}$$

$$S_{32}(k) = mod\left(S_2(k), floor\big(S_2(k)\big)\right) \tag{4.22}$$

$$S_4(k) = f^{-1}\big(A_l(i), H_{31}(k)\big) \tag{4.23}$$

$$S_5(k) = XOR\big(S_4(k), B_{dl}(i)\big) \tag{4.24}$$

$$S_6(k) = S_5(k) + S_{32}(k) \tag{4.25}$$

$$S_7(k) = Denormalizasyon\big(S_6(k)\big) \tag{4.26}$$

$$S_8(k) = W_{dl}^{-1} S_7(k) \tag{4.27}$$

$f^{-1}$ fonksiyonu Eşitlik 4.17'de belirtilen kaotik Tent Map'in tersidir ve Eşitlik 4.12'deki normalizasyon fonksiyonunun tersi Eşitlik 4.26'dır.

*Adım 6:* $3 \times (N \times N)$ boyutlarındaki $S_8$ matrisi $N \times N$ piksel ile üç renk bileşenli görüntü haline dönüştürülür. Eğer $r > 1$ ise, $r = r - 1$ ve $S = S_8$ yapılarak 2. adıma dönülür ve iterasyon tekrar gerçekleştirilir. Aksi halde, şifre çözme işlemi tamamlanmıştır ve $S_8$ orijinal görüntü olarak elde edilmiştir.

### 4.3. Algoritmanın Güvenlik ve Başarım Analizleri

İyi bir şifreleme işlemi tüm kriptanalitik, istatistiksel ve kaba kuvvet ataklarına karşı güçlü olmalıdır. Gerçekleştirilen şifreleme işlemine bağlı olarak elde edilen sonuçlarla orijinal görüntüye ait bilgiler karşılaştırılarak başarım ve güvenlik analizleri alt bölümlerde yapılmıştır. Şifreleme işleminin başarılı olması için tüm analizlerden başarılı sonuç elde edilmesi gerekmektedir. Aksi takdirde şifreleme işleminde eksiklikler olduğu öngörülecektir. Bu analizler:

a. Anahtar alanı güvenliği,
b. Histogram analizi,
c. Anahtar hassaslığı,
d. Korelasyon katsayı analizi,
e. Bilgi entropi analizi,
f. Hız analizi

gibi algoritmanın güvenliği açısından önemli yere sahip analizlerdir. Alt bölümlerde çalışmada kullanılan algoritma için gerçekleştirilen analizlere ait sonuçlar verilmiştir. Analizler sonucu algoritmanın yüksek başarıma sahip olduğu gözlemlenmiştir.

#### 4.3.1. Anahtar alanı güvenliği

Anahtar güvenliği iki farklı durum içerir. Kaba kuvvet ataklarına karşı dayanıklılığını sağlayan anahtar boşluğunun uzunluğu bunlardan biridir. Eğer kısa bir anahtara sahipse kısa bir zamanda en iyi şifreleme algoritması bile kırılabilir. Fakat yeteri derecede uzun anahtarlı bir şifreleme algoritmasını kırmak çok zordur. Diğer durum anahtar geri dönüştürememe özelliğidir. Anahtarı hesaplanabilir bir şekilde ele geçirmek mümkün olmamalıdır. Bu çalışmada, gizli anahtar için 160 bit bir doğrulama kodu kullanılmıştır. $R, N_0, p, q$ değerleri de gizli anahtara ek olarak kullanılarak algoritmayı daha güçlü kılmaktadır. Dolayısıyla, en az 224 bit bir doğrulama kodu bahsedilen algoritmada uygulanabilmektedir. Seçilen anahtar boyutunun yeterli olup olmadığını incelemek için bazı araştırmalar yapılmıştır.

Lian (2009), yaptığı güvenlik analizine göre kendi kriptosisteminde anahtar boyutunu ($2^n$) $2^{64}$ olarak almıştır. Ayrıca kaba kuvvet ataklarına karşı sistem güvenliği sağlamak amacıyla anahtar uzunluğunun $N \geq 64$ olarak belirlenmesini tavsiye etmektedir. Lenstra ve Verheul (2001), simetrik anahtarlı kriptosistemlerin anahtar boyutlarından bahsetmiştir. En iyi bilinen simetrik anahtarlı kriptosistem olan ve 1977'de bulunan Data Encryption Standard (DES) anahtar boyutunun 56 bitten meydana geldiğini belirtmiştir. Diğer simetrik anahtarlı kriptosistemler ve anahtar boyutları:

- İki anahtar üçlü DES, anahtar boyutu 112,
- IDEA, anahtar boyutu 128,
- RC5, anahtar boyutu değişken,
- Advanced Encryption Standard (AES), anahtar boyutu 128, 192 ve 256 bit (Lenstra ve Verheul, 2001).

Lenstra ve Verheul (2001), 2016 yılında 83 bit simetrik kriptosistem anahtar boyutunun yeterli olacağını düşünmüştür. Asimetrik kriptosistemlerde kullanılan anahtar boyutunun ise 2016'da 1664 bit olacağını öngörmüştür. Simetrik kriptosistemlerin aksine, asimetrik kriptosistemlerde anahtar boyutları daha büyük olmaktadır. Çizelge 4.1'de yıllara göre kriptosistemlerde oluşacak anahtar boyutlarının alt sınırının yer aldığı değerleri Lenstra ve Verheul (2001) çalışmalarında tahmini olarak hesaplamıştır.

**Çizelge 4.1.** Kriptosistemlerin yıllara göre anahtar boyutları tahmini.

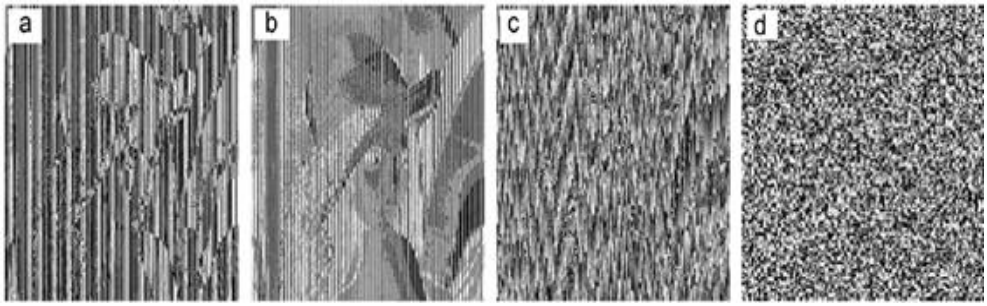
| Yıl / Kriptosistem | Simetrik Anahtarlı | Asimetrik Anahtarlı |
|---|---|---|
| 2020 | 86 bit | 1881 bit |
| 2030 | 93 bit | 2493 bit |
| 2040 | 101 bit | 3214 bit |
| 2050 | 109 bit | 4047 bit |

Elde edilen sonuçlara göre asimetrik kripto sistemlerde yer alan anahtar boyutlarının, simetrik kripto sistemlere göre daha hızlı artacağı görülmektedir.

Asimetrik kriptosistemlerde asal sayıların kullanıldığını da hesaba katarsak, 2050'de 4047 bit olacağı öngörülen anahtar boyutun basamak sayısı 200-250 arasında olan asal sayılara tekabül edeceği anlaşılmaktadır. Çizelge 4.1'e göre bu yöntemde seçilen 160 bit doğrulama kodunun 2050 yılına kadar yeterli olacağı anlaşılmaktadır.

### 4.3.2. Histogram analizi

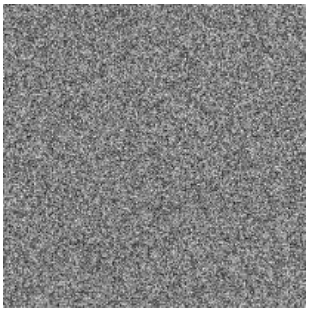
Bir görüntü histogramı, kendi renk yoğunluğu seviyesine karşı piksellerin yoğunluğunun dağılımını göstermektedir. Yapılan görüntü şifrelemenin histogram değerlerinin uygulanabilirliğini göstermek amacıyla "Lena", "Baboon", "Peppers" ve renk yoğunluğu düşük olan görüntüler seçilerek sonuçlar gözlenmiştir. $R = 2$ alınarak, orijinal görüntü, şifreli görüntü ve deşifre edilen görüntünün üç ana bileşen (R, G ve B renkleri) değerleri kıyaslanmıştır. Şifreli görüntünün histogram değerleri oldukça düzgün ve beyaz gürültüyü andıran iyi istatistiksel özelliklere sahip olduğu görülmüştür. Bu sayede, şifreli görüntüden orijinal görüntüdeki piksellerin sırası ve değerleri hakkında hiçbir bilgi elde edilemez. Dolayısıyla şifreli görüntü, orijinal görüntü ve önerilen şifreleme işlemi hakkında herhangi bir istatistiksel saldırıya maruz kalınması adına bir ipucu sağlamaz.




**Şekil 4.4.** Şifrelenmiş görüntüler (a) AES algoritması (b) Tent Map yöntemi (c)Kaotik nöral ağ (d) Bigdeli, vd. (2012)'nin nöral ağı (Bigdeli, vd., 2012).

Bigdeli vd. (2012)'de çalışılan Lena görüntüsünün dört yöntemle şifrelenmiş hali Şekil 4.4'de görülmektedir. Geleneksel AES algoritması (Mollin, 2006), sadece Tent Map yöntemiyle yapılan şifreleme (Masuda ve Aihara, 2002), kaotik nöral ağ ile yapılan şifreleme (Lian, 2009) ve farklı bir kaotik nöral ağ ile yapılan şifrelemeye (Bigdeli, vd., 2012) ait gri seviye görüntüler elde edilmiştir. Şifrelenmiş görüntüleri

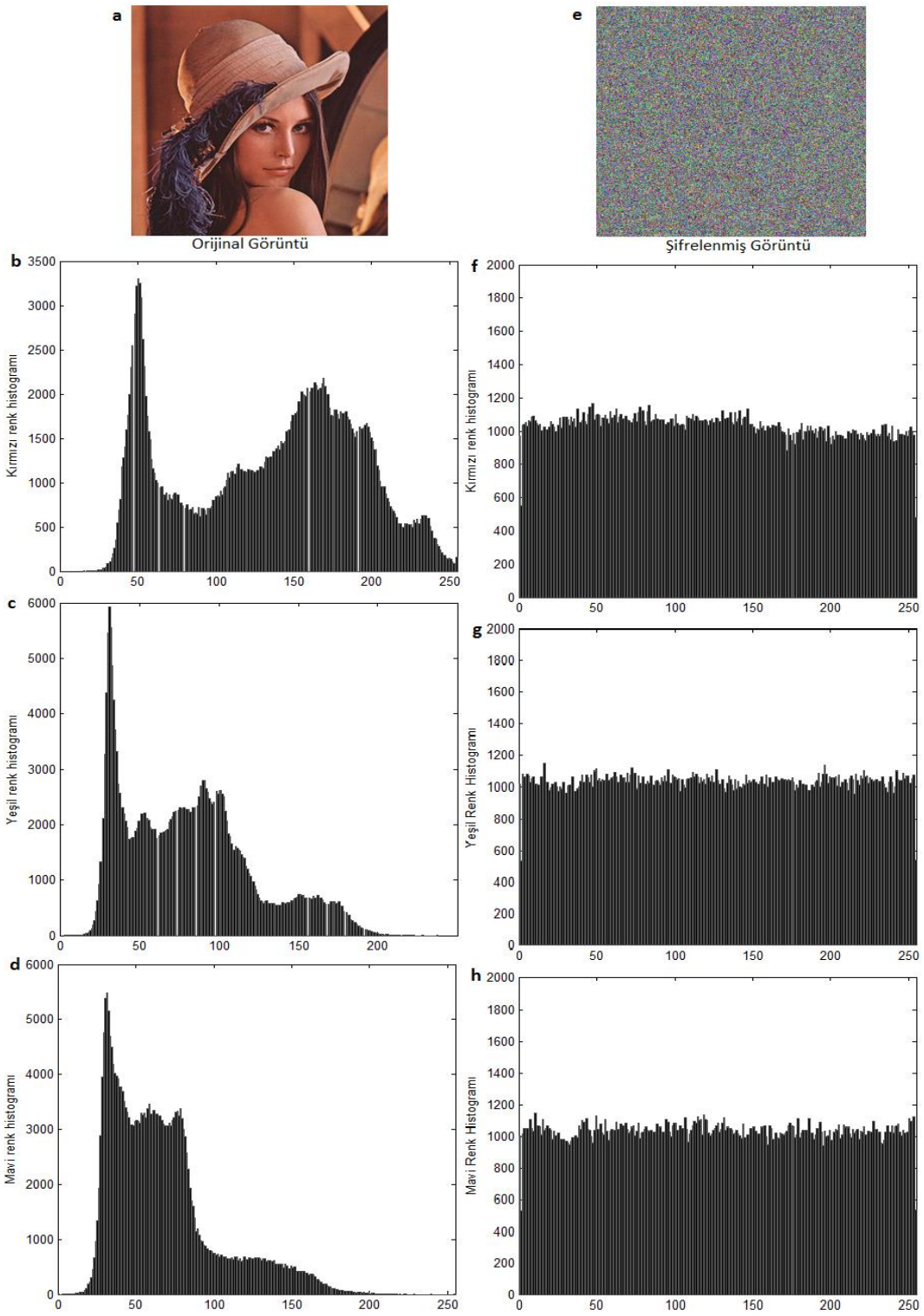
kıyasladığımızda a ve b görüntüleri fark edilebilir düzeydedir. Şekil 4.4'ün c ve d görüntülerinde herhangi bir şekilde orijinal görüntüye ait bir ize rastlanmamaktadır. Güvenlik ve fark edilebilirlik açısından en yüksek başarıma sahip olanının d görüntüsü olduğu görülmektedir.



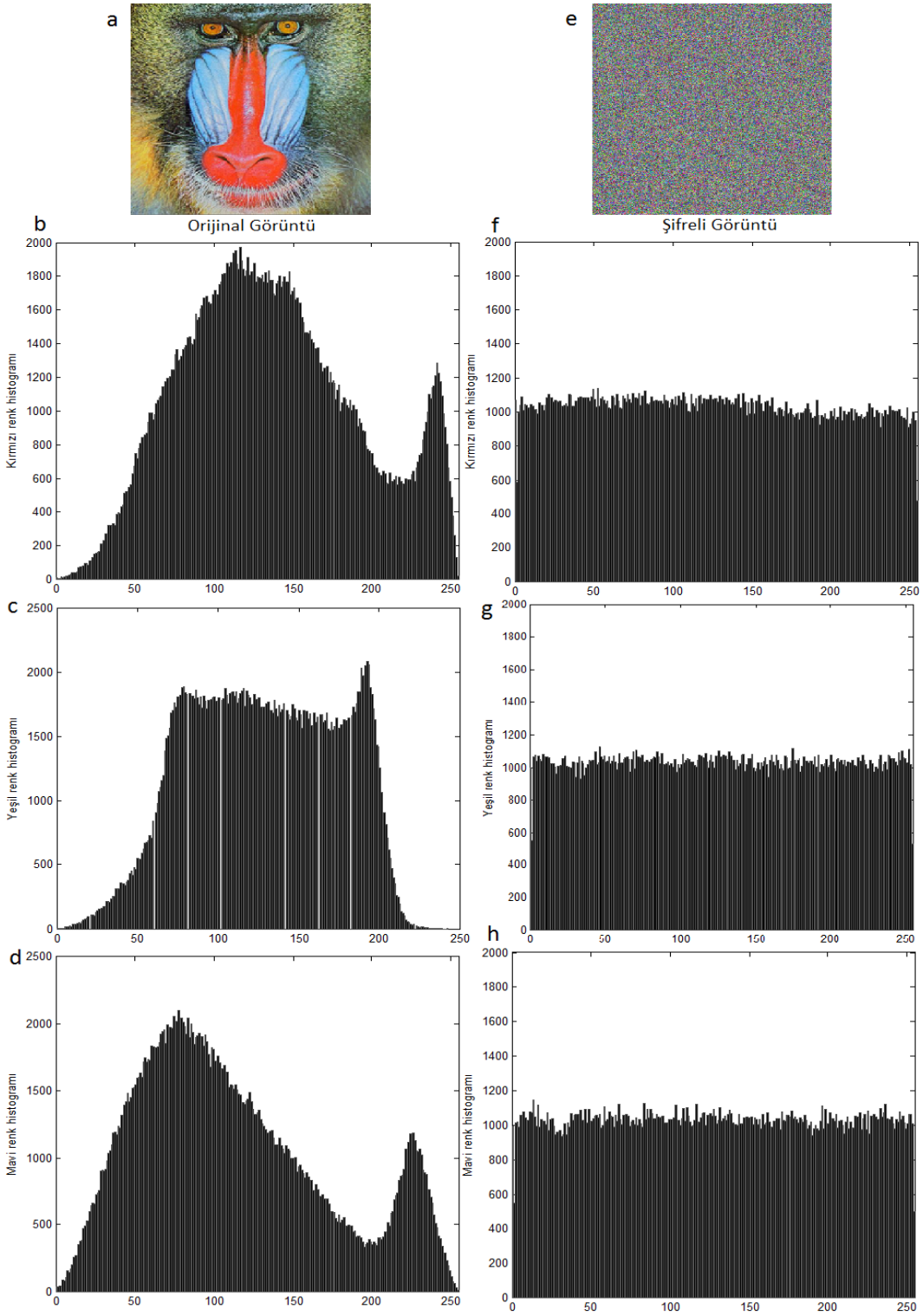
**Şekil 4.5.** Bu çalışmada şifrelenmiş Lena görüntüsü.

Buna ek olarak Şekil 4.4'de görülen gri seviye görüntü bu çalışmada kullanılan "Lena" görüntüsünün şifrelenmiş halidir. Bigdeli ve arkadaşlarının (2012) yaptığı şifrelemenin sonucu Şekil 4.4'deki (d) görüntüsüdür. Bu görüntü ile çalışmamızda yapılan şifreleme (Şekil 4.5) kıyaslandığında benzer sonuçlar verdiği görülmektedir.

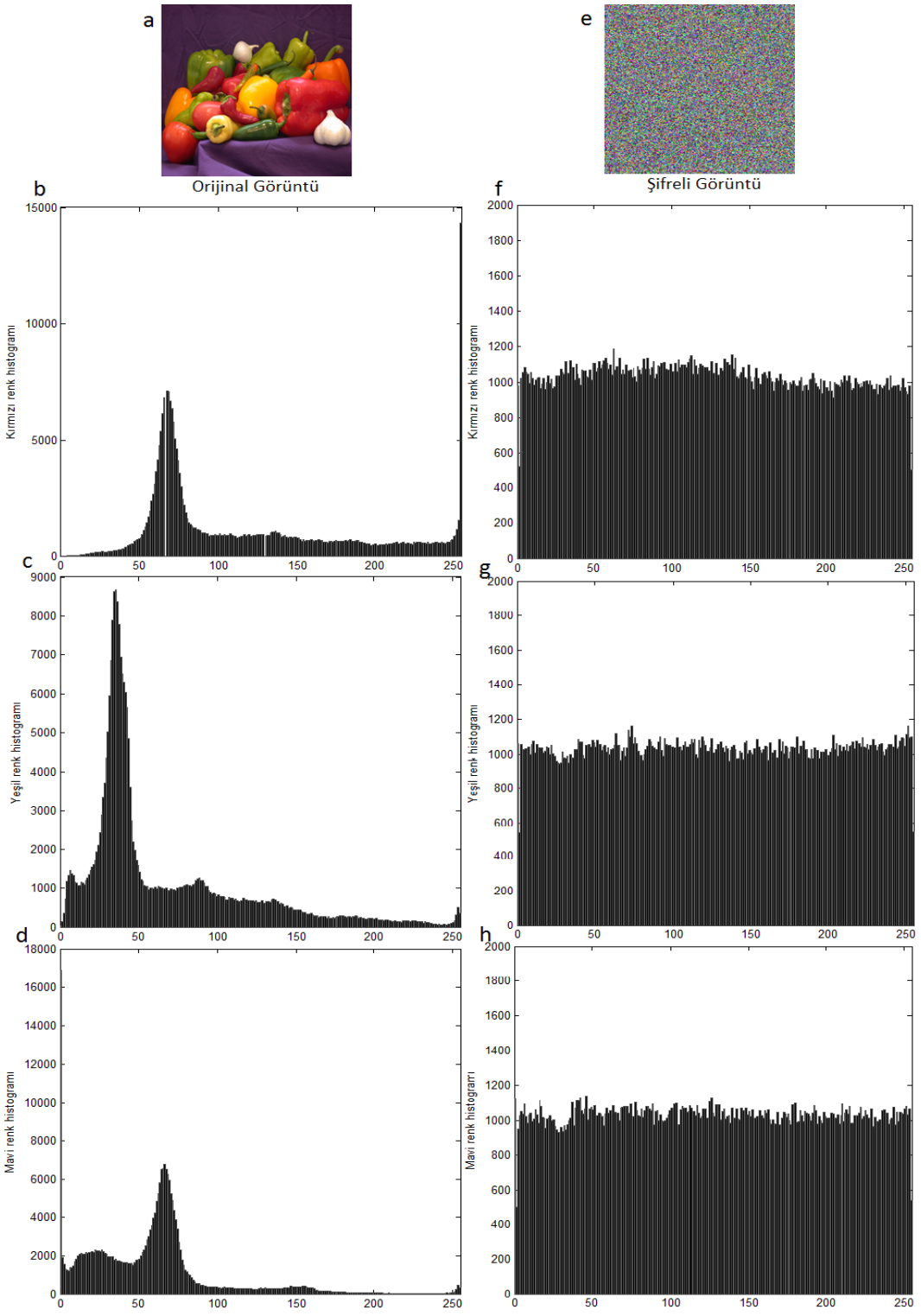
Şekil 4.6, Şekil 4.7 ve Şekil 4.8'de sırasıyla $512 \times 512$ boyutlarında olan "Lena", "Baboon" ve "Peppers" görüntülerinin orijinal hali, orijinal haline ait kırmızı, yeşil ve mavi histogramları, şifreli hali ve şifreli haline ait kırmızı, yeşil ve mavi histogramları verilmiştir. Orijinal ve şifreli görüntü histogramları birbiri ile karşılaştırıldığında başarılı bir sonuç elde edildiği görülmektedir.




**Şekil 4.6.** Histogram analizi. (a,b,c,d) ve (e,f,g,h) sırasıyla orijinal Lena görüntüsü ve şifrelenmiş Lena görüntüsü kırmızı, yeşil ve mavi histogramları.




**Şekil 4.7.** Histogram analizi. (a,b,c,d) ve (e,f,g,h) sırasıyla orijinal Baboon görüntüsü ve şifrelenmiş Baboon görüntüsü kırmızı, yeşil ve mavi histogramları.




**Şekil 4.8.** Histogram analizi. (a,b,c,d) ve (e,f,g,h) sırasıyla orijinal Peppers görüntüsü ve şifrelenmiş Peppers görüntüsü kırmızı, yeşil ve mavi histogramları.

### 4.3.3. Anahtar hassaslığı

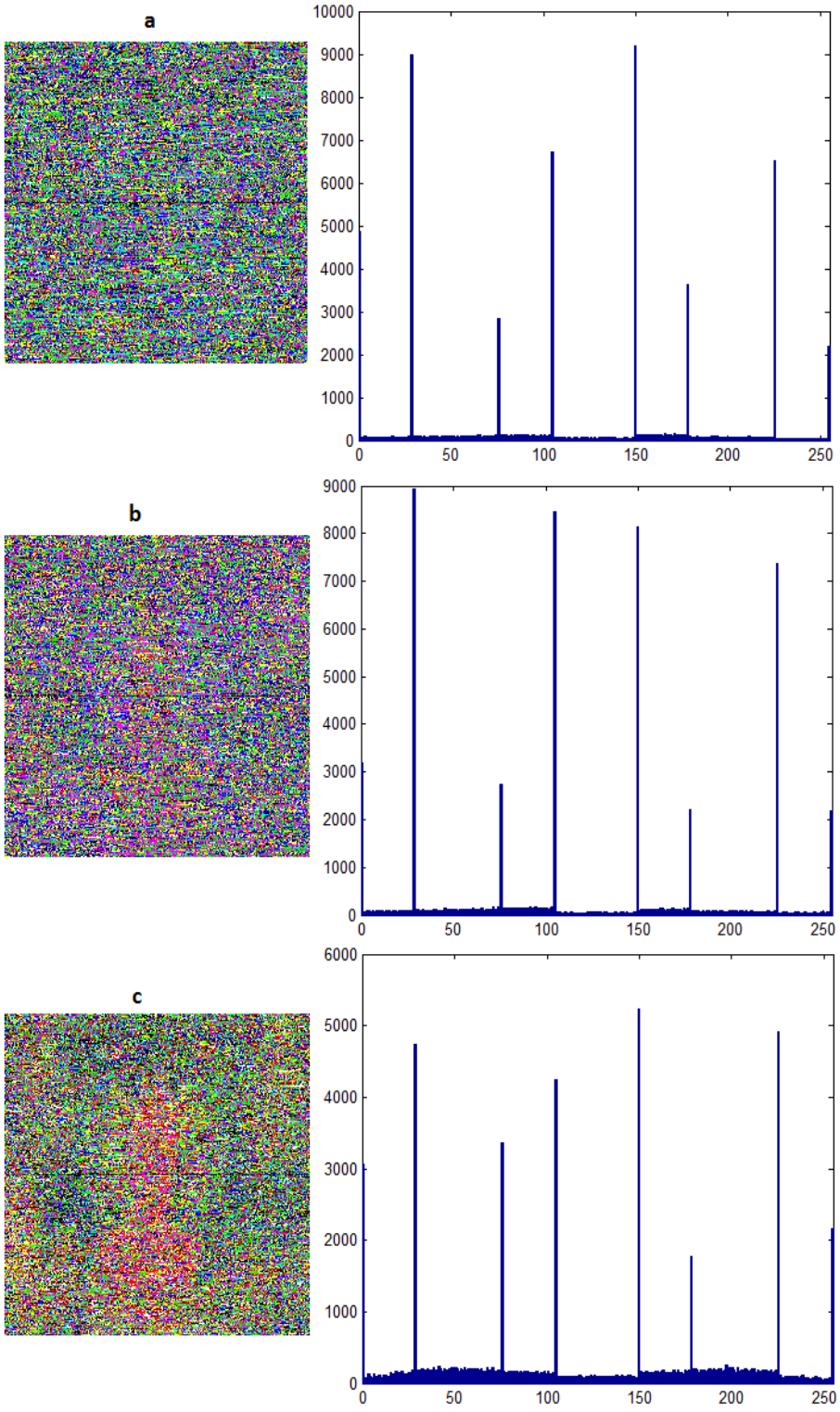
Bu algoritmada anahtar hassaslığını göstermek amacıyla, gizli anahtarda çok küçük değişiklikler yapılarak aynı koşullarda şifrelemeler yapılmıştır. Gizli anahtar olarak kullanılan $x_1(0), y_1(0), z_1(0), x_2(0), y_2(0), z_2(0), x_3(0), y_3(0), z_3(0)$ parametreleri $10^{-14}$, $10^{-15}$, $10^{-16}$ seviyelerinde değiştirilerek şifre çözmeye etkileri incelenmiştir. Eşitlik 4.28, 4.29 ve 4.30'da gizli anahtarların orijinal hali mevcuttur.

$$x_1(0) = 0.0051, x_2(0) = 0.0073, x_3(0) = 0.0095 \quad (4.28)$$

$$y_1(0) = 4.0035, y_2(0) = 3.5501, y_3(0) = 5.0008 \quad (4.29)$$

$$z_1(0) = 5.75001, z_2(0) = 4.9904, z_3(0) = 11.1101 \quad (4.30)$$

"Baboon" görüntüsü için şifre çözme sonucu elde edilen sonuçlar Şekil 4.9'daki gibi olmaktadır. Her şifre çözme işlemi için oluşan deşifre görüntü ve histogram değerleri ayrı ayrı görülmektedir. Görüldüğü üzere gizli anahtardaki çok küçük bir değişiklik bile deşifre görüntüyü orijinal görüntüden tamamen farklı hale getirmektedir. Bu gözlemlere dayanarak, gizli anahtarda sadece küçük bir değişikliğin meydana gelmesi hem piksel değerlerinde hem de işaretlerde değişikliğe neden olmaktadır. Örnek olması açısından, $x_1(0) = 0.0051, y_2(0) = 3.5501$ ve $z_3(0) = 11.1101$ başlangıç değerleri $10^{-14}$, $10^{-15}$ veya $10^{-16}$ seviyesinde değiştirilerek sırasıyla $x_1(0) = 0.0051000000000001$, $y_2(0) = 3.45010000000001$, $z_3(0) = 11.11010000000001$ olarak belirlenmiştir ve sırasıyla Şekil 4.9'daki (a), (b), (c) görüntüleri ve görüntülere ait histogramlar elde edilmiştir. Görüldüğü gibi bu değişiklik şifre çözme işlemini imkansız hale getirmektedir. Bu sonuçlara göre algoritmanın çok küçük bir değişime karşı gösterdiği davranışa bakılarak çok dayanıklı olduğu ve veri şifrelemede yüksek güvenlik sağladığı söylenebilir.




**Şekil 4.9.** Anahtar hassaslığı analizi, (a) x1 (b) y2 ve (c) z3'e bağlı şifre çözme.

### 4.3.4. Korelasyon katsayı analizi

Korelasyon, iki ya da daha fazla değişken arasındaki ilişkiyi artış ve azalış yönünden incelemektedir. Orijinal görüntüdeki bitişik pikseller arasındaki korelasyon oldukça yüksek olmaktadır. Etkili bir şifreleme algoritması bitişik pikseller arasındaki ilişkiyi azaltmalıdır (Bigdeli, vd., 2012; Chen, vd., 2004). Korelasyon katsayısı $k_{xy}$ Eşitlik 4.31'deki formül ile hesaplanmaktadır.

$$\begin{cases} e(x) = \frac{1}{N_l}\sum_{i=1}^{N_l} x_i \\ d(x) = \frac{1}{N_l}\sum_{i=1}^{N_l}(x_i - e(x))^2 \\ cov(x,y) = \frac{1}{N_l}\sum_{i=1}^{N_l}(x_i - e(x))(y_i - e(y)) \\ k_{xy} = \frac{cov(x,y)}{\sqrt{d(x)}\sqrt{d(y)}} \end{cases} \tag{4.31}$$

Eşitliklerde $x$ ve $y$ görüntüdeki bitişik iki pikselin gri seviye değerlerini, $cov(x,y)$ meydana gelen değişikliği, $d(x)$ varyans ve $e(x)$ ortalama değeri temsil etmektedir. Şekil 4.10'da sırasıyla "Lena" görüntüsünün dikey, yatay ve çapraz bitişik piksellerinin orijinal ve şifrelenmiş halleri rasgele 5000 bitişik piksel çifti alınarak kıyaslanmıştır.

**Çizelge 4.2.** Orijinal görüntülerin bitişik piksellerindeki korelasyon değerleri.

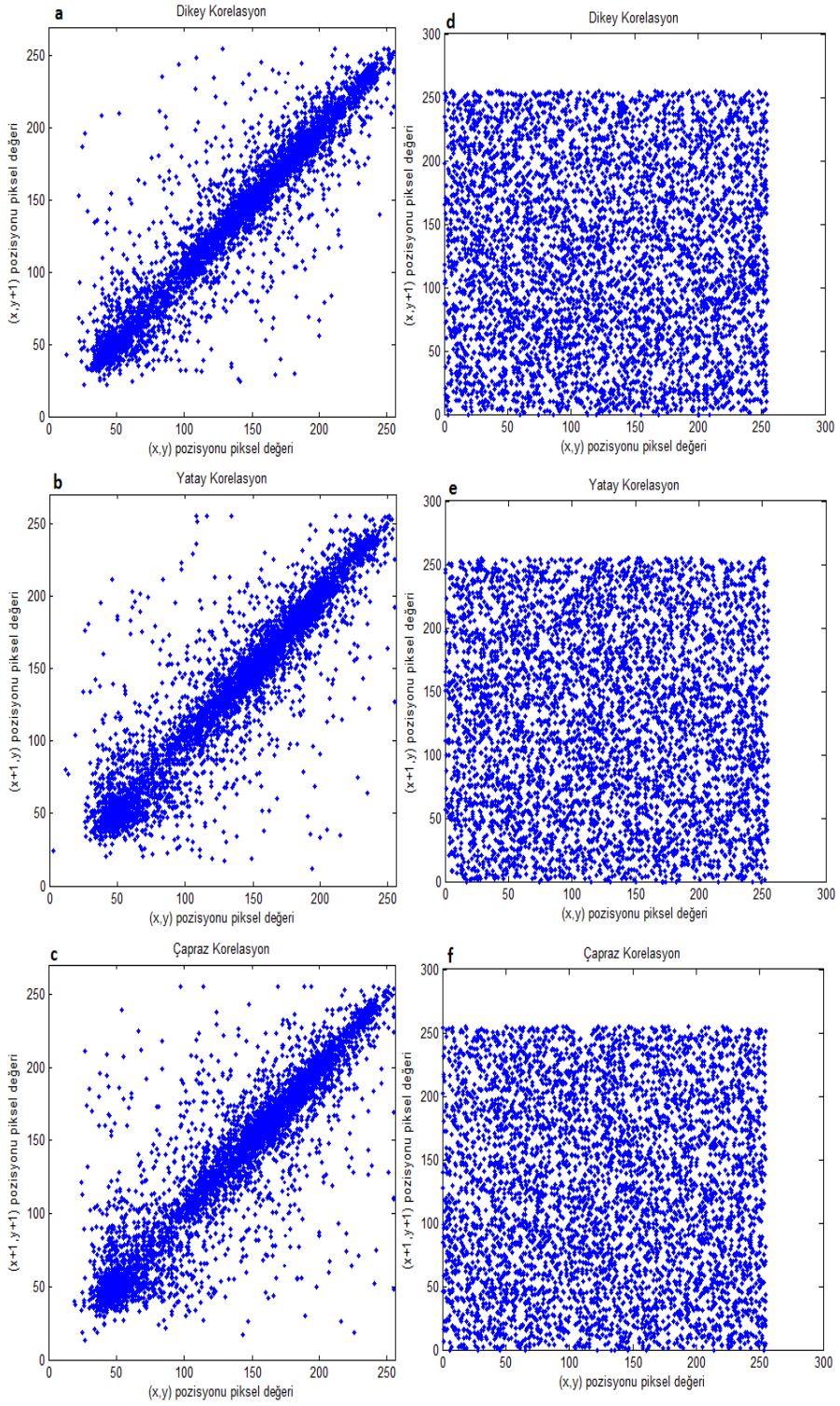
| Orijinal Görüntü | Dikey | Yatay | Çapraz |
|---|---|---|---|
| Lena | 0.94 | 0.9227 | 0.8983 |
| Baboon | 0.7585 | 0.83 | 0.7727 |
| Peppers | 0.9772 | 0.9793 | 0.9630 |
| Diğer | 0.9239 | 0.6427 | 0.5527 |

Grafikler incelendiğinde orijinal görüntüdeki bitişik piksellerin birbiriyle çok yüksek ilişkiye sahip olduğu, şifreli görüntüdeki iki komşu piksel arasındaki korelasyona bakıldığında ihmal edilebilir derecede küçük olduğu görülmektedir. Çizelge 4.2'de orijinal görüntülerin korelasyon değerleri listelenmiştir. Çizelge 4.3'de

şifreli görüntülerin dikey, yatay ve çapraz bitişik piksellerinin korelasyon değerleri görülmektedir. Elde edilen değerlerin oldukça küçük olduğu görülmektedir. "Diğer" olarak belirtilen görüntü renk yoğunluğu düşük bir görüntüdür.

**Çizelge 4.3.** Şifreli görüntülerin bitişik piksellerindeki korelasyon değerleri.

| Şifreli Görüntü | Dikey | Yatay | Çapraz |
|---|---|---|---|
| Lena | -0.0432 | -0.0145 | -0.0011 |
| Baboon | 0.0079 | -0.0038 | -0.0273 |
| Peppers | 0.0098 | -0.0141 | 0.0143 |
| Diğer | 0.0271 | 0.0122 | -0.0015 |




**Şekil 4.10.** Dikey, yatay, çapraz bitişik piksel korelasyon değerleri. (a), (b), (c) orijinal Lena görüntüsü ve (d), (e), (f) şifrelenmiş Lena görüntüsü.

### 4.3.5. Bilgi entropi analizi

Entropi, bir sistemdeki belirsizliklerin derecesini ifade etmektedir. Bir $m$ mesajı belirlediğimizde bilgi entropisi $E(m)$ Eşitlik 4.32'deki gibi hesaplanır (Bigdeli, vd, 2012).

$$E(m) = -\sum_{j=0}^{2^n-1} p(m_j) log_2 \frac{1}{p(m_j)} \quad (4.32)$$

$p(m_j)$, $m_j$'nin oluşma olasılığını ve $log_2$ 2 tabanında logaritmayı ifade eder. Rasgele bir süreçte her sembol eşit olasılığa sahiptir. $n = 8$ alındığında her sembol $p(m_j) = 2^{-8}$ oranında eşit olasılığa sahiptir. Böylece entropideki dağılım sonucu $E(m) = 8$ olur. Çizelge 4.4'de görülen sonuçlar "Lena", "Baboon", "Peppers" ve renk yoğunluğu düşük olan bir görüntü (Diğer) için entropi değerlerini göstermektedir. Elde edilen entropi değerleri incelendiğinde ideal değer olan 8'e çok yakın olduğu görülmektedir. Sonuç olarak şifreli görüntünün rasgele bir kaynağa yakın olduğu ve entropi ataklarına karşı güvenli olduğu görülmektedir.

**Çizelge 4.4.** KNA tabanlı şifrelenen görüntülerinin entropi değerleri.

| Görüntü | R | G | B |
|---|---|---|---|
| Lena | 7.9928 | 7.9937 | 7.9928 |
| Baboon | 7.9931 | 7.9938 | 7.9931 |
| Peppers | 7.9930 | 7.9934 | 7.9929 |
| Diğer | 7.9691 | 7.9675 | 7.9573 |

### 4.3.6. Hız analizi

Güvenlik konularının yanı sıra, gerçek zamanlı görüntü şifreleme ve şifre çözme süreleri de önemlidir. Çalışma süresini ölçmek amacıyla 1.60 GHz işlemci, 3 GB RAM donanımlı bir bilgisayar ile Matlab programının 2012 sürümü kullanılmıştır.

**Çizelge 4.5.** KNA tabanlı görüntü şifreleme süresi.

| Görüntü boyutu | Şifreleme Süresi (saniye) |
|---|---|
| $256 \times 256$ | 0.95 s |
| $512 \times 512$ | 3.77 s |
| $1024 \times 1024$ | 15.93 s |
| $2048 \times 2048$ | 62.70 s |

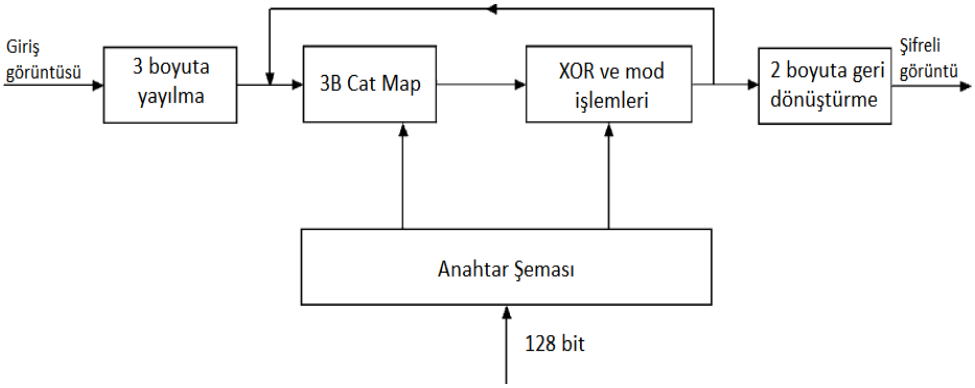
Çizelge 4.5'de görülen şifreleme hızlarını hesaplamak amacıyla rasgele seçilen beş farklı görüntüye ait şifreleme sürelerinin ortalaması alınmıştır. Bu süreler yaklaşık olarak birbirine eşit çıkmaktadır. Elde edilen sonuçlara göre şifreleme hızı 205 kb/s olarak hesaplanmıştır.

# 5. 3B KAOTİK CAT MAP TABANLI GÖRÜNTÜ ŞİFRELEME

3B KCM tabanlı görüntü şifreleme algoritması, şifre çözme algoritması ve algoritmanın güvenlik ve başarım analizleri bölümlerinden meydana gelmektedir. Chen, vd. (2004) kullandığı şifreleme algoritması ve adımları kullanılmıştır.

## 5.1.Şifreleme Algoritması

*Adım 1:* Anahtar üretimi. 128 bit bir dizi anahtar olarak seçilir ve 3B Cat Map'in (Bkz. Eşitlik 3.8) birkaç parametresi ve Logistic Map $a_x, b_x, a_y, b_y, a_z, b_z, L_g$ ve $T$ değerleri üzerine haritalanan sekiz gruba bölünür. Şifreleme blok diyagramı Şekil 5.1'de görülmektedir.




**Şekil 5.1.** 3B Cat Map ile görüntü şifreleme öbek şeması (Chen, vd., 2004).

*Adım 2:* İki boyutlu bir görüntü bir algoritmaya bağlı olarak üç boyutlu birkaç matris haline getirilir. Kullanılan görüntü $W$ piksel genişlik ve $H$ piksel yükseklikten oluşmaktadır. İlk önce görüntünün tüm pikselleri sırasıyla $N_1 \times N_1 \times N_1$, $N_2 \times N_2 \times N_2, \dots, N_k \times N_k \times N_k$ boyutlarındaki birkaç küpten oluşan yapılara bölünür. Bir görüntüyü birkaç küpe bölmek için aşağıdaki koşul sağlanmalıdır.

$$W \times H = N_1^3 + N_2^3 + \cdots + N_k^3 + R \tag{5.1}$$

$N_k \in \{2, 3, \dots, M\}$ değeri her küpün bir kenarının uzunluğunu, $M$ değeri maksimum oluşabilecek küp sayısını ve $R \in \{0, 1, \dots, 7\}$ değeri tüm küpler oluşturulduktan sonra kullanılmayan piksel sayısını belirtmektedir. R değeri,

görüntünün yükseklik ve genişliğinin çarpımından $N_k$ değerlerinin toplamını çıkardığımızda kalan değeri ifade etmektedir.

*Adım 3:* 3B Cat Map gerçekleştirilir. Her bir küp için $a_x, b_x, a_y, b_y, a_z, b_z$ kontrol parametrelerini kullanarak üç boyutlu ayrık Cat Map (Bkz. Eşitlik 3.8) uygulanır ve bu sayede küplerde bulunan piksel değerlerinin karışması sağlanır.

*Adım 4:* Yayılma süreci. Bu süreçte ilk değerlere $x(0) = L_g$ ve $S(0) = T$ atanır ve yayılma işlemi Eşitlik 5.2 ve 5.3'deki algoritmaya göre gerçekleştirilir.

*Adım 5:* Üç boyutlu halde karıştırılan küpler tekrar iki boyutlu görüntü haline dönüştürülür. Üç boyutlu küpler uygun bir şekilde düzenlenir ve ardından göstermek veya saklamak amacıyla iki boyutlu bir görüntüye dönüştürülür.

Adım 3 ve 4'te yapılan işlemler güvenlik belirli bir seviyeye gelinceye kadar düzenli bir şekilde tekrarlanır. İterasyon sayısı arttıkça daha güvenli bir şifreleme gerçekleşir, fakat hesaplama maliyeti ve zaman gecikmeleri gibi dezavantajlar ortaya çıkar. Yukarıda belirtilen adımlar gerçekleştirildikten sonra şifre çözme işlemi benzer bir şekilde gerçekleştirilir. Adım 3 ve 4'te yapılan işlemlerin tersi alınır. Şifreleme ve şifre çözme süreçleri benzer yapılara sahip olduğundan dolayı, aynı algoritmik karmaşıklığa ve zaman tüketimine sahip olurlar. Kaotik Cat Map tabanlı görüntü şifrelemeye ait adımlar kısaca yukarıda verilmiştir. Bu işlemlerin genişletilmiş hali devam eden bölümlerde açıklanacaktır.

### 5.1.1. Haritanın ayrıklaştırılması

Chen, vd. (2004), şifreleme sonlu bir yapıda çalışan bir tür dönüşüm olduğu için görüntü şifrelemede kaotik bir harita elde etmek amacıyla bir ayrıklaştırma yapmanın gerekli olduğunu belirtmişlerdir. Ayrıca karıştırma özelliği, başlangıç koşullarına ve parametrelerine hassas bağlılık gibi önemli özelliklerin korunması gerektiğini söylemişlerdir. Ayrıklaştırılmış harita 3B Cat Map kaotik sistemidir (Bkz. Eşitlik 3.8).

Kullanılan 3B Cat Map kaotik sisteminin avantajı parametre sayısının fazla olmasıdır. 3B Cat Map sisteminde altı adet parametre mevcut iken, 2B Cat Map sisteminde iki adet parametre mevcuttur. Bu nedenle görüntü şifrelemede kullanılan

anahtar boyutu artacak ve karıştırılan görüntü yapılan herhangi bir atağa karşı daha güçlü olacaktır.

### 5.1.2. Yayılma süreci

Bir şifreleme algoritmasını yayılma işlemine sokmak için iki sebep vardır. Yayılma süreci, ayrıklaştırılmış kaotik haritayı tersi olmayan bir duruma getirebilir. Bu süreç, gerçek görüntünün her bir bitinin etkisini yayarak önemli ölçüde şifreli görüntünün tüm istatistiksel özelliklerini değiştirebilir. Dolayısıyla güvenli bir şifreleme şeması için bir yayılma mekanizması gereklidir. Aksi takdirde istenmeyen bir şahıs tarafından orijinal bilgi ve şifreli bilgi kıyaslanarak önemli bilgiler ele geçirilebilir. Yayılma sürecinde, XOR işlemi, mod alma işlemleri ve 3B Cat Map'in bitişik piksellere uygulanma işlemi gerçekleştirilecektir (Chen, vd., 2004).

İlk olarak iki sayı seçilir. Bunlardan biri başlangıç koşulu olarak kullanmak amacıyla (0,1) aralığında kayan noktalı sayı $L_g$, diğeri ise $T$ bir tamsayıdır. $L_g$ başlangıç değeri olarak kullanılarak kaotik Logistic Map ile istenilen boyutta bir dizi sayı üretilir.

$$x(i+1) = 4x(i)[1 - x(i)] \tag{5.2}$$

Logistic Map (Eşitlik 5.2) kullanılarak elde edilen değerler (0.2,0.8) alt aralığında ise bir sonraki adıma geçilir. Aksi takdirde iterasyon (0.2,0.8) alt aralığında değerler elde edilene kadar devam ettirilir. Bu değerlerin arasında 0.5 kötü nokta olarak adlandırılır. 0.5 değerine kötü nokta denilmesi, iterasyonu başlangıç noktasına geri döndürmesi ve aynı değerleri üreterek tekrara neden olmasından kaynaklanmaktadır (Chen, vd., 2004). Eğer bu durumla karşılaşılırsa Logistic Map değerlerine küçük bir değişiklik uygulanabilir. Önce Logistic Map ile uygun bir değer üretilir. Ardından elde edilen bu değer uygun bir ölçekleme ve örnekleme ile yükseltilerek sayısal hale getirilir. Sayısal veri $\varphi(i)$ olarak oluşturulur ve görüntüdeki mevcut piksel değerleri ve önceki piksel değerleri XOR işlemine tabi tutulur. Bu işlem Eşitlik 5.3'deki matematiksel formül ile ifade edilir.

$$E(i) = \varphi(i) \oplus \{[I(i) + \varphi(i)\,]modN\} \oplus E(i-1) \tag{5.3}$$

Eşitlik 5.3'de $E(i)$ şifrelenmiş piksel değerini, $E(i-1)$ şifrelenmiş bir önceki piksel değerini, $I(i)$ mevcut piksel değerini ve $N$ gri seviye görüntü için renk seviyesini ifade etmektedir. Gri seviye görüntülerde renk seviyesi $N = 256$ ile temsil edilmektedir.

### 5.1.3. Anahtar şeması

Kriptolojinin esaslarından biri de kullanılan anahtarın hassaslığının yüksek olmasıdır. Şifreli bilgi anahtar ile yakın bir ilişkiye sahip olmalıdır (Avasare ve Kelkar, 2015). Chen, vd. (2004), bu gereksinimi karşılamak için iki yol olduğunu öne sürmektedir. Bunlardan biri şifreleme süreci boyunca kullanılan anahtarı şifrelenen bilgi içine iyice karıştırmaktır. Görüntü şifrelemede bu işlemi yaparken, görüntünün her pikseliyle anahtar matematiksel işlemlere dahil edilerek birbirine bağlı ve iteratif bir şekilde ilerleyen bir yapı elde edilmektedir. Diğer gereksinim, doğru bir rassallık sağlayan ve güvenlik açısından önemli olan iyi bir anahtar üretim mekanizması kullanmaktır (Chen, vd., 2004).

Çalışmada kullanılan şifreleme algoritmasında kullanılan anahtar, kaotik map sisteminin parametrelerini oluşturmaktadır. Anahtar, kayan noktalı sayı, tamsayı, kullanıcıdan alınan herhangi bir karakter dizisi veya bir bit dizisinden meydana gelebilir. Çeşitli şekillerde oluşturulabilen anahtar bir dönüştürme işlemi uygulanarak kullanılmak istenen yapıya çevrilir ve yayılma mekanizmasında kullanılır (Chen, vd., 2004). Anahtar üretmek amacıyla üç denklemden oluşan Chen kaotik sistemi kullanılır (Eşitlik 5.4).

$$\begin{cases} x_{i+1} = a(y_i - x_i) \\ y_{i+1} = (c-a)x_i - x_i z + c y_i \\ z_{i+1} = x_i y_i - bz \end{cases} \tag{5.4}$$

Eşitlik 5.4'de $a, b$ ve $c$ kaotik sisteme ait parametrelerdir. Bu parametreler $a = 35,\ \ b = 3$ ve $20 \leq c \leq 28.4$ olduğunda Chen sistemi kaotik davranış

sergilemektedir. Bu değerler farklı olduğunda, başka bir kaotik sistem meydana gelebilir. Dolayısıyla oluşan yeni sistem Chen kaotik sistemi olarak kullanılamaz. $c$ parametresi değiştirilerek sistemin davranışı incelendiğinde aşırı hassas olduğu görülmektedir. Bundan dolayı Chen, vd. (2004), çalışmalarında $c$ parametresini üretilen şifreleme anahtarını kontrol etmek amacıyla kullanmışlardır.

Çalışmada kullanılan anahtar 128 bit bir ikili diziden meydana gelmektedir. İkili dizi, onluk sistemde temsil edilen $a_x, b_x, a_y, b_y, a_z, b_z, L_g$ ve $T$ değerlerinin karşılıkları olarak sekiz parçaya bölünmektedir. Logistic Map'in başlangıç değeri $L_g$ ve mod işleminin başlangıç değeri T, Chen kaotik sistemi ile sırasıyla 100 ve 200 kez iterasyon yapılarak oluşan değerler ($z_{100}, z_{200}$) Eşitlik 5.5 ve 5.6'daki gibi elde edilir.

$$L_g = z_{100}/60 \tag{5.5}$$

$$T = round(z_{100}/60 \times 255) \tag{5.6}$$

$round$ fonksiyonu, ondalıklı sayıyı tamsayıya yuvarlama işlemini gerçekleştirir. 3B Cat Map sisteminde kullanılacak olan $a_x$ ve $b_x$ parametreleri de benzer şekilde elde edilir. Bu işlemlerden sonra $a_x$, $b_x$ ve Chen kaotik sisteminde kullanılacak olan $c$ parametrelerini hesaplamak için sırasıyla Eşitlik 5.7, 5.8 ve 5.9 kullanılır. $N$ değeri, 3B Cat Map uygulanacak olan görüntünün bir kısmına ait kenar boyutudur.

$$a_x = round(z_{100}/60 \times N) \tag{5.7}$$

$$b_x = round(z_{200}/60 \times N) \tag{5.8}$$

$$c = a \times 8.4 + 20 \tag{5.9}$$

Ayrıca Chen, vd. (2004), Chen kaotik sistemine ait başlangıç koşulları olan $x_0, y_0$ ve $z_0$ değerlerini $a_x$ ve $b_x$ parametreleri kullanarak Eşitlik 5.10, 5.11 ve 5.12'yi kullanarak üretmişlerdir.

$$x_0 = b_x \times 80 - 40 \quad (5.10)$$

$$y_0 = a_x \times 80 - 40 \quad (5.11)$$

$$z_0 = b_x \times 60 \quad (5.12)$$

## 5.2. Şifre Çözme Algoritması

Simetrik şifreleme kullanıldığı için şifre çözme algoritması, şifreleme aşamalarının tersi alınarak bulunur. Şifreleme işleminde uygulanan 1. ve 2. adımlar aynı şekilde tekrarlanır.

*Adım 1:* $a_x, b_x, a_y, b_y, a_z, b_z, L_g$ ve $T$ değerleri hesaplanır.

*Adım 2:* Görüntünün tüm pikselleri sırasıyla birkaç küpten oluşan $N_1 \times N_1 \times N_1$, $N_2 \times N_2 \times N_2, \dots, N_k \times N_k \times N_k$ boyutlarındaki yapılara bölünür.

*Adım 3:* Şifreleme işleminde uygulanan 3B Cat Map algoritmasının tersi uygulanır. $a_x, b_x, a_y, b_y, a_z, b_z$ kontrol parametreleri kullanılarak 3B ayrık Cat Map sistemi (Bkz. Eşitlik 3.8) uygulanır. Parametreler değişmez ancak algoritmanın içeriğinde bir kısım değişiklik yapılır.

*Adım 4:* Yayılma sürecinin tersi uygulanır. Bu süreçte ilk değerlere $x(0) = L_g$ ve $S(0) = T$ atanır ve yayılma işlemi Eşitlik 5.2 ve 5.3 kullanılarak gerçekleştirilir. Şifreleme işleminden farklı olan tek adım Eşitlik 5.3'deki denklem yerine Eşitlik 5.13'ün kullanılmasıdır.

$$I(i) = \{\varphi(i) \oplus E(k) \oplus E(k-1) + N - \varphi(i)\} mod N \quad (5.13)$$

Adım 5: Şifrelemenin 3. adımında karıştırılan küpler tekrar ilk haline gelmiştir. Bu küpler şifrelemenin 5. adımında olduğu gibi iki boyutlu görüntü haline dönüştürülür.

Şifreleme algoritmasında 3. ve 4. adımlar kaç kez tekrarlanmışsa, şifre çözme algoritmasında da aynı şekilde iterasyon yapılır. Bu işlemler sonucunda orijinal görüntü kayıpsız bir şekilde elde edilir.

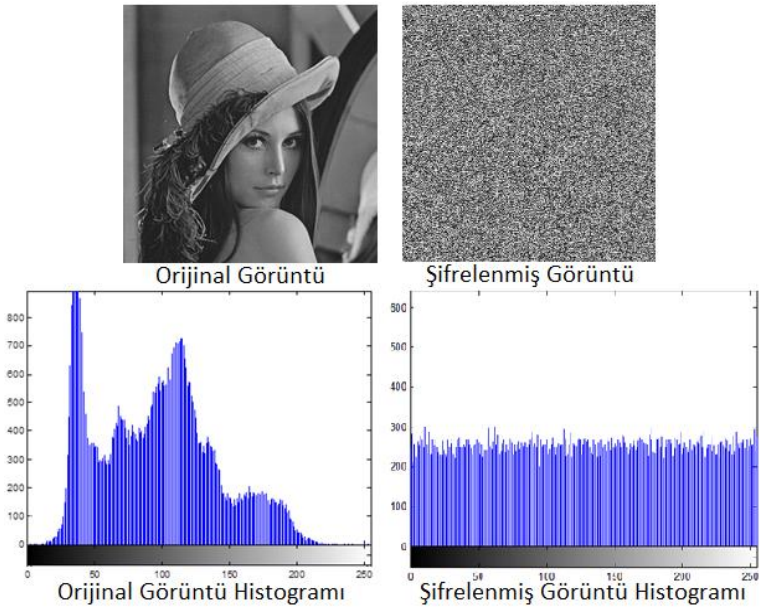
## 5.3. Algoritmanın Güvenlik ve Başarım Analizleri

İyi bir şifreleme işlemi tüm kriptanalitik, istatistiksel ve kaba kuvvet ataklara karşı güçlü olmalıdır. Gerçekleştirilen şifreleme işlemine bağlı olarak elde edilen sonuçlarla orijinal görüntüye ait bilgiler karşılaştırılarak başarım ve güvenlik analizleri alt bölümlerde yapılmıştır.

### 5.3.1. Anahtar alanı güvenliği

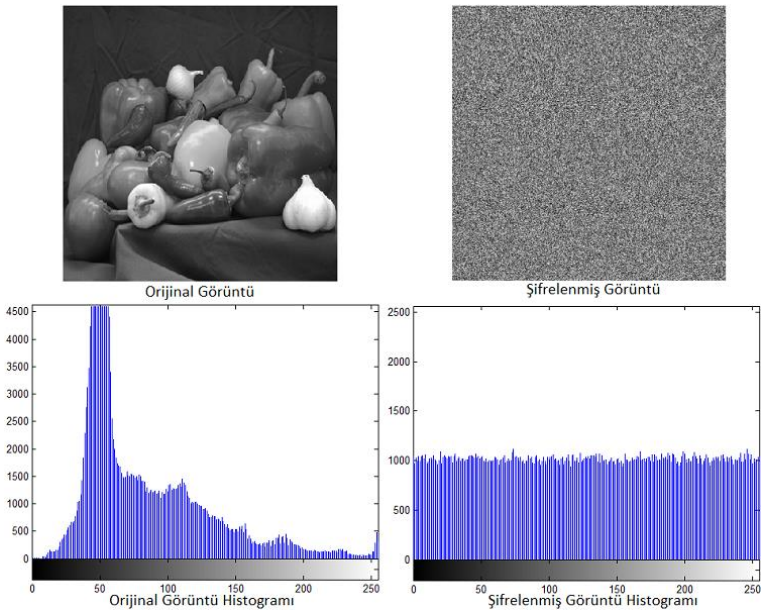
Anahtar alanı güvenliği, kontrol parametrelerinin sayısına bağlı olarak artmaktadır. Bu algoritmada kontrol parametrelerine ait anahtar uzunluğu 128 bit ve buna bağlı anahtar alan boyutu $2^{128}$ olmaktadır. 3B Cat Map anahtar açısından algoritmaya büyük avantaj sağlamaktadır. Bunun sebebi sahip olduğu $a_x, b_x, a_y, b_y, a_z, b_z$ parametreleridir. Anahtar ve kontrol parametrelerinin tüm olası kombinasyonları tahmin ile doğrudan elde edilebilir. Fakat 3B Cat Map kontrol parametrelerinin kombinasyonları ayrıntılı bir aramayı önlemek amacıyla yeterince büyüktür. Chen, vd. (2004) kontrol parametrelerinin tüm kombinasyonlarının elde edilebilmesi için kabaca bir hesap yapmışlardır. Mevcut şifreleme yöntemine göre $512 \times 512$ bir görüntü olduğu varsayıldığında, bu görüntü $64 \times 64 \times 64$ boyutunda bir küpten oluşabilmektedir. $a_x, b_x, a_y, b_y, a_z, b_z$ parametrelerinin hepsi 1 ile 64 aralığında olacağından, mümkün olan kontrol parametrelerinin kombinasyonları $64^6 = 2^{36}$ olmaktadır. Buna ek olarak, her bir adımda farklı bir şifreme anahtarı kullanıldığını varsayarsak bu kombinasyonlar katlanarak artacak ve saldırılara karşı daha güçlü bir algoritma elde edilecektir. $512 \times 512$ boyutlarında bir görüntü 2B Cat Map için yeterince büyük olan $2^{18}$ civarında anahtar alanına sahiptir. 3B Cat Map anahtar alanı, 2B Cat Map anahtar alanına kıyasla çok büyüktür (Chen, vd., 2004).

### 5.3.2. Histogram analizi

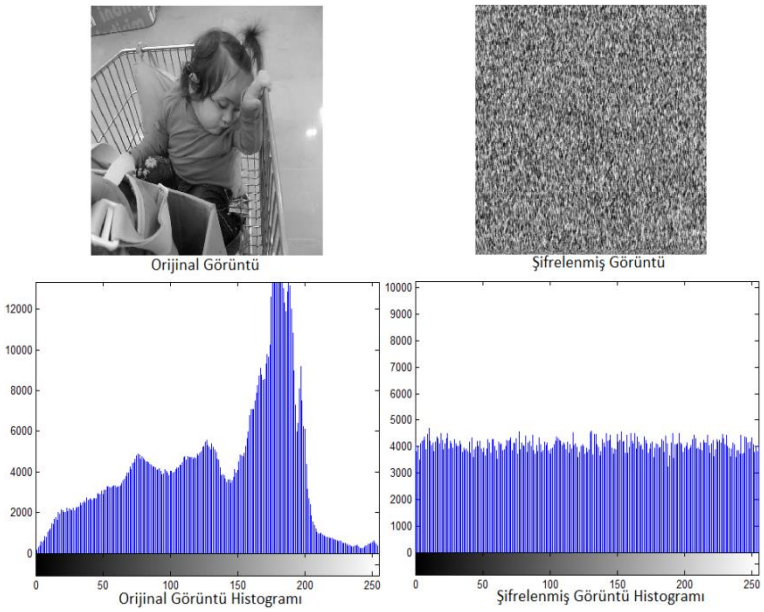



**Şekil 5.2.** 256x256 orijinal ve şifrelenmiş görüntüye ait histogramlar.

Farklı boyutlarda 256 renk gri seviye görüntüler seçilerek şifrelenmiştir. Orijinal görüntüler ve şifreli görüntülerin histogram değerleri karşılaştırılmıştır. Şekil 5.2, Şekil 5.3 ve Şekil 5.4'de sırasıyla $256 \times 256$, $512 \times 512$, $1024 \times 1024$ piksel görüntü, görüntüye ait histogram, şifrelenmiş görüntü ve şifrelenmiş görüntüye ait histogram bulunmaktadır. Farklı boyutlardaki bu görüntüler şifrelendiğinde ortaya çıkan histogramlar incelendiğinde, orijinal görüntü histogramı ile arasında hiçbir benzerlik bulunmamaktadır. Ayrıca şifrelenmiş görüntü histogramlarına bakıldığında belirli bir düzeyde olduğundan herhangi bir görüntü ile ilişkilendirmenin neredeyse imkansız olduğu görülmektedir.




**Şekil 5.3.** 512x512 orijinal ve şifrelenmiş görüntüye ait histogramlar.

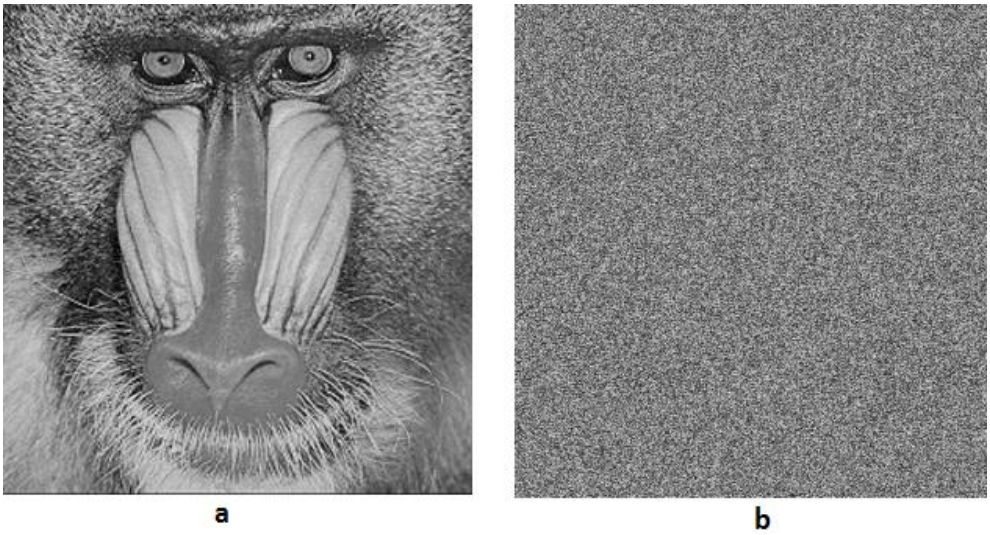



**Şekil 5.4.** 1024x1024 orijinal ve şifrelenmiş görüntülere ait histogramlar.

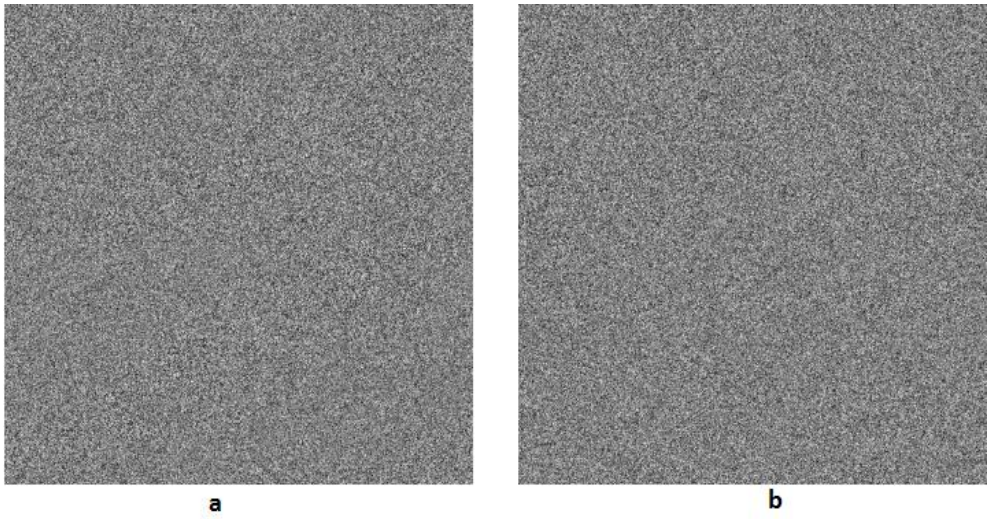
### 5.3.3. Anahtar hassaslığı

Algoritmada anahtar 16 karakter olarak belirlenmiştir. Her karakterin 8 bit olduğu düşünülürse anahtar uzunluğu 128 bit olmaktadır. Anahtar hassaslığını ölçmek amacıyla $512 \times 512$ boyutlarında bir görüntü 16 karakterden oluşan bir anahtar ile

şifrelenir. 16 karakter uzunluğundaki anahtarın 1 karakteri değiştirilerek şifre çözme işlemi gerçekleştirilir. Şifre çözme işlemi sonucu orijinal görüntü veya benzer bir görüntünün elde edilip edilmediği kontrol edilir. Şekil 5.5'de bir görüntü (a) ve bu görüntünün şifrelenmiş hali (b) görülmektedir. Şifrelenmiş görüntü anahtarın farklı herhangi iki karakterinin sırasıyla değiştirilmesi ile şifre çözme işlemine tabi tutularak Şekil 5.6'daki (a) ve (b) görüntüler elde edilmiştir. Her şifre çözme işleminde bir karakter değiştirilmiştir. Elde edilen sonuçlar incelendiğinde anahtarın karakter boyutunda çok hassas olduğu söylenebilir. Çünkü anahtardaki herhangi bir karakterin değişmesi sonucu yapılan şifre çözme işleminde orijinal görüntüyle ilgili herhangi bir ipucu elde edilememektedir ve Şekil 5.6'da görüldüğü gibi ortaya tamamen farklı görüntüler çıkmaktadır. Ayrıca anahtarın Chen kaotik sistemine giriş olarak uygulanan kısmı bit bazında $10^{-14}$ seviyesinde değiştirildiğinde de tamamen farklı bir görüntü elde edilmektedir.




**Şekil 5.5.** (a) Baboon görüntüsü ve (b) 3B Cat Map ile şifrelenmiş hali.



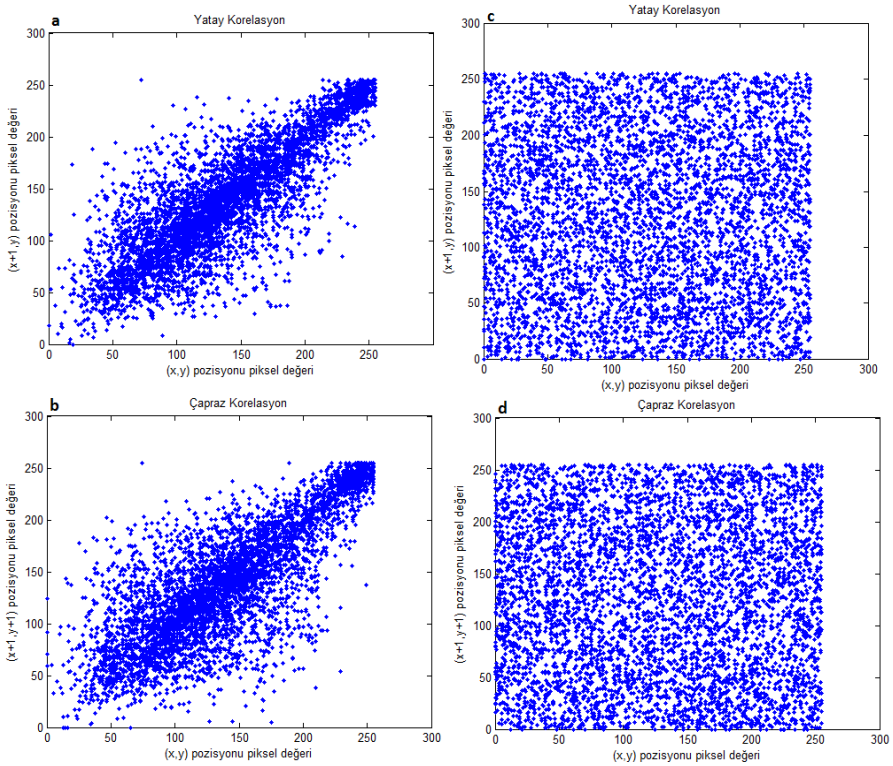

**Şekil 5.6.** Tek karakter değiştirilerek şifre çözme ile oluşan görüntüler.

### 5.3.4. Korelasyon katsayı analizi

Korelasyon katsayı analizi Bölüm 4.3.4'de anlatılmıştır. Şekil 5.7'de sırasıyla "Baboon" görüntüsünün yatay ve çapraz bitişik piksellerinin orijinal ve şifrelenmiş halleri rastgele 5000 bitişik piksel çifti alınarak kıyaslanmıştır. Şekil 5.7 incelendiğinde orijinal görüntüdeki bitişik piksellerin birbiriyle çok yüksek ilişkiye sahip olduğu, şifreli görüntüdeki iki komşu piksel arasındaki korelasyona bakıldığında ihmal edilebilir derecede küçük olduğu görülmektedir. Ayrıca Çizelge 5.1'de şifreli görüntülerin bitişik piksellerindeki korelasyon değerleri verilmiştir. "Diğer" renk yoğunluğu düşük herhangi bir görüntüdür.

**Çizelge 5.1.** Şifreli gri seviye görüntülerin bitişik piksellerindeki korelasyon değerleri.

| Şifreli Görüntü | Dikey | Yatay | Çapraz |
|---|---|---|---|
| Lena | -0.2035 | 0.0008 | -0.0078 |
| Baboon | -0.3078 | -0.0031 | 0.0030 |
| Peppers | -0.0841 | -0.0100 | -0.0111 |
| Diğer | 0.1056 | -0.0018 | -0.0041 |




**Şekil 5.7.** Yatay ve çapraz bitişik piksel korelasyon değerleri. (a), (b) Baboon görüntüsü ve (c), (d) şifrelenmiş Baboon görüntüsü.

### 5.3.5. Bilgi entropi analizi

Bilgi entropi analizine daha önce değinilmiştir (Bkz. Bölüm 4.3.5). Çizelge 5.2'de görülen sonuçlar "Lena", "Baboon", "Peppers" ve renk yoğunluğu düşük olan bir görüntü için entropi değerlerini göstermektedir. Elde edilen entropi değerleri incelendiğinde ideal değer olan 8'e çok yakın olduğu görülmektedir. Sonuç olarak şifreli görüntünün rasgele bir kaynağa yakın olduğu ve entropi ataklarına karşı güvenli olduğu görülmektedir.

**Çizelge 5.2.** Şifreli görüntülerin entropi değerleri.

| Görüntü | Gri Seviye |
|---|---|
| Lena | 7.9967 |
| Baboon | 7.9970 |
| Peppers | 7.9971 |
| Diğer | 7.9778 |

### 5.3.6. Hız analizi

Güvenlik konularının yanı sıra, gerçek zamanlı görüntü şifreleme ve şifre çözme süreleri de önemlidir. Çalışma süresini ölçmek amacıyla 1.60 GHz işlemci, 3 GB RAM özelliklerine sahip bir bilgisayar ile Matlab 2012 sürümü kullanılmıştır.

**Çizelge 5.3.** KCM tabanlı görüntü şifreleme süresi.

| Görüntü boyutu | Şifreleme Süresi (saniye) |
|---|---|
| $256 \times 256$ | 0.24 s |
| $512 \times 512$ | 0.93 s |
| $1024 \times 1024$ | 3.59 s |
| $2048 \times 2048$ | 14.86 s |

Çizelge 5.3'de görülen şifreleme hızlarını hesaplamak amacıyla beş farklı görüntüye ait şifreleme sürelerinin ortalaması alınmıştır. Bu süreler yaklaşık olarak birbirine eşit çıkmaktadır. Elde edilen sonuçlara göre şifreleme hızı 268 kb/s olarak hesaplanmaktadır.

# 6. SONUÇLAR

Bu tezde, asimetrik anahtarlı şifreleme, görüntü steganografi, kaotik sistemler ve bu kaotik sistemler ile yapılan iki farklı görüntü şifreleme çalışması gerçekleştirilmiştir. Görüntü steganografi uygulamasından önce veriler RSA asimetrik şifreleme algoritması ile şifrelenmiştir. RSA algoritması asal çarpanlara ayırmanın zorluğuna dayandığından yaklaşık 100 basamaklı iki asal sayı çarpılarak yaklaşık 200 basamaklı bir sayı ile şifreleme gerçekleştirilir. Ayrıca gizli ve açık olmak üzere iki anahtarın bulunması algoritmayı güçlü kılmaktadır. Günümüzde süper bilgisayarlar teorik olarak en fazla 128 basamaklı asal sayıları hesaplayabildiğinden dolayı 200 basamaklı bir anahtarı çarpanlarına ayırması olanaksızdır. Fakat kullanılan asal sayıların çok büyük olması ve bundan dolayı anahtara bağlı olarak şifrelenen veri boyutunun büyümesinin bir dezavantaj olduğu görülmüştür.

Düz metnin RSA ile şifrelenmesi sonrası, bu şifreli metnin LSB ve L3B yöntemleri ile görüntü steganografi uygulamasının üzerinde bu yöntemlerin üstünlük ve sakıncaları tartışılmıştır. Ayrıca veri kayıplarına bağlı olarak görüntü formatlarının veri gömme işlemine etkileri incelenmiştir. Verinin formatı değiştirildiğinde veya veri fiziksel yolla başka bir noktaya gönderildiğinde sıkıştırma işlemlerine bağlı olarak kayıplar oluşmaktadır. Bu açıdan kullanılan görüntü formatı steganografi uygulamalarında önemli bir yere sahiptir.

Görüntü steganografi, yani veri gömme uygulamasında bitmap dosya formatı kullanılmıştır. Steganografi uygulamalarında JPEG formatı desteklenmez ve kullanımı da tavsiye edilmez. Bunun yerine 24 bit bitmap, 256 renk veya gri tonlamalı görüntüler kullanılmalıdır. Genelde 256 gri tonlamalı resimlerin kullanımı önerilmektedir (Şahin, 2007). Bazı formatlar görüntü sıkıştırma işlemi uyguladıkları için veri kayıplarına neden olmaktadır. Bundan dolayı yapılan çalışmada 24 bit bitmap görüntüler kullanılmıştır.

LSB yöntemi ile yapılan veri gizlemede piksel renk tonundaki değişiklik 0 veya 1 olmaktadır. Bu değişikliğin insan gözüyle fark edilebilmesi olanaksızdır. Piksel değerindeki fark en az 3 olduğunda farklı bir renk tonuna geçiş başlamaktadır. Bundan dolayı görüntüde meydana gelen değişikliğin insan gözüyle fark edilebilmesi için renk tonundaki farkın üçten fazla olması gerekmektedir. Bu açıdan bakıldığında LSB

yöntemi uygulanan görüntüde renk tonundaki değişiklik fark edilememektedir. Bir görüntüye ait 8 pikselin kırmızı değerlerine LSB ve L3B yöntemleri kullanılarak veri gömüldükten sonra meydana gelen değişiklikler görülmektedir (Bkz. Çizelge 2.4). LSB ve L3B steganografi yöntemlerinin arasındaki farklar bazı parametreler baz alınarak kıyaslanmıştır (Çizelge 6.1). LSB yönteminin L3B'ye karşı daha üstün olduğu söylenebilir, fakat bu her zaman geçerli değildir.

**Çizelge 6.1.** LSB ve L3B arasındaki farklar.

| Parametre / Yöntem | LSB | L3B |
|---|---|---|
| Veri gömme hızı | Çok hızlı | Orta |
| 256x256 bir görüntüye gizlenebilen veri boyutu | Maksimum 24.576 karakter | Maksimum 73.728 karakter |
| Görüntü renk tonu değişikliği | Fark edilemez | Fark edilebilir |
| Orijinal görüntü ve örtü görüntüsü histogram farkı | Düşük | Orta |
| Bir pikseldeki minimum- maksimum değişen bit sayısı | 0-3 | 0-9 |

Görüntü steganografide internet üzerinde çok kullanılan ve renk yoğunluğu düşük görüntüler kullanıldığında meydana gelen değişikliğin fark edilmesi daha kolay olmaktadır. Bu açıdan bakıldığında seçilen görüntüler de steganografi açısından önem arz etmektedir.

Tent Map, 2B ve 3B Cat Map, Lorenz, Chua, Lü ve Chen kaotik sistemlerinin x-y, x-z ve y-z fazları, kaotik zaman serileri, kaotik olmasını sağlayan başlangıç koşulları ve parametrelerin aldığı değerler, ürettiği rasgele değerlerin bulunduğu frekans aralığı gibi özellikleri ayrıntılı bir şekilde incelenmiştir. 1, 2 ve 3 boyutlu kaotik sistemler kullanılmıştır. Sürekli zamanlı kaotik sistemlerin başlangıç koşulları ve parametre sayısı bakımından ayrık zamanlı kaotik sistemlere göre daha kullanışlı ve avantajlı olduğu görülmüştür. Fakat bu diğer kaotik sistemlerin kullanılmaması gerektiği anlamına gelmemektedir. Her kaotik sitemin kullanıldığı yere göre belirli üstünlüklere sahip olduğu görülmüştür.

Kaotik sistemlerin incelenmesindeki asıl neden görüntü şifrelemede kullanılmasıdır. Bahsedilen kaotik sistemlerin kullanıldığı KNA ve KCM tabanlı görüntü şifreleme algoritmalarından elde edilen analiz sonuçları birbiri ile kıyaslanmıştır (Çizelge 6.2).

**Çizelge 6.2.** KNA ve KCM algoritmalarının karşılaştırılması.

| Parametre / Yöntem | KNA | KCM |
|---|---|---|
| Anahtar alanı güvenliği | 224 bit | 128 bit |
| Histogram analizi | Güvenli | Güvenli |
| Anahtar hassaslığı | $10^{-14}$ seviyesinde | $10^{-14}$ seviyesinde |
| Korelasyon katsayı analizi | 0,0147 | 0,0307 |
| Bilgi entropi analizi | 7,986 | 7,9921 |
| Hız analizi | 205 kb/s | 268 kb/s |

KNA'da 224 bit, KCM'de 128 bit anahtar kullanılmıştır. Kaotik tabanlı şifrelemeye ait algoritmaların her ikisi de anahtar güvenliği açısından günümüz şartlarında değerlendirildiğinde (Bkz. Çizelge 4.1) yeterlidir. KNA'de kullanılan başlangıç koşullarının ve parametrelerinin fazla olması anahtar boyutunun daha büyük olmasını sağlamıştır ve anahtarı KCM'ye göre daha güvenli hale getirmiştir.

Histogram analizinde önemli olan husus orijinal görüntüdeki renkler, renklerin dağılımı ve görüntünün boyutu gibi şifrelemede sorun olabilecek parametrelerin şifreli görüntünün histogramında büyük bir değişikliğe neden olmamasıdır. Şifreli görüntüye ait histogram değerlerinin birbirine yakın olması (her renk tonundan yaklaşık olarak birbirine eşit miktarda olması) şifrelemenin çok başarılı olduğunun işaretidir (Bkz. Şekil 4.6, Şekil 4.7, Şekil 4.8, Şekil 5.2, Şekil 5.3, Şekil 5.4). KNA tabanlı görüntü şifrelemede kırmızı, yeşil ve mavi renk tonları için ayrı ayrı histogram değerleri incelenirken, KCM tabanlı görüntü şifrelemede gri seviye histogram değerleri incelenmiştir. Her iki uygulamada da orijinal görüntünün ve şifrelenmiş görüntünün histogram değerleri karşılaştırılmıştır. Elde edilen sonuçlar incelendiğinde yüksek başarım elde edildiği görülmüştür.

KNA tabanlı görüntü şifrelemede elde edilen histogram sonuçlarından bazıları istenilen başarımı vermemiştir. Bunun sebebi kullanılan kaotik sistemlerin ürettiği değer aralıklarının birbirinden farklı olmasıdır. Aradaki bu farklılık histogram değerlerini belirli bir alana yığmıştır. Yüksek başarım elde etmek amacıyla tüm kaotik sistemlerin ürettiği değer aralıkları birbirine yaklaştırılmıştır. Örneğin Chua sisteminde üretilen değerler -0.508 ile 0.508 aralığında ve Lü sisteminde üretilen değerler -32.09 ile 30.474 arasında iken Lorenz sisteminde -25.62 ile 26.18 arasında olmaktadır. Bu değerlerin hepsi çarpma ve bölme işlemleri uygulanarak Lorenz sistemine ait aralığa çekilmiştir ve istenilen histogram değerleri elde edilmiştir. Aralıkların birbirine yakın olması elde edilen histogramların belirli bir alana yığılmasını engellemiştir.

KNA ve KCM tabanlı görüntü şifreleme uygulamalarında kullanılan kaotik sistemler $10^{-14}$, $10^{-15}$ ve bazıları $10^{-16}$ seviyelerinde anahtar hassaslığı göstermektedir. Genellikle anahtar değeri $1 \times 10^{-14}$ kadar değiştirildiğinde şifrelemede elde edilen sonuçlar tamamen değişmektedir ve orijinal görüntüyü elde etmek imkansız hale gelmektedir. Her iki şifreleme algoritması anahtar hassaslığı konusunda başarılı sonuçlar vermiştir.

Her iki algoritmada şifreli görüntüden rasgele bitişik dikey, yatay ve çapraz 5000 piksel alınarak üç farklı korelasyon katsayı analizi yapılmıştır. Bu analizler incelendiğinde elde edilen sonuçlar KNA (Bkz. Çizelge 4.2 ve 4.3) ve KCM (Bkz. Çizelge 5.1) tabanlı görüntü şifreleme algoritmaları açısından son derece başarılıdır. KNA tabanlı görüntü şifreleme algoritmasında elde edilen korelasyon katsayıları genellikle daha küçük olduğundan KCM tabanlı görüntü şifrelemeye göre daha iyi başarım gösterdiği söylenebilir. Çizelge 6.2'de elde edilen korelasyon katsayılarının ortalamaları görülmektedir.

Entropi sonuçları her iki algoritma da ideal değer olan 8'e çok yakın çıkmıştır. Bu sonuçlar yüksek başarım elde edildiğini göstermektedir. KNA tabanlı şifrelemede RGB görüntü, KCM tabanlı şifrelemede ise gri seviye görüntü kullanıldığından analiz sonuçları Çizelge 6.3'de görüldüğü gibi olmaktadır. Çizelge 6.2'de elde edilen entropi değerlerinin ortalamaları görülmektedir.

**Çizelge 6.3.** KNA ve KCM tabanlı şifrelenen görüntülerin entropi değerleri.

| Görüntü / Yöntem | KNA Tabanlı Görüntü Şifreleme | | | KCM Tabanlı Görüntü Şifreleme |
|---|---|---|---|---|
| | R | G | B | Gri Seviye |
| Lena | 7.9928 | 7.9937 | 7.9928 | 7.9967 |
| Baboon | 7.9931 | 7.9938 | 7.9931 | 7.9970 |
| Peppers | 7.9930 | 7.9934 | 7.9929 | 7.9971 |
| Diğer | 7.9691 | 7.9675 | 7.9573 | 7.9778 |

Çizelge 6.4'e göre KNA ve KCM tabanlı görüntü şifreleme hızları sırasıyla yaklaşık 205 kb/s ve 268 kb/s 'dir. KCM tabanlı görüntü şifreleme gri seviye olduğundan (8 bit) KNA tabanlı görüntü şifrelemede kullanılan görüntüye (24 bit) göre boyutu kıyaslandığında 3 kat daha küçüktür. İki algoritma hız açısından kıyaslanırken buna dikkat edilmelidir. Bu sonuçlara göre KCM tabanlı görüntü şifreleme yönteminin KNA tabanlı görüntü şifrelemeye göre yaklaşık 1.3 kat daha hızlı olduğu görülmektedir.

**Çizelge 6.4.** KNA ve KCM tabanlı görüntü şifreleme süreleri.

| Görüntü boyutu | KNA ile şifreleme süresi (saniye) | KCM ile şifreleme süresi (saniye) |
|---|---|---|
| $256 \times 256$ | 0.95 s | 0.24 s |
| $512 \times 512$ | 3.77 s | 0.93 s |
| $1024 \times 1024$ | 15.93 s | 3.59 s |
| $2048 \times 2048$ | 62.70 s | 14.86 s |

3B KCM tabanlı görüntü şifreleme gri seviye görüntüleri şifrelemek için geliştirilmiş olmasına rağmen RGB görüntüleri şifrelemek için uyarlanabilir. Şifreleme süresi 3 katına çıkacaktır, fakat başarılı sonuçlar vereceği düşünülmektedir. Ayrıca KNA ve KCM algoritmalarındaki yapılar birlikte kullanılarak daha başarılı bir algoritma gerçekleştirmek mümkün olabilir. Genel anlamda yapılan analizlere bakıldığında iki algoritmanın da görüntü şifrelemede başarılı sonuçlar verdiği görülmüştür.

# KAYNAKLAR


Akgül, A., "İnternet Üzerinden Kaos Tabanlı Yeni Bir Güvenli Multimedya İletişim Sistemi Tasarım ve Gerçekleştirilmesi", Doktora Tezi, ***Sakarya Üniversitesi,*** (2015).

Avasare, M.G., Kelkar, V.V., "Image Encryption Using Chaos Theory", ***Communication, Information & Computing Technology (ICCICT)***, 1-6(2015).

Badem H., Güneş, M., "Video Formatına Veri Gizleme Amacıyla Gömülmüş Bir Steganografi Uygulamasının Geliştirilmesi", ***KSU Mühendislik Bilimleri Dergisi***, 14(2)(2011).

Bigdeli N., Farid Y., Afshar K., "A novel image encryption/decryption scheme based on chaotic neural networks", ***Engineering Applications of Artificial Intelligence*** 25:753–765(2012).

Bodur, R., "Kaotik Kriptoloji", prezi.com/ctfcvejylukf/kaotik-kriptoloji, (15.03.2016).

Botmart, T., Niamsup, P., "Adaptive control and synchronization of the perturbed Chua's system", ***Math. Comput. Simulation***, 75(1–2):37–55(2007).

Chandramouli, R., Memon, N., "Analysis Of LSB Based Image Steganography Techniques", ***Computer Communication and Informatics (ICCCI)***, 1019-1022(2001).

Chen, G., Mao, Y., Chui, C.K., "A symmetric image encryption scheme based on 3D chaotic cat maps", ***Elsevier Chaos, Solitons and Fractals,*** (21):749–761(2004).

Chen, G., Ueta, T., "Yet another chaotic attractor", ***Int J Bifurcat Chaos,*** 9(7):1465–6(1999).

Çayıroğlu, İ., İleri Algoritma Analizi Ders Notları, Yapay Sinir Ağları, ***Karabük Üniversitesi***, (2016).

Dagar, S., "RGB Based Dual Key Image Steganography", ***The Next Generation Information Technology Summit (4th International Conference)***, 316-320(2013).

Dalkıran, İ., Danışman, K., "Artificial Neural Network Based Chaotic Generator For Cryptology", ***Turk J Elec Eng & Comp Sci, Tübitak***, 18(2):225-240(2010).

gizliilimler.tr.gg/Kelebek-Etkisi-ve-Kaos-Teorisi.htm, ***Gizli İlimler Kütüphanesi sitesi***, (20.02.2016).

**KAYNAKLAR (Devam Ediyor)**

González, O.A., Han, G., de Gyvez, J.P., and Edgar, "CMOS Cryptosystem Using a Lorenz Chaotic Oscillator", Proceedings ***of the IEEE International Symposium on Circuits and Systems, ISCAS '99***, 5:442-445(1999).

Guo, J., Guo Y., Li, L., Li, M., "A Universal JPEG Image Steganalysis Method Based On Collaborative Representation", ***Security, Pattern Analysis, and Cybernetics (SPAC)***, 285-289(2014).

Hongjun, L., Xingyuan, W., "Color image encryption based on one-time keys and robust chaotic maps", ***Computers and Mathematics with Applications,*** 59:3320-3327(2010).

Karakuzu, C., Yapay Sinir Ağları Ders Notları, ***Bilecik Şeyh Edebali Üniversitesi***, (2016).

Karim, M., S.M., Rahman, M.S., Hossain, M.I. "A New Approach for LSB Based Image Steganography using Secret Key", ***Computer and Information Technology (ICCIT)***, (2011).

Karpinskyy, M., Kinakh, Y., "Reliability of RSA Algorithm and its Computational Complexity", ***Intelligent*** Data ***Acquisition and Advanced Computing Systems: Technology and Applications***, 494-496(2003).

Kriptolojiye Giriş Ders Notları, ***Uygulamalı Matematik Enstitüsü, Kriptografi Bölümü***, ODTÜ, (2004).

Kurtuldu, Ö., Arıca, N., "İmge Kareleri Kullanan Yeni Bir Steganografi Yöntemi", ***Journal of Naval Science and Engineering,*** 5(1):107-118(2009).

Laskar, S.A., Hemachandran, K., "High Capacity data hiding using LSB Steganography and Encryption", ***International Journal of Database Management Systems***, 4(6):57-68(2012).

Lenstra, A.K., Verheul E.R., "Selecting Cryptographic Key Sizes", ***Journal Cryptology***, 14:255–293(2001).

Li, D., Yin, Z., "Connecting the Lorenz and Chen systems via nonlinear control", ***Commun. Nonlinear Sci. Numerical Simulation***, 14(3):655–667(2009).

Li, J., Xing, Y., Qu, C., Zhang, J., "An Image Encryption Method Based on Tent and Lorenz Chaotic Systems", ***Software Engineering and Service Science (ICSESS)***, 582-586(2015).

**KAYNAKLAR (Devam Ediyor)**

Liu, H., Wang, X., "Triple-image encryption scheme based on one-time key stream generated by chaos and plain images", ***The Journal of Systems and Software,*** 86***:***826-834(2013).

Lorenz, E.N., "Deterministic Nonperiodic Flow", ***Journal of the Athmosferic Sciences***, 20:130-141(1963).

Lü, J., Chen, G., Zhang, S., "The compound structure of a new chaotic attractor" ***Chaos Solitons Fractals,*** 14(5):669–672(2002).

Masuda, N., Aihara, K., "Cryptosystems With Discretized Chaotic Maps", ***IEEE Transactions On Circuits And Systems: Fundamental Theory And Applications***, 49(1):28-40(2002).

Mollin, R.A., "An Introduction to Cryptography", ***CRC Press***, New York, (2006).

Nabiyev, V., Günay, A., "Şifreleme Yönteminin Tespiti Amacıyla Çeşitli Şifreleme Algoritmalarının Araştırılması", ***Karadeniz Teknik Üniversitesi***, (2010).

Orhan, N.T., "Kaos Teorisi ve Sağlık - Hastalık Kavramı Üzerine Etkisi", ***F.N. Hem. Derg.***, 21(2):116-121(2013).

Oğraş, H., Turk, M., "Digital Image Encryption Scheme using Chaotic Sequences with a Nonlinear Function", ***World Academy of Science Engineering and Technology***, (2012).

Özdemir, K., "Sürekli-Zamanlı Kaos İle Rastgele Sayı Üreteci Tasarımı", Yüksek Lisans Tezi, ***İstanbul Teknik Üniversitesi***, (2008).

Pamuk, N., "Dinamik Sistemlerde Kaotik Zaman Dizilerinin Tespiti", ***Balıkesir Üniversitesi Fen Bilimleri Enstitüsü Dergisi***, 15:77-91(2013).

Prusty, A.K., Pattanaik, A., Mishra, S., "An Image Encryption & Decryption Approach Based on Pixel Shuffling Using Arnold Cat Map & Henon Map", ***International Conference on Advanced Computing and Communication Systems***, 1-6(2013).

Selvi, G.K., Mariadhasan, L., Shunmuganathan, K.L., "Steganography Using Edge Adaptive Image", ***Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference***, 1023-1027(2012).

Sevinç, A., "Lorenz Kaotik Sistemi İçin Adaptif Bir Gözleyici", ***Gazi Üniversitesi Mühendislik Fakültesi Dergisi***, 18:57-66(2003).

**KAYNAKLAR (Devam Ediyor)**

Stork, M., "Discrete-Time Chaotic Systems, Impulsive Synchronization and Application in Communication", ***New Circuits and Systems Conference (NEWCAS)***, 189-192(2011).

Şahin, A., "Görüntü Steganografide Kullanılan Yeni Metodlar ve Bu Metodların Güvenilirlikleri", Doktora Tezi, ***Trakya Üniversitesi***, (2007).

Thangadurai, K., Devi, G.S., "An Analysis of LSB Based Image Steganography Techniques", ***Computer Communications and Informatics International Conference***, 3:1-4(2014).

***Wikipedia***, "https://tr.wikipedia.org/wiki/Adi_diferansiyel_denklemler", Adi Diferansiyel Denklemler, (19.05.2016).

***Wikipedia***, "https://en.wikipedia.org/wiki/Chaos_theory", (19.05.2016).

***Wikipedia***, "Kaos Kuramı", https://tr.wikipedia.org/wiki/Kaos_kuram%C4%B1, (15.03.2016).

Wang, Y., Wong K., Liao, X., Xiang, T., Chen, G., "A chaos-based image encryption algorithm with variable control parameters", Chaos, Solitons and Fractals, 41:1773-1783(2009).

Wong, K., Kwok, B.S., Law, W.S., "A fast image encryption scheme based on chaotic standard map", ***Elsevier Physics Letter A,*** 372(15):2645-2652(2008).

Xiao, D., Liao, X., Wei, P., "Analysis and improvement of a chaos-based image encryption Algorithm", ***Chaos, Solitons and Fractals,*** 40:2191–2199(2009)**.**

Yerlikaya, T., Buluş, E., Buluş., N, "RSA Şifreleme Algoritmasının Pollard RHO Yöntemi İle Kriptoanalizi", ***Akademik Bilişim***, Kütahya, (2007).

Yıldırım, H.M., "Bilgi Güvenliği ve Kriptoloji", ***Uluslararası Adli Bilişim Sempozyumu***, (2014).

Zeghid, M., Machhout, M., Khriji, L., Baganne, A., Tourki, R., "A Modified AES Based Algorithm for Image Encryption", ***International Journal of Computer Science and Engineering***, 1(1):70-75(2007).

Zheng. Y., Nian. Y., Sun, F., "Synchronization of discrete-time chaotic systems based on Takagi-Sugeno fuzzy model", ***International Conference on Computational Intelligence and Natural Computing***, 320-323(2009).

# ÖZGEÇMİŞ

**Kişisel Bilgiler**

Adı Soyadı : Sefa TUNÇER

Doğum Yeri ve Tarihi : Dörtdivan / 15.05.1992

**Eğitim Durumu**

Lisans Öğrenimi : Sakarya Üniversitesi Bilgisayar Mühendisliği Bölümü

Bildiği Yabancı Diller : İngilizce

Bilimsel Faaliyetleri :

1. Tunçer S., Karakuzu C., "Public-Key Encryption Algorithms Performance Analysis", International Congress on Natural and Engineering Sciences (ICNES'15), Sarajevo, Bosnia-Herzegovinia, 9-13 September, 2015.
2. "VIII. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı", Eğitim Sertifikası, ODTÜ, 31 Ekim 2015.
3. "Havelsan 2. Üniversite Sanayi Buluştayı", Katılım Belgesi, 29-30 Nisan 2016.
4. Tunçer S., Karakuzu C., "Veri Güvenliğini Artırmak Amacıyla Bilgiyi Şifreleme ve Steganografik Yöntemlerle Görüntüye Gizleme", Tokat, 11-13 Mayıs, 2016.

**İş Deneyimi**

Stajlar : Mysis Bilgi Teknolojileri (20 gün)
Arvena Yazılım (20 gün)

Projeler :

Çalıştığı Kurumlar : Bilecik Şeyh Edebali Üniversitesi

**İletişim**

Adres : Bahçelievler Mah. Belde Sk. No:41/3 Merkez/BİLECİK

Tel : 05531851814

E-Posta Adresi : sefa.tuncer@bilecik.edu.tr

**Akademik Çalışmaları**

– Tunçer S., Karakuzu C., “Public-Key Encryption Algorithms Performance Analysis”, International Congress on Natural and Engineering Sciences (ICNES’15), Sarajevo, Bosnia-Herzegovinia, 9-13 September, 2015.

– Tunçer S., Karakuzu C., “Veri Güvenliğini Artırmak Amacıyla Bilgiyi Şifreleme ve Steganografik Yöntemlerle Görüntüye Gizleme”, Elektrik-Elektronik ve Bilgisayar Sempozyumu, Tokat, 11-13 Mayıs, 2016.

**Yabancı Dil Bilgisi**

– İngilizce

– Okuma (iyi), Yazma (iyi), Dinleme (iyi), Konuşma(orta)

**Tarih:03/06/2016**