T.C.

YILDIZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

KAOTİK VE BİYOMETRİK ZAMAN SERİLERİ İLE GÖRÜNTÜ GÜVENLİĞİ

Ramazan CENKER

YÜKSEK LİSANS TEZİ

Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Haberleşme Programı

Danışman

Dr. Öğr. Üyesi Zehra Gülru ÇAM TAŞKIRAN

Haziran, 2022

T.C.

YILDIZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

KAOTİK VE BİYOMETRİK ZAMAN SERİLERİ İLE GÖRÜNTÜ GÜVENLİĞİ

Ramazan CENKER tarafından hazırlanan tez çalışması 28.06.2022 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Elektronik ve Haberleşme Mühendisliği Anabilim Dalı, Haberleşme Mühendisliği Programı **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Dr. Öğr. Üyesi Zehra Gülru ÇAM TAŞKIRAN
Yıldız Teknik Üniversitesi
Danışman

Jüri Üyeleri

Dr. Öğr. Üyesi Zehra Gülru ÇAM TAŞKIRAN, Danışman
Yıldız Teknik Üniversitesi _____

Doç. Dr. Umut Engin AYTEN, Üye
Yıldız Teknik Üniversitesi _____

Dr. Öğr. Üyesi İmran GÖKER, Üye
İstanbul Arel Üniversitesi _____

Danışmanım Dr. Öğr. Üyesi Zehra Gülru ÇAM TAŞKIRAN sorumluluğunda tarafımca hazırlanan Kaotik ve Biyometrik Zaman Serileri ile Görüntü Güvenliği incelemesi başlıklı çalışmada veri toplama ve veri kullanımında gerekli yasal izinleri aldığımı, diğer kaynaklardan aldığım bilgileri ana metin ve referanslarda eksiksiz gösterdiğimi, araştırma verilerine ve sonuçlarına ilişkin çarpıtma ve/veya sahtecilik yapmadığımı, çalışmam süresince bilimsel araştırma ve etik ilkelerine uygun davrandığımı beyan ederim. Beyanımın aksinin ispatı halinde her türlü yasal sonucu kabul ederim.

Ramazan CENKER

İmza

Aileme

ve

biricik eşime

TEŞEKKÜR

Kaotik ve Biyometrik Zaman Serileri ile Görüntü Güvenliği incelemesi konusunda hazırladığım yüksek lisans tezimde, bilgi ve tecrübeleri ile bana destek olan ve yol gösteren değerli Hocam ve Tez Danışmanım Dr. Öğr. Üyesi Zehra Gülru Çam Taşkıran'a teşekkür ederim.

Hayatım boyunca her konuda yanımda olan sevgili aileme ve eşime teşekkürlerimi sunarım.

Ramazan CENKER

İÇİNDEKİLER

SİMGE LİSTESİ vii

KISALTMA LİSTESİ viii

ŞEKİL LİSTESİ ix

TABLO LİSTESİ x

ÖZET xii

ABSTRACT xiv

1 GİRİŞ 16

1.1 Literatür Özeti 17

1.2 Tezin Amacı. 20

1.3 Hipotez....20

2 KAOTİK SİSTEMLER 22

2.1 Kesirli Dereceli Lorenz Sistemi....22

2.2 Kesirli Dereceli Rössler Sistemi 23

2.3 Kesirli Dereceli Chen Sistemi 23

2.4 Kesirli Dereceli Lü Kaotik Sistemi 23

3 LYAPUNOV ÜSTELLERİ 24

3.1 Kesirli Dereceli Sistemler için Lyapunov Üstellerinin Hesaplanması. 24

3.2 Tam Sayı Dereceli Sistemler için Lyapunov Üstellerinin Hesaplanması .25

4 KULLANILAN METRİKLER 27

4.1 Kullanılan Kaotik Görüntü Şifreleme Algoritması 27

4.2 Histogram Eşitleme. 27

4.3 Satır Döndürme 29

4.4 Sütun Döndürme 29

4.5 XOR Operasyonu 29

4.6 Piksel Değişim Oranı Sayısı. 29

4.7 Birleşik Ortalama Değişim Yoğunluğu 30

4.8 Entropi 30

4.9 Kaotik Sistemlerde Başlangıç Koşullarının Değerlendirme Ölçütlerine Etkisi 31

4.9.1 Kaotik Sistemlerde Başlangıç Koşullarındaki Değişikliğin Piksel Değişim Oranına Etkisi. 31

4.9.2 Kaotik Sistemlerde Başlangıç Koşullarındaki Değişikliğin Birleşik Ortalama Değişim Yoğunluğuna Etkisi 32

4.9.3 Kaotik Sistemlerde Başlangıç Koşullarındaki Değişikliğin Şifreli Görüntünün Entropi Değerine Etkisi 34

4.10 Lorenz Sistemi ile Kaotik Anahtar Kullanılarak Başlangıç Koşullarının Değerlendirme Ölçütlerine Etkisi 35

4.10.1 Lorenz Sistemi ile Kaotik Anahtar Kullanılarak Başlangıç Koşullarındaki Değişikliğin Piksel Değişim Oranına Etkisi 35

4.10.2 Lorenz Sistemi ile Kaotik Anahtar Kullanılarak Başlangıç Koşullarındaki Değişikliğin Birleşik Ortalama Değişim Yoğunluğuna Etkisi 36

4.10.3 Lorenz Sistemi ile Kaotik Anahtar Kullanılarak Başlangıç Koşullarındaki Değişikliğin Şifreli Görüntünün Entropi Değerine Etkisi 37

5 EKG **38**

5.1 EKG Bilgilerinin Farklı Örnek Kaydırmalarının Piksel Değişim Oranına Etkisi 40

5.2 EKG Bilgilerinin Farklı Örnek Kaydırmalarının Birleşik Ortalama Değişim Yoğunluğuna Etkisi. 44

5.3 EKG Bilgillerinin Farklı Örnek Kaydırmalarının Şifreli Görüntünün Entropi Değerine Etkisi. 47

6 SONUÇ VE ÖNERİLER **48**

KAYNAKÇA **49**

TEZDEN ÜRETİLMİŞ YAYINLAR **54**

SİMGE LİSTESİ

ms	Milisaniye

KISALTMA LİSTESİ

AES	Advanced Encryption Standard (Gelişmiş Şifreleme Standardı)
dB	Decibel (Desibel)
DES	Data Encryption Standard (Veri Şifreleme Standardı)
DNA	Deoxyribonucleic Acid (Deoksiribo Nükleik Asit)
EKG	Elektrokardiyografi
FIR	Finite Impulse Response (Sonlu Dürtü Yanıtı)
FFT	Fast Fourier Transform (Hızlı Fourier Dönüşümü)
IDEA	International Data Encryption Standard (Uluslarasi Veri Şifreleme Algoritması)
NPCR	Number of Pixel Change Rate (Piksel Değişim Oranı Sayısı)
UACI	Unified Average Changing Intensity (Birleşik Ortalama Değişim Yoğunluğu)
XOR	eXclusive OR (Özel veya)
1D	One Dimensional (Tek Boyutlu)
3D	Three Dimensional (Üç Boyutlu)

ŞEKİL LİSTESİ

Şekil 3.1 Kesirli dereceli Lorenz sistemi kullanılarak elde edilen görüntü örnekleri 24

Şekil 3.2 Tam sayı dereceli Lü sistemi kullanılarak elde edilen görüntü örnekleri.....26

Şekil 4.1 EKG Verileri Kullanılarak Görüntü Şifreleme Algoritması 27

Şekil 4.2 EKG Sinyali Histogram Eşitleme 28

Şekil 4.3 Lorenz sistemi kullanılarak elde edilen görüntü örnekleri. 35

Şekil 4.4 Lorenz sistemi kullanılarak elde edilen görüntü örnekleri. 35

Şekil 5.1 Tipik EKG Sinyali.....38

Şekil 5.2 EKG Sinyalinin Farklı Filtreleme Sonuçlarının Frekans Gösterimi 39

Şekil 5.3 EKG Sinyalinin Farklı Filtreleme Sonuçlarının Zaman Gösterimi 39

Şekil 5.4 Farklı kişilerden alınan EKG sinyalleri ile elde edilen görüntü örnekleri. 40

Şekil 5.5 Farklı kişilerden alınan EKG sinyalleri ile elde edilen görüntü örnekleri 40

TABLO LİSTESİ

Tablo 3.1 Kesirli Dereceli Kaotik Sistemlerde Parametre Değişikliğinin Lyapunov Üstellerine Etkisi.....25

Tablo 3.2 Tam Sayı Dereceli Kaotik Sistemlerde Parametre Değişikliğinin Lyapunov Üstellerine Etkisi.....26

Tablo 4.2 Tam Sayı Dereceli Kaotik Sistemlerde Başlangıç Koşullarının Piksel Değişim Oranı Sayısına Etkisi 32

Tablo 4.3 Kesirli Dereceli Kaotik Sistemlerde Başlangıç Koşullarının Birleşik Ortalama Yoğunluğuna Etkisi 33

Tablo 4.4 Tam Sayı Dereceli Kaotik Sistemlerde Başlangıç Koşullarının Birleşik Ortalama Yoğunluğuna Etkisi 33

Tablo 4.5 Kesirli Dereceli Kaotik Sistemlerde Başlangıç Koşullarındaki Değişiklikliğin Şifreli Görüntünün Entropi Değerine Etkisi 34

Tablo 4.6 Tam Sayı Dereceli Kaotik Sistemlerde Başlangıç Koşullarındaki Değişiklikliğin Şifreli Görüntünün Entropi Değerine Etkisi 34

Tablo 4.7 Başlangıç Koşullarının Piksel Değişim Oranına Etkisi. 36

Tablo 4.8 Başlangıç Koşullarının Birleşik Ortalama Değişim Yoğunluğuna Etkisi 37

Tablo 4.9 Başlangıç Koşullarının Şifreli Görüntünün Entropi Değerine Etkisi. 38

Tablo 5.1 Farklı Kişilerden Alınan EKG Bilgilerinin Piksel Değişim Oranına Etkisi ..41

Tablo 5.2 Farklı Kişilerden Alınan Filtrelenmiş EKG Bilgilerinin Piksel Değişim Oranına Etkisi. 41

Tablo 5.3 Farklı Kişilerden Alınan EKG Bilgilerinin Farklı Örnek Kaydırmalarının Piksel Değişim Oranına Etkisi 42

Tablo 5.4 Farklı Kişilerden Alınan Filtrelenmiş EKG Bilgilerinin Farklı Örnek Kaydırmalarının Piksel Değişim Oranına Etkisi 42

Tablo 5.5 Kişilerden Alınan EKG Bilgilerinin Farklı Örnek Kaydırmalarının Piksel Değişim Oranına Etkisi 43

Tablo 5.6 Kişilerden Alınan Filtrelenmiş EKG Bilgilerinin Farklı Örnek Kaydırmalarının Piksel Değişim Oranına Etkisi 43

Tablo 5.7 Farklı Kişilerden Alınan EKG Bilgilerinin Birleşik Ortalama Yoğunluğuna Etkisi 44

Tablo 5.8 Farklı Kişilerden Alınan Filtrelenmiş EKG Bilgilerinin Birleşik Ortalama Yoğunluğuna Etkisi 44

Tablo 5.9 Farklı Kişilerden Alınan EKG Bilgilerinin Farklı Örnek Kaydırmalarının Birleşik Ortalama Yoğunluğuna Etkisi. 45

Tablo 5.10 Farklı Kişilerden Alınan Filtrelenmiş EKG Bilgilerinin Farklı Örnek Kaydırmalarının Birleşik Ortalama Yoğunluğuna Etkisi 45

Tablo 5.11 Kişilerden Alınan EKG Bilgilerinin Farklı Örnek Kaydırmalarının Birleşik Ortalama Yoğunluğuna Etkisi. 46

Tablo 5.12 Kişilerden Alınan Filtrelenmiş EKG Bilgilerinin Farklı Örnek Kaydırmalarının Birleşik Ortalama Yoğunluğuna Etkisi 46

Tablo 5.13 Kişilerden Alınan EKG Bilgilerinin Farklı Örnek Kaydırmaları ile Şifreli Görüntünün Entropi Değerine Etkisi. 48

Tablo 5.14 Kişilerden Alınan Filtrelenmiş EKG Bilgilerinin Farklı Örnek Kaydırmaları ile Şifreli Görüntünün Entropi Değerine Etkisi 48

ÖZET

Kaotik ve Biyometrik Zaman Serileri ile Görüntü Güvenliği

Ramazan CENKER

Haberleşme Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

Danışman: Dr. Öğr. Üyesi Zehra Gülru ÇAM TAŞKIRAN

Artan veri trafiği sebebiyle multimedya güvenliğinin önemi gün geçtikçe artmaktadır. Verilerin güvenli bir şekilde iletilmesi ve saklanması için kaotik şifreleme, kullanılan kabul görmüş yöntemlerden biridir. Kaotik işaretlerin başlangıç koşullarına yüksek hassasiyetle bağlı olmasının, anahtar duyarlılığını artıracağı ve açık metin ataklarına karşı dayanıklılık sağlayacağı düşünülmektedir. Bu çalışmada bu öngörünün doğrulanması amacıyla farklı kaotik sistemlerin farklı parametreler ile çalıştırılması sonucu elde edilen kaotik zaman serilerinin bu anlamda bir incelemesi yapılmıştır. İncelemede hem tam sayı dereceli hem de kesirli dereceli dinamik sistemler kullanılmış ve bu anlamda da bir karşılaştırma yapılabilmiştir. Birbirine komşu noktalardan başlatılan kaotik işaretlerin yörüngesel uzaklaşmaları Lyapunov mesafesi ile takip edilmiş, bu mesafeler ile kriptoloji güvenliği arasında bir ilişki kurmak amacıyla, bu işaretlerin kullanıldığı kaotik şifreleme yöntemi ile şifrelenmiş görüntülerin ortalama entropi, piksel değişim oranı sayısı ve birleşik ortalama değişim yoğunluğu parametreleri incelenmiştir. Buna göre yörüngesel uzaklığı fazla olan dizilerle şifrelenmiş görüntülerin anahtar duyarlılığının arttığı ve açık metin ataklarına karşı daha

güvenli olduğu, fakat şifrelenmiş görüntünün entropisinin doğrudan bu değere bağlı olmadığı sayısal olarak doğrulanmıştır.

Çalışmanın devamında literatürde güvenilirliği ispatlamış bir kaotik şifreleme yöntemi kullanılarak, EKG verilerinin güvenli haberleşme alanında kullanımı incelenmiştir. Kaotikliği literatürde tartışmalı bir konu olan EKG verileri, bu yöntemde doğrudan kaotik sayı dizileri yerine kullanılarak şifrelenmiş görüntülerin NPCR, UACI ve entropi değerleri üzerinden bir güvenlik analizi yapılmıştır. Elde edilen sonuçlara göre kişinin, kullanılan faz kaydırma örnek sayısının ve EKG alınan zamanın anahtar olarak belirlenmesi ile elde edilen sayı dizisinin bu yöntemle kullanılabilir olduğu gözlemlenmiştir. Sağlıklı EKG verilerinin periyodikliği yanında barındırdığı kaotik özelliklerin yeterliliği gösterilmiştir.

Anahtar Kelimeler: Kaos; Kaotik şifreleme; EKG; Açık metin saldırısı; Entropi.

ABSTRACT

Image Security by Using Chaotic and Biometric Time Series

Ramazan CENKER

Department of Electronic and Communications Engineering

Master of Science Thesis

Supervisor: Dr. Öğr. Üyesi Zehra Gülru ÇAM TAŞKIRAN

Due to the increasing data traffic, the multimedia security is gaining importance day by day. Chaotic encryption is one of the accepted methods used to securely transmit and store data. Because of the fact that chaotic signals are highly sensitive to initial conditions, it is thought that it will increase key sensitivity and provide resistance against plain text attacks. In this study, in order to verify this prediction, an analysis of the chaotic time series obtained as a result of operating different chaotic systems with different parameters was studied in this sense. Both integer order and fractional order dynamical systems were used in the study and a comparison could be made in this sense. The orbital divergences of chaotic signals initiated from points adjacent to each other were followed by the Lyapunov distance, in order to establish a relationship between these distances and cryptology security, the average entropy of the images encrypted with the chaotic encryption method using these signals, number of pixel change rate and unified average changing intensity parameters were examined. Accordingly, it has been numerically verified that the key sensitivity of the images encrypted with sequences with higher orbital distances increases and is more secure to plaintext attacks, but the entropy of the encrypted image is not directly dependent on this value.

In the continuation of the study, the use of ECG data in the field of secure communication was studied using a chaotic encryption method, which has proven its reliability in the literature. In this method, a security analysis was performed on the NPCR, UACI and entropy values of the encrypted images using ECG data, the kaoticity of which is a controversial issue in the literature, instead of directly chaotic number sequences in this method. According to the results obtained, it was observed that the sequence of numbers obtained by determining the person, the number of phase shift samples used, and the time taken on the ECG as the key can be used with this method. In addition to the periodicity of healthy ECG data, the adequacy of the chaotic features it contains has been shown.

Keywords: Chaos; Chaotic encryption; ECG; Plain text attacks; Entrophy.

1
GİRİŞ

1.1 Literatür Özeti

Multimedya verileri metin, ses, video, grafik ve görüntülerden oluşur. Günümüzde ses, görüntü ve video olmak üzere multimedya alanında gelişmeler olmaya devam etmektedir. Multimedya verilerinin internet üzerinden artan kullanımıyla birlikte güvenli multimedya verileri talebi ortaya çıkar. Dijital olarak bilginin geniş alanda kullanımı ağ teknolojisi ve bilgisayar bilimi ile desteklenir. Bununla birlikte, yasadışı telefon dinleme, gözden geçirme veya müdahale nedeniyle ağ üzerinden özellikle tıbbi ve askeri görüntü gibi bazı özel görüntülerin iletilmesi için güvenlik eksikliği barizdir. Kategorize etmek gerekirse simetrik kriptografi ve asimetrik kriptografi olmak üzere iki sınıfa [1, 2] ayrılır. Kullanıcı bilgileri için, özellikle metinsel içerik biçiminde çok sayıda etkili şifre sağlamıştır.

Bir görüntünün kendine özgü bazı özellikleri vardır. Görüntü şifreleme, toplu veri kapasitesi ve pikseller arasındaki yüksek korelasyon gibi özellikleri nedeniyle diğer multimedya bileşenleri şifrelemesinden farklı olduğundan uluslararası veri şifreleme algoritması (IDEA), veri şifreleme standardı (DES) veya gelişmiş şifreleme standardı (AES) gibi şifrelemede kullanılan yöntemler görüntü şifrelemesi açısından verimli seçenekler değildir [3, 4]. Kaosa dayalı görüntü şifreleme yöntemleri görüntü içeriğini korumak açısından da son zamanlarda cazip hale gelmiştir. Görüntü şifrelemedeki en son eğilim; başlangıç koşullarına duyarlılık, periyodik olmama, yakınsama ve kontrol parametreleri gibi bazı kendine özgü özelliklere dayalı kaostur. Literatürde kaos kullanan çok sayıda uygulama göz önünde bulundurularak, bitişik pikseller arasında var olan yüksek korelasyon azaltılır. Bu görüntü şifreleme algoritmasına Arnold harita dönüşümü örnek verilebilir [8, 9]. Ayrıca piksel konumları değiştirilse bile; orijinal görüntünün sahip olduğu gri dağılım aynı kalacağından görüntünün güvenliğini sağlamak için yeterli olamayacaktır. Pikseller için istatistiksel dağılımı yeniden formüllendirmek adına piksel difüzyonu işlemi kullanılır. Orijinal görüntüde,

önemli olan tamamen farklı bir şifreli görüntü ile sonuçlanacak, yani bir çığ efekti gerçekleştirecek şekilde küçük bir değişiklik yapmaktır. Bu sebeple şifreleme sürecine sıkıştırmalı algılama da dahil edilmiştir ve iyi bir etki göstermiştir [10].

1989 gibi erken bir tarihte Matthews [11], basit bir doğrusal olmayan yinelemeli fonksiyondan kaotik bir rasgele sayı dizisinin elde edilebileceğini kanıtlamış ve bunu kriptografik kullanım için uygulamıştır. Bu çalışmada pikseller için bit düzeyinde permütasyon kullanılarak (1D) tek boyutlu çarpık bir çadır haritasının kullanıldığı simetrik bir görüntü şifreleme algoritması sunulmuştur [12]. El Assad ve Farajallah tarafından, bit permütasyon katmanını takip eden difüzyon katmanı yapısı bayt permütasyonu yerine önerilmiştir [13]. Bit düzeyinde permütasyon işlemi çift difüzyon etkisi yaratmasına rağmen beraberinde daha uzun bir zaman tüketimine yol açmaktadır. Bu sürenin daha az olması ile görüntü şifrelemede Lojistik harita sıklıkla tercih edilir [14]. Ek olarak, zayıf güvenlik ve küçük bir anahtar gibi bazı dezavantajlara sahip olduğu gösterilmiştir. Wang ve Luan Lojistik haritanın bu dezavantajlarının üstesinden gelebilmek adına üç boyutlu (3B) bağlantılı bir lojistik harita önermişlerdir [15]. Ek olarak görüntüler için çeşitli yeni ve geliştirilmiş şifreleme şemaları bildirilmiştir [16-18], bu da kaosa dayalı şifreleme yöntemlerinin geliştirilmesine neden olmaktadır. DNA dizisini kullanan yaygın saldırılara direnmek için Chai ve diğerleri yeni bir şifreleme şeması önermiştir [19]. Önerilen şemada ikili sistemler ila ondalık sistemler arasındaki değişim zaman maliyetinin artmasına neden olacaktır. DNA bazlı yöntem için de bu problem görülebilir [20]. Dolayısıyla yeni bir hiper kaos tabanlı algoritma önerilmiştir [21]. Yeni kaotik sistemde daha büyük bir Lyapunov üsteli hesaplanmış ancak düz görüntüdeki toplam değişmezliği dikkate alınmamıştır. Farklı bir çalışmada rasgele bir dizi oluşturmak için hiperkaotik bir sistem kullanan düz bağlantılı bir görüntü şifreleme sistemi tasarlanmıştır [22]. Bu sistem iyi bir performans sergilese de yalnızca sabit gizli anahtarlar kullanır.

Fu ve arkadaşları bir görüntüyü şifrelemek için Arnold haritası ve kaotik diziler kullanılarak iki aşamalı bit seviye karıştırma fonksiyonu işlemi ile difüzyon etkisinin elde edilebileceği bir bit seviye permütasyon şeması önermiştir fakat düşük güvenlik sağlamaktadır [23]. Piksel permütasyonu ardından piksel difüzyonu prensibine sahip bazı görüntü şifreleme algoritmalarıyla

kıyaslandığında algoritma hesaplama karmaşıklığı daha azdır. Bununla birlikte, Jolfaei ve arkadaşları [24], seçilen bir açık metin saldırısı uygulanırsa görüntü şifreleme için yalnızca permütasyon şemasının bozulabileceğine dikkat çekmiştir. Orijinal bir görüntü $m \times n$ boyutunda olduğunda; farklı renk yoğunluğu sayısı L, seçilmesi gereken düz görüntü sayısı $\log_L(mn)$ olacaktır. Görüntü şifreleme için önerilmiş bir permütasyon-difüzyon mimarisi döngüsünde ilk aşamada satır ve sütun permütasyonları kullanılmış ve difüzyon aşamasında gri değerleri değiştirmek için bir afin şifre uygulanmıştır [25]. Bununla birlikte bir böl ve yönet stratejisiyle seçilen bir düz metin karmaşık bir doğrusal ilişkiye sahip bu algoritmaya verimli bir şekilde saldırabilir [26]. Ek olarak çok sayıda başka kriptanaliz yöntemi vardır [27-30].

Şifre kırma yöntemlerinin ayrıntılı bir analizi yapıldıktan sonra, mevcut görüntü şifreleme algoritmalarının dezavantajlarının şu şekilde olduğu sonucuna varılabilir:

(1) Yalnızca permütasyon yapısının kullanılması

(2) Yalnızca difüzyon yapısının kullanılması

(3) Bir permütasyon-difüzyon mimarisi döngüsünün oluşturulması

(4) Sabit anahtarlar

(5) Anahtar bağımlılığı

Bu sınırlamaların üstesinden gelebilmek için; genel olarak kaotik haritalar kullanılmaya başlanmıştır.

Bu çalışmalardan birinde kaotik dinamik sistemin başlangıç koşullarının anahtar olduğu bir karışıklık-permütasyon tabanlı görüntü şifreleme algoritması tasarlamak için hiperkaotik bir Rossler haritası kullanılmıştır [31]. Ancak aynı boyuttaki herhangi bir orijinal görüntünün permütasyon ve difüzyon işlemleri açısından anahtar akışları için herhangi bir değişiklik olmayacaktır. Ardından klinik bilgilerin gizliliği ve mahremiyeti için karışıklık yayılım yapısına sahip yeni bir şifreleme yöntemi önerilmiştir [32]. Kaotik diziyi oluşturmak için 1 boyutlu bir lojistik harita kullanılmıştır. Bu yöntem küçük gizli anahtar alanı, tek biçimli olmayan kaotik veri dağılımı ve süreksiz kaotik aralıklar gibi çok sayıda dezavantaj

barındırmaktadır. 3 boyutlu (3D) kaotik bir sistem rasgele sayıların üretilmesi amacıyla kullanılmıştır [33]. Bununla birlikte, sürekli sabit anahtarlar elde edilmesi S-kutusu oluşturma algoritması için gereklidir. Gizli anahtarlar için piksel toplamının hesaplandığı orijinal görüntü tabanlı bir anahtar dizisi üretimi önerilmiştir [34]. Ek olarak orijinal görüntüde aynı toplama sahip iki pikselin değişmesi anahtar akışında herhangi bir değişikliğe sebep olmayacaktır. Bu nedenle bu şema toplam değişmezliğinden muzdariptir.

Bu çalışmada ise sabit anahtarlar ve toplam değişmezliği problemlerini çözmek için kullanılan güvenilirliği ispatlanmış kaotik tabanlı bir yöntem kullanılmıştır [35]. Kaotik haritanın sabit anahtar problemini ele alması açısından kaotik zaman serisi yerine bir elektrokardiyograf (EKG) sinyali kullanılmıştır.

Bilgi güvenliği alanında EKG sinyallerinin kullanımı oldukça sınırlıdır. Genelde EKG sinyallerinin güvenli iletimi ve saklanması adına çalışmalar yapılmıştır [36, 37, 38]. Bu çalışmada bunlardan farklı olarak EKG sinyalinin saklanması değil, bu sinyalin düzensiz yapısı gereği ortaya çıkan özellikleri kullanılarak, kaotik şifreleme yöntemlerinde kaos işareti yerine kullanımı incelenmiştir.

EKG sinyallerini bu amaçla kullanan bir çalışmada EKG sinyalinin QRS dalgaları arasındaki mesafe sürekli olarak ölçülerek, bu veriye dayalı dinamik bir anahtar oluşturulmuş ve kullanılmıştır [39]. Bu çalışmada elde edilen sonuçlarda, açık metin güvenliği açısından yetersiz sonuç elde edilmiştir. Farklı bir çalışmada EKG dalga formu uzun vadeli eğilimlere ve kısa vadeli kaotik değişimlere sahip olduğundan, anahtarlar EKG dalga formundaki uzun vadeli eğilimlerin ortadan kaldırılmasıyla oluşan artık sinyallerden rasgele anahtarlar üretilmiştir. P dalgası atriyumun depolarizasyon impulsunu temsil eder; QRS kompleksi ventriküler depolarizasyonu temsil ederken, T dalgası ventriküllerin repolarizasyonunu temsil eder. R-tepe noktası, EKG dalga formunun en belirgin özelliği olduğundan, bir kalp atışını temsil etmek için kullanılabilir. Bu dalgaların arasındaki zaman gecikmeleri kullanılarak bu anahtarlar oluşturulmuştur [40]. Benzer bir çalışmada yine EKG sinyali içerisindeki bazı ayırt edici özellikler kullanılarak sonlu uzunluklu anahtarlar oluşturulmuştur [41].

Bu çalışmada doğrudan EKG verisi dijital hale getirilerek kaotik sayı dizisi yerine kullanılması incelenmiştir. EKG sinyalleri MIT-BIH Normal Sinus Rhythm Database veritabanı üzerinden alınmıştır [42]. Genel olarak EKG işaretleri periyodik işaretler olarak kabul edilir. Fakat aritmi, kalp krizi, taşikardi gibi durumlarda bu sinyallerin kaotik özellikler taşıdığı kabul görmüştür [43]. Normal sağlıklı EKG ritmi için ise tartışmalar söz konusudur. EKG sinyallerinde R-tepe tespiti yaparken kaotik yöntemlerin kullanılması, bu sinyalin kaotik bileşenler taşıdığını göstermektedir [44]. Farklı çalışmalarda sağlıklı ve hasta kişilere ait EKG sinyallerinin ayrılması için yine kaotik özellikler kullanılmıştır [45, 46]. Sağlıklı kişilere ait EKG sinyallerinin Lyapunov üstelleri hesaplandığında, kaotik anlamda çelişkili sonuçlar elde edilmektedir. Kaotik sinyaller pozitif Lyapunov üstelleri üretir. Sağlıklı insanlara ait EKG sinyallerinin üstellerinin, hasta kişilere ait EKG üstellerinden daha küçük olduğu da gösterilmiştir [47]. Fakat içerisindeki kaotik bileşenlerin şifreleme güvenliği açısından yeterliliği incelenmeye açıktır.

1.2 Tezin Amacı

Bu çalışmada literatürde güvenilirliği ispatlamış bir kaotik şifreleme yöntemi kullanılarak, EKG verilerinin güvenli haberleşme alanında kullanımı incelenmiştir. Kaotikliği literatürde tartışmalı bir konu olan EKG verileri, bu yöntemde doğrudan kaotik sayı dizileri yerine kullanılarak şifrelenmiş görüntülerin NPCR, UACI ve entropi değerleri üzerinden bir güvenlik analizi yapılmıştır. Elde edilen sonuçlara göre kişinin, kullanılan faz kaydırma örnek sayısının ve EKG alınan zamanın anahtar olarak belirlenmesi ile elde edilen sayı dizisinin bu yöntemle kullanılabilir olduğu gözlemlenmiştir. Sağlıklı EKG verilerinin periyodikliği yanında barındırdığı kaotik özelliklerin yeterliliği gösterilmiştir.

1.3 Hipotez

Bu çalışmada açık metin ataklarına karşı güvenliğin bir ölçüsü olan NPCR, UACI değerleri ve şifrelenmiş görüntünün entropisi hesaplanarak, EKG verisinin kaotik şifreleme yöntemleri ile kullanılıp kullanılamayacağı test edilmiştir. Önce kaotik olduğu bilinen Lorenz sisteminden elde edilen sayı dizileri ile, literatürde işlerliği bilinen bir kaotik şifreleme yöntemi uygulanarak bu değerler elde edilmiştir. Daha

sonra aynı yöntem için, kaotik sayı dizileri yerine EKG verileri konmuş ve elde edilen değerler kaotik verilerle elde edilen değerlerle karşılaştırılmıştır. Elde edilen simülasyon sonuçlarına göre, normal EKG sinyalleri kaotik olarak tanımlanamamasına rağmen, kaotik şifreleme yöntemlerinde kullanıldıklarında güvenli şifreleme yapılmasına olanak sağlamaktadırlar. Sadece farklı kişilere ait EKG verileri değil, ayrıca aynı kişiye ait farklı zamanlarda kaydedilmiş veriler, ya da farklı faz kaydırmalarına tabi tutulan EKG verileri de farklı güvenli diziler oluşmasını sağlamaktadırlar.

2
KAOTİK SİSTEMLER

Kaos ilk olarak 1963 yılında E. Lorenz tarafından tanıtıldı [53]. O zamandan beri kaos, dünyadaki birçok bilim adamı ve araştırma grubu için araştırma odaklarından biri olmuştur ancak özellikle iletişim alanında verimli bir şekilde kullanılması sadece birkaç on yıl olmuştur. Kaos, kaotik maskeleme ilkesiyle [54] iletişim mahremiyetinde bile cihaz ve sistemlerdeki düzensiz davranışların [55] kontrol edilmesi gibi kontrol uygulamalarında ve güvenli iletişim, kaotik bant radyo ve şifreleme sağlayan aynı veya farklı iki sistemin senkronizasyonunda [55] önemli bir rol oynamıştır. Kaotik sistemlerin ayrıca hava durumunu, bulaşıcı hastalıkları ve ekonomiyi tahmin etmek için uygulanabilecek kısa vadeli tahminlerde uygulamaları vardır.

Bir kaotik sistem, aynı anda iki çözümün çok benzer iki koşul için çok farklı olduğu diferansiyel denklemlerden oluşur. Birçok kaotik sistem, yukarıda tartışıldığı gibi kaos yaratmak üzere tasarlanmıştır. Bu kaotik sistemler, faz uzayında bir dizi noktadan oluşan çekiciler üretir. Bu çekiciler periyodik değildir, dolayısıyla geleneksel sistemler onları üretemez [56]. Otonom olmayan sistemde kaos, sistemde sadece 2 değişken olsa bile ortaya çıkabilir ve otonom durumda, en az üç durum değişkeniyle ortaya çıkabilir [57]. Çoğu zaman kaotik sistemler tamsayı derecelidir ancak kesirli dereceli hesabı incelenerek, kesirli dereceli kaotik sistemlerin dinamik doğaları nedeniyle doğada gözlemlenebilen sistemlerin modellenmesinde daha iyi olduğu gözlenmiştir. Kesirli dereceli sistemler doğada yerel değildir çünkü gelecekteki durumları yalnızca mevcut durumlarına değil aynı zamanda geçmiş durumlarının koşullarına da bağlıdır [58].

2.1 Kesirli Dereceli Lorenz Sistemi

Lorenz, kaosu tanıttıktan sonra 1963'te kaotik bir sistem tasarladı. Kesirli dereceli kaotik Lorenz sistemi aşağıdaki denklemlere sahip olacaktır.

Burada 'q' kesirli derece olarak alınır ve q Є (0,1) olacaktır.

$$\frac{d^q x}{dt^q} = \sigma(y - x) \tag{2.1}$$

$$\frac{d^q y}{dt^q} = rx - xz - y \tag{2.2}$$

$$\frac{d^q z}{dt^q} = -bz + xy \tag{2.3}$$

2.2 Kesirli Dereceli Rössler Sistemi

Kesirli dereceli Rössler sistemi denklemleri şu şekildedir.

$$\frac{d^q x}{dt^q} = -y - z \tag{2.4}$$

$$\frac{d^q y}{dt^q} = x + ay \tag{2.5}$$

$$\frac{d^q z}{dt^q} = b + z(x - c) \tag{2.6}$$

2.3 Kesirli Dereceli Chen Sistemi

Kesirli dereceli Chen sistemi denklemleri şu şekildedir.

$$\frac{d^q x}{dt^q} = a(y - x) \tag{2.7}$$

$$\frac{d^q y}{dt^q} = cy - xz + (c - a) \tag{2.8}$$

$$\frac{d^q z}{dt^q} = -bz + xy \tag{2.9}$$

2.4 Kesirli Dereceli Lü Kaotik Sistemi

Kesirli Dereceli Chen sistemi denklemleri şu şekildedir.

$$\frac{d^q x}{dt^q} = a(y - x) \tag{2.10}$$

$$\frac{d^q y}{dt^q} = cy - xz \tag{2.11}$$

$$\frac{d^q z}{dt^q} = -bz + xy \tag{2.12}$$

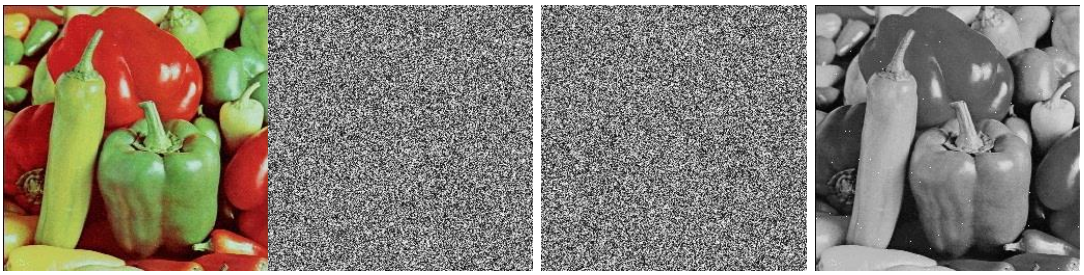
3
LYAPUNOV ÜSTELLERİ

Yakın başlangıç koşullarında oluşturulan faz uzayı karakteristiklerinin yörüngeleri arasındaki etkileşim ve farkların ifadesidir. Eğer sistemin en az bir pozitif Lyapunov üsteli varsa sistem kaotiktir. En büyük üstel negatif ise; sistem zaman içinde bir değere yakınsar ve başlangıç koşullarına bağımsız hale gelir [59]. En büyük üstel pozitif ise; yörüngeler arasındaki mesafe gittikçe artar ve sistem başlangıç koşullarına karşı hassastır, yani kaotiktir denir. Eğer birden fazla pozitif Lyapunov üsteli varsa sistem hiper kaotiktir [60].

3.1 Kesirli Dereceli Sistemler için Lyapunov Üstellerinin Hesaplanması

Bu çalışmada Tablo 3.1 ve 3.2'de görülen Chen, Lorenz, Lü ve Rössler sistemlerinin hem kesirli dereceli hem de tamsayı dereceli halleri için, dinamik parametrelerde değişiklik yapılarak, farklı Lyapunov üstellerine sahip zaman serileri elde edilmiştir. Lyapunov üstellerinin hesaplanmasında bir boyutlu zaman serilerinin zamanda ötelenmesi ile elde edilen faz kaydırmalı uzaylar kullanılmıştır [60].

Kullanılan parametreler, başlangıç koşulları ve elde edilen Lyapunov üstelleri kesirli dereceli sistemler için Tablo 3.1'de verilmiştir.



(a)Orijinal görüntü (b)Şifreli görüntü (1) (c)Şifreli görüntü (2) (d)Şifresi çözülmüş görüntü

Şekil 3.1 Kesirli dereceli Lorenz sistemi kullanılarak elde edilen görüntü örnekleri

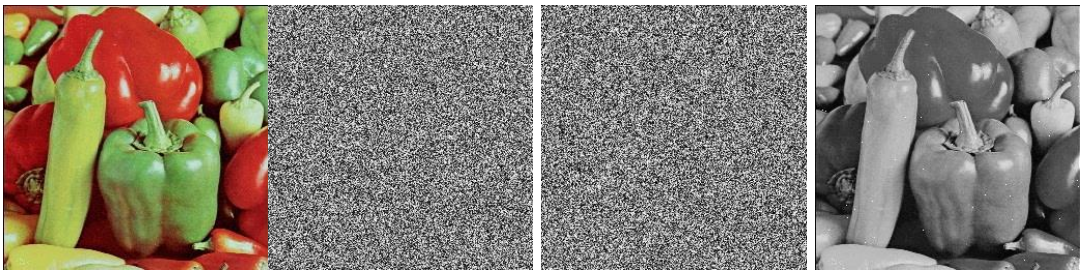
Tablo 3.1 Kesirli Dereceli Kaotik Sistemlerde Parametre Değişikliğinin Lyapunov Üstellerine Etkisi

Kaotik Sistem	Kesir Dereceli Sistem													
	Model Parametreleri				Kesir Dereceleri			Başlangıç Koşulları			Lyapunov Üstelleri			
	a	b	c	d	q1	q2	q3	Y0(1)	Y0(2)	Y0(3)	L1	L2	L3	Ortalama
Chen	35	3	28	-7	0.9	0.9	0.9	-9	-5	14	5,3444	5,9197	4,9270	5,3970
	35	3	23	-7	0.9	0.9	0.9	-9	-5	14	6,6203	6,9242	5,8589	6,4678
Lorenz	10	28	8/3		0.993	0.993	0.993	0.1	0.1	0.1	2,9044	3,7023	2,4145	3,0070
	10	50	8/3		0.993	0.993	0.993	0.1	0.1	0.1	4,4203	5,9282	4,6354	4,9946
Lü	36	3	25		0.985	0.99	0.98	0.2	0.5	0.3	4,6927	4,5383	3,8293	4,3534
	36	3	20		0.985	0.99	0.98	0.2	0.5	0.3	2,8978	2,7366	2,5227	2,7190
Rössler	0.2	0.2	5.7		0.9	0.85	0.95	0.5	1.5	0.1	3,9475	3,7998	0,8423	2,8632
	0.5	0.2	10		0.9	0.85	0.95	0.5	1.5	0.1	4,5204	4,3666	0,8588	3,2486

Elde edilen bu farklı yörüngesel uzaklıklara sahip zaman serileri ile, literatürde bulunan bir kaotik şifreleme yöntemi ile görüntü şifrelenmesi işlemi yapılmış [35], ve elde edilen şifreli ve geri deşifre edilmiş görüntülerin şifreleme güvenliği açısından incelenmesi yapılmıştır. Şekil 3.1'de Kesirli dereceli Lorenz sistemi kullanılarak elde edilen görüntü örnekleri verilmiştir.

3.2 Tam Sayı Dereceli Sistemler için Lyapunov Üstellerinin Hesaplanması

Şekil 3.2'de Tam sayı dereceli Lü kaotik sistemi kullanılarak elde edilen görüntü örnekleri verilmiştir.



(a)Orijinal görüntü (b)Şifreli görüntü (C1) (c) Şifreli görüntü (C2) (d) Şifresi çözülmüş görüntü

Şekil 3.2 Tam sayı dereceli Lü sistemi kullanılarak elde edilen görüntü örnekleri

Tablo 3.2 Tam Sayı Dereceli Kaotik Sistemlerde Parametre Değişikliğinin Lyapunov Üstellerine Etkisi

Kaotik Sistem	Tam Sayı Dereceli Sistem													
	Model Parametreleri				Kesir Dereceleri			Başlangıç Koşulları			Lyapunov Üstelleri			
	a	b	c	d	q1	q2	q3	Y0(1)	Y0(2)	Y0(3)	L1	L2	L3	Ortalama
Chen	35	3	28	-7	1	1	1	-9	-5	14	7,1355	7,3146	5,8511	6,7670
	35	3	20	-7	1	1	1	-9	-5	14	4,6346	4,5097	3,8686	4,3376
Lorenz	10	28	8/3		1	1	1	0.1	0.1	0.1	3,2894	4,4773	3,3097	3,6921
	10	24	8/3		1	1	1	0.1	0.1	0.1	2,2225	3,0847	2,2707	2,5259
Lü	36	3	20		1	1	1	0.2	0.5	0.3	3,4998	3,803	3,1485	3,4837
	36	3	25		1	1	1	0.2	0.5	0.3	5,8697	6,0735	4,9759	5,6397
Rössler	0.2	0.2	5.7		1	1	1	0.5	1.5	0.1	2,3134	2,0818	0,9501	1,7817
	0.5	0.2	4.7		1	1	1	0.5	1.5	0.1	1,4177	1,0465	1,1045	1,1895

Kullanılan parametreler, başlangıç koşulları ve elde edilen Lyapunov üstelleri tam sayı dereceli sistemler için Tablo 3.2'de verilmiştir.

4
KULLANILAN METRİKLER

4.1 Kullanılan Kaotik Görüntü Şifreleme Algoritması

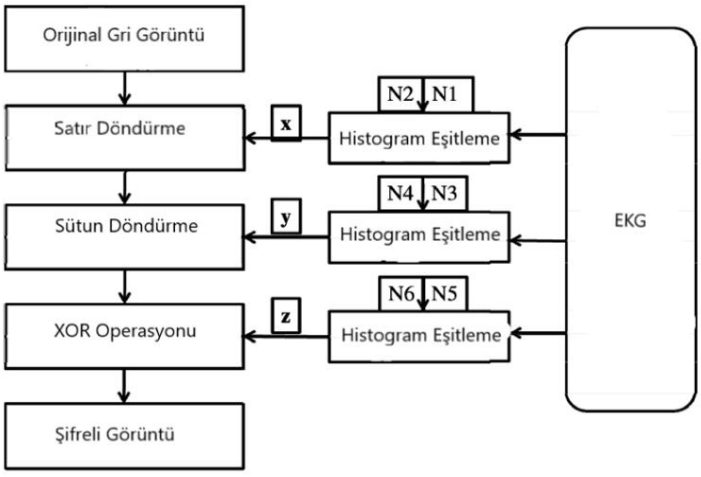
Genel şifreleme işlemini tamamlamak için dört aşama kullanılmıştır [35].

a) Histogram Eşitleme

b) Satır Döndürme

c) Sütun Döndürme

d) XOR Operasyonu



Şekil 4.1 EKG Verileri Kullanılarak Görüntü Şifreleme Algoritması

Kullanılan görüntü şifreleme algoritmasının akış diyagramı Şekil 4.1'de verilmiştir.

4.2 Histogram Eşitleme

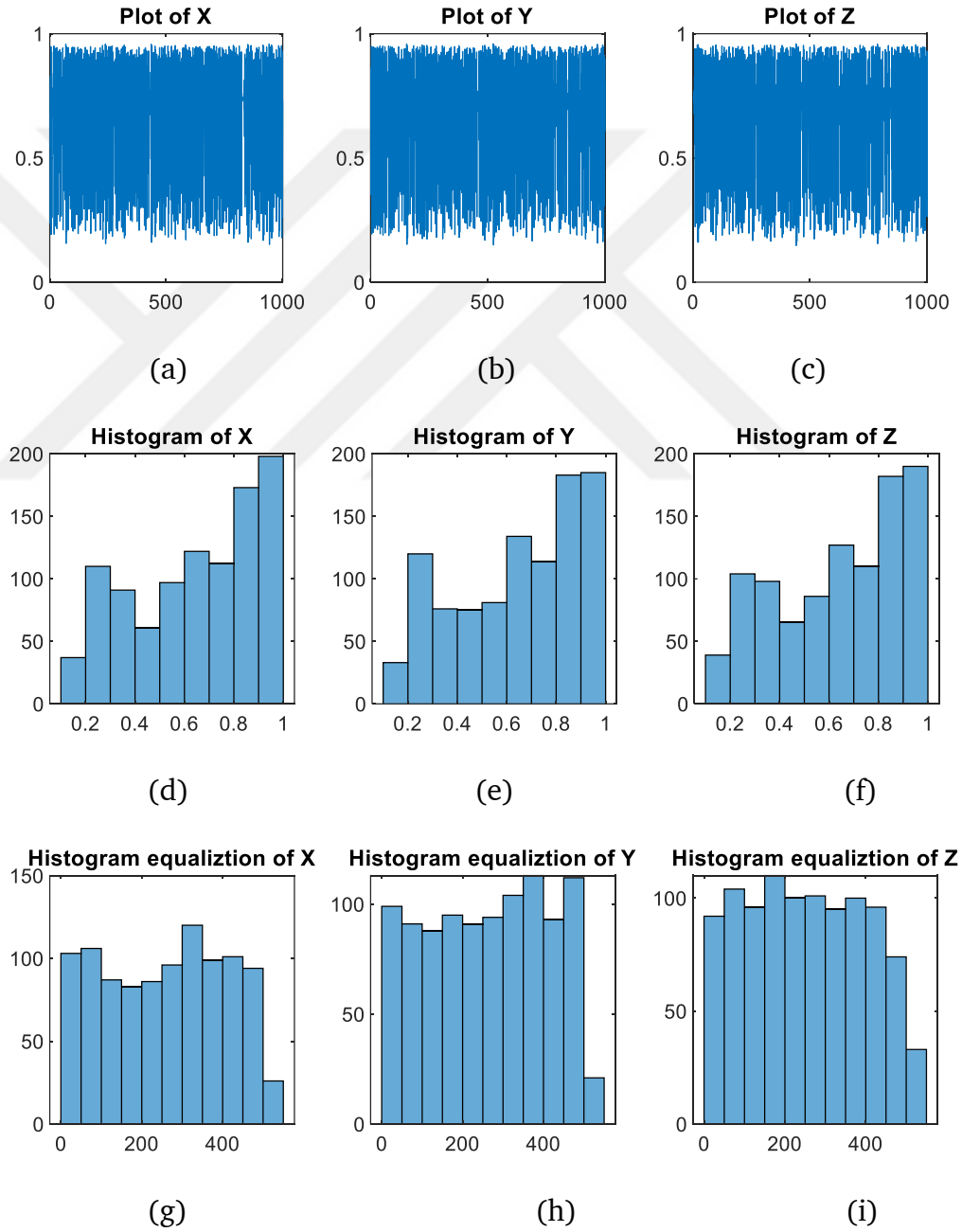
Şekil 4.1'de görüldüğü gibi x, y, z olarak adlandırılan 3 farklı kaotik sinyale ait histogramların homojen olmayan dağılıma sahip olduğu açıktır. Daha yüksek güvenlik için histogramı eşitlememiz gerekir. M×N boyutunda gri bir görüntü varsa M satır sayısını N ise sütun sayısını temsil eder. Ardından aşağıdaki formüller kullanılarak histogram eşitlenir:

$$x = (intege(x \times N2))mod\ N \quad (4.1)$$

$$y = (intege(y \times N4))mod\ M \quad (4.2)$$

$$z = (intege(z \times N6))mod\ 256 \quad (4.3)$$

Burada, N2, N4, N6 genellikle 10000'den büyük büyük bir rasgele sayıdır. Basitlik açısından N2, N4 ve N6'nın eşit olduğu da düşünülebilir. Şekil 4.2(g), (h) ve (i) eşitlenmiş histogramı N1=500, N3=600, N5=700 rasgele sayıları, N2=N4=N6=100000, M = 256, N=256 değerleri kullanılarak göstermektedir.



Şekil 4.2 EKG Sinyali Histogram Eşitleme

4.3 Satır Döndürme

Görüntü piksel permütasyonu amacıyla satır sütununun döndürme işlemi yapılır. M×N boyutuna sahip gri bir görüntünün satırını döndürebilmek için kaos dizisinin M uzunluklu bir parçasını seçmemiz gerekir. Öncelikle rasgele sayı N dizisi değeri girişi; sonrasında N1 dizininden başlayarak seçilen M sayısına göre Denklem 4.1 kullanılarak 'x' değerine göre satırı döndürülür. Güvenliği artırmak için EKG sinyali kullanılarak elde edilen anahtar değeri çift olduğunda sola ve değeri tek ise sağa döndürme işlemi gerçekleştirilir.

4.4 Sütun Döndürme

Sütun döndürme, satır döndürme ile aynıdır. M×N boyutunda gri bir görüntünün satırını döndürmek için N boyutlu bir sayı dizisi seçmemiz gerekir. Öncelikle rasgele sayı N3 değeri girişi; sonrasında N3 dizininden başlayarak seçilen N sayısına göre Denklem 4.2 kullanılarak 'y' değerine göre satırı döndürülür. Güvenliği artırmak için EKG sinyali kullanılarak elde edilen anahtar değeri çift olduğunda yukarı döndürülür ve değeri tek ise aşağı döndürme işlemi gerçekleştirilir. Satır sütununun döndürülmesinden sonra görüntü şifrelenir ancak sorun histogram saldırısına neden olabilecek değişmeyen histogramdır. Bu saldırıyı engellemek için görüntü piksel değerini değiştiren başka bir adıma ihtiyaç olduğu aşikardır.

4.5 XOR Operasyonu

Şifreleme işleminin son adımı XOR işlemidir. XOR işlemi piksel değerini yeni değere değiştirir ve EKG sinyali kullanılarak elde edilen anahtarı bilmeden tersine çeviremez. Öncelikle rasgele sayı N5 değeri girişi yapılır ve M × N görüntüsü 1×MN görüntüsüne dönüştürülür. Bundan sonra, EKG sinyalini (dizinin N5. elemanından başlayarak) ve satır-sütun kaydırılmış görüntü XOR işlemine tabi tutulur ve sonunda şifreli görüntü elde edilmektedir.

4.6 Piksel Değişim Oranı Sayısı

Şifreli görüntü açık metnin değiştirilmesine karşı hassas değilse, kriptanalist şifrelenmiş görüntüden çok faydalı bilgiler alabilir. Açık metin saldırılarının

hassasiyetini kontrol etmek için Piksel Değişim Oranı Sayısı (NPCR) ve Birleştirilmiş Ortalama Değişme Yoğunluğu (UACI) olmak üzere iki kriter kullanılmaktadır. İki şifreli görüntü arasındaki farklı piksel sayılarının yüzdesi olarak tanımlanan NPCR aşağıdaki şekilde ifade edilir.

$$\mathrm{NPCR} = \frac{\Sigma_{\mathrm{i,j}}\, \mathrm{D(i,j)}}{\mathrm{M} \times \mathrm{N}} \times 100\% \tag{4.4}$$

4.7 Birleşik Ortalama Değişim Yoğunluğu

Şifreli Birleşik Ortalama Değişim Yoğunluğu; M×N iki şifreli görüntü arasındaki farkların ortalama yoğunluğu olarak aşağıda tanımlanmıştır.

$$\mathrm{UACI} = \frac{1}{\mathrm{M} \times \mathrm{N}}\, \Sigma_{\mathrm{i,j}}\, \frac{|\mathrm{c1(i,j)} - \mathrm{c2(i,j)}|}{255} \times 100\% \tag{4.5}$$

Burada C1 ve C2 farklı anahtar kullanılarak şifrelenmiş iki farklı şifreli görüntüdür.

D (i, j) aşağıdaki gibi tanımlanır:

$$\mathrm{D\ (i,\ j)} = \begin{Bmatrix} 1\ if\ C1(i,j) \neq C2(i,j) \\ 0\ if\ C1(i,j) = C2(i,j) \end{Bmatrix} \tag{4.6}$$

4.8 Entropi

Bir sembol kaynağı S'nin entropisi H aşağıdaki denklemle hesaplanabilir [51].

$$H(S) = -\Sigma_{\mathrm{i=0}}^{N-1} P(S_i) log_2 P(S_i) \tag{4.7}$$

Burada P(Si) Si sembolünün olasılığını temsil eder ve entropi bit olarak ifade edilir. Kaynak S eşit olasılıkla 28 sembol yayarsa S = {s1, s2. . . s256}, o zaman entropinin sonucu gerçek bir rastgele kaynağa karşılık gelen ve mesaj kaynağı S için ideal entropi değerini temsil eden H(S) = 8'dir.

Gri değerin dağılımı ne kadar düzgün olursa, bilgi entropisi o kadar büyük olur. Şifrelenmiş bir görüntünün bilgi entropisi ideal 8 değerinden önemli ölçüde düşükse, görüntü güvenliğini tehdit eden bir öngörülebilirlik olasılığı olacaktır.

4.9 Kaotik Sistemlerde Başlangıç Koşullarının Değerlendirme Ölçütlerine Etkisi

4.9.1 Kaotik Sistemlerde Başlangıç Koşullarındaki Değişikliğin Piksel Değişim Oranına Etkisi

Tablo 3.1 ve 3.2'de verilen Lyapunov üstellerinin elde edilmesini sağlayan diziler kullanılarak şifreleme ve deşifreleme işlemleri ile elde edilmiş görüntüler, NPCR parametresi açısından incelenmiş ve Tablo 4.1'de kesirli dereceli sistemler için, Tablo 4.2'de de tam sayı dereceli sistemler için verilen değerler elde edilmiştir.

Tablo 4.1 Kesirli Dereceli Kaotik Sistemlerde Başlangıç Koşullarının Piksel Değişim Oranına Etkisi

Kaotik Sistem	Kesir Dereceleri			Kesir Dereceli Sistem 1			Kesir Dereceli Sistem 2				
				Başlangıç Koşulları			Başlangıç Koşulları			NPCR	Lyapunov Üstelleri
	q1	q2	q3	Y0(1)	Y0(2)	Y0(3)	Y0(1)	Y0(2)	Y0(3)		Ortalama
Chen	0.9	0.9	0.9	-9	-5	14	-9	-5	14.01	99,5972	5,3970
	0.9	0.9	0.9	-9	-5	14	-9	-5	14.01	99,6811	6,4678
Lorenz	0.993	0.993	0.993	0.1	0.1	0.1	0.1	0.1	0.11	99,5895	3,0070
	0.993	0.993	0.993	0.1	0.1	0.1	0.1	0.1	0.11	99,5972	4,9946
Lu	0.985	0.99	0.98	0.2	0.5	0.3	0.2	0.5	0.31	99,6231	4,3534
	0.985	0.99	0.98	0.2	0.5	0.3	0.2	0.5	0.31	99,6185	2,7190
Rossler	0.9	0.85	0.95	0.5	1.5	0.1	0.5	1.5	0.11	99,3866	2,8632
	0.9	0.85	0.95	0.5	1.5	0.1	0.5	1.5	0.11	99,5529	3,2486

Tablo 4.2 Tam Sayı Dereceli Kaotik Sistemlerde Başlangıç Koşullarının Piksel Değişim Oranı Sayısına Etkisi

Kaotik Sistem	Kesir Dereceleri			Tam Sayı Dereceli Sistem 1			Tam Sayı Dereceli Sistem 2				
				Başlangıç Koşulları			Başlangıç Koşulları			NPCR	Lyapunov Üstelleri
	q1	q2	q3	Y0(1)	Y0(2)	Y0(3)	Y0(1)	Y0(2)	Y0(3)		Ortalama
Chen	1	1	1	-9	-5	14	-9	-5	14.01	99,6201	6,7670
	1	1	1	-9	-5	14	-9	-5	14.01	99,6094	4,3376
Lorenz	1	1	1	0.1	0.1	0.1	0.1	0.1	0.11	99,6552	3,6921
	1	1	1	0.1	0.1	0.1	0.1	0.1	0.11	99,6231	2,5259
Lu	1	1	1	0.2	0.5	0.3	0.2	0.5	0.31	99,617	3,4837
	1	1	1	0.2	0.5	0.3	0.2	0.5	0.31	99,6307	5,6397
Rossler	1	1	1	0.5	1.5	0.1	0.5	1.5	0.11	99,6048	1,7817
	1	1	1	0.5	1.5	0.1	0.5	1.5	0.11	99,6048	1,1895

4.9.2 Kaotik Sistemlerde Başlangıç Koşullarındaki Değişikliğin Birleşik Ortalama Değişim Yoğunluğuna Etkisi

Tablo 3.1 ve 3.2'de verilen Lyapunov üstellerinin elde edilmesini sağlayan diziler kullanılarak şifreleme ve deşifreleme işlemleri ile elde edilmiş görüntüler, UACI parametresi açısından incelenmiş ve Tablo 4.3'te kesirli dereceli sistemler için, Tablo 4.4'te de tam sayı dereceli sistemler için verilen değerler elde edilmiştir.

Tablo 4.3 Kesirli Dereceli Kaotik Sistemlerde Başlangıç Koşullarının Birleşik Ortalama Yoğunluğuna Etkisi

Kaotik Sistem				Kesir Dereceli Sistem 1			Kesir Dereceli Sistem 2				
	Kesir Dereceleri			Başlangıç Koşulları			Başlangıç Koşulları			UACI	Lyapunov Üstelleri
	q1	q2	q3	Y0(1)	Y0(2)	Y0(3)	Y0(1)	Y0(2)	Y0(3)		Ortalama
Chen	0.9	0.9	0.9	-9	-5	14	-9	-5	14.01	33,4124	5,3970
	0.9	0.9	0.9	-9	-5	14	-9	-5	14.01	33,5874	6,4678
Lorenz	0.993	0.993	0.993	0.1	0.1	0.1	0.1	0.1	0.11	33,4633	3,0070
	0.993	0.993	0.993	0.1	0.1	0.1	0.1	0.1	0.11	33,2680	4,9946
Lu	0.985	0.99	0.98	0.2	0.5	0.3	0.2	0.5	0.31	33,3543	4,3534
	0.985	0.99	0.98	0.2	0.5	0.3	0.2	0.5	0.31	33,5674	2,7190
Rossler	0.9	0.85	0.95	0.5	1.5	0.1	0.5	1.5	0.11	38,4550	2,8632
	0.9	0.85	0.95	0.5	1.5	0.1	0.5	1.5	0.11	33,0641	3,2486

Tablo 4.4 Tam Sayı Dereceli Kaotik Sistemlerde Başlangıç Koşullarının Birleşik Ortalama Yoğunluğuna Etkisi

Kaotik Sistem				Tam Sayı Dereceli Sistem 2			Tam Sayı Dereceli Sistem 2				
	Kesir Dereceleri			Başlangıç Koşulları			Başlangıç Koşulları			UACI	Lyapunov Üstelleri
	q1	q2	q3	Y0(1)	Y0(2)	Y0(3)	Y0(1)	Y0(2)	Y0(3)		Ortalama
Chen	1	1	1	-9	-5	14	-9	-5	14.01	33,3646	6,7670
	1	1	1	-9	-5	14	-9	-5	14.01	33,5127	4,3376
Lorenz	1	1	1	0.1	0.1	0.1	0.1	0.1	0.11	33,3258	3,6921
	1	1	1	0.1	0.1	0.1	0.1	0.1	0.11	33,5773	2,5259
Lu	1	1	1	0.2	0.5	0.3	0.2	0.5	0.31	33,5725	3,4837
	1	1	1	0.2	0.5	0.3	0.2	0.5	0.31	33,4923	5,6397
Rossler	1	1	1	0.5	1.5	0.1	0.5	1.5	0.11	33,5725	1,7817
	1	1	1	0.5	1.5	0.1	0.5	1.5	0.11	33,3573	1,1895

4.9.3 Kaotik Sistemlerde Başlangıç Koşullarındaki Değişikliğin Şifreli Görüntünün Entropi Değerine Etkisi

Tablo 3.1 ve 3.2'de verilen Lyapunov üstellerinin elde edilmesini sağlayan diziler kullanılarak şifreleme ve deşifreleme işlemleri ile elde edilmiş görüntüler, Entropi parametresi açısından incelenmiş ve Tablo 4.5'te kesirli dereceli sistemler için, Tablo 4.6'da da tam sayı dereceli sistemler için verilen değerler elde edilmiştir.

Tablo 4.5 Kesirli Dereceli Kaotik Sistemlerde Başlangıç Koşullarındaki Değişiklikliğin Şifreli Görüntünün Entropi Değerine Etkisi

Kaotik Sistem				Kesir Dereceli Sistem 1			Kesir Dereceli Sistem 1				
	Kesir Dereceleri			Başlangıç Koşulları			Başlangıç Koşulları			Entropi	
	q1	q2	q3	Y0(1)	Y0(2)	Y0(3)	Y0(1)	Y0(2)	Y0(3)	Entropi 1	Entropi 2
Chen	0.9	0.9	0.9	-9	-5	14	-9	-5	14.01	7,9896	7,9893
	0.9	0.9	0.9	-9	-5	14	-9	-5	14.01	7,9894	7,9893
Lorenz	0.993	0.993	0.993	0.1	0.1	0.1	0.1	0.1	0.11	7,989	7,9891
	0.993	0.993	0.993	0.1	0.1	0.1	0.1	0.1	0.11	7,9896	7,9892
Lu	0.985	0.99	0.98	0.2	0.5	0.3	0.2	0.5	0.31	7,9898	7,9897
	0.985	0.99	0.98	0.2	0.5	0.3	0.2	0.5	0.31	7,9886	7,9887
Rossler	0.9	0.85	0.95	0.5	1.5	0.1	0.5	1.5	0.11	7,6535	7,6585
	0.9	0.85	0.95	0.5	1.5	0.1	0.5	1.5	0.11	7,9892	7,9892

Tablo 4.6 Tam Sayı Dereceli Kaotik Sistemlerde Başlangıç Koşullarındaki Değişiklikliğin Şifreli Görüntünün Entropi Değerine Etkisi

Kaotik Sistem				Tam Sayı Dereceli Sistem 1			Tam Sayı Dereceli Sistem 1				
	Kesir Dereceleri			Başlangıç Koşulları			Başlangıç Koşulları			Entropi	
	q1	q2	q3	Y0(1)	Y0(2)	Y0(3)	Y0(1)	Y0(2)	Y0(3)	Entropi 1	Entropi 2
Chen	1	1	1	-9	-5	14	-9	-5	14.01	7,9888	7,9891
	1	1	1	-9	-5	14	-9	-5	14.01	7,9894	7,9893
Lorenz	1	1	1	0.1	0.1	0.1	0.1	0.1	0.11	7,9889	7,9896
	1	1	1	0.1	0.1	0.1	0.1	0.1	0.11	7,9889	7,9889
Lu	1	1	1	0.2	0.5	0.3	0.2	0.5	0.31	7,9889	7,9891
	1	1	1	0.2	0.5	0.3	0.2	0.5	0.31	7,989	7,9887
Rossler	1	1	1	0.5	1.5	0.1	0.5	1.5	0.11	7,9886	7,9885
	1	1	1	0.5	1.5	0.1	0.5	1.5	0.11	7,9883	7,9883

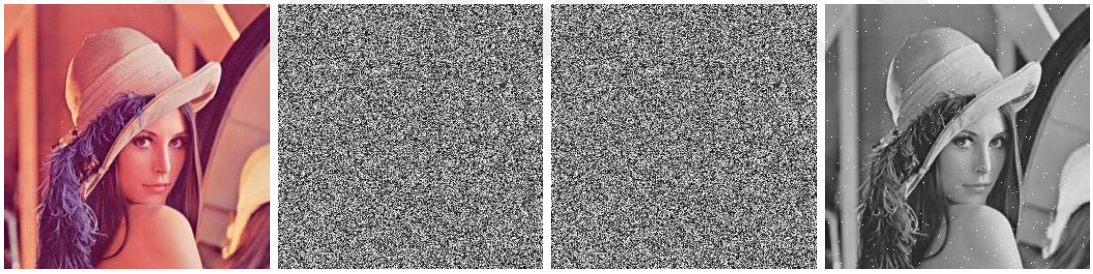
4.10 Lorenz Sistemi ile Kaotik Anahtar Kullanılarak Başlangıç Koşullarının Değerlendirme Ölçütlerine Etkisi

4.10.1 Lorenz Sistemi ile Kaotik Anahtar Kullanılarak Başlangıç Koşullarındaki Değişikliğin Piksel Değişim Oranına Etkisi

Lorenz, kaosu tanıttıktan sonra 1963'te kaotik bir sistem tasarladı. Kaotik Lorenz sistemi denklemleri (2.1), (2.2) ve (2.3)'de verilmiştir. $\sigma = 10$, r =28 ve b = 8/3 değerlerinde seçilmiştir.

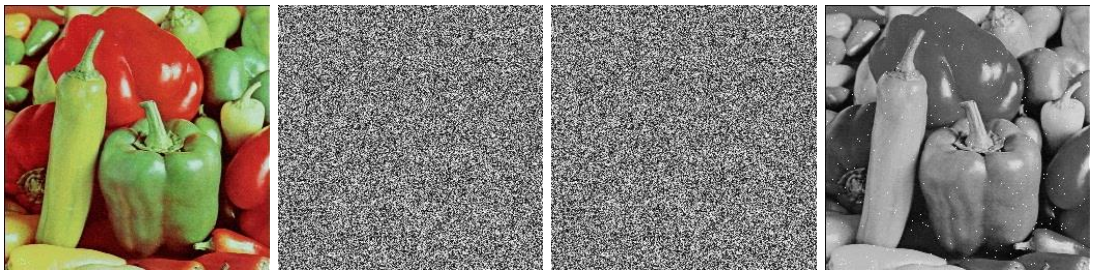
Kullanılan algoritmanın performans başarımının test edilebilmesi için Lorenz sistemi; farklı başlangıç koşulları altında değerlendirme parametrelerinin değişimi açısından karşılaştırılmıştır.

Şekil 4.3(a)'da verilen orijinal Lena görüntüsü, Şekil 4.3(b) ve Şekil 4.3(c) farklı başlangıç koşulları ile çalıştırılan Lorenz sistemlerinden elde edilen kaotik sayı dizileri ile oluşturulan şifreli görüntülerdir. Şekil 4.3(d) ise şifrelenmiş olan 4.3(b) görüntüsünün şifresinin çözülmesiyle elde edilmiş görüntüdür.



(a)Orijinal görüntü (b)Şifreli görüntü(C1) (c)Şifreli görüntü(C2) (d)Şifresi çözülmüş görüntü

Şekil 4.3 Lorenz sistemi kullanılarak elde edilen görüntü örnekleri



(a)Orijinal görüntü (b)Şifreli görüntü(C1) (c)Şifreli görüntü(C2) (d)Şifresi çözülmüş görüntü

Şekil 4.4 Lorenz sistemi kullanılarak elde edilen görüntü örnekleri

Şekil 4.4(a)'da verilen orijinal Peppers görüntüsü, Şekil 4.4(b) ve Şekil 4.4(c) farklı başlangıç koşulları ile çalıştırılan Lorenz sistemlerinden elde edilen kaotik sayı dizileri ile oluşturulan şifreli görüntülerdir. Şekil 4.4(d) ise şifrelenmiş olan 4.4(b) görüntüsünün şifresinin çözülmesiyle elde edilmiş görüntüdür.

Tablo 4.7 Başlangıç Koşullarının Piksel Değişim Oranına Etkisi

Orijinal Görüntü	Başlangıç Koşulları 1			Başlangıç Koşulları 2			NPCR
	x(1)	y(1)	z(1)	x(1)	y(1)	z(1)	
Peppers	0.9	0.9	0	0.91	0.91	0.01	99,5941
	0.9	0.9	0	0.9	0.9	0.1	99,5865
Blur	0.9	0.9	0	0.91	0.91	0.01	99,5804
	0.9	0.9	0	0.9	0.9	0.1	99,6277
Lena	0.9	0.9	0	0.91	0.91	0.01	99,5850
	0.9	0.9	0	0.9	0.9	0.1	99,6002
Mandrill	0.9	0.9	0	0.91	0.91	0.01	99,6094
	0.9	0.9	0	0.9	0.9	0.1	99,6063

Şekil 4.3 ve Şekil 4.4'te elde edilen görüntüler ile birlikte farklı görüntüler de Tablo 4.7'de Piksel Değişim Oranı Sayısı açısından karşılaştırılmıştır. Birbirine yakın komşuluklarda başlangıç değerleri ile elde edilen, kaotik olduğu bilinen bu dizilerle yapılan şifreleme sonucu elde edilen NPCR değerleri Tablo 4.7'de verilmiştir.

4.10.2 Lorenz Sistemi ile Kaotik Anahtar Kullanılarak Başlangıç Koşullarındaki Değişikliğin Birleşik Ortalama Değişim Yoğunluğuna Etkisi

Şekil 4.3 ve Şekil 4.4'te elde edilen görüntüler ile birlikte farklı görüntüler de Tablo 4.8'de Birleşik Ortalama Değişim Yoğunluğu açısından karşılaştırılmıştır. Birbirine yakın komşuluklarda başlangıç değerleri ile elde edilen, kaotik olduğu bilinen bu dizilerle yapılan şifreleme sonucu elde edilen UACI değerleri Tablo 4.8'de verilmiştir.

Tablo 4.8 Başlangıç Koşullarının Birleşik Ortalama Değişim Yoğunluğuna Etkisi

Orijinal Görüntü	Başlangıç Koşulları 1			Başlangıç Koşulları 2			UACI
	x(1)	y(1)	z(1)	x(1)	y(1)	z(1)	
Peppers	0.9	0.9	0	0.91	0.91	0.01	33,4059
	0.9	0.9	0	0.9	0.9	0.1	33,4760
Blur	0.9	0.9	0	0.91	0.91	0.01	33,3830
	0.9	0.9	0	0.9	0.9	0.1	33,5880
Lena	0.9	0.9	0	0.91	0.91	0.01	33,3708
	0.9	0.9	0	0.9	0.9	0.1	33,4657
Mandrill	0.9	0.9	0	0.91	0.91	0.01	33,3369
	0.9	0.9	0	0.9	0.9	0.1	33,4264

4.10.3 Lorenz Sistemi ile Kaotik Anahtar Kullanılarak Başlangıç Koşullarındaki Değişikliğin Şifreli Görüntünün Entropi Değerine Etkisi

Şekil 4.3 ve Şekil 4.4'te elde edilen görüntüler ile birlikte farklı görüntüler de Tablo 4.9'da şifreli görüntünün entropi değeri açısından karşılaştırılmıştır. Birbirine yakın

komşuluklarda başlangıç değerleri ile elde edilen, kaotik olduğu bilinen bu dizilerle yapılan şifreleme sonucuelde edilen Entropi değerleri Tablo 4.9'da analiz edilmiştir.

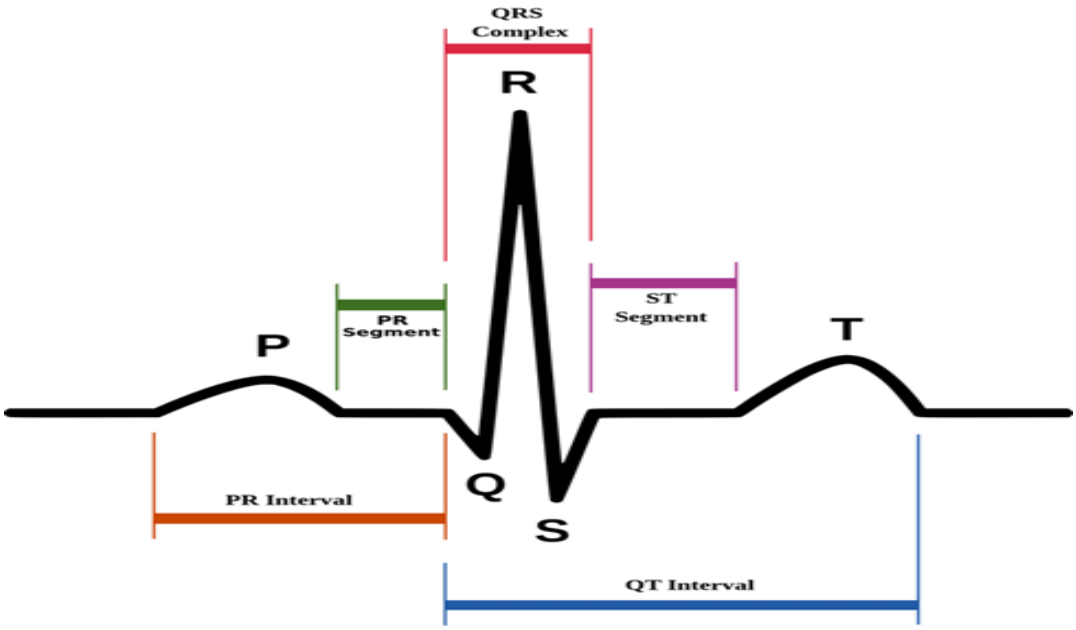
Bu analizlerden alınan değerler güvenli şifrelemeyi sağladığı bilinen kaotik bir dizi ile elde edilmiş sonuçlardır.

Tablo 4.9 Başlangıç Koşullarının Şifreli Görüntünün Entropi Değerine Etkisi

Orijinal Görüntü	Başlangıç Koşulları 1			Başlangıç Koşulları 2			Entropi	
	x(1)	y(1)	z(1)	x(1)	y(1)	z(1)	Entropi 1	Entropi 2
Peppers	0.9	0.9	0	0.9	0.9	0.1	7,9892	7,9888
Blur	0.9	0.9	0	0.9	0.9	0.1	7,9898	7,9891
Lena	0.9	0.9	0	0.9	0.9	0.1	7,9899	7,9898
Mandrill	0.9	0.9	0	0.9	0.9	0.1	7,9894	7,9897

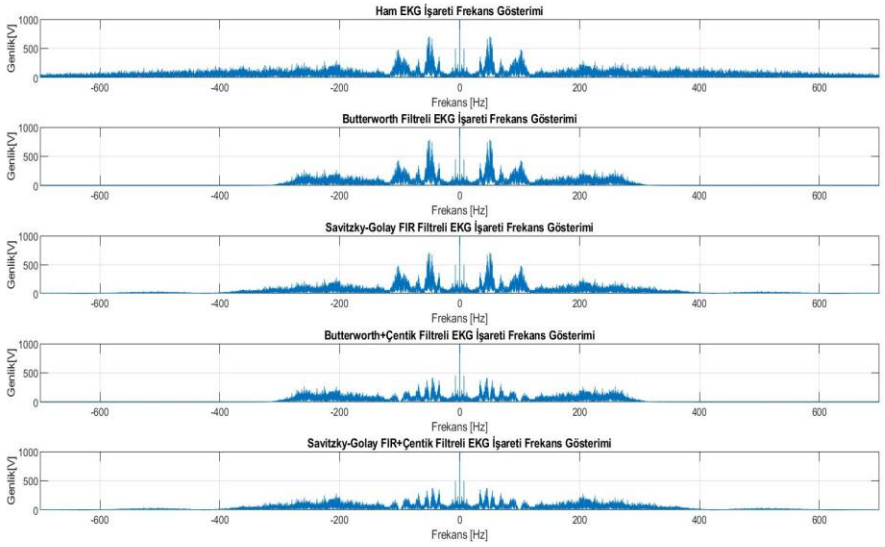
5
EKG

EKG, her kalp döngüsü boyunca kalp atışının elektriksel aktivitesini kaydederek hastanın kalp parametrelerini sağlayan bir tanı aracıdır. Şekil 5.1'de gösterildiği gibi, tipik bir tek döngülü EKG dalga formu, aralıklar ve segmentlerle ayrılan P dalgası, QRS kompleksi ve T dalgasından oluşur. P dalgasından önceki yatay kısım taban çizgisi olarak adlandırılır. P dalgası, atriyal kas sisteminin depolarizasyonunu temsil eden ve 80-110 ms bir süreye sahip olan pozitif polariteye sahip ilk yukarı doğru sapmadır. QRS kompleksinin üç dalgası, süresi 60 ila 100 ms arasında olan, atriyumun repolarizasyonunun ve ventriküllerin depolarizasyonunun birleşik sonuçlarına karşılık gelir. Q dalgası ilk aşağı doğru sapmadır ve en büyük dalga olarak R dalgası her zaman Q dalgasından sonraki ilk yukarı doğru sapmadır, S dalgası ise R dalgasını hemen takip eden negatiftir. Ventriküler gevşeme, ventriküllerin repolarizasyonunu takip eder ve yönü QRS kompleksi ile tutarlı olan T dalgası ile temsil edilir [48].

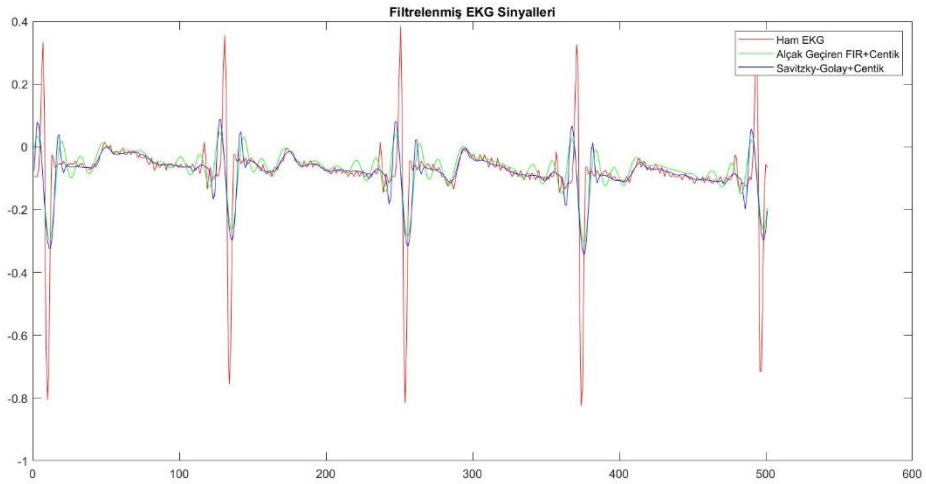


Şekil 5.1 Tipik EKG Sinyali

Veritabanından edinilen EKG sinyallerinde bulunan yüksek frekans gürültülerini gidermek amacıyla Alçak Geçiren FIR filtresi kullanılmıştır. Sonlu darbe cevabı filtresi, durdurma bandı zayıflatması 60 Db seviyesindedir. Parks-McClellan algoritması ile maksimum dalgalanma tüm frekanslar için minimize edilmeye çalışılmıştır. Ham EKG verisi ve filtrelenmiş verilere ait FFT spektrumları Şekil 5.2'de verilmiştir. Şelik 5.3'te kullanılan orijinal ve filtrelenmiş EKG verilerinin dalga şekilleri görülebilir.



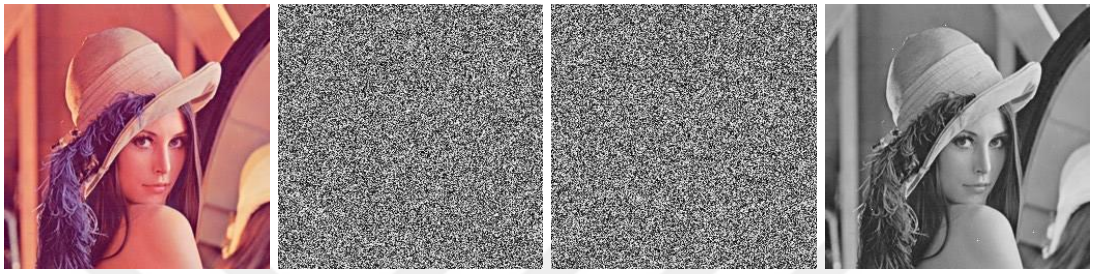
Şekil 5.2 EKG Sinyalinin Farklı Filtreleme Sonuçlarının Frekans Gösterimi



Şekil 5.3 EKG Sinyalinin Farklı Filtreleme Sonuçlarının Zaman Gösterimi

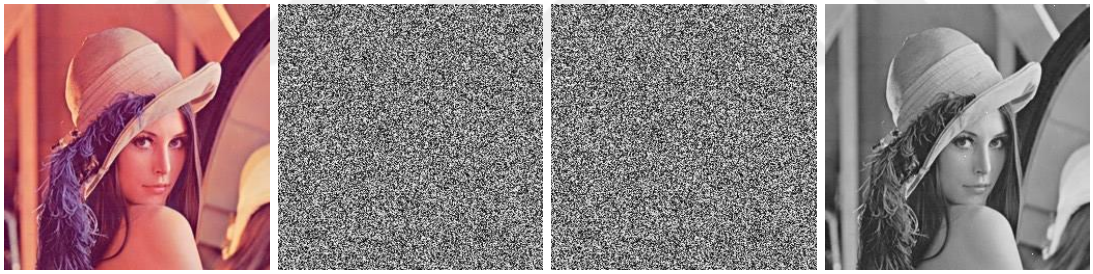
EKG sinyalleri öncelikle doğrudan kullanılmış olup sonra da aynı işlemler filtrelenmiş sinyallerle yapılmıştır.

Şekil 5.4(a) orijinal test görüntüsü, Şekil 5.4(b) ve 5.4(c), farklı kişilerin EKG sinyallerinin doğrudan sayı dizisi olarak kullanılması sonucu elde edilen görüntülerdir. Şekil 5.4(d) ise şifrelenmiş olan 5.4(b) görüntüsünün şifresinin çözülmesiyle elde edilmiş görüntüdür. Şekil 5.4'te elde edilen görüntüler kişilere ait EKG sinyalini 1 örnek kaydırarak elde edilen yeni faz uzayları kullanılarak elde edilmiştir. Şekil 5.5'te de aynı işlem 10 örnek kaydırılarak elde edilen uzaya ait örnekler verilmiştir.



(a)Orijinal görüntü (b)Şifreli görüntü(C1) (c)Şifreli görüntü(C2) (d)Şifresi çözülmüş görüntü

Şekil 5.4 Farklı kişilerden alınan EKG sinyalleri ile elde edilen görüntü örnekleri



(a)Orijinal görüntü (b)Şifreli görüntü(C1) (c)Şifreli görüntü(C2) (d)Şifresi çözülmüş görüntü

Şekil 5.5 Farklı kişilerden alınan EKG sinyalleri ile elde edilen görüntü örnekleri

5.1 EKG Bilgilerinin Farklı Örnek Kaydırmalarının Piksel Değişim Oranına Etkisi

İlk olarak EKG sinyallerinin açık metin ataklarına karşı güvenli anahtarlar olup olamayacağının incelenmesi amacıyla farklı kişilerden alınmış EKG sinyalleri ile şifrelenmiş aynı görüntülerin NPCR'leri karşılaştırılmış ve sonuçlar Tablo 5.1'de sunulmuştur. Farklı faz kaydırma sayılarına rağmen her seferinde NPCR'lerin güvenli şifrelemeyi doğrulayacak bir değer verdiği görülmektedir. Kullanılan

yöntem ile yapılan testler sonucunda görüntü şifrelemede EKG anahtarlarının yüksek bir duyarlılığa sahip olduğu anlaşılmıştır.

Tablo 5.1 Farklı Kişilerden Alınan EKG Bilgilerinin Piksel Değişim Oranına Etkisi

Kaydırılan Örnek Sayısı	Sağlıklı Denek Bilgisi		NPCR
1	1.Denek	2.Denek	99,6368
	1.Denek	3.Denek	99,6140
	2.Denek	3.Denek	99,6384
10	1.Denek	2.Denek	99,6185
	1.Denek	3.Denek	99,6307
	2.Denek	3.Denek	99,5972
17	1.Denek	2.Denek	99,6216
	1.Denek	3.Denek	99,6094
	2.Denek	3.Denek	99,6017

EKG sinyallerinin filtrelendiğinde elde edilen sonuçlar ise Tablo 5.2'de verilmiştir. Filtrelenmiş sinyallerle de yüksek anahtar duyarlılığına sahip güvenli şifreleme yapılabildiği gözlemlenmiştir.

Tablo 5.2 Farklı Kişilerden Alınan Filtrelenmiş EKG Bilgilerinin Piksel Değişim Oranına Etkisi

Kaydırılan Örnek Sayısı	Sağlıklı Denek Bilgisi		NPCR
1	1.Denek	2.Denek	99,5651
	1.Denek	3.Denek	99,5789
	2.Denek	3.Denek	99,6445
10	1.Denek	2.Denek	99,6124
	1.Denek	3.Denek	99,6017
	2.Denek	3.Denek	99,6216
17	1.Denek	2.Denek	99,5880
	1.Denek	3.Denek	99,5865
	2.Denek	3.Denek	99,6017

Farklı örnek kaydırmalar ile elde edilen sağlıklı EKG verileri kaotiklik anlamında çelişkili sonuçlar vermekte ve literatürde sağlıklı normal EKG verilerinin kaotik kabul edilemeyeceği sonucu hakimdir [43]. Fakat burada gördüğümüz gibi kaotik dizilerle yapılan şifreleme yöntemleri EKG verileri ile de kullanılabilmektedir.

Tablo 5.3 Farklı Kişilerden Alınan EKG Bilgilerinin Farklı Örnek Kaydırmalarının Piksel Değişim Oranına Etkisi

Sağlıklı Denek Bilgisi 1	Kaydırılan Örnek Sayısı	Sağlıklı Denek Bilgisi 2	Kaydırılan Örnek Sayısı	NPCR
1.Denek	10	2.Denek	1	99,6078
1.Denek	10	2.Denek	10	99,5987
1.Denek	10	2.Denek	17	99,5712

Ham EKG verileri ile yapılan şifrelemede elde edilen sonuçlar Tablo 5.3'te, EKG sinyallerinin filtrelendiğinde elde edilen sonuçlar ise Tablo 5.4'te verilmiştir. Filtrelenmiş EKG sinyalleri ile yapılan şifrelemelerde piksel Değişim oranının daha yüksek sonuçlar verdiği gözlemlenmiştir.

Tablo 5.4 Farklı Kişilerden Alınan Filtrelenmiş EKG Bilgilerinin Farklı Örnek Kaydırmalarının Piksel Değişim Oranına Etkisi

Sağlıklı Denek Bilgisi 1	Kaydırılan Örnek Sayısı	Sağlıklı Denek Bilgisi 2	Kaydırılan Örnek Sayısı	NPCR
1.Denek	10	2.Denek	1	99,6231
1.Denek	10	2.Denek	10	99,6063
1.Denek	10	2.Denek	17	99,5895

İkinci olarak yine farklı kişilerden alınan EKG verilerinin farklı kaydırma oranları ile yeni faz uzayları elde edilerek uygulanmıştır. Elde edilen sonuçlar Tablo 5.5'te verilmiştir. Faz uzayının farklı kaydırmalarla oluşturulmasının şifreleme güvenliği açısından bariz bir farklılık oluşturmadığı gözlemlenmiştir.

Tablo 5.5 Kişilerden Alınan EKG Bilgilerinin Farklı Örnek Kaydırmalarının Piksel Değişim Oranına Etkisi

Sağlıklı Denek Bilgisi	Kaydırılan Örnek Sayısı		NPCR
1.Denek	1	10	99,5773
	10	10	99,5514
	17	10	99,5422
2.Denek	1	10	99,5331
	10	10	99,5285
	17	10	99,5850

Aynı kişiden farklı zamanlarda alınan EKG verisi farklı örnek sayılarınca kaydırılarak farklı uzaylar elde edilmiş ve Piksel Değişim Oranı analizi bu örnekler için yapılmıştır. Farklı sinyalle elde edilen farklı uzaylar, Tablo 5.5'te görüldüğü gibi, tamamen farklı zaman serileri ürettiği için yine şifreleme güvenliği anlamında başarılı sonuçlar vermiştir. Bu sayede sağlıklı EKG verisinin literatürde periyodik olarak kabul edilmesine rağmen, aynı kişiden farklı zamanlarda alınan EKG verilerinin aynı anahtarı üretmediği gösterilmiştir. Sağlıklı insanlar dahi EKG sinyalleri ile sürekli olarak güvenli anahtarlar üretmektedir.

EKG sinyallerinin filtrelendiğinde elde edilen sonuçlar ise Tablo 5.6'da verilmiştir.

Tablo 5.6 Kişilerden Alınan Filtrelenmiş EKG Bilgilerinin Farklı Örnek Kaydırmalarının Piksel Değişim Oranına Etkisi

Sağlıklı Denek Bilgisi	Kaydırılan Örnek Sayısı		NPCR
1.Denek	1	10	99,6246
	10	10	99,6277
	17	10	99,6231
2.Denek	1	10	99,5331
	10	10	99,6231
	17	10	99,6124

5.2 EKG Bilgilerinin Farklı Örnek Kaydırmalarının Birleşik Ortalama Değişim Yoğunluğuna Etkisi

Tablo 5.7 Farklı Kişilerden Alınan EKG Bilgilerinin Birleşik Ortalama Yoğunluğuna Etkisi

Kaydırılan Örnek Sayısı	Sağlıklı Denek Bilgisi		UACI
1	1.Denek	2.Denek	33,9043
	1.Denek	3.Denek	33,4521
	2.Denek	3.Denek	33,4144
10	1.Denek	2.Denek	33,6864
	1.Denek	3.Denek	33,4053
	2.Denek	3.Denek	33,3632
17	1.Denek	2.Denek	33,6640
	1.Denek	3.Denek	33,3917
	2.Denek	3.Denek	33,4743

Şekil 5.4 ve Şekil 5.5'te elde edilen görüntüler Tablo 5.7'de Birleşik Ortalama Değişim Yoğunluğu açısından analiz edilmiştir. Birleşik Ortalama Değişim Yoğunluğu en fazla %33.9043 olarak elde edilmiştir. Bu da yine farklı kişilere ait EKG verilerinin anahtar olarak kaotik şifreleme yöntemlerine uygulanabilir olduğunu göstermektedir.

EKG sinyallerinin filtrelendiğinde elde edilen sonuçlar ise Tablo 5.8'de verilmiştir.

Tablo 5.8 Farklı Kişilerden Alınan Filtrelenmiş EKG Bilgilerinin Birleşik Ortalama Yoğunluğuna Etkisi

Kaydırılan Örnek Sayısı	Sağlıklı Denek Bilgisi		UACI
1	1.Denek	2.Denek	33,4999
	1.Denek	3.Denek	33,4520
	2.Denek	3.Denek	33,5592
10	1.Denek	2.Denek	33,3905
	1.Denek	3.Denek	33,4610
	2.Denek	3.Denek	33,4637
17	1.Denek	2.Denek	33,3792
	1.Denek	3.Denek	33,4532
	2.Denek	3.Denek	33,5665

Tablo 5.9 Farklı Kişilerden Alınan EKG Bilgilerinin Farklı Örnek Kaydırmalarının Birleşik Ortalama Yoğunluğuna Etkisi

Sağlıklı Denek Bilgisi 1	Kaydırılan Örnek Sayısı	Sağlıklı Denek Bilgisi 2	Kaydırılan Örnek Sayısı	UACI
1.Denek	10	2.Denek	1	33,4076
1.Denek	10	2.Denek	10	33,5312
1.Denek	10	2.Denek	17	33,6015

Birleşik Ortalama Yoğunluğu analizi, yine farklı kişilerden alınan EKG verilerinin farklı kaydırma oranları ile yeni faz uzayları elde edilerek uygulanmıştır. Elde edilen sonuçlar Tablo 5.9'da verilmiştir. Faz uzayının farklı kaydırmalarla oluşturulmasının şifreleme güvenliği açısından bariz bir farklılık oluşturmadığı gözlemlenmiştir.

EKG sinyallerinin filtrelendiğinde elde edilen sonuçlar ise Tablo 5.10'da verilmiştir.

Tablo 5.10 Farklı Kişilerden Alınan Filtrelenmiş EKG Bilgilerinin Farklı Örnek Kaydırmalarının Birleşik Ortalama Yoğunluğuna Etkisi

Sağlıklı Denek Bilgisi 1	Kaydırılan Örnek Sayısı	Sağlıklı Denek Bilgisi 2	Kaydırılan Örnek Sayısı	UACI
1.Denek	10	2.Denek	1	33,4933
1.Denek	10	2.Denek	10	33,4628
1.Denek	10	2.Denek	17	33,5881

Tablo 5.11 Kişilerden Alınan EKG Bilgilerinin Farklı Örnek Kaydırmalarının Birleşik Ortalama Yoğunluğuna Etkisi

Sağlıklı Denek Bilgisi	**Kaydırılan Örnek Sayısı**		**UACI**
1.Denek	1	10	33,2148
	10	10	33,2321
	17	10	33,1516
2.Denek	1	10	33,9405
	10	10	33,7338
	17	10	33,5854

Aynı kişiden farklı zamanlarda alınan EKG verisi farklı örnek sayılarınca kaydırılarak farklı uzaylar elde edilmiş ve Birleşik Ortalama Yoğunluğu analizi bu örnekler için yapılmıştır. Farklı sinyalle elde edilen farklı uzaylar, Tablo 5.11'de görüldüğü gibi, tamamen farklı zaman serileri ürettiği için yine şifreleme güvenliği anlamında başarılı sonuçlar vermiştir. Bu sayede sağlıklı EKG verisinin literatürde periyodik olarak kabul edilmesine rağmen, aynı kişiden farklı zamanlarda alınan EKG verilerinin aynı anahtarı üretmediği gösterilmiştir. Sağlıklı insanlar dahi EKG sinyalleri ile sürekli olarak güvenli anahtarlar üretmektedir.

EKG sinyallerinin filtrelendiğinde elde edilen sonuçlar ise Tablo 5.12'de verilmiştir.

Tablo 5.12 Kişilerden Alınan Filtrelenmiş EKG Bilgilerinin Farklı Örnek Kaydırmalarının Birleşik Ortalama Yoğunluğuna Etkisi

Sağlıklı Denek Bilgisi	**Kaydırılan Örnek Sayısı**		**UACI**
1.Denek	1	10	33,5080
	10	10	33,4162
	17	10	33,4896
2.Denek	1	10	33,5339
	10	10	33,4143
	17	10	33,3777

5.3 EKG Bilgillerinin Farklı Örnek Kaydırmalarının Şifreli Görüntünün Entropi Değerine Etkisi

Farklı kişilerden ve farklı kaydırılan örnek sayıları ile alınan EKG bilgilerinin anahtar olarak kullanıldığında elde edilen sonuçlar Tablo 5.13'de analiz edilmiştir. Bu değerlerin hepsinin ideal entropi değeri H(S)=8'e oldukça yakın olduğu, yani EKG sinyallerinin gerekli olan entropiyi sağladığı görülmektedir.

Tablo 5.13 Kişilerden Alınan EKG Bilgilerinin Farklı Örnek Kaydırmaları ile Şifreli Görüntünün Entropi Değerine Etkisi

Sağlıklı Denek Bilgisi	Kaydırılan Örnek Sayısı		
	1	10	17
1.Denek	7,9849	7,9856	7,9845
2.Denek	7,9841	7,9845	7,9831
3.Denek	7,9871	7,9869	7,9868

EKG sinyallerinin filtrelendiğinde elde edilen sonuçlar ise Tablo 5.14'de verilmiştir.

Tablo 5.14 Kişilerden Alınan Filtrelenmiş EKG Bilgilerinin Farklı Örnek Kaydırmaları ile Şifreli Görüntünün Entropi Değerine Etkisi

Sağlıklı Denek Bilgisi	Kaydırılan Örnek Sayısı		
	1	10	17
1.Denek	7,9895	7,9891	7,9899
2.Denek	7,9892	7,9896	7,9885
3.Denek	7,9895	7,9882	7,9893

6
SONUÇ VE ÖNERİLER

Bu bölümde ele alınacak simülasyon testleri için literatürde sıklıkla kullanılan Lena görüntüsü seçilerek kişilere ait farklı zamanlarda alınmış EKG sinyalleri ve farklı kişilere ait EKG sinyallerinin farklı sayıda örnek kaydırılmasıyla; EKG verilerinin görüntü şifrelemede doğrudan sayı dizisi olarak kullanılmasının uygun olup olmadığı incelenmiştir. Kullanılan algoritmanın güvenliğini değerlendirmek için bazı yaygın güvenlik analizleri kullanılmıştır.

Intel(R) Core(TM) i5-8265U 1.80 GHz CPU ile Windows 10 Home Single Language platformu ile donatılmış bir bilgisayar kullanılarak; tüm simülasyonlar Matlab R2022a yazılımı tarafından gerçekleştirilmiştir. Analizler önce kaotik olduğu bilinen original Lorenz sistemi üzerinde gerçekleştirilerek kaotik bir sistemde, güvenli olduğu bilinen bir yaklaşımla elde edilen değerler verilmiş, daha sonra da kaotikliği tartışmalı olan sağlıklı insan EKG verileri ile aynı analizler yapılarak, bu anahtarlarla elde edilen şifrelenmiş görüntülerin güvenliği hakkında çıkarım yapılmıştır. Simülasyonlar için Boston'daki Beth İsrail Hastanesi'ndeki Aritmi Laboratuvarı'na sevk edilen deneklerden sağlıklı 3'ünün uzun vadeli EKG kayıtları kullanılmıştır [42]. Kullanılan deneklerin baskın bir aritmileri ya da enfarktüs durumları yoktur. Elde edilen görüntülerin hassasiyetini sayısal olarak değerlendirmek için, (5.1) ve (5.2) ile tanımlanan Piksel Değişim Oranı Sayısı (NPCR) [49,50], Birleşik Ortalama Değişim Yoğunluğu (UACI) ve (5.3) ile tanımlanan entropi değerleri kullanılmıştır.

Yapılan analizler sonucunda elde edilen değerler referans makalede elde edilen değerlerle karşılaştırıldığında [35]; sağlıklı EKG verisinin literatürde periyodik olarak kabul edilmesine rağmen, aynı kişiden farklı zamanlarda alınan EKG verilerinin aynı anahtarı üretmediği gösterilmiştir. Sağlıklı insanlar EKG sinyalleri ile sürekli olarak güvenli anahtarlar üretmektedir.

KAYNAKÇA

[1] X. Q. Zhou, H. K. Huang, S. L. Lou, “Authenticity and integrity of digital mammography images,” IEEE Transactions on Medical Imaging, vol. 20, no. 8, pp. 784–791, 2001.

[2] S. K. Rajput, N. K. Nishchal, “Known-plaintext attack on encryption domain independent optical asymmetric cryptosystem,” Optics Communications, vol. 309, pp. 231–235, 2013.

[3] W. Liu, K. Sun, C. Zhu, “A fast image encryption algorithm based on chaotic map, ”Optics and Lasers in Engineering, vol. 84, pp. 26–36, 2016.

[4] Y. Wu, Y. Zhou, J. P. Noonan, S. Agaian, “Design of image cipher using latin squares,” Information Sciences, vol. 264, pp. 317–339, 2014.

[5] J.-X. Chen, Z.-L. Zhu, C. Fu, H. Yu, “An improved permutation-diffusion type image cipher with a chaotic orbit perturbing mechanism,” Optics Express, vol. 21, no. 23, pp. 27873–27890, 2013.

[6] G. Ye, X. Huang, L. Y. Zhang, Z. Wang, “A self-cited pixel summation based image encryption algorithm,” Chinese Physics B, vol. 26, no. 1, p. 010501, 2017.

[7] X.Huang, G. Ye, “An efficient self-adaptive model for chaotic image encryption algorithm,” Communications in Nonlinear Science and Numerical Simulation, vol. 19, no. 12, pp. 4094–4104, 2014.

[8] A. Kanso, M. Ghebleh, “A novel image encryption algorithm based on a 3D chaotic map,” Communications in Nonlinear Science and Numerical Simulation, vol. 17, no. 7, pp. 2943–2959, 2012.

[9] N. R. Zhou, T. X. Hua, L. H. Gong, D. J. Pei, Q. H. Liao, “Quantum image encryption based on generalized Arnold transform and double random-phase encoding,” Quantum Information Processing, vol. 14, no. 4, pp. 1193–1213, 2015.

[10] N. Zhou, S. Pan, S. Cheng, Z. Zhou, “Image compression encryption scheme based on hyper-chaotic system and 2D compressive sensing,” Optics & Laser Technology, vol. 82, pp. 121–133, 2016.

[11] R. Matthews, “On the derivation of a “chaotic” encryption algorithm,” Cryptologia, vol. 13, no. 1, pp. 29–42, 1989.

[12] G. Zhou, D. Zhang, Y. Liu, Y. Yuan, Q. Liu, “A novel image encryption algorithm based on chaos and Line map,” Neurocomputing, vol. 169, pp. 150–157, 2015.

[13] S. El Assad, M. Farajallah, “A new chaos-based image encryption system,” Signal Processing: Image Communication, vol. 41, pp. 144–157, 2016.

[14] S. Mohammad Seyedzadeh, S. Mirzakuchaki, “A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map,” Signal Processing, vol. 92, no. 5, pp. 1202–1215, 2012.

[15] X. Wang, D. Luan, “A novel image encryption algorithm using chaos and reversible cellular automata,” Communications in Nonlinear Science and Numerical Simulation, vol. 18, no. 11, pp. 3075–3085, 2013.

[16] I. Hussain, T. Shah, M. A. Gondal, “Application of S box and chaotic map for image encryption,” Mathematical and Computer Modelling, vol. 57, no. 9-10, pp. 2576–2579, 2013.

[17] S.-J. Xu, J.-Z. Wang, S.-X. Yang, “An improved image encryption algorithm based on chaotic maps,” Chinese Physics B, vol. 17, no. 11, pp. 4027–4032, 2008.

[18] B. Norouzi, S. M. Seyedzadeh, S. Mirzakuchaki, M. R. Mosavi, “A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos,” Multimedia Tools and Applications, vol. 74, no. 3, pp. 781–811, 2013.

[19] X. Chai, Y. Chen, L. Broyde, “A novel chaos-based image encryption algorithm using DNA sequence operations,” Optics Lasers in Engineering, vol. 88, pp. 197–213, 2017.

[20] R. Guesmi, M. A.B. Farah, A. Kachouri, M. Samet, “A novel chaos-based image encryption using DNA sequence operation and Secure hash algorithm SHA-2,” Nonlinear Dynamics, vol. 83, no. 3, pp. 1123–1136, 2016.

[21] Y. Liu, X. Tong, J. Ma, “Image encryption algorithm based on hyper-chaotic system and dynamic S-box,” Multimedia Tools and Applications, vol. 75, no. 13, pp. 7739–7759, 2016.

[22] Y. Zhang, “The image encryption algorithm with plain text related shuffling,” IETE Technical Review, vol. 33, no. 3, pp. 310–322, 2015.

[23] C. Fu, B. Lin, Y.Miao, X. Liu, J. Chen, “A novel chaos-based bit-level permutation scheme for digital image encryption,” Optics Communications, vol. 284, no. 23, pp. 5415–5423, 2011.

[24] A. Jolfaei, X.Wu, V. Muthukkumarasamy, “On the Security of Permutation-Only Image Encryption Schemes,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 2, pp. 235–246, 2016.

[25] H. Zhu, C. Zhao, X. Zhang, L. Yang, “An image encryption scheme using generalized Arnold map and affine cipher,” Optik - International Journal for Light and Electron Optics, vol. 125, no. 22, pp. 6672–6677, 2014.

[26] Y. Liu, L. Y. Zhang, J. Wang, Y. Zhang, K.-W. Wong, “Chosen-plaintext attack of an image encryption scheme based on modified permutation–diffusion structure,” Nonlinear Dynamics, vol. 84, no. 4, pp. 2241–2250, 2016.

[27] Y. Zhang, D. Xiao, W. Wen, M. Li, “Breaking an image encryption algorithm based on hyper-chaotic system with only one round diffusion process,” Nonlinear Dynamics, vol. 76, no. 3, pp. 1645–1650, 2014.

[28] C. Li, “Cracking a hierarchical chaotic image encryption algorithm based on permutation,” Signal Processing, vol. 118, pp. 203–210, 2016.

[29] R. Rhouma, S. Belghith, “Cryptanalysis of a new image encryption algorithm based on hyper-chaos,” Physics Letters A, vol. 372, no. 38, pp. 5973–5978, 2008.

[30] B. Nini, C. Lemmouchi, “Security analysis of a three dimensional rotation-based image encryption,” IET Image Processing, vol. 9, no. 8, pp. 680–689, 2015.

[31] F. Abundiz-P´erez, C. Cruz-Hern´andez, M. A. Murillo-Escobar, R. M. L´opez-Guti´errez, A. Arellano-Delgado, “A Fingerprint Image Encryption Scheme Based on Hyperchaotic Rossler Map,” Mathematical Problems in Engineering, vol. 2016, Article ID 2670494, 15 pages, 2016.

[32] M. A. Murillo-Escobar, L. Cardoza-Avenda˜no, R. M. L´opez- Guti´errez, C. Cruz-Hern´andez, “A Double Chaotic Layer Encryption Algorithm for Clinical Signals in Telemedicine,” Journal of Medical Systems, vol. 41, p. 59, 2017.

[33] U. Cavusoglu, S. Kac¸ar, I. Pehlivan, A. Zengin, “Secure image encryption algorithm design using a novel chaos based S-Box,” Chaos, Solitons & Fractals, vol. 95, pp. 92–101, 2017.

[34] M. Mollaeefar, A. Sharif, M. Nazari, “A novel encryption scheme for colored image based on high level chaotic maps,” Multimedia Tools and Applications, vol. 76, no. 1, pp. 607–629, 2017.

[35] Hossain, M. B., Rahman, M. T., Rahman, A. S., & Islam, S. (2014, May). A new approach of image encryption using 3D chaotic map to enhance security of multimedia component. In 2014 International Conference on Informatics, Electronics & Vision (ICIEV) (pp. 1-6). IEEE.

[36] Mathivanan, P., A. Balaji Ganesh, R. Venkatesan. "QR code–based ECG signal encryption/decryption algorithm." Cryptologia 43.3 (2019): 233-253.

[37] Algarni, Abeer D., et al. "Encryption of ECG signals for telemedicine applications." Multimedia Tools and Applications 80.7 (2021): 10679-10703.

[38] Sufi, Fahim, Ibrahim Khalil. "Enforcing secured ecg transmission for real time telemonitoring: A joint encoding, compression, encryption mechanism." Security and Communication Networks 1.5 (2008): 389-405.

[39] Wang, H., Bai, T., Pang, Y., Wang, W., Lin, J., Li, G., ... & Jiang, X. (2016, October). The dynamic encryption method based on ecg characteristic value. In International Conference in Communications, Signal Processing, and Systems (pp. 431-438). Springer, Singapore.

[40] Zheng, G., Fang, G., Shankaran, R., & Orgun, M. A. (2015). Encryption for implantable medical devices using modified one-time pads. IEEE Access, 3, 825-836.

[41] Huang, P., Li, B., Guo, L., Jin, Z., & Chen, Y. (2016, December). A robust and reusable ecg-based authentication and data encryption scheme for ehealth systems. In 2016 IEEE global communications conference (GLOBECOM) (pp. 1-6). IEEE.

[42] Goldberger, A., Amaral, L., Glass, L., Hausdorff, J., Ivanov, P. C., Mark, R., ... & Stanley, H. E. (2000). Physio Bank, Physio Toolkit, and PhysioNet: Components of a new research resource for complex physiologic signals. Circulation [Online]. 101 (23), pp. e215–e220.

[43] Kurtser, Polina, Ofer Levi, Vladimir Gontar. "Detection and classification of ECG chaotic components using ANN trained by specially simulated data." International Conference on Engineering Applications of Neural Networks. Springer, Berlin, Heidelberg, 2012.

[44] Gupta, V., Mittal, M., & Mittal, V. (2019). R-peak detection using chaos analysis in standard and real time ECG databases. IRBM, 40(6), 341-354.

[45] Gorshkov, O., & Ombao, H. (2021). Multi-Chaotic Analysis of Inter-Beat (RR) Intervals in Cardiac Signals for Discrimination between Normal and Pathological Classes. Entropy, 23(1), 112.

[46] Übeyli, E. D. (2009). Adaptive neuro-fuzzy inference system for classification of ECG signals using Lyapunov exponents. Computer methods and programs in biomedicine, 93(3), 313-321.

[47] Casaleggio, A., & Braiotta, S. (1997). Estimation of Lyapunov exponents of ECG time series—the influence of parameters. Chaos, Solitons & Fractals, 8(10), 1591-1599.

[48] Zheng, L., Wang, Z., & Tian, S. (2022). Comparative study on electrocardiogram encryption using elliptic curves cryptography and data encryption standard for applications in Internet of medical things. Concurrency and Computation: Practice and Experience, 34(9), e5776.

[49] G. Ye, H. Zhao, H. Chai, “Chaotic image encryption algorithm using wave-line permutation and block diffusion,” Nonlinear Dynamics, vol. 83, no. 4, pp. 2067–2077, 2016.

[50] M. Kumar, A. Iqbal, P. Kumar, “A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie-Hellman cryptography,” Signal Processing, vol. 125,pp. 187–202, 2016.

[51] S. Larptwee, W. San-Um, “Implementation of Rössler Chaotic System through Inherent Exponential Nonlinearity of a Diode with Two-Channel Chaotic.

[52] Niyojeet Shrirao, Alpana Pandey, Ramji Gupta. (2019). “A review: Analysis of fractional order chaotic systems “, International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE).

[53] Aleksei Tepljakov, Eduard Petlenkov, Emmanuel A. Gonzalez, Ivo Petras, “Design of a Matlab Design of a Matlab-Based Teaching tool in Introductory Fractional-order systems and controls”, The 47TH Annual Frontiers in Education (FIE) Conference, 2017.

[54] Leon 0.Chua, Chai Wah Wu, Anshan Huang, Guo-Qun Zhong,”A Universal Circuit for Studying and Generating Chaos-Part I: Routes to chaos.

[55] Choksi Hetal, Dr. M. G. Timol, “On the Formulation of Fractional Differential Equation from Differential Equation”, International Journal of Dynamics of Fluids. ISSN 0973-1784 Volume 13, Number 2 pp. 209-218, 2017.

[56] K M Ibrahim, K., R K Jamal, & F.H Ali, “Chaotic behaviour of the Rossler model and its analysis by using bifurcations of limit cycles and chaotic attractors.”, Journal of Physics: Conference Series. 1003. Institute of Physics Publishing, 2018.

[57] Alpana Pandey, R.K. Baghel, R. P. Singh, “Analysis and Circuit Realization of a New Autonomous Chaotic System, International Journal of Electronics and Communication Engineering ISSN 0974-2166 Volume 5, Number 4 pp. 487-495, 2012.

[58] Petráš, I. “A note on the fractional-order Chua's system.”, Chaos, Solitons and Fractals, 38(1), 140-147, 2008.

[59] Özer, A. B. ve Akın, E., (2005). “Tools for Detecting Chaos”, SAÜ Fen Bilimleri Enstitüsü Dergisi 9 (1):60-66.

[60] Wolf, A., Swift, J. B., Swinney, H. L. ve Vastano, J. A., (1985). "Determining Lyapunov Exponents from a Time Series", PhysicaD, 16: 285-317.

TEZDEN ÜRETİLMİŞ YAYINLAR

Konferans Bildirileri

1. R. Cenker, Z. G. Çam Taşkıran, “Yörünge Farklılıklarının Multimedya Güvenliğine Etkisi,” 8. Uluslararası Marmara Fen Bilimleri Kongresi 13-14 Mayıs, 2022, pp. 437-444.