
GAZİ ÜNİVERSİTESİ
Gazi
1926

# GÜVENLİ VERİ İLETİMİ İÇİN DEĞİŞTİRİLMİŞ CHUA DEVRESİ YARDIMIYLA TASARLANAN RENKLİ GÖRÜNTÜ ŞİFRELEME SİSTEMİ UYGULAMASI

**Batuhan ARPACI**

**YÜKSEK LİSANS TEZİ**
**BİLİŞİM SİSTEMLERİ ANABİLİM DALI**

**GAZİ ÜNİVERSİTESİ**
**BİLİŞİM ENSTİTÜSÜ**

**TEMMUZ 2019**

Batuhan ARPACI tarafından hazırlanan "GÜVENLİ VERİ İLETİMİ İÇİN DEĞİŞTİRİLMİŞ CHUA DEVRESİ YARDIMIYLA TASARLANAN RENKLİ GÖRÜNTÜ ŞİFRELEME SİSTEMİ UYGULAMASI" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Bilişim Sistemleri Anabilim Dalına YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

**Danışman:** Prof. Dr. Erol KURT

Teknoloji Fakültesi, Elektrik Elektronik Mühendisliği, Gazi Üniversitesi

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

**Başkan :** Dr. Ögr. Üyesi Javad RAHEBİ

Mühendislik Fakültesi, Elektrik Elektronik Mühendisliği, Türk Hava Kurumu Üniversitesi

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

**Üye :** Prof. Dr. Recep DEMİRCİ

Teknoloji Fakültesi, Bilgisayar Mühendisliği, Gazi Üniversitesi

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

Tez Savunma Tarihi: 05/07/2019

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

Doç. Dr. Aslıhan TÜFEKCİ

Bilişim Enstitüsü Müdürü

## ETİK BEYAN

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

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

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

# GÜVENLİ VERİ İLETİMİ İÇİN DEĞİŞTİRİLMİŞ CHUA DEVRESİ YARDIMIYLA TASARLANAN RENKLİ GÖRÜNTÜ ŞİFRELEME SİSTEMİ UYGULAMASI

(Yüksek Lisans Tezi)

Batuhan ARPACI

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Temmuz 2019

## ÖZET

Kaotik bir elektronik devre olan değiştirilmiş Chua devresi (DCD) kullanılarak, yeni bir şifreleme sistemi geliştirildi. Bu devrenin önemi, geniş parametre uzayı ve frekans bağımlı yapısıyla hiper kaotik özellik göstermesidir. Diğer yandan her şifreleme için tek sefer kullanılacak olan benzersiz gizli anahtar üretimi sağlandı. Üretilen gizli anahtardan kaotik üreteç DCD'nin başlangıç parametreleri çıkarıldı ve bu parametrelerle kaotik sistem çözdürülerek elde edilen rastgele sayılar şifreleme yapmak için dönüştürüldü. Daha sonra, tasarlanan şifreleme algoritmasında, görüntü şifrelemenin standart adımları olan karıştırma ve nüfuz etme fonksiyonları görüntüye uygulandı. Bunlardan karıştırma metodu, görüntüye bit düzeyinde uygulanarak piksel değerlerinin de değişmesi sağlandı. Şifreleme işleminin ardından sistemin performansını ölçmek için, gizli anahtar boyutu analizi, gizli anahtar ve açık resim hassasiyet analizi, histogram analizi, korelasyon analizi, diferansiyel analiz, bilgi entropisi analizi, gürültü ataklarına karşı direnç analizi ve hız analizi gibi bazı güvenlik testleri uygulandı. Elde edilen bulgular, tasarlanan sistemin görüntü şifrelemek için yeterli seviyede olduğunu göstermektedir.

Bilim Kodu : 92403

Anahtar Kelimeler : Değiştirilmiş Chua devresi, kaotik seriler, renkli görüntü şifreleme, bit düzeyinde karıştırma

Sayfa Adedi : 129

Tez Yöneticisi : Prof. Dr. Erol KURT

# COLOR IMAGE ENCRYPTION SYSTEM DESIGNED WITH THE MODIFIED CHUA CIRCUIT FOR SECURITY DATA TRANSMISSION

(M. Sc. Thesis)

Batuhan ARPACI

GAZİ ÜNİVERSİTESİ

INFORMATICS INSTITUTE

July 2019

## ABSTRACT

A new encryption system has been designed and implemental by using a Modified Chua's Circuit (MCC) which is an electronic chaotic circuit. The importance of this circuit is the hyper-chaotic property with its wide parameter space and frequency dependent structure. On the other hand, unique secret key generation is provided one time for each encryption. The initial parameters of the chaotic generator DCD have been extracted from the secret key generated and the random numbers obtained by solving the chaotic system with these parameters have been transformed to make the encryption. Then, in the designed encryption algorithm, mixing and penetration functions which are the standard steps of image encryption have been applied to the image. Mixing method have applied in bit-level to the image to change the pixel values. In order to measure the performance of the system after the encryption process, some security tests such as secret key size analysis, secret key and plain image sensitivity analysis, histogram analysis, correlation analysis, differential analysis, information entropy analysis, resistance to noise attacks analysis and speed analysis have been applied. The results show that the designed system is sufficient to image encryption.

Science Code : 92403

Key Words : Modified Chua Circuit, chaotic sequences, color image encryption, bit level scrambling

Page Number : 129

Supervisor : Prof. Dr. Erol KURT

# TEŞEKKÜR

Çalışmalarımda çok emeği olan, yönlendirmeleriyle beni destekleyen danışmanım Sayın Prof. Dr. Erol KURT' a sonsuz teşekkürlerimi sunarım. Tez çalışmam boyunca yardımlarını eksik etmeyen Kayhan ÇELİK' e teşekkürü bir borç bilirim. Hayatımın her anında bana destek olan aileme ve değerli eşim Fatma Pelin Arpacı' ya sevgi ve saygılarımı sunarım.

# İÇİNDEKİLER

**Sayfa**

**Sayfa**

**Sayfa**

# ÇİZELGELERİN LİSTESİ

**Çizelge** **Sayfa**

# ŞEKİLLERİN LİSTESİ

**Şekil** **Sayfa**

**Şekil** **Sayfa**

**Şekil** **Sayfa**

**Şekil** **Sayfa**

# RESİMLERİN LİSTESİ

**Resim** **Sayfa**

**Resim** **Sayfa**

# SİMGELER VE KISALTMALAR

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

| **Simgeler** | **Açıklama** |
|---|---|
| **K** | Renkli görüntünün kırmızı renk bileşeni |
| **Y** | Renkli görüntünün yeşil renk bileşeni |
| **M** | Renkli görüntünün mavi renk bileşeni |

| **Kısaltmalar** | **Açıklama** |
|---|---|
| **DCD** | Değiştirilmiş Chua Devresi |

# 1.GİRİŞ

Günümüz modern dünyasında, ağ ve bilgi teknolojilerinin büyük bir hızla gelişimi, iletişim alanındaki güvenlik ihtiyacını her geçen gün arttırmaktadır [1-4]. Özellikle endüstriyel projeler, askeri uygulamalar gibi iletişimin kritik öneme sahip olduğu alanlardaki güvenli iletişim büyük bir önem arz etmektedir. Gelişmiş Şifreleme Standardı (AES), Veri Şifreleme Standardı (DES) ya da Uluslararası Veri Şifreleme Algoritması (IDEA) gibi geleneksel yöntemlerin, çeşitli testler yardımıyla zayıflıkları tespit edilmiş ve artık şifreleme için yetersiz kaldığı ortaya konmuştur [4-6]. Dolayısıyla, bu alanda yeni şifreleme metotlarının denenmesi ve uygulanması önemli bir konu haline gelmiştir.

Teknolojinin her geçen gün gelişim kaydetmesi, teknolojiyi kullanım alışkanlıklarımızı ve ihtiyaçlarımızı değiştirmektedir. Özellikle, iletişim gereksinimlerimiz değişmekte, aslında iletişim için kullandığımız veri büyüklüğü artmaktadır. Teknolojinin hayatımızın her alanına girdiği şu dönemde, multimedya verileri gibi büyük verilerle yapılan iletişimin güvenli bir şekilde yapılabilmesi adına çeşitli şifreleme sistemleri ortaya konmuştur [7-9]. Özellikle, geleneksel metotların, büyük verilerle yapılan iletişim için yeterli güvenlik oluşturamaması, farklı disiplinlerin bu alana uygulanması için araştırmalara yol açmıştır [10-13]. Bu farklı disiplinler içerisinden kaos, şifrelemeye uygunluğu ile ön plana çıkmış ve birçok uygulama alanı geliştirilmiştir [14].

Kaotik sistemler, başlangıç koşullarına hassas bağlılığı ile öngörülemez özelliğe sahip ve içerisinde bir düzeni barındıran yapılardır. Bu yapı, kaotik sistemlerin şifreleme için bir altyapı sağlayabilmesine olanak verir [15-18]. Literatürde, şifreleme alanında birçok kez kaotik sistemlerden yararlanılmıştır. Birçok araştırmacı kaos tabanlı şifreleme sistemleri tasarlamış ve uygulamıştır. Bu sistemlerin en büyük artısı kaotik sistemlerden elde edilen rastgele sayıların şifreleme sistemi için kullanılmasıdır. Herhangi bir kaotik sistemden elde edilen sayı dizileri şifreleme için büyük avantaj sağlamaktadır. Aslında kaos tabanlı sistemlerin kullanılmasındaki ana amaç kaotik sistemden elde edilen bu sayıların birbirini tekrar etmemesi ve başlangıç durumlarına hassas bağlı olarak değişmesidir.

Kaosun şifreleme sistemlerindeki uygulama alanları arasında, görüntü şifreleme önemli bir yere sahiptir. Literatürde kaos tabanlı birçok görüntü şifreleme sistemi mevcuttur [19-20]. Kaos tabanlı resim şifreleme sistemlerindeki kaotik yapılar, genel olarak rastgele sayı üretici

olarak kullanılmaktadır. Üretilen rastgele sayılar ile resim şifreleme standartlarına uygun şekilde şifreleme yapılır. Aslında resim şifrelemenin iki önemli standardı vardır [21,22]. Bunlardan karıştırma yöntemi, görüntü piksellerinin yerleri değiştirilerek karıştırma işleminin yapılmasını amaçlar. Diğeri ise nüfuz etme yöntemidir ve bu yöntemle piksel değerlerinin değiştirilmesi sağlanır. Şifreleme işleminin etkili olabilmesi için bu hedeflerin gerçekleştirilmesi beklenir.

Ağ uygulamaları ve bilgi teknolojilerinin gelişmesi, ağ üzerinden gönderilen veri boyutunun artmasına yol açmaktadır. Renkli görüntü gibi büyük veri kapasiteli bilgilerin ağ üzerinden iletimi esnasında verinin güvenliğini sağlamak adına, geleneksel yöntemlerin kullanılamayacağının anlaşılması ile beraber, çeşitli kaos tabanlı şifreleme sistemleri ortaya konmuştur. Bu sistemlerin hem etkili bir şifreleme gerçekleştirmesini hem de şifreleme maliyetinin uygun düzeyde tutulmasını sağlamak temel alınmalıdır. Ayrıca literatürdeki bazı algoritmalar, renkli görüntünün kırmızı, yeşil ve mavi renk katmanlarını birbirinden bağımsız şifreleyerek çalışmaktadır [8,23]. Diğer taraftan, renkli bir görüntüyü bir bütün olarak ele alıp, renk bileşenlerini birbiri ile etkileşim içerisinde şifrelemek bileşenler arasındaki korelasyonun azalmasına ve daha etkili bir şifreleme yapılabilmesine olanak sağlar.

Genelde renkli resim şifreleme sistemleri piksel düzeyinde işlem yapacak şekilde tasarlanmıştır. Fakat son zamanlarda, bit düzeyinde birçok renkli resim şifreleme algoritması tasarlanmıştır [24,25]. Bit düzeyinde yapılan bir karıştırma işlemi piksellerin yerlerini değiştirdiği gibi, değerlerini de değiştirir. Bu sayede hem karıştırma hem de nüfuz etme standart süreçleri tek seferde uygulanır. Diğer yandan, bit düzeyinde şifreleme yapmak zaman maliyetini arttıracağından, mümkün olduğunca uygun bir algoritma tasarlanmalıdır. Böylelikle verimlilik sağlanmış olur.

Bu çalışmada kaos tabanlı yeni bir şifreleme algoritması sunulmuştur. Şifreleme ve şifre çözme işlemlerini gerçekleştirebilmek için, Kurt'un Değiştirilmiş Chua Devresinden (DCD) yararlanılır [26]. Devrenin çözümünden elde edilen rastgele sayılar şifreleme algoritmasında kullanılmak üzere dönüştürülür. Bu kaotik sistemin başlangıç parametreleri, gizli anahtara, belirli fonksiyonların uygulanması ile elde edilir. Bu fonksiyonların asıl işlevi, gizli anahtarda meydana gelen en ufak bir değişimi tüm başlangıç parametrelerine olabildiğince yansıtmaktır. Gizli anahtar ise SHA-256 [27,28] algoritması yardımıyla, açık resimden elde

edilir. Bu algoritma, şifrelenecek resimde meydana gelen ufak bir değişiklikte, oluşacak gizli anahtarın oldukça fazla değişmesini sağlamaktadır. Bu da bilinen açık metin saldırılarına ve seçilmiş açık metin saldırılarına karşı sistemi dirençli yapar. Diğer taraftan tasarlanan şifreleme algoritması bit düzeyinde şifreleme yaparak, şifreleme için temel basamak olan karıştırma ve nüfuz etme adımlarını birleştirir. Ayrıca bu algoritmada renkli resmin K,Y ve M renk bileşenlerinin birbiriyle bağlantılı şekilde şifrelenmesiyle korelasyonun azaltılması amaçlanmıştır.

Hazırlanan bu tez kapsamında, literatürde bulunan resim şifreleme algoritmalarının eksik yönleri tespit edilerek, bunlara çözüm getirebilecek bir algoritma tasarlanması amaçlanmıştır. Tasarlanan sisteme birçok test uygulanarak, sistemin etkinliği ölçülmüş, deneysel uygulamalar ile sistemin verimliliği desteklenmeye çalışılmıştır. Ayrıca hızlı ve bütünleşik bir geliştirme ortamı sağlamak, farklı algoritmaların testlerini ve karşılaştırmalarını yapabilmek, deneysel sonuçları etkili bir biçimde gözlemleyebilmek ve herhangi bir rastgele sayı üretecinin hızlı bir şekilde şifreleme sistemine entegre çalışabilmesini sağlayabilmek adına bir yazılım hazırlanmış ve kompakt bir sistem kurulmuştur. Bu yazılım ile ayrıca, ilerde bu konu üzerine çalışma yapacak araştırmacıların hızlı geri dönüşler alması amaçlanmıştır. Bütün bu çalışmalarla, etkili ve verimli bir kaos tabanlı renkli resim şifreleme sistemi oluşturulmuştur.

# 2. LİTERATÜR TARAMASI

## 2.1. Kaos Kavramı

Zamana göre öngörülemeyen şekilde evrilen ve başlangıç durumuna hassas bağlılık gösteren sistemlere "kaotik sistemler" denir. Bu tür sistemlerin göstermiş olduğu davranışa da kaos denir. Her bilim alanında öngörülemez dinamik süreçler bulunur. Sözgelimi, dengeden uzak bulunan kimyevi süreçlerden, çok cisim problemi içeren astrofizik konularına ve atom molekül fiziği ile güç elektroniği konularına kadar pek çok alanda kaos görülebilmektedir. Bu sebeptendir ki; kaos bir alanın değil, aslında bir sürecin bilim dalıdır. Gündelik hayatta rastladığımız insan ve hayvan hareketlerinden atmosferik türbülans hareketlerine kadar evrende gördüğümüz bu öngörülemez sistemler kaosun inceleme odağını oluşturur.

Kaosun bilimsel incelemesi deterministik kaos sergileyen sistemlerde yapılır. Yani sistemin kaosa götüren parametreleri ve etkileşim formülasyonları bilinmelidir. Kaos'u, başlangıç koşullarına hassas bağlı, gürültü benzeri davranış sergileyen ve geniş güç spektrumları içeren düzensizliğin düzeni olarak tanımlayabiliriz.

Henri Poincare 1900'lü yılların başında "kaos" terimini ilk kullanan kişidir [29]. Poincare, Güneş sisteminin hareketini açıklayan denklem sisteminin çözümünün, sistemin başlangıç koşullarına hassas bağımlı olduğunu, ancak başlangıç koşullarının asla doğru olarak saptanamayacağını belirtmiştir. Dolayısıyla güneş sisteminin kararlı olup olmadığının belirlenemeyeceğini göstermiştir. Bu bilinmezlik, tahmin edilemezliği de "kaos" olarak tasvir etmiştir.

## 2.2. Kaotik Sistemler

Kaotik sistemler matematik, eğitim bilimleri, sosyal bilimler, astronomi, mühendislik gibi birçok farklı alanda karşımıza çıkmaktadır. Bu sistemlerin önemli özelliklerinden biri, ürettikleri çözümün düzensiz davranış göstermesi ve aperiyodik (periyodik-olmayan) olmasıdır [30-32]. Bu sistemlerin bir diğer önemli özelliği ise sistemin çözümünün başlangıç koşullarına hassas bağlı olmasıdır. Dolayısıyla başlangıç koşullarında meydana gelebilecek ufak bir değişiklik, sistemin çözümünün çok farklı şekilde sonuçlanmasına sebep olabilir.

Dinamik sistemi, bir sistemde zamanla meydana gelen gelişmenin matematiksel olarak ifade edilmesi şeklinde açıklayabiliriz. Dinamik sistemler için sistem çözümü sabit nokta yöntemi vb. yöntemler ile yapılabilir. Fakat kaotik bir sistem için, bunun aksine analitik bir çözümden bahsedemeyiz ve çözüm kapalı çevrimlere oturmayacaktır. Fakat bu kaotik süreçlerin kontrolünü sağlayabilmek adına, eldeki verinin bir şekilde analiz edilmesi gerekmektedir. Bu verilere Fourier analizi, olasılık dağılımları gibi doğrusal yaklaşımlı çeşitli çözümler uygulanabilir. Fakat bu çözümler, verilerin elde edildiği sistemlerin doğrusal olmamasından kaynaklı olarak tatmin edici olmaz. Bu nedenle doğrusal olmayan zaman dizilerini analiz etmek amacıyla farklı arayışlar ortaya çıkmıştır. Kaos hakkında bilimsel olarak yapılan ilk araştırma, Lorenz' in 1963 yılında sıvılardaki türbülansla alakalı bir çalışmasıdır. Lorenz' in araştırmasındaki denklem çözümü, doğrusal olmayan durumlar içermekteydi. 1970' li yıllardan itibaren kaosun analizinde farklı çalışmalar da ortaya konmuş, Ruelle ve Takens 1971 yılında sıvılardaki türbülansı açıklarken garip çekici kavramını ortaya atmıştır [33].

Kaosun doğasındaki oluşan düzen tartışması ise Greick ile başlamıştır. Wolf, Lyapunov üstellerden hareketle, bu tür kaotik sistemlerin başlangıç bilgisinin üstel bir hızla değiştiğini ve tahmin edilebilirliğinin ortadan kaybolduğunu ortaya koymuştur [33]. Kaotik çözümü olan belirli başlangıç koşullarına çok yakın bir diğer farklı grup için yapılan kaotik çözüm birbirlerinden çok uzakta değer alabilir. Yani çözüm bir diğerinden üstel olarak farklı zamanlarda uzaklaşır. Bu uzaklaşmanın ölçüsü de Lyapunov üsteli olarak adlandırılır. Analitik çözümlerdeki gibi süreklilik sağlanamaz.

Sistemin kaotik davranış sergilemesini sağlayan belirli başlangıç bilgileri, o sistemin en önemli dinamikleridir. Bir başlangıç parametresi belirli bir aralıkta seçildiğinde, sistem kaotik özellik gösteriyorsa, o parametre literatürde çatallanma parametresi olarak adlandırılır [34]. Belirlenen aralıkta, bu tür parametrelerin değerindeki ufak bir değişiklik, çözümde büyük farklılıklara neden olur.

Kaotik sistemlerin bazıları, sürekli zamanlı diferansiyel denklemlerle bazıları ayrık zamanlı fark denklemleri ile gösterilebilir. Denklemlerle ifade edilebilen bu tür kaotik sistemler literatürde deterministik kaos olarak bilinir. Kaotik sistemlerin matematiksel modelleri, yapısı gereği doğrusal özellik göstermez. Bu sistemlerin matematiksel bir model olarak ifade edilebilmesi determinizm kavramını ortaya koyarken, uzun dönemdeki davranışının tahmin edilemez oluşu, bu sistemleri doğrusal olmayan sistemler altında ele alınan birçok modelden

farklı kılmaktadır. Kaotik bir sistemin modellemesi basit olmasına rağmen, davranışı çok karmaşık görünmektedir.

Kaotik sistemin, diğer bir değişle, tahmin edilemeyen davranışlar sergileyen doğrusal olmayan sistemin bazı belirleyici özellikleri vardır [35]. Bu özellikler temel olarak:

- Sistemin analitik bir çözümünün olmaması,
- Herhangi bir başlangıç koşulunun belirlenememesi (belirsizlik ilkesi),
- Başlangıç parametrelerine yüksek duyarlılık,
- Rastgele değil deterministik olması,
- Gürültü benzeri güç spektrumlarına sahip olmasıdır.

Edward Lorenz adlı meteorolojist, meteorolojik değişimlerin başlangıç koşullarına hassas bağlılığını tespit etti. Lorenz havadaki ısı değişimlerini gösterebilmek için, aşağıdaki denklemin sayısal çözümünü arıyordu.

$$\begin{aligned} \frac{dx}{dt} &= -ax + ay \\ \frac{dy}{dt} &= bx - y - zx \\ \frac{dz}{dt} &= -cx + xy \end{aligned} \tag{2.1}$$

Denklemi, tekrarlama yöntemiyle çözmeye çalışan Lorenz, zaman değişkeni değiştikçe $(x, y, z)$ noktasının üç boyutlu uzayda çizdiği yörüngenin değiştiğini ve ortaya çıkan grafiğin iki nokta civarında yoğunlaştığını gösterdi. Bu yığılma noktalarına Lorenz Çekerleri ya da Garip Çekerler denir [36].

Lorenz'in bu buluşundan sonra, kaosa olan ilgi artmaya başladı ve kaos örnekleri çoğaldı. Türbülans ve kaos, lojistik haritada kaos, doğrusal olmayan salınıcılar, fraktallar gibi çeşitli kaos örnekleri bulundu. Son zamanlarda Mandelbrot ve Winfree tarafından dikkate değer birtakım çalışmalar yapıldı. Mandelbrot, bilgisayar ortamında yeni bir geometrik anlayışla grafikler elde etmeyi başardı. Matematiksel biyolojinin bulunmasıyla birlikte Winfree kalp atışları gibi biyolojik ritimleri inceledi. Günümüzde, bir sürecin bilimi olan kaos teorisi çok farklı alanlara çözüm getirmektedir [32, 37].

Literatürde kaotik sistemlerin analizi, birçok farklı şekilde yapılabilmektedir. Bunlardan bazıları, Poincare Haritalama, Güç Spektrumları, Fraktan Boyut Analizi ve Lyapunov Üstelleridir [33]. Bu ölçütler sayesinde sistemin, hangi başlangıç parametrelerinin hangi aralıkta değişmesiyle kaosa sürüklendiği tespit edilebilir.

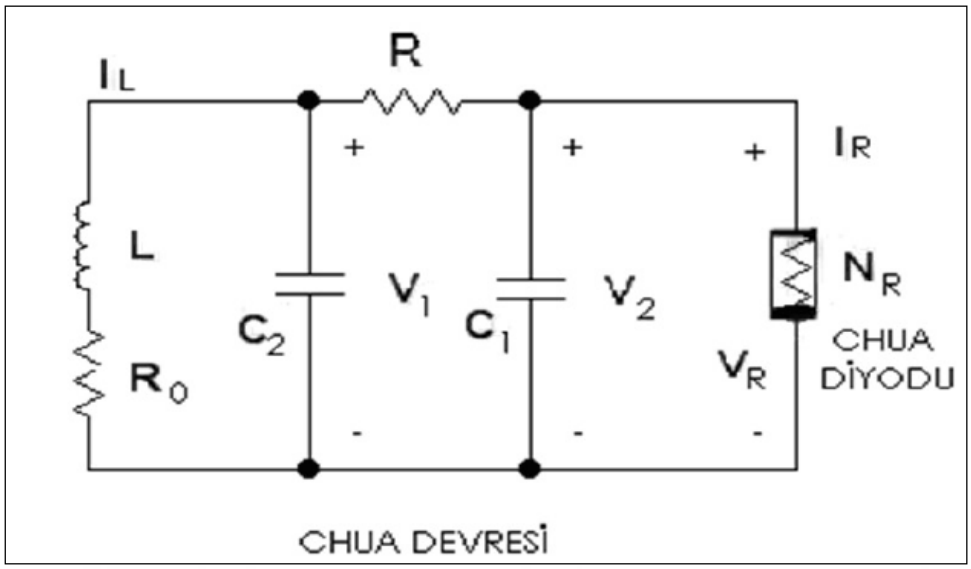
### 2.3. Kaotik Elektronik Devreler

Paul Linsay tarafından 1981' de "Harmoniksiz sürülen bir salınıcıdaki periyot katlanımı ve kaotik davranış" adlı makalesinden sonra elektronik devrelerde de kaotik sinyallerin oluşabileceği ortaya çıktı. O günden itibaren yapılan çalışmalar elektronik kaosun birtakım gerçeklerini ortaya çıkardı. Bu gerçekler:

- Devre kurulumlarının birçoğu basittir.
- Bilgisayar benzetimi ve benzer yöntemlerle gözlenen veriler doğrulanabilir ve kontrol edilmesi kolaydır.

Literatürdeki çalışmalar, deterministik bir devrenin gürültü üretebileceğini göstermiştir. Bu durumun sağlanabilmesi devrenin başlangıç koşullarına bağlıdır. Aslında, kaotik elektronik devreler, periyodik olmayan salınımlar üreten devreleri ele alır. Chua devre ailesi de bu kaotik özellik gösteren sistemlere örnek olarak gösterilebilir [32].

1983 yılında Chua, kendi adı ile anılan ve kaotik dinamikler sergileyen bir osilatör devresi üretmiştir. Bu devre, birçok dinamik davranışı barındıran üçüncü dereceden basit bir otonom devreden meydana gelmektedir. Şekil 2.1' de Chua devresi örneği gösterilmektedir.




Şekil 2.1. Chua Devresi

Chua devresi, en kompleks kaosun varlığının, sayısal verilerle doğrulanabildiği, matematiksel açıdan kanıtlanabildiği, deneylerle gerçek zamanlı olarak kurulabildiği en basit devrelerden biridir. Bu devre kapasitör, indüktör gibi enerji depolayan elemanlardan, lineer dirençten ve Chua diyodu olarak bilinen lineer olmayan bir dirençten meydana gelmektedir. Chua devresinin durum denklemleri aşağıdaki gibidir [38]:

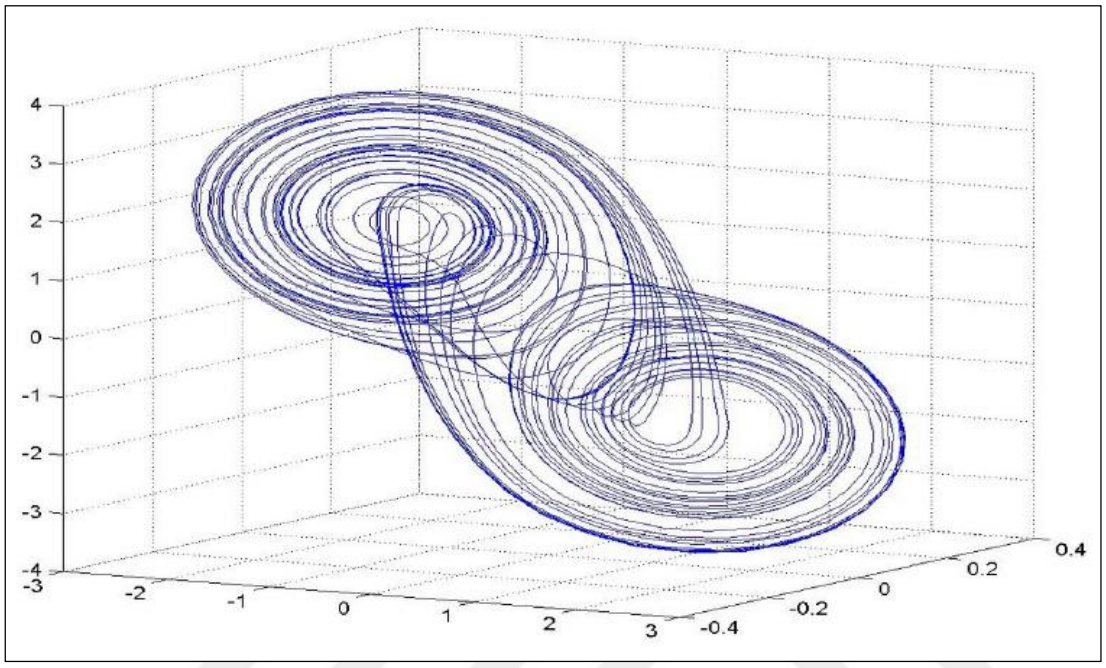
$$\begin{aligned} \dot{v}_1 &= \frac{g}{c_1}(v_2 - v_1) - \frac{1}{c_1} g(v_1) \\ \dot{v}_2 &= -\frac{g}{c_2}(v_2 - v_1) + \frac{1}{c_2} i_L \\ \dot{i}_L &= -\frac{R_C}{L} i_L - \frac{1}{L} v_2 \end{aligned} \tag{2.2}$$

Eş. 2.2' de $g(v_1)$ olarak tanımlanan, nonlineer direnç $N_R$ 'nin bölüm bölüm doğrusal karakteristiğini temsil eder.

$N_R$'nin iç bölgede $G_a$ ve dış bölgede $G_b$ eğimli $V - I$ karakteristiği vardır. Bu karakteristik değerlerin analitik hesabı aşağıda verilen Eş. 2.3 ile yapılır.

$$g(v_1) = \begin{cases} G_b V_R + (G_b - G_a) B_P & ; V_R < -B_P \\ G_a V_R & ; -B_P < V_R < B_P \\ G_b V_R + (G_a - G_b) B_P & ; V_R > B_P \end{cases} \tag{2.3}$$

Sistemin kaotik özellik gösterdiği parametre değerleri sırasıyla $B_p = 1.56$, $G_a = -8/7$ ve $G_b = -5/7$' dir. Verilen bu başlangıç parametre değerlerine ait olan kaotik Chua çekicisi Şekil 2.2' de gösterilmiştir.




Şekil 2.2. Chua Kaotik Çekicisi

Yukarıda tanıtılan Chua diyotlu Chua devresinin yanı sıra çift kıvrım ve katlı torus Chua devresi, Sürülen RL-diyot devresi gibi farklı devre tipleri de mevcuttur [32].

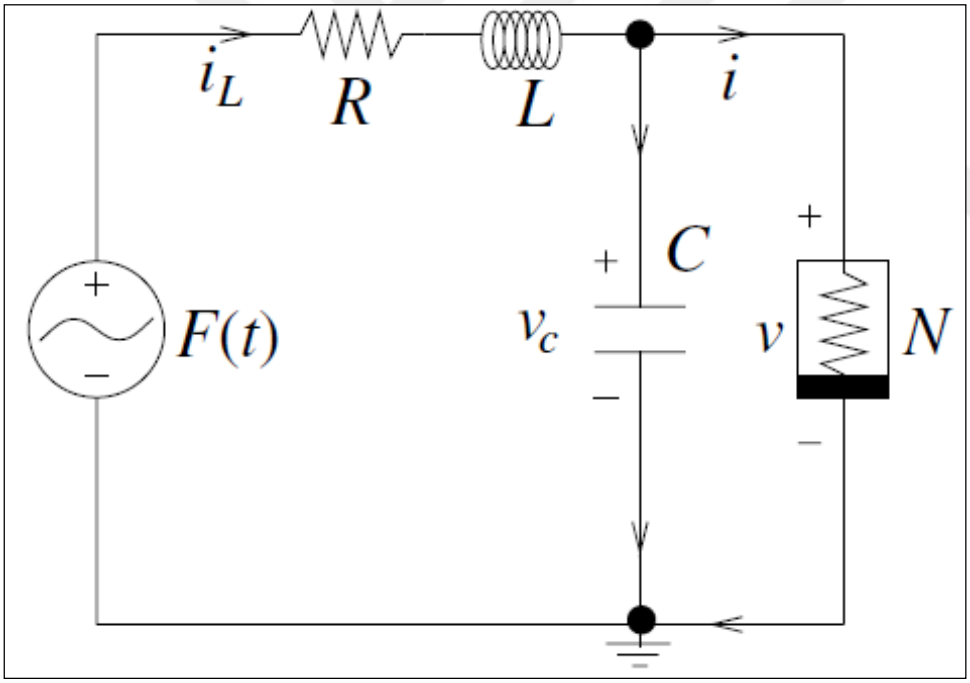
Bu çalışmada [Kurt, 2006] tarafından üretilen zamana bağlı Chua diyotlu değiştirilmiş Chua devresi ele alınacaktır. Bu devrenin analitik çözümleri ve simülasyonlarına ilerleyen bölümlerde yer verilmiştir.

## 2.4. Değiştirilmiş Chua Devresi

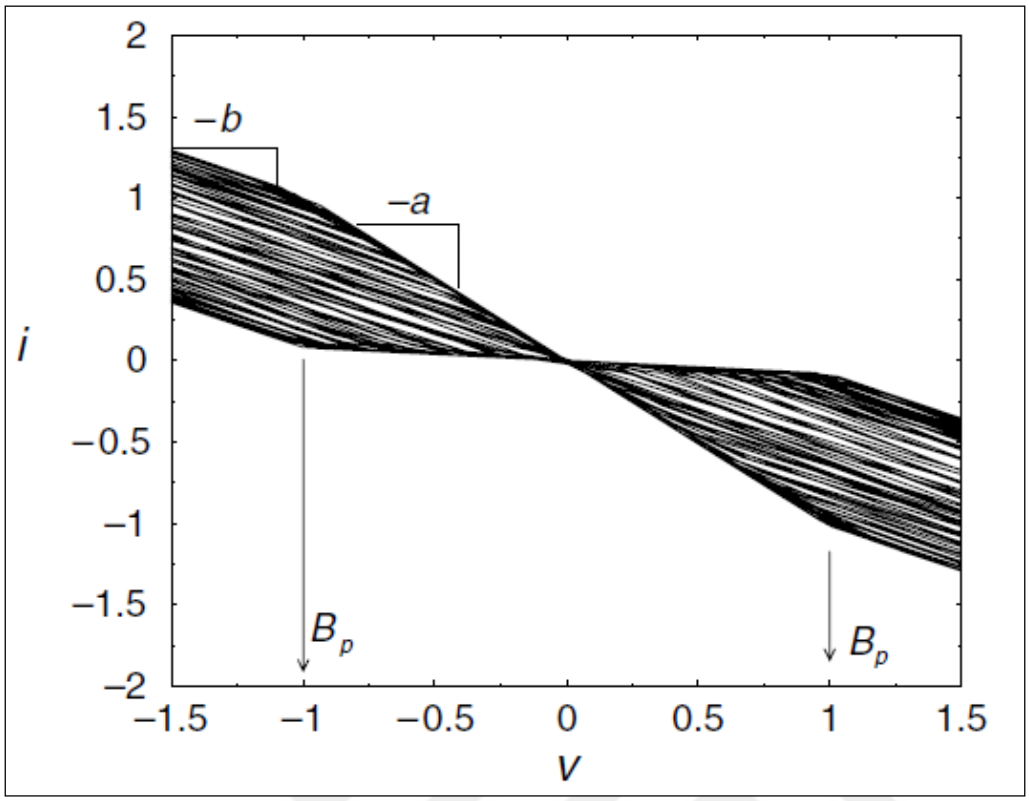
Elektronik devreler, belirli şartlar altında kaotik özellik gösterebilirler. Kaos tabanlı uygulamalar gerçekleştirilmek istendiğinde, elektronik bir devreden yararlanmak elverişli olabilir. Çünkü, hem devre kurulumunun basit olması hem de çözümlerin bilgisayar benzetimleriyle kolayca gözlemlenip kontrol edilebilmesi, elektronik devreleri kaos üretmek için cazip hale getirmektedir. Bu kaotik devreler arasından Chua elektronik devre ailesi, gerçek zamanlı sistem oluşturmak için oldukça elverişli ve basittir.

1980'li yılların başında Leon O. Chua tarafından literatüre kazandırılan Chua devreleri, farklı değişiklerle irdelenmektedir. Kaos üreten Chua devreleri arasından, E. Kurt tarafından üretilen "Değiştirilmiş Kaotik Chua Devresi", bilgisayar benzetiminin kolaylıkla yapılabilmesi, gerçek zamanlı olarak uygulanabilirliği, geniş ölçekli parametre uzayı ve özellikle frekansa bağlı olarak farklı rejimler üretebilmesi sebebiyle bu çalışmanın ilerleyen bölümlerinde kaos üretmek için kullanılmıştır.

Devre şeması Şekil 2.3' de gösterilen Chua devresinde $N$ diyotu zamana bağlı belli bir frekansta titreşir. Bu durum Şekil 2.4' de gösterilmiştir. Belirli alt ve üst limitler çerçevesinde belirli gerilimler için elde edilen akım değerleri çok farklı değerler almakta, bu durum devrenin farklı karmaşık çekiciler oluşturabilmesine sebep olmaktadır. Özellikle devrenin gerilim ve akımı o devre dinamiğinin önemli bir parçasıdır.




Şekil 2.3. Zamana bağlı Chua Diyotlu Chua Devresi.




Şekil 2.4. Zamana bağlı Chua diyotu.

Devre aşağıdaki şekilde tanımlanmıştır:

$$C\frac{dV_C}{dt} = I_L - g(V_C)$$
$$L\frac{dI_L}{dt} = -RI_L - V_C + F\sin(\Omega t) \tag{2.4}$$

Bu devreye Kirchoff kanunları uygulanarak, indüktör *L* boyunca, kapasitör *C* ve akım $i_L$ 'ye karşı voltaj *v* için dinamik eşitlikler 1. dereceden 2 tane otonom olmayan diferansiyel denklem şeklinde yazılmıştır. Burada *F* genlik, $\Omega$ ' de harici voltajın açısal frekansıdır. Burada en önemli terim olan $g(V_C)$ devredeki lineer olmayan akımı yani (Bkz. Şekil 2.3)' deki *N*' yi ifade eder.

$$g(V_C) = G_b V_C + \frac{1}{2}(G_a - G_b)(|V_C + B_P(t)| - |V_C + B_P(t)|) \tag{2.5}$$

Burada $B_P(t)$ , 3. Denklemde verilen standart Chua diyotunun değiştirilmiş halidir. Standart Chua diyotu zaman bağımsız iken, bu değiştirilmiş Chua diyotu zaman bağımlı bir terime $B_P(t) = B_P \sin(\Phi t)$ sahiptir

Eş. 2.4 ve Eş. 2.5 denklemlerinin boyutsuz ifadelerini elde etmek için, aşağıdaki yeni sayılar tanımlanır:

$$\begin{aligned} &v_C = xB_P, \quad \mathrm{i_L} = yGB_P, \quad \mathrm{G} = \frac{1}{\mathrm{R}}, \\ &\omega = \frac{\Omega C}{G}, \quad \phi = \frac{\Phi C}{G}, \quad \mathrm{t} = \frac{rC}{G}. \end{aligned} \tag{2.6}$$

Zaman birimi *t* olarak yeniden tanımlandığında, aşağıdaki boyutsuz formlar Eş. 2.4 ve Eş. 2.6 kullanılarak elde edilir

$$\begin{aligned} \dot{x} &= y - bx - \frac{1}{2}(a-b)\left[|x+\sin(\phi t)| - |x-\sin(\phi t)|\right] \\ \dot{y} &= -\beta(y+x) + f\sin(\omega t) \end{aligned} \tag{2.7}$$

Burada $\beta = C/LG^2$, $f = F\beta/B_P$, $a = G_a/G$ ve $b = G_b/G$ eşitlikleri vardır. Voltaj ve akım sırasıyla *x* ve *y* ile ifade edilir.

Chua diyotunu içeren doğrusal olmayan devreler üzerine daha önce yapılan çalışmalara göre, sürüş genliği *f*'nin çatallanma parametresi olarak kullanılabileceği tespit edilmiştir [26]. Sürüş genliği 0'dan yukarı doğru arttırıldığında, devre çatallanma ve kaos dinamikleri sergiler. Bu durumda denklem dinamikleri $a$, $b$, $\phi$, $\beta$, $\omega$ ve $f$ parametrelerine sıkı sıkıya bağlıdır. İlerleyen bölümlerde farklı parametre değerleri için devrenin kaotik çekicileri gösterilmektedir.

Literatürde, dinamik bir sistemin faz uzayının karmaşıklığını tanımlayabilmek için, yani kaosu tespit edebilmek için kaotik çekicilerin yanı sıra, Lyapunov üstellerini kullanmak da etkili yöntemlerden birisidir. Aslında kaotik çekiciler tek başına kaosu tanıtmak için yeterli olmaz. Kaotik çekiciler çözümün rastgele gürültü olmadığını belirli deterministik özellikler gösterdiğini ifade etmek için kullanılır. Lyapunov üstelleri [33,39] ise, birbirine yeterli seviyede yakın iki başlangıç noktasının, faz uzayı içinde zamanla birbirinden ortalama bir

üstelle uzaklaşıp, yakınlaşmaları yani karmaşık bir yapının olup olmadığını işaret eder. Faz uzayının boyutuna göre her bir boyut için Lyapunov üsteli aşağıdaki gibi hesaplanır [33]:

$$d(t) = d_0 e^{\lambda t}, \tag{2.8}$$

$$\lambda = \frac{1}{t_N - t_0} \sum_{k=1}^{N} \log_2 \frac{d(t_k)}{d(t_{k-1})}. \tag{2.9}$$

Burada, iki başlangıç şartı arasındaki mesafe $d_0$ olmak üzere, daha sonraki bir zaman dilimindeki mesafe Eş. 2.8'deki gibi gösterilir. Faz uzayındaki *n* tane boyut için Lyapunov üsteli, $\lambda_1, \lambda_2, ..., \lambda_n$ olacak şekilde $\lambda_1$ en büyük üstel olmak üzere, Lyapunov üstel spektrumu $\lambda_1 > \lambda_2, ...,$ şeklinde yazılır. Kaotik bir sistemin varlığından söz edebilmek için en az bir pozitif Lyapunov üsteline ihtiyaç vardır. Yani, herhangi bir sistem için $\lambda_1 > 0$ sistemin kaotik olduğunu işaret eder. Aksine $\lambda_1 < 0$ olduğu durumda sistem düzenli davranış gösterir. Bu negatif üstel, sistemin düzenli periyodik hareket sergilediğini gösterir.

Lyapunov üstelleri, dinamik bir sistemin çekicilerinin tiplerini sınıflandırmaya yardımcı olur [33]. Üç boyutlu bir faz uzayı ele alındığında, $(\lambda_1, \lambda_2, \lambda_3)$ Lyapunov üstelleri olacak şekilde; $(-,-,-), (0,-,-), (0,0,-), (+,0,-)$ şeklinde farklı Lyapunov spektrumları ile karşılaşılabilir. '+' üstel, çekicinin kaotik olduğunu, '0' üstel, hareket boyunca üstelden daha yavaş bir değişim olduğunu ve '-' üstel de uzayın bir çekicisinin var olduğunu gösterir. Bu şekilde ilerleyerek, daha büyük boyutlarda Lyapunov spektrumlarının üstelleri yazılabilir.

Lyapunov yöntemi dışında, dinamik bir sistemin kaotik özellik sergilediğini göstermek için, Poincare haritalama, güç spektrumları, fraktal boyut analizi gibi yöntemler literatürde gösterilmiştir [33].

Farklı alanlarda kaotik özellik gösteren sistemlerin analizleri sonucunda elde edilen verilerin, farklı uygulamalarda değerlendirilmesi ile kaosun farklı disiplinlere uygulanması sağlanmıştır. Doğası gereği kaos, araştırmacıların oldukça ilgisini çekmekte ve literatürde oldukça yaygın şekilde kullanılmaya devam etmektedir.

## 2.5. Güvenli İletişim

Günümüz internet ve ağ teknolojisi artan bir ivme ile günden güne gelişme kaydetmektedir. İnsanların iletişim ihtiyaçları da buna bağlı olarak değişmekte ve gelişmektedir. Teknolojinin yaygın bir şekilde kullanılmasıyla, bilginin bütünlüğü, erişilebilirliği, korunması gibi bilgi transferi açısından önemli konular ön plana çıkmaktadır. Kriptoloji, literatürde bilgi güvenliğini sağlamak adına kullanılan yaygın bir çalışma disiplinidir [40-42]. Kriptolojinin ana işlevi gereği, gönderici tarafından bilginin anlaşılabilirliği yok edilir ve sadece alıcı tarafında bu bilginin elde edilmesi sağlanır.

Kriptoloji bir şifreleme sanatıdır. Önemli bilgiler, güvenli olmayan kanallardan gönderilirken genellikle bu bilgiyi korumak için şifreleme kullanılır. Verinin güvenli bir ortamda şifrelenerek, güvenli olmayan kanal boyunca şifreli olarak aktarılması ve ardından alıcı tarafında sağlıklı bir şekilde çözülebilmesi kriptolojinin ana amacıdır.

Şifreleme sistemleri açık anahtarlı ve gizli anahtarlı olmak üzere ikiye ayrılır. Açık anahtarlı sistemlerde biri açık diğeri gizli olmak üzere iki çeşit anahtar kullanılır. Açık anahtara herkes erişebilirken, gizli anahtar sadece kişiye özeldir. Açık anahtar kullanılarak şifreli mesaj gönderilebilir ve alıcı gizli anahtar yardımıyla bu mesajı çözer. Literatürde RSA (Rivest-Shamir-Adleman), El Gamal gibi açık anahtarlı şifreleme sistemleri geliştirilmiştir [43]. Gizli anahtarlı şifrelemede ise tek bir gizli anahtar bulunur. Bu anahtar hem açık mesajı şifreler hem de şifrelenmiş bu mesajı çözer. Bu çeşit bir şifrelemede anahtarın gizliliği çok önemlidir. AES (Advanced Encryption Standart), DES (Data Encryption Standart), IDEA (International Data Encryption Algorithm) vb. birçok şifreleme sistemi gizli anahtarlı şifreleme yöntemlerine örnek verilebilir [43-45]. Açık anahtarlı şifreleme yöntemi genellikle dijital imza uygulamalarında kullanılırken, gizli anahtarlı şifreleme resim şifreleme, video şifreleme vb. birçok alanda uygulanabilir. Gizli anahtarlı şifreleme de önemli olan anahtarın güvenilirliğidir.

Ağ üzerinden gerçekleştirilen bilgi alışverişinin boyutu her geçen gün üzerine koymaktadır. Bu kapasite artışını takiben gönderilen verinin güvenliğinin de sağlanması önemli bir durum haline gelmektedir. Özellikle multimedya verilerin ağ üzerinden iletiminin yaygınlaşmasıyla ve AES, DES gibi geleneksel şifreleme sistemlerinin bu verilerin bütünlüğünün ve

gizliliğinin sağlanmasında yetersiz kaldığı tespit edildiği için yeni şifreleme mekanizmaları geliştirilmektedir.

Diğer multimedya verilerine nispeten görüntü bilgisi, iletişimde daha yaygın olarak kullanılan bir veri çeşididir. Dolayısıyla literatürde, görüntünün gizliliği ve güvenliğinin sağlanması için birçok algoritma önerilmiştir. Genel olarak üç çeşit görüntü şifreleme yöntemi vardır [46-49]. Bunlardan ilki yayılma yöntemidir. Bu yöntem resmin piksellerinin yer değiştirmesi şeklinde açıklanabilir. Fakat piksellerin değerlerini etkilemediği için istatistiksel ataklara karşı tek başına yeterli olmaz. Bir diğer yöntem ise nüfuz etmedir. Bu sayede görüntü bilgisinin piksel değerleri değiştirilir. Bu yöntemin tek başına kullanılması da bilinen açık metin saldırısı, seçilmiş açık metin saldırısı ve kaba kuvvet saldırısı gibi ataklara karşı zayıf kalır. Görüntü şifreleme sistemlerindeki bu zayıflıkları gidermek için bu iki ölçütün birleştirilmesi önerilmiştir. Böylelikle hem istatistiksel ataklara karşı hem de kaba kuvvet saldırıları, bilinen açık metin saldırıları gibi ataklara karşı sisteme direnç sağlanmış olur. Dolayısıyla şifreleme sisteminin zayıf yönleri ve eksiklikleri giderilerek daha verimli ve güvenilir bir yapının oluşması sağlanmış olur.

### 2.6. Görüntü Şifreleme ve Çözme Algoritmaları

AES, DES ve IDEA gibi çeşitli geleneksel yöntemler, özellikle büyük verilerin iletimi konusunda, güvenli iletişim standartlarını sağlayamadığı için, iletişim esnasında bir güvenlik tedbiri olarak kullanılamıyor [50-53]. Dolayısıyla literatürde çeşitli yöntemlerle büyük boyutlu multimedya verilerin güvenli iletimi sağlanmaya çalışılmıştır. DNA tabanlı algoritmalar, optik kriptoloji, kaotik kriptoloji gibi çeşitli şifreleme sistemleri tasarlanmıştır [54-56]. Özellikle kaosun şifreleme alanında son zamanlardaki yaygın kullanımı ve bu durumun diğer şifreleme sistemlerine nispeten daha iyi sonuçlar vermesi kaosun bu alandaki uygulamalarına yönelik ilgiyi giderek arttırmaktadır [57]. Kaotik sistemler üzerine kurulan bu şifreleme algoritmaları, kimi zaman iyi sonuçlar verirken beraberinde bazı dezavantajları da getirmektedir [58, 59]. Özellikle renkli görüntüdeki veri boyutu fazla olduğu için tasarlanan kaos tabanlı şifreleme sistemleri performans ve maliyet açısından eksik kalabilir.

Kaos tabanlı ilk şifreleme 1989 yılında sunulmuştur [60]. 1997 yılında ise ilk kez kaos tabanlı resim şifreleme yöntemi ile bir resim şifrelenmiştir [61]. Zamanla kaos tabanlı şifreleme algoritmaları yaygınlaşmış ve birçok sistem geliştirilmiştir. Kaos tabanlı bu resim

şifreleme algoritmalarında genel olarak kaotik sistem tarafından üretilen diziler yardımıyla görüntüye birtakım işlemler uygulanır. Amaç orijinal görüntünün rastgele bir gürültüye dönüşmesini sağlamaktır. Böylelikle verinin gizliliği ve güvenliği sağlanmış olur.

Kaotik boyutuna göre kaos tabanlı resim şifreleme algoritmaları üç çeşittir. İlki düşük boyutlu kaotik sistem tabanlı resim şifreleme algoritmalarıdır [62]. İkincisi hiper kaotik sistem tabanlı resim şifreleme algoritmalarıdır [63, 64]. Üçüncüsü ise hem diğer şifreleme algoritmalarını hem de kaotik sistemleri aynı şifreleme işleminde kullanarak uygulanır [46].

Düşük boyutlu kaotik sistem tabanlı şifreleme algoritmalarının bilgisayarlar üzerinde yapılan uygulamalarında dinamik bozulmaların yaşanması, güvenilirliğini düşürüyor. Bazı düşük boyutlu kaotik sistemler kayan nokta yöntemi ile çözüldüğünden, performans hızları açısından düşük kalabiliyor. Bu da gerçek zamanlı şifrelemeleri olanaksız hale getiriyor. Diğer yandan, bu tür basit yapılı kaotik sistemler doğrudan resim şifreleme için kullanıldığı takdirde, kaotik yörüngelerinden yararlı bilgiler çıkarılabiliyor. Bu tür eksiklikleri gidermek için hiper kaotik sistemler görüntü şifrelemede kullanılmaya başlanmıştır [14,48,65].

Hiper kaotik bir sistemin bilgisayar gerçeklemesinde de, nihayetinde sonlu kaotik yörüngeler periyodik hale gelecektir. Fakat eğer kaotik sistem yeterince yüksek boyutlu ise bu periyotlar öyle uzun olur ki gerçek zamanlı uygulamalarda sadece periyodik olmayan kısımlar gözlemlenebilir. Değişken uzayının genişliği sayesinde güvenlik de genişletilmiş olur.

Hem diğer şifreleme algoritmalarının hem de kaotik bir sistemden yararlanılarak yapılan şifreleme algoritmaları da literatürde mevcuttur. Bu şekilde bir şifreleme algoritmasında yayılma ve nüfuz etme şifreleme standartları ayrı ayrı ele alınarak şifreleme sistemi tasarlanabilir. Bu şekilde yapılan bir şifreleme güvenilirliği arttırabileceği gibi, hız ve maliyet açısından şifreleme sistemini olumsuz olarak etkileyebilir.

Kaos tabanlı şifreleme sistemleri gerçeklerken, literatürde görüntü şifreleme için kullanılan yayılma ve nüfuz etme standartları birbirinden bağımsız şekilde uygulanmaktadır [28, 66]. Bu adımlar birleştirilerek de uygulanabilir. Kaotik bir sistemden elde edilen tek bir çıktı, hem yayılma hem de nüfuz etme işlemi için kullanılabilir. Burada amaç performans ve hız iyileştirmesidir. Böylelikle büyük boyutlu veriler için şifreleme işlemi tek seferde gerçekleştirilmiş olur.

Literatürde renkli resim şifreleme algoritmalarında resmin K (kırmızı), Y (yeşil) ve M (mavi) bileşenleri ayrı ayrı şifrelenebilir. K, Y ve M bileşenlerinin birbirini etkilemesiyle de şifreleme gerçekleştirilebilir. Bu, bileşenler arasındaki korelasyonu azaltarak daha tatmin edici sonuçlar oluşturur.

Literatürde, kaos tabanlı bir renkli görüntü şifreleme sistemi gerçekleştirilirken, veri boyutu, uygulanabilirlik, korelasyon vb. karşılaşılan zorluklardandır. Bu zorluklar, önerilen bazı kaos tabanlı şifreleme sistemlerini zayıflatmakta, yapılan güvenlik testleri ile bu durum ortaya konmaktadır. Bu çalışmada, literatürde karşılaşılan eksiklikleri giderebilecek etkili bir kaos tabanlı renkli görüntü şifreleme şemasının tasarlanması amaçlanmıştır.

## 2.7. Görüntü Şifrelemede Kullanılan Kaotik Üreteçler

Literatürde görüntü şifreleme algoritmaları için birçok kaotik sistem uygulanmıştır. Bu sistemlerden elde edilen kaotik sayılar, rastgele benzeri davranış sergilerken sistemin başlangıç koşullarına da hassas şekilde bağlı olur. Bu kaotik üreteçler zamana bağlı olduğu gibi ayrık zamanlı sistemlerde olabilir. Literatürde görüntü şifrelemede kullanılan bazı üreteçler ve sistem dinamikleri aşağıda gösterilmiştir.

Lojistik harita aşağıdaki gibi tanımlanır [62] :

$$f(x) = \lambda x(1-x) \tag{2.10}$$

Burada $\lambda$, $(0,4]$ aralığında sınırlıdır. Bu fonksiyonun iterasyon yöntemi ile çözümü şu şekildedir:

$$x_{n+1} = \lambda x_n (1-x_n) \tag{2.11}$$

Başlangıç değeri $x_0$ olacak şekilde kaotik sinyal üretmek için kullanılır.

1978 yılında keşfedilen kaotik Henon haritası aşağıdaki gibi tanımlanır [67]:

$$\begin{aligned} x_{k+1} &= y_k + 1 - a x_k^{\,2} \\ y_{k+1} &= b x_k \end{aligned} \tag{2.12}$$

Burada *a* ve *b*'nin belirli değerler için sistem kaotik özellik gösterebilir [68].

Rössler kaotik sistemi aşağıdaki gibi tanımlanır [69]:

$$\begin{aligned} \dot{x} &= -(y+z) \\ \dot{y} &= x + ay \\ \dot{z} &= b + z(x-c) \end{aligned} \tag{2.13}$$

Burada belirli *a*, *b* ve *c* parametreleri için sistem kaotik davranış sergiler.

Bu sistemler dışında Arnold haritası [15], 3 boyutlu Cat haritası[70], Lorenz [71], Chua [72] vb. birçok kaotik sistem resim şifrelemede kaotik üreteç olarak kullanılmaktadır. Burada birbirine alternatif olarak çıkan sistemler mevcuttur. Bunun yanı sıra Henon haritası, Arnold haritası gibi bazı kaotik haritaların birtakım zayıflıkları olmasından dolayı resim şifreleme için hiper kaotik sistemler vb. daha güçlü kaotik davranış sergileyen sistemler literatürde önerilmiştir [73, 74]. Diğer yandan bazı kaotik haritalar özellikle düşük boyutlu oldukları ve geniş parametre uzaylarına sahip olmadıkları için birleştirilerek yada yüksek boyutlara dönüştürülerek aynı kaos tabanlı şifreleme sisteminde kullanılmaktadır. Bir şifreleme sisteminde birden fazla kaotik sistem kullanmak ya da yüksek boyutlu sistemler kullanmak bir yandan güvenliği arttırırken diğer yandan performansı, uygulanabilirliği zorlaştırabilir. Bu çalışmada, güvenliği ve performansı uygun ve dengeli düzeyde tutacak şekilde etkili ve verimli bir kaos tabanlı renkli resim şifreleme sistemi tasarlandı. Bunun için gerçek zamanlı uygulanabilirliği basit olan, belirli parametre aralığında hiper kaotik özellik gösteren geniş parametre uzayına sahip değiştirilmiş Chua devresi (DCD) [26], tasarlanan şifreleme sisteminde kaotik üreteç olarak kullanıldı. Böylelikle DCD' nin kriptoloji uyarlaması literatüre sunuldu.

## 2.8. Görüntü Şifreleme İçin Güvenlik Testleri

Literatürde, görüntü şifreleme sistemlerinin güvenilirliğini ve farklı şekillerde gelen saldırıların sistemi zayıflatıp zayıflatmadığını ölçmek için bazı güvenlik testleri sunulmuştur. Bu testlerden bazıları aşağıdaki bölümlerde açıklanmaktadır.

### 2.8.1. Anahtar uzayı analizi

Bu analiz, bir resim şifreleme sisteminin kaba kuvvet saldırılarına karşı dayanıklı olup olmadığının tespiti içindir. Tahmin yoluyla anahtarın tespitini engellemek için, anahtar uzayının boyutunun tatmin edici seviyede olması gerekmektedir. DES algoritması, anahtar boyutunun düşüklüğünden dolayı eleştirilmiştir. Diffie ve Hellman anahtar deneme yanılma yöntemiyle 20 milyon dolara mal edilecek bir sistemle DES'in kırılabileceğini öne sürmüşlerdir. Bu eleştiriler doğrultusunda DES'in anahtar uzunluğu 128 bite çıkarılarak sistemin güvenilirliği arttırılmıştır. Genel olarak, anahtar uzayının geçerli boyutu $2^{100}$ 'ün üzerinde olmalıdır [75]. Böylelikle şifreleme sistemi kaba kuvvet saldırılarına karşı direnç gösterebilir.

### 2.8.2. Anahtar hassasiyeti ve açık görüntü hassasiyeti analizi

İyi tasarlanmış bir şifreleme algoritması, anahtar değişimine hassas şekilde bağlı olmalıdır. Şifreleme aşamasında anahtarda meydan gelecek en ufak bir değişiklik şifreli mesajı tamamen değiştirmelidir. Aynı şekilde şifrelenmiş bir mesajı çözerken kullanılan anahtarda ufak bir değişiklik yapıldığında gerçek mesaj başarılı bir şekilde elde edilmemelidir. Böylelikle sistem gizli anahtara hassas bağlı olur ve gizli anahtarın kolaylıkla deşifresinin önüne geçilmiş olur.

Aynı şekilde farklı görüntülerin şifrelenmiş durumları da birbirinden tamamen farklı olmalıdır. Görüntüde gerçekleştirilecek ufak bir değişiklik görüntünün şifrelenmiş halini tamamen değiştirmelidir. Böylece şifreleme sistemi düz görüntüye hassas biçimde bağlı olur. Sonuç olarak sistemin zayıflatılabilmesi engellenir.

### 2.8.3. Bilinen açık metin ve seçilmiş açık metin analizi

Bilinen açık metin saldırısında, saldırganın elinde bir grup açık mesaj ve bunlara karşılık gelen şifreli mesajlar bulunur. Bu bilgiler kullanılarak gizli anahtar elde edilmesi amaçlanır [76]. 1994 yılında Matsui tarafından gerçekleştirilen kriptoanaliz bu tür bir ataktır [77].

Seçilmiş açık metin ataklarında saldırgan, bilinmeyen bir anahtarla şifrelenmiş açık mesajlara erişebilmektedir. Burada şifreleme öyle tasarlanmalıdır ki saldırganın elindeki açık mesajların şifrelenmiş durumları, saldırganın eline geçmemelidir. Saldırgan şifreli

mesajlara eriştiği takdirde, şifreli ve açık mesaja diferansiyel analiz uygulayarak anahtarı elde etmeye çalışır.

### 2.8.4. Diferansiyel atak analizi

Diferansiyel atak aslında bir seçilmiş açık metin saldırısıdır. Saldırgan, düz görüntüleri sürekli değiştirmek suretiyle bu görüntülere karşılık gelen şifreli görüntülerle analiz yaparak gizli anahtarı elde etmeye çalışır. Diferansiyel ataklara karşı direnci ölçmek için, düz görüntüde çok küçük bir değişiklik yapılarak şifrelenmiş görüntünün, düz görüntünün şifreli halinden tamamen farklı olması beklenir. Literatürde bu farkı ölçebilmek, diğer bir değişle diferansiyel atak analizi yapabilmek için NPCR (number of pixels change rate) [78] ve UACI (unified average changing intensity) [79] kullanılır. $C_1$ ve $C_2$ sırasıyla düz görüntünün şifreli hali ve düz görüntünün çok küçük bir değişikliğe uğramış halinin şifreli hali olmak üzere ve görüntünün genişliği $W$ yüksekliği $H$ olacak şekilde, NPCR ve UACI değerlerinin nasıl hesaplanacağı aşağıdaki formül ile ifade edilmiştir:

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \tag{2.14}$$

$$\mathrm{UACI} = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \tag{2.15}$$

Burada $D(i,j)$ şu şekilde hesaplanır:

$$D(i,j) = \begin{cases} 1, C_1(i,j) \neq C_2(i,j) \\ 0, C_1(i,j) = C_2(i,j) \end{cases} \tag{2.16}$$

Literatürde, NPCR'nin ortalama değeri yaklaşık olarak 0,9961 [78] iken UACI'nın ortalama yaklaşık değeri 0,3346'dır [79].

### 2.8.5. Bilgi entropisi analizi

Bu analiz, şifrelenmiş bir görüntüde piksellerin rastgele dağılımlarının ne derece olduğunu hesaplamak için kullanılan en önemli analizdir. Bu hesap aşağıdaki gibi yapılır [80]:

$$H(m)=\sum_{i=0}^{2^n-1} p(m_i)\log\frac{1}{p(m_i)} \tag{2.17}$$

Burada $H(m)$, bilgi kaynağı olan $m_i$'nin bilgi entropisini temsil ederken $p(m_i)$ , $m_i$'nin olasılığını gösterir. $H(m)$'nin 8 olması demek ölçüle bilginin tamamen rastgele olması demektir. Dolayısıyla iyi bir şifreleme sisteminde, şifreleme işleminin ardından görüntünün bilgi entropisi değerinin 8'e yakın olması beklenir [81].

### 2.8.6. Korelasyon analizi

Orijinal herhangi bir görüntünün pikselleri arasında ilişki bulunur. İstatistiksel ataklarla başa çıkmak amacıyla şifreli bir görüntüdeki komşu iki pikselin korelasyonu minimum seviyede olmalıdır. Şifreli görüntüdeki her çift pikselin korelasyon katsayısı $r_{xy}$ aşağıdaki formülde gösterildiği gibi hesaplanır [82]:

$$r_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{2.18}$$

$$\mathrm{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \tag{2.19}$$

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i,\qquad D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2 \tag{2.20}$$

Burada *x* ve *y,* görüntüdeki iki komşu pikselin gri gösterge çizelgesindeki değerleridir. *N* ise görüntüden seçilen piksel sayısını gösterir. Şifreli görüntüden seçilen herhangi bir piksel grubu için hesaplanan korelasyon katsayısının 0'a yakın yada 0'ın altında çıkması pikseller arasındaki korelasyonun çok az olduğunu gösterir. Bu da şifreleme sistemini istatistiksel ataklara karşı dayanıklı yapar.

### 2.8.7. Histogram analizi

Görüntü histogramı, görüntünün istatistiksel bir özelliğidir ve görüntünün renk bileşenlerinin gri seviyede piksel sayısını çizerek piksellerin görüntü boyunca nasıl dağıldığını gösterir. İstatistiksel ataklara karşı çıkmak için şifreli görüntünün her gri seviyesi için düzgün dağılım göstermesi gerekir. Böylelikle yeterli seviyede rastgele bir dağılım sağlanmış olur.

### 2.8.8. Gürültü saldırılarına karşı dayanıklılık analizi

Gerçek iletişim kanallarında, şifrelenmiş görüntünün kanal boyunca çok çeşitli gürültülere maruz kalması kaçınılmazdır. Bu gürültü orijinal görüntünün geri elde edilmesini zorlaştıracaktır. Bu yüzden, şifreleme sistemlerinde gürültüye karşı dayanıklılık önemli bir performans ölçütüdür. PSNR (peak signal-to-noise ratio) saldırıdan sonra şifresi çözülen görüntünün kalitesini ölçmek için kullanılır. Gri seviye bir görüntü için PSNR aşağıdaki gibi hesaplanır [83]:

$$\mathrm{PSNR} = 10 \times \log_{10}\left(\frac{255 \times 255}{MSE}\right)(dB) \tag{2.21}$$

$$\mathrm{MSE} = \frac{1}{mn}\sum_{i=1}^{m}\sum_{i=1}^{n}\left\|I_1(i,j) - I_2(i,j)\right\|^2 \tag{2.22}$$

Burada MSE (mean square error) şifresi çözülmüş görüntü $I_2(i,j)$ ile orjinal görüntü $I_1(i,j)$ arasındaki ortalama hatayı gösterir ve *m, n* sırasıyla görüntünün genişliği ve yüksekliğidir.

### 2.8.9. Görüntü kaybına karşı dayanıklılık analizi

Şifreli görüntünün iletimi esnasında, paket kaybından veya üçüncü şahısların kötü niyetli imhalarından kaynaklı olarak bazı veriler kaybolabilir. Bu analiz, bazı verileri kaybolmuş olan şifreli görüntüden orijinal görüntünün ne kadar çıkarılabildiğini test etmek için kullanılır. PSNR, gürültü kaybına karşı dayanıklılık analizi için de bir performans ölçütü olarak kullanılabilir.

### 2.8.10. Hız analizi

Güvenlik gereksinimleri karşılandığında çalışma süresi, gerçek zamanlı şifreleme sistemi uygulamaları için önemli bir faktör haline gelir. Bir şifreleme işleminde, çarpma, bölme gibi matematiksel hesaplamalar, döngüsel işlemler oldukça zaman alır. Diğer yandan, herhangi bir görüntü şifreleme işlemi için rastgele sayı üretecinden elde edilen sayı dizilerinin boyutu sistemin performansını etkiler. Bu nedenle şifreleme için gerekli olan sayı dizisi ve tasarlanan algoritmada yararlanılan diğer operasyonlar, görüntü şifreleme metodunun etkinliğini değerlendirmek için kullanılabilir.

# 3. GÖRÜNTÜ ŞİFRELEME İÇİN KULLANILACAK KAOTİK ÜRETECİN TANITIMI VE ANALİZİ

Literatürde kaos tabanlı görüntü şifreleme algoritmaları için kullanılan bir çok kaotik sistem vardır. Bilindiği gibi, bir şifreleme algoritması için düşük boyutlu kaotik sistemin kullanılması çok kolaydır. Fakat basit dinamik karakteristikler, basit şifreleme kodu ve daha az parametre dizisi gibi düşük boyutlu kaotik sistemin bazı kusurları ciddi güvenlik problemlerine neden olabilir. Düşük boyutlulara kıyasla yüksek boyutlu kaotik sistem daha karmaşık bir yapıya, daha fazla sistem değişkenine ve parametreye sahiptir. Bu karakterlerin tümü sistemin şifreleme anahtarı olarak kullanılabileceğini garanti eder. Aynı zamanda sistemin anahtar uzayı artacak, üretilen sayı dizileri daha düzensiz ve tahmin edilemez olacaktır. Bu sebeplerden dolayı şifreleme sistemini yüksek boyutlu bir kaotik sistem ile tasarımlamak daha iyi bir seçim olacaktır. Tasarlanacak şifreleme sistemi için Kurt'un Değiştirilmiş Chua devresi (DCD) kaotik üreteç olarak kullanılacaktır [26]. Eş. 2.7'de tanımladığımız DCD kaotik sisteminin durum denklemlerini zamandan bağımsız şekilde incelemek için aşağıdaki forma dönüştürelim:

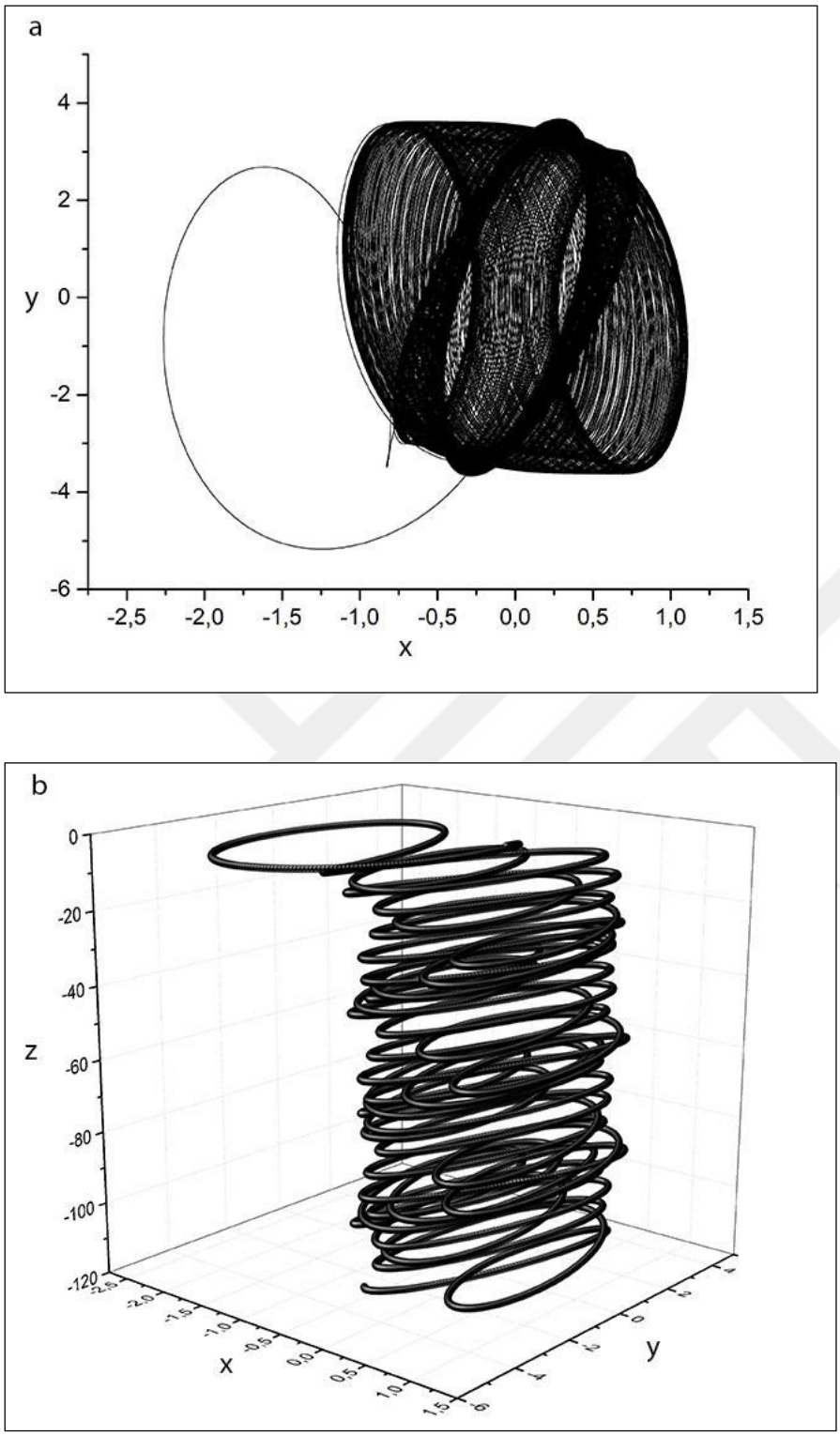
$$\begin{cases} \dot{x} = y - bx - \frac{1}{2}(a-b)\left[\,|x+\sin(z)| - |\,x-\sin(z)|\,\right], \\ \dot{y} = -\beta(y+x) + f\sin(v), \\ \dot{z} = \phi, \\ \dot{v} = \omega \end{cases} \tag{3.1}$$

Bu devrede, $a, \mathrm{b}, \phi, \beta, \omega, f$ sistem dinamiklerini kontrol eden kontrol parametreleridir. Özellikle sürüş genliği $f$ arttırıldığı zaman sistem karmaşık davranışlar sergiler ve kaotik özellik gösterir [26].

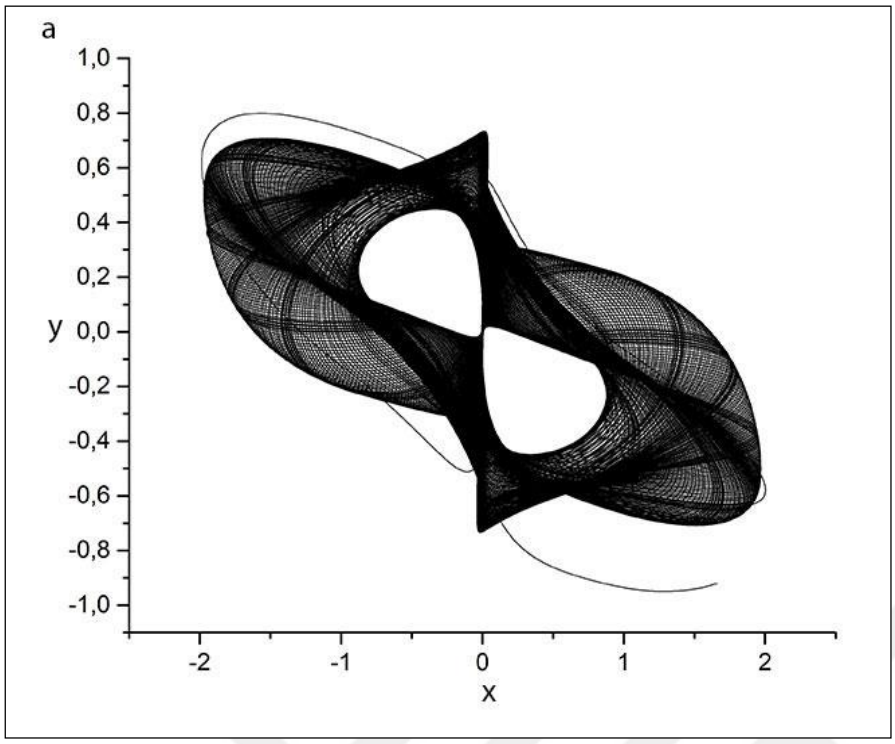
DCD'yi bir MatLab fonksiyonu olan *ode45* ile çözdürebiliriz. Ya da bir başka seçenek, sistemi iterasyon yöntemi ile çözdürmektir. Bu sistemin iterasyon metodu kullanılarak çözülmesi için Eş. 3.1'deki diferansiyel denklemleri aşağıdaki forma dönüştürürüz:

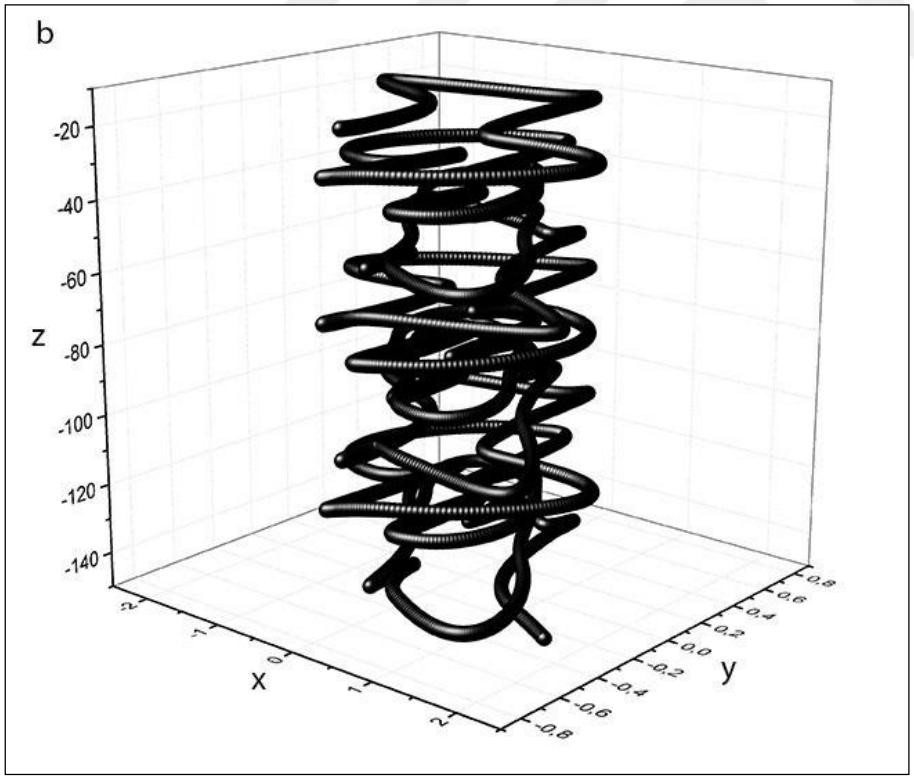
$$\begin{cases} x_{n+1} = x_n + (y_n - bx_n - \frac{1}{2}(a-b)\left[\,|x_n+\sin(z_n)| - |\,x_n-\sin(z_n)|\,\right])dt \\ y_{n+1} = y_n + (-\beta(y+x) + f\sin(v))dt \\ z_{n+1} = z_n + \phi dt \\ v_{n+1} = v_n + \omega dt \end{cases} \tag{3.2}$$

Şifreleme sisteminin tasarımına geçmeden önce DCD'nin farklı çözüm uzaylarını inceleyelim. DCD'nin farklı parametre değerleri için 2 ve 3 boyutlu çıktıları aşağıda gösterilmiştir:

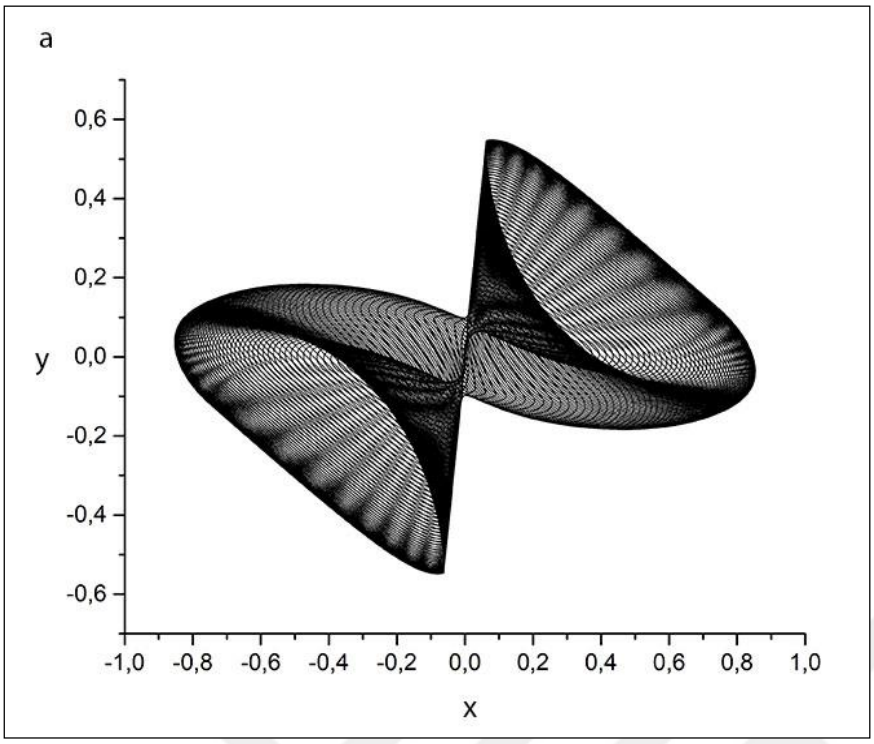


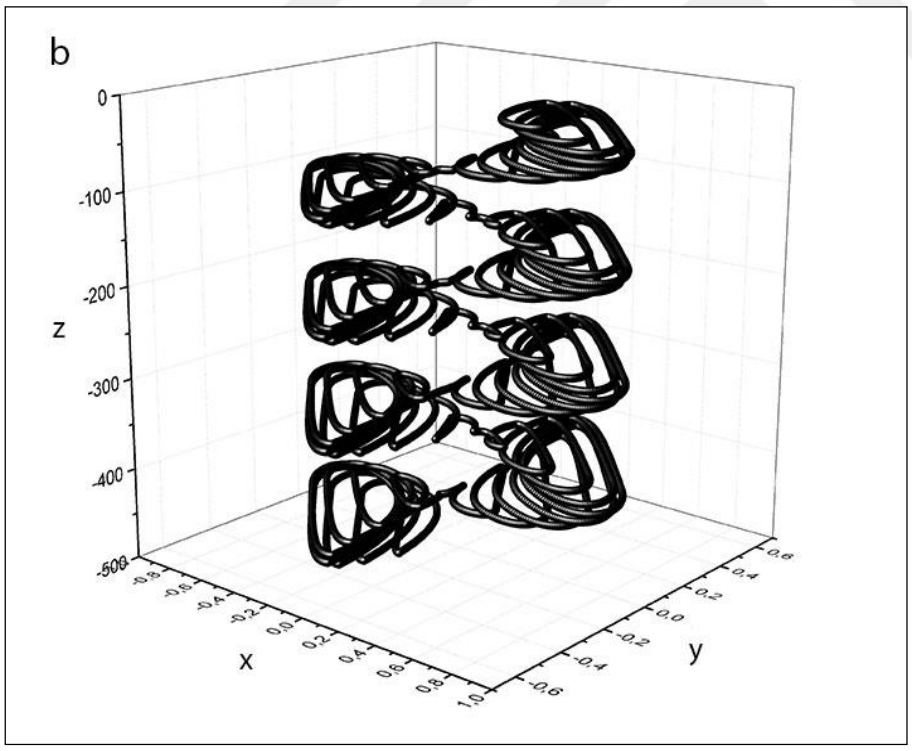

Şekil 3.1. Başlangıç parametreleri $a=-1{,}29, b=1{,}68, \beta=0{,}66,\ f=19{,}19, \omega=-5{,}73$ ve $\phi=-2{,}59$ olan kaotik çekicinin 2 ve 3 boyutlu gösterimleri sırasıyla (a) ve (b) ‘ deki gibidir.



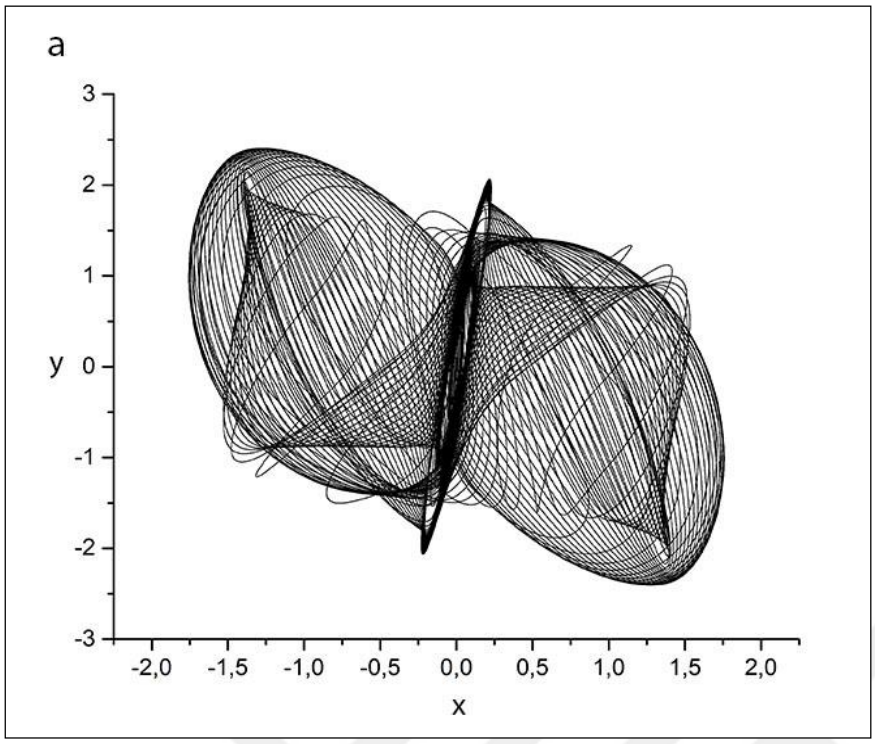



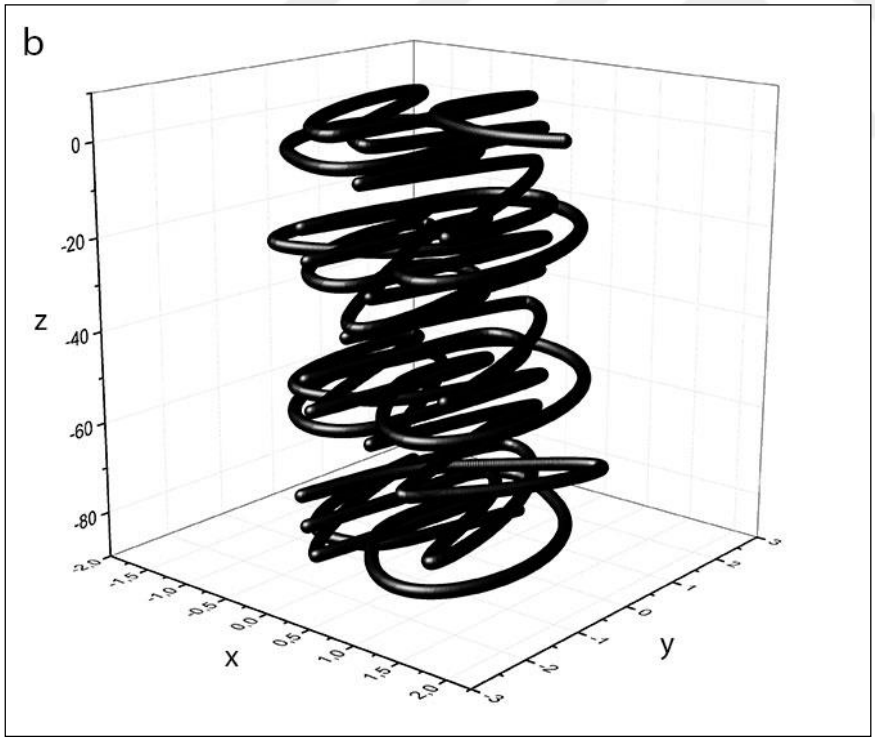

Şekil 3.2. Başlangıç parametreleri $a=-9{,}17, b=3{,}62, \beta=1{,}65, f=-1{,}86, \omega=8{,}36$ ve $\phi=-5{,}09$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir.



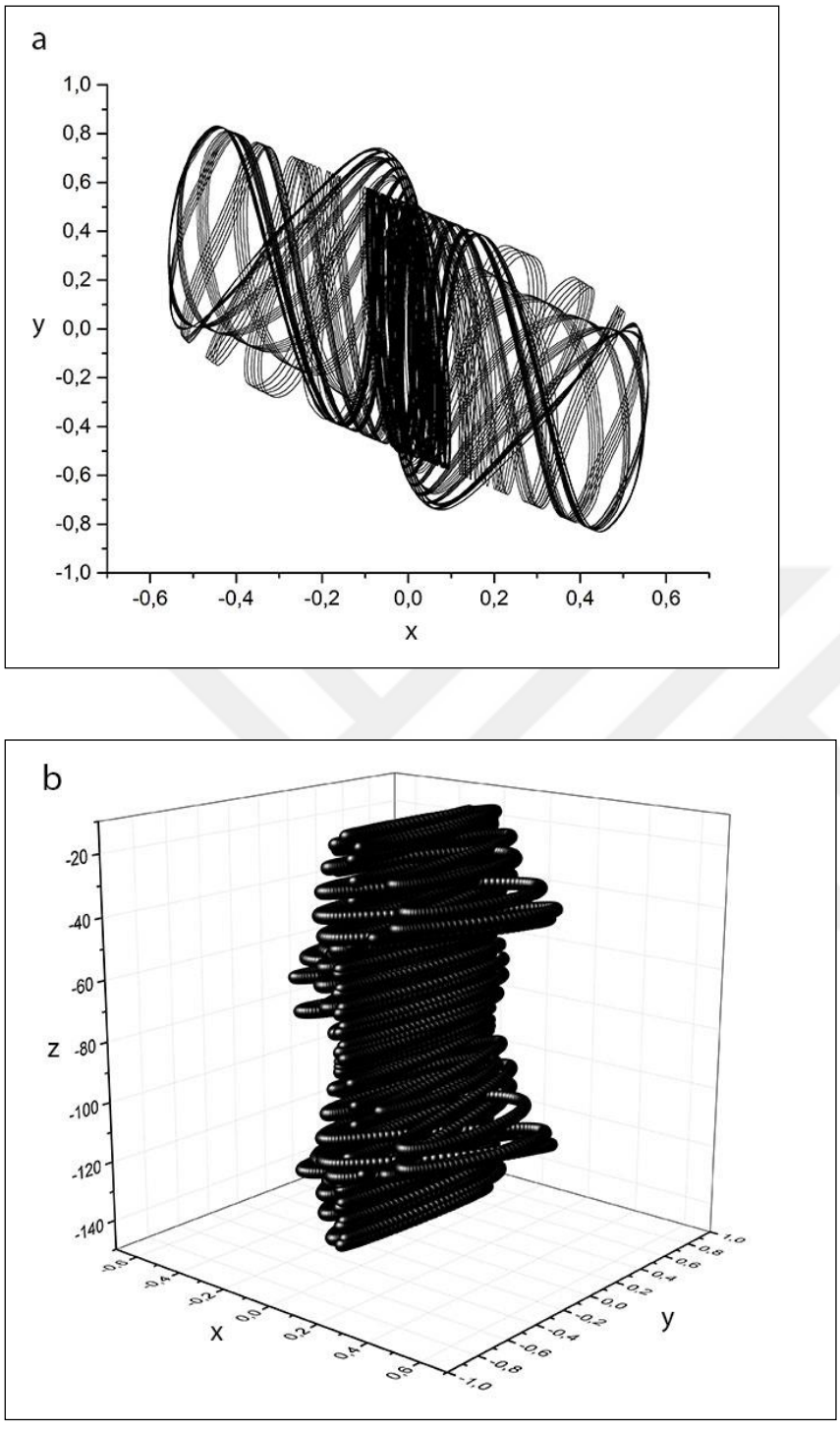




Şekil 3.3. Başlangıç parametreleri $a = -3{,}13, b = 2{,}68, \beta = 7{,}67, f = 4{,}81, \omega = -0{,}26$ ve $\phi = -4.92$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir.

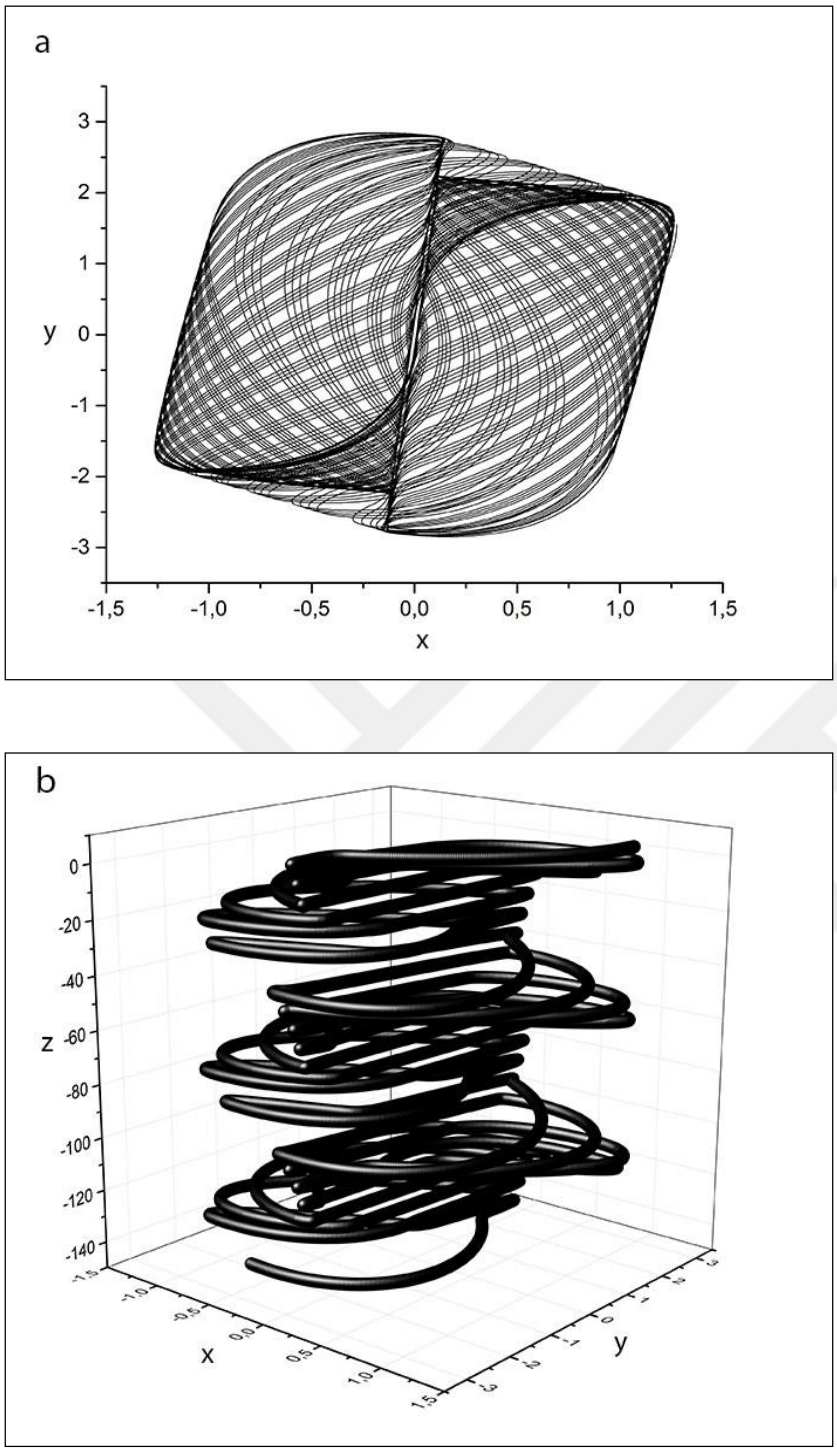


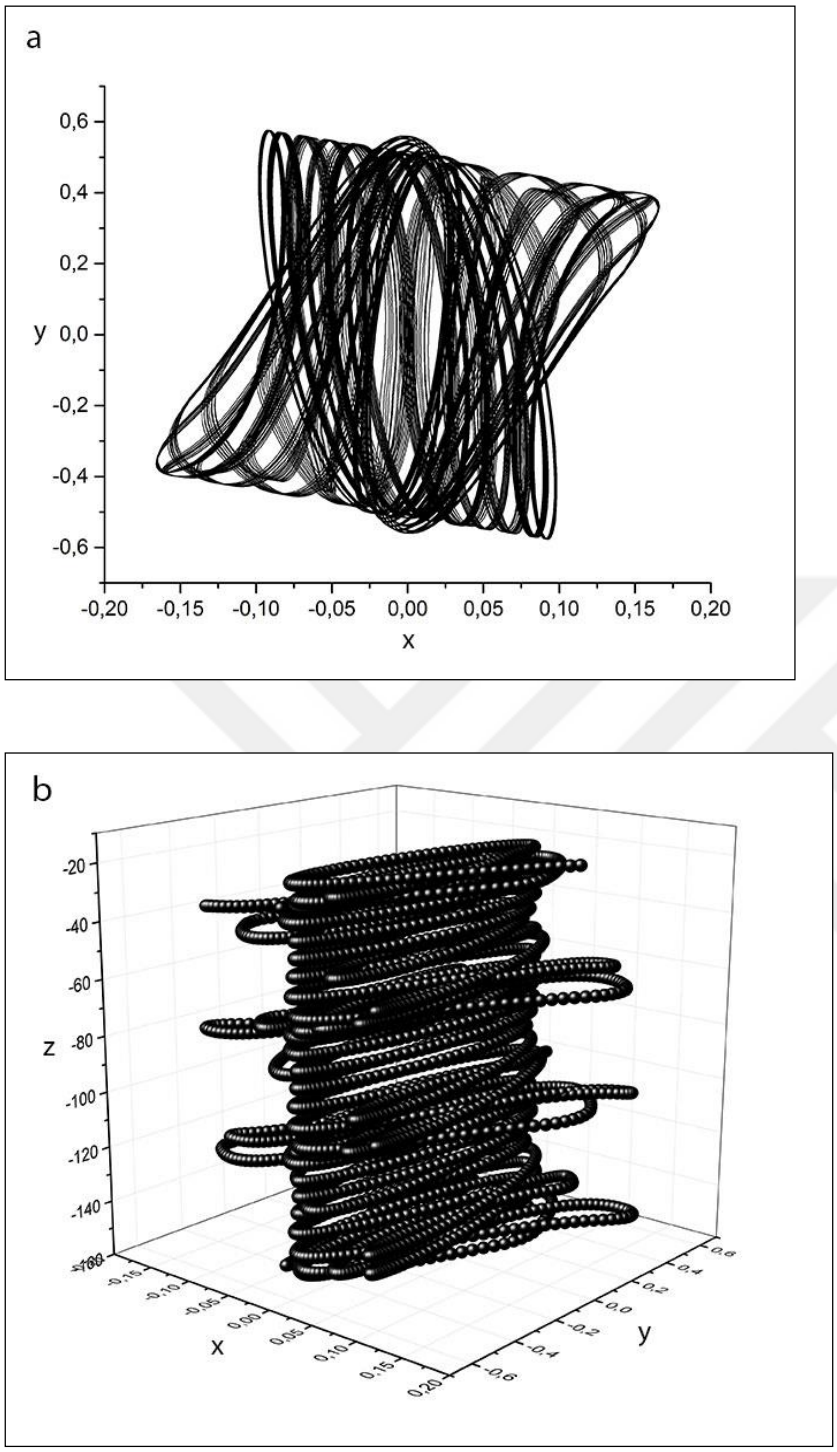

Şekil 3.4. Başlangıç parametreleri $a=-3{,}13, b=2{,}68, \beta=0{,}67,\ f=5{,}31, \omega=-3{,}26$ ve $\phi=-1{,}82$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir.



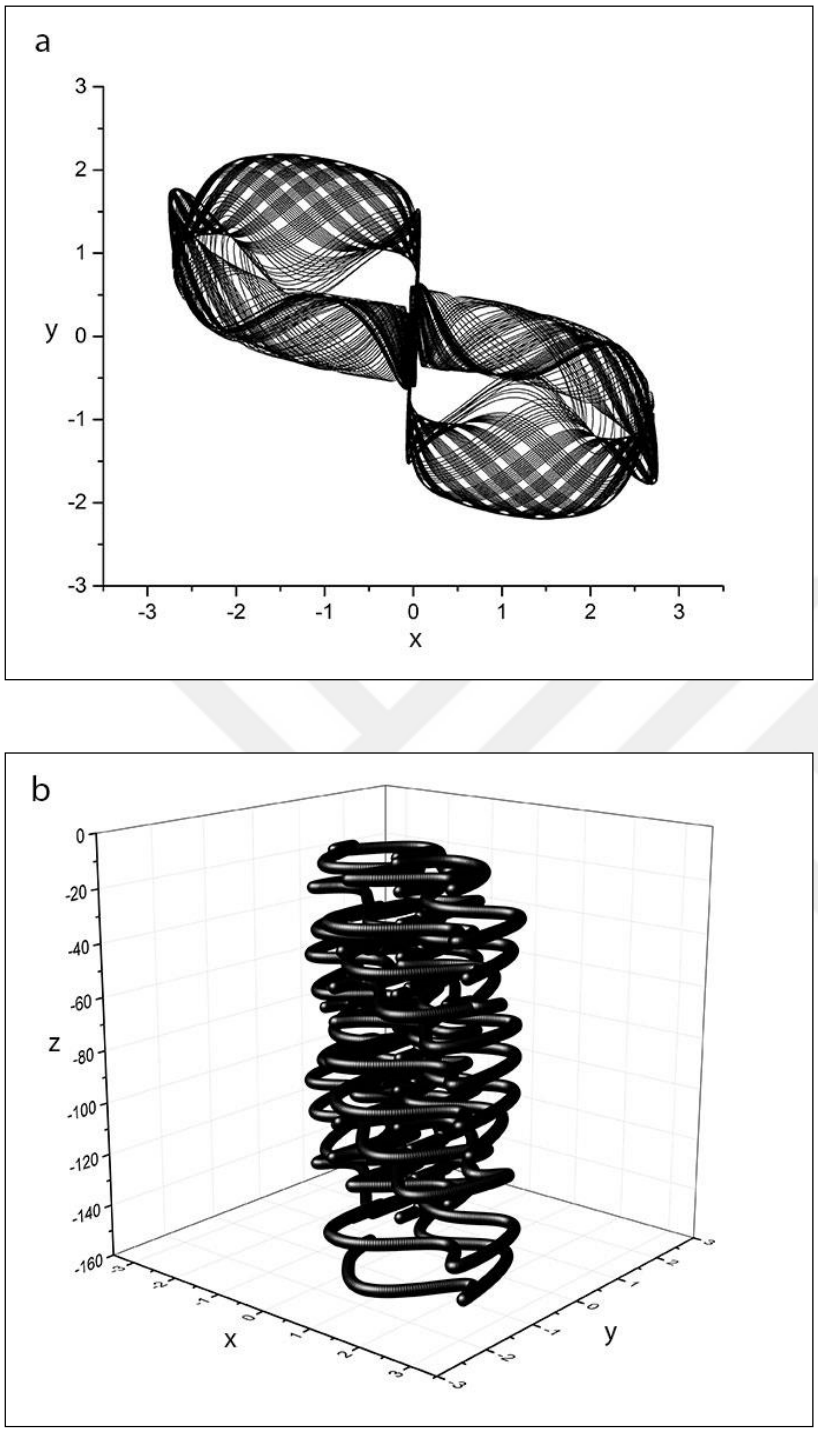

Şekil 3.5. Başlangıç parametreleri $a=-4{,}31, b=2{,}68, \beta=9{,}61, f=-8{,}17, \omega=-13{,}61$ ve $\phi=-3{,}33$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir.



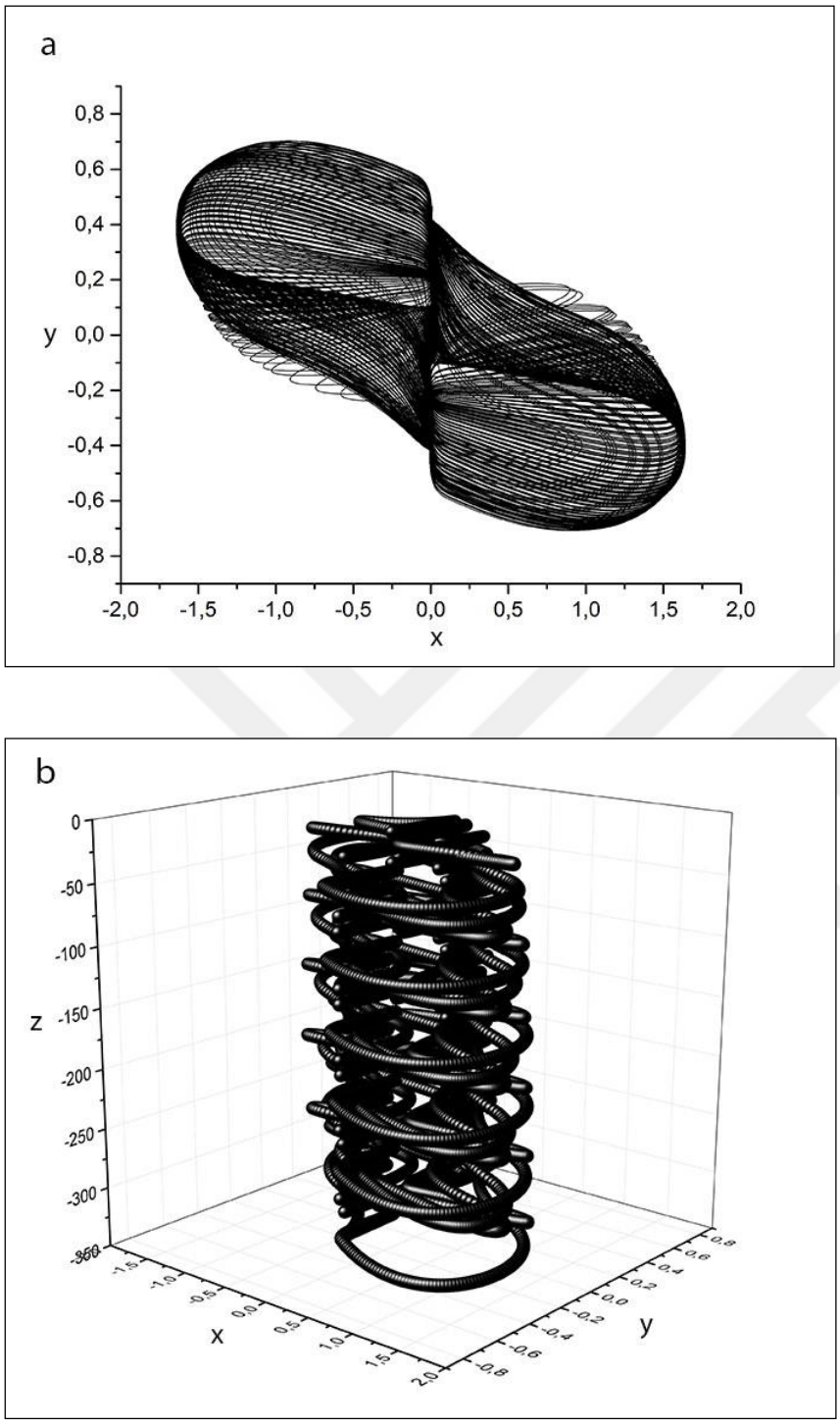

Şekil 3.6. Başlangıç parametreleri $a=-1{,}13, b=9{,}68, \beta=1{,}67, f=-5{,}81, \omega=1{,}94$ ve $\phi=-2{,}19$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir



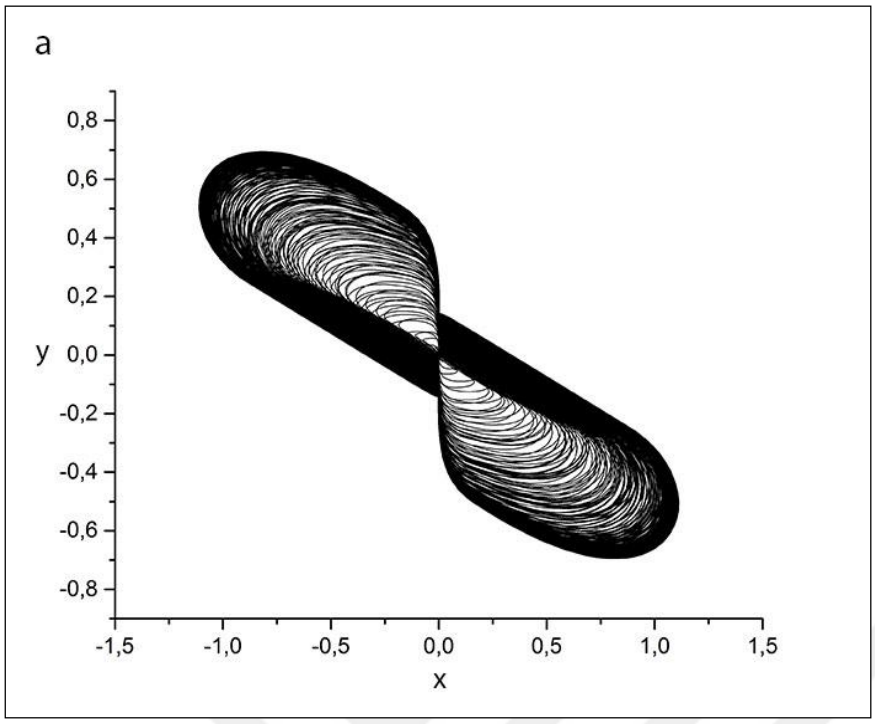

Şekil 3.7. Başlangıç parametreleri $a=-4{,}31, b=2{,}68, \beta=9{,}61, f=-8{,}17, \omega=-13{,}61$ ve $\phi=-6{,}33$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir.

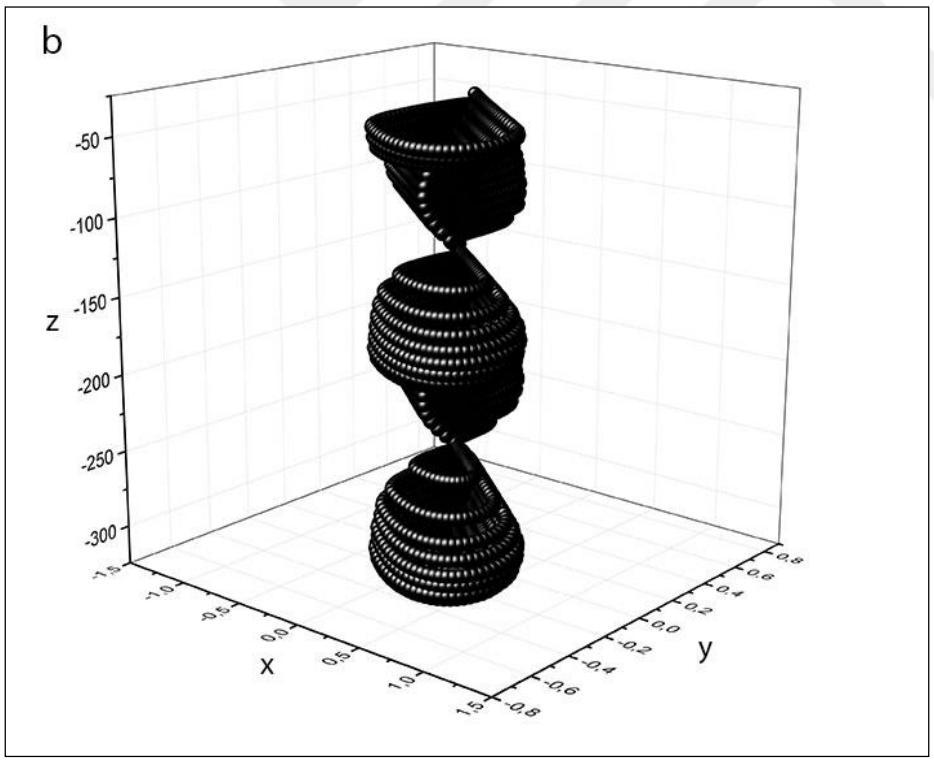



Şekil 3.8. Başlangıç parametreleri $a = -9{,}17, b = 3{,}62, \beta = 1{,}65, f = -5{,}86, \omega = -12{,}93$ ve $\phi = -2{,}53$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir

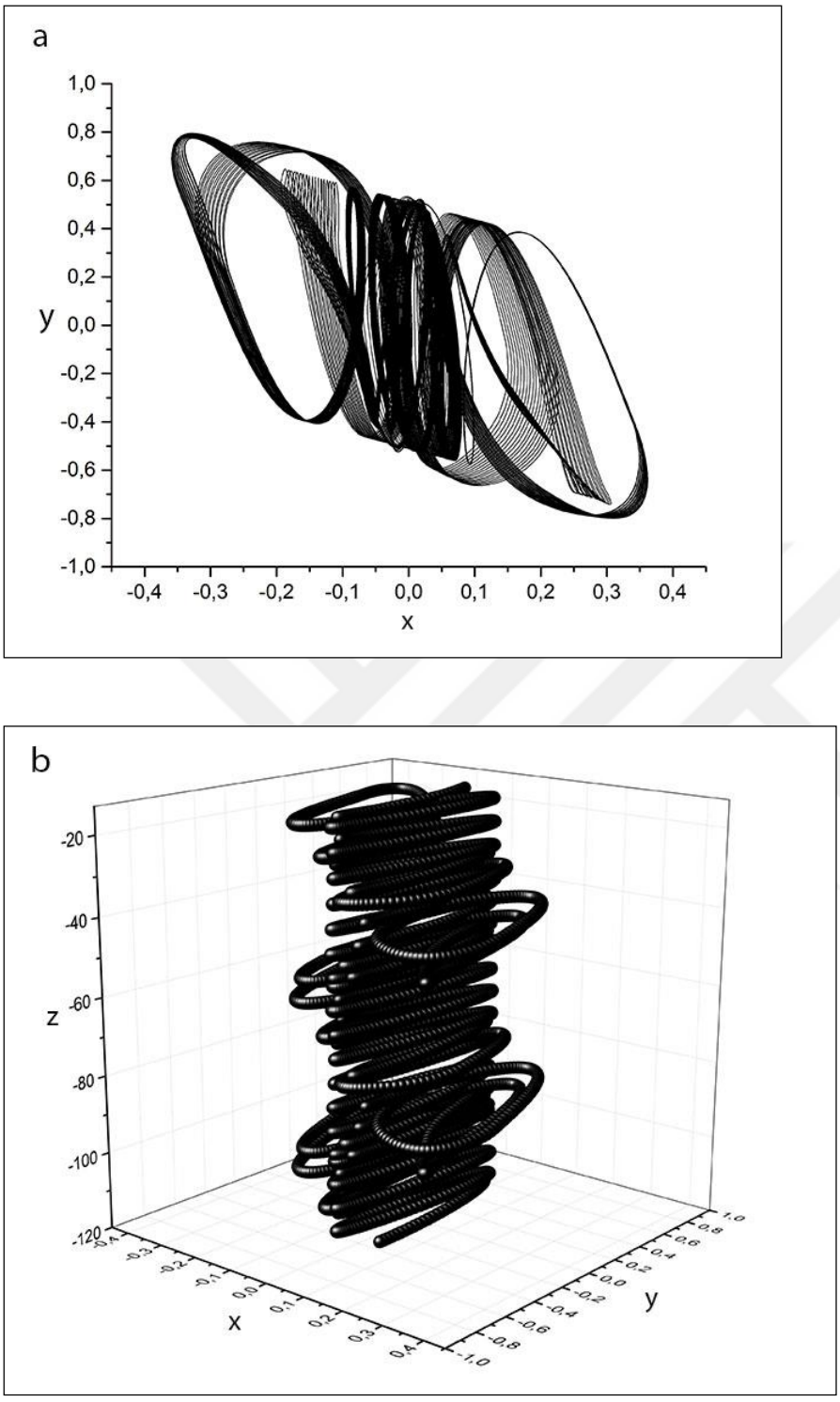



Şekil 3.9. Başlangıç parametreleri $a=-15{,}81, b=21{,}62, \beta=1{,}65, f=-1{,}86, \omega=-8{,}36$ ve $\phi=-5{,}37$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir

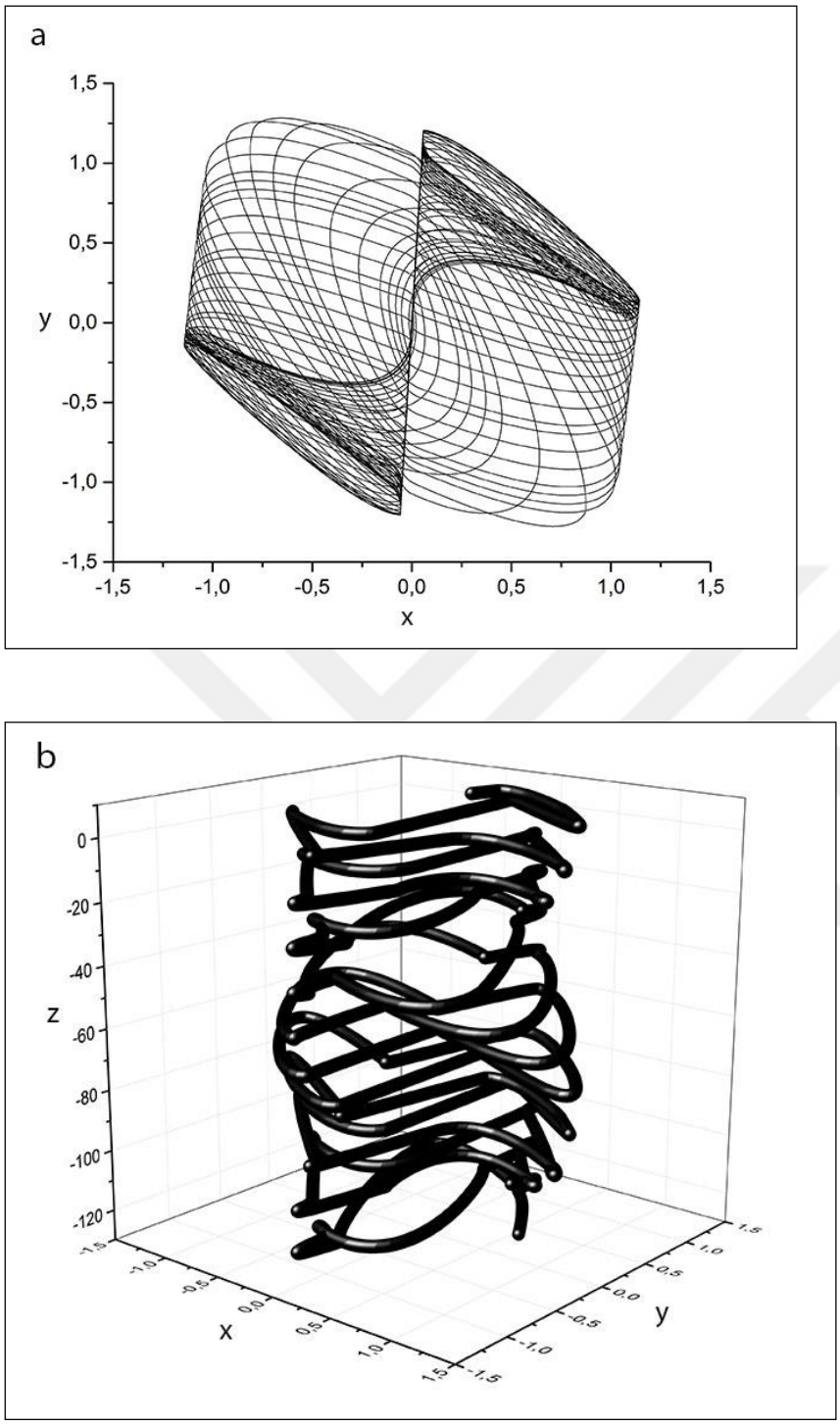


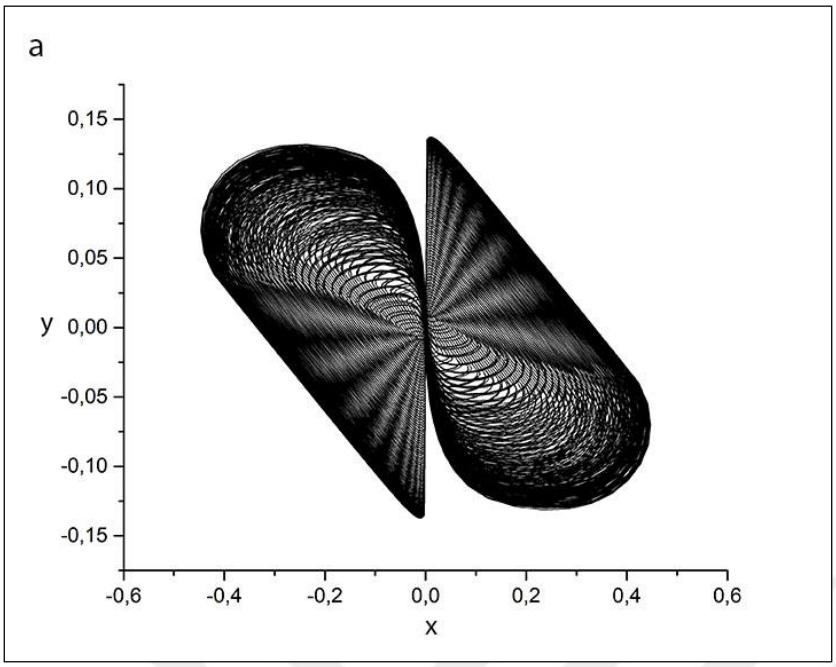

Şekil 3.10. Başlangıç parametreleri $a=-15{,}81, b=21{,}62, \beta=12{,}65, f=-1{,}86, \omega=-0{,}36$ ve $\phi=-7{,}37$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir

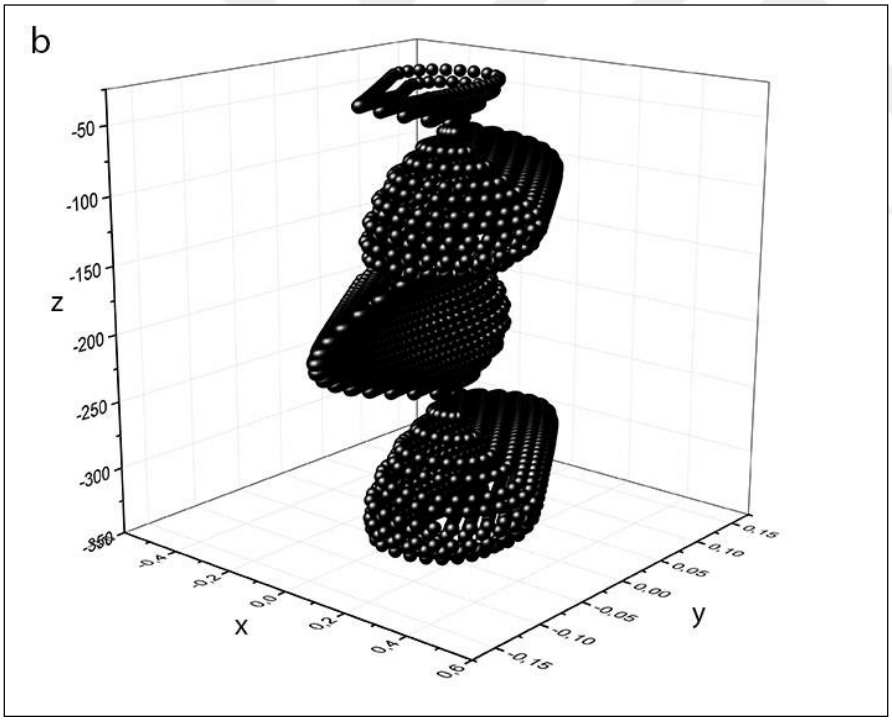



Şekil 3.11. Başlangıç parametreleri $a=-4{,}31, b=2{,}68, \beta=9{,}61, f=-8{,}17, \omega=-13{,}61$ ve $\phi=-4{,}33$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir.

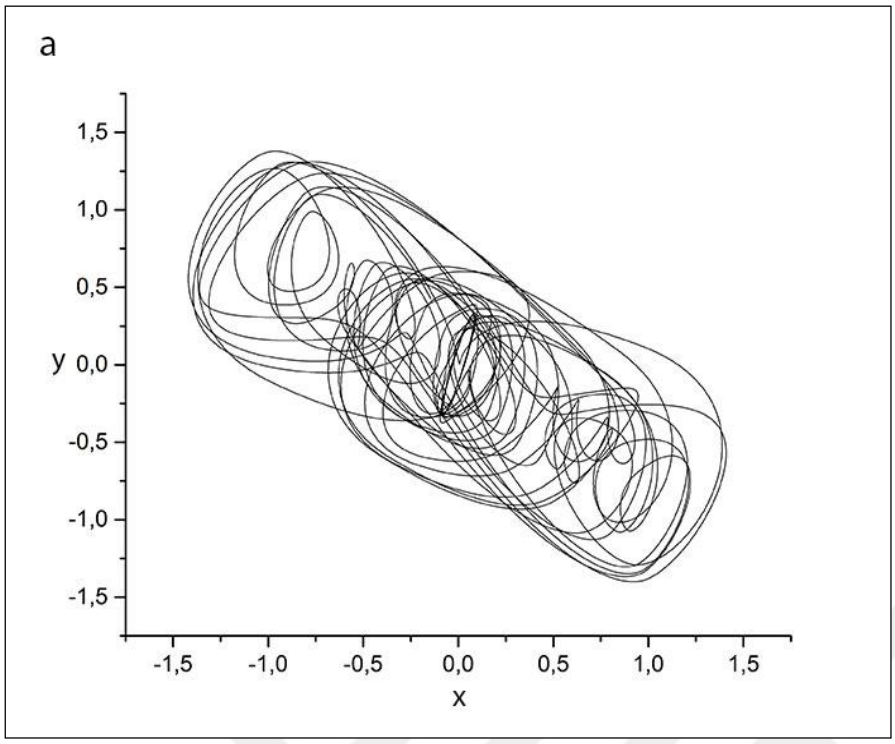


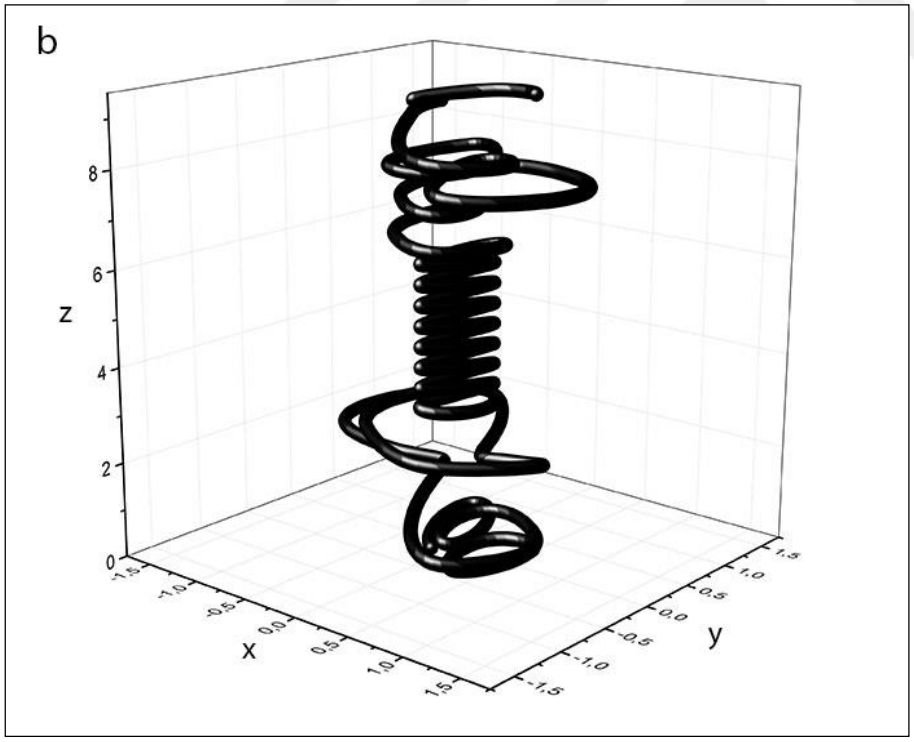

Şekil 3.12. Başlangıç parametreleri $a=-1{,}31, b=9{,}68, \beta=9{,}61, f=-12{,}17, \omega=-0{,}61$ ve $\phi=-1{,}31$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir.



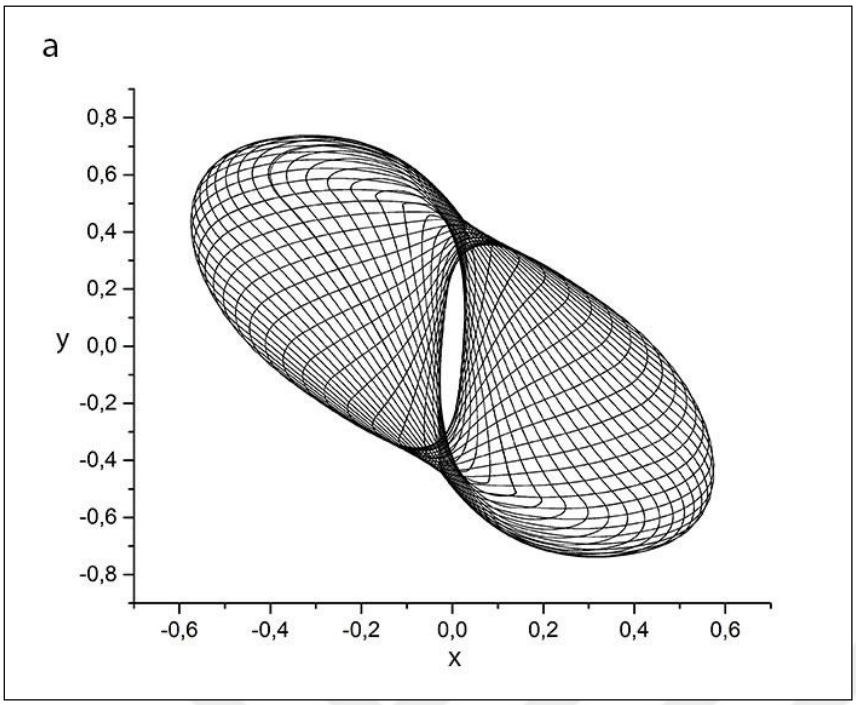



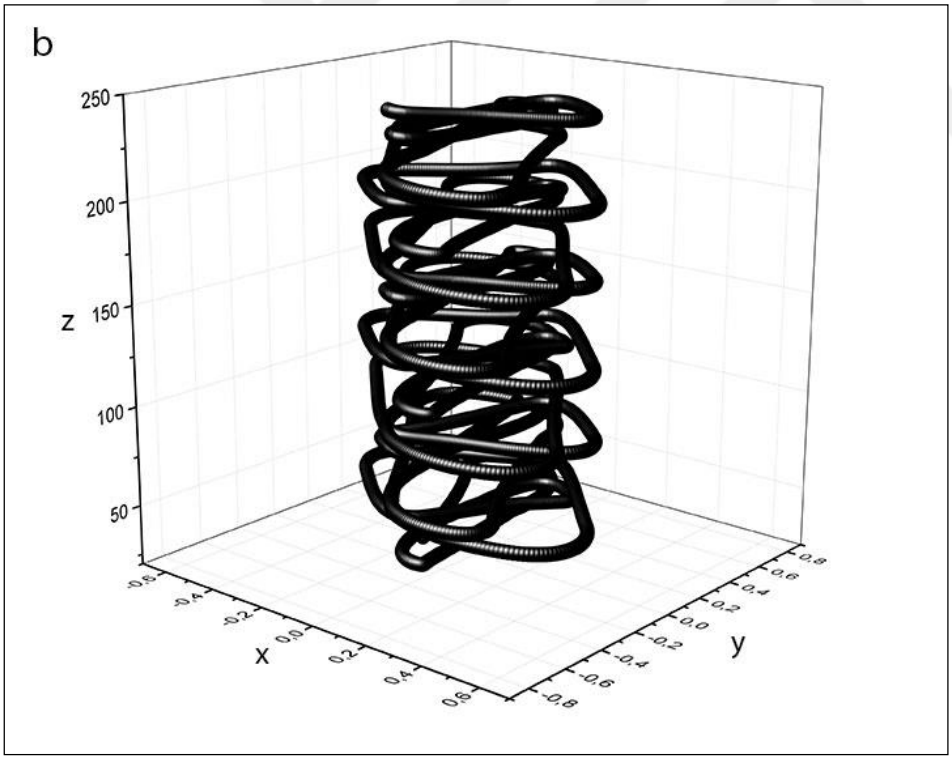

Şekil 3.13. Başlangıç parametreleri $a=-15{,}81, b=21{,}62, \beta=12{,}65, f=-1{,}86, \omega=-0{,}36$ ve $\phi=-11{,}37$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir



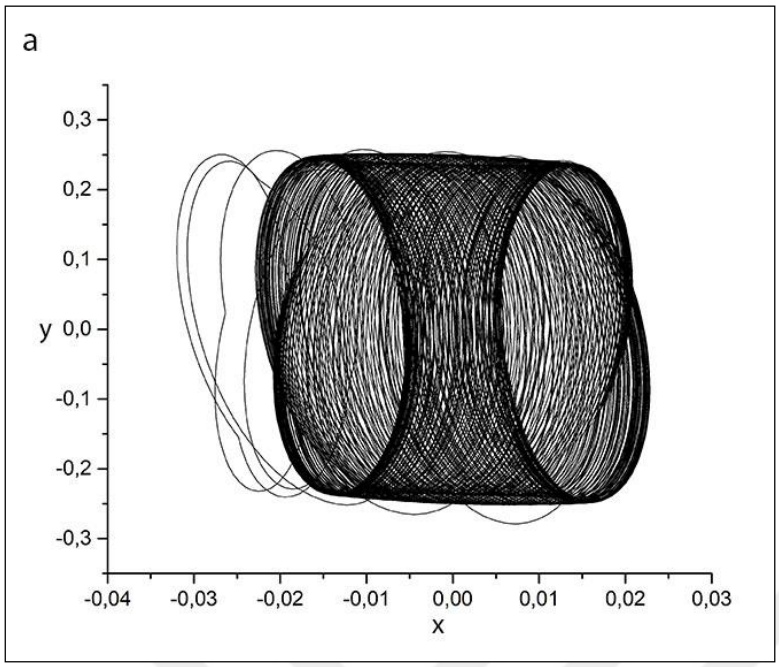



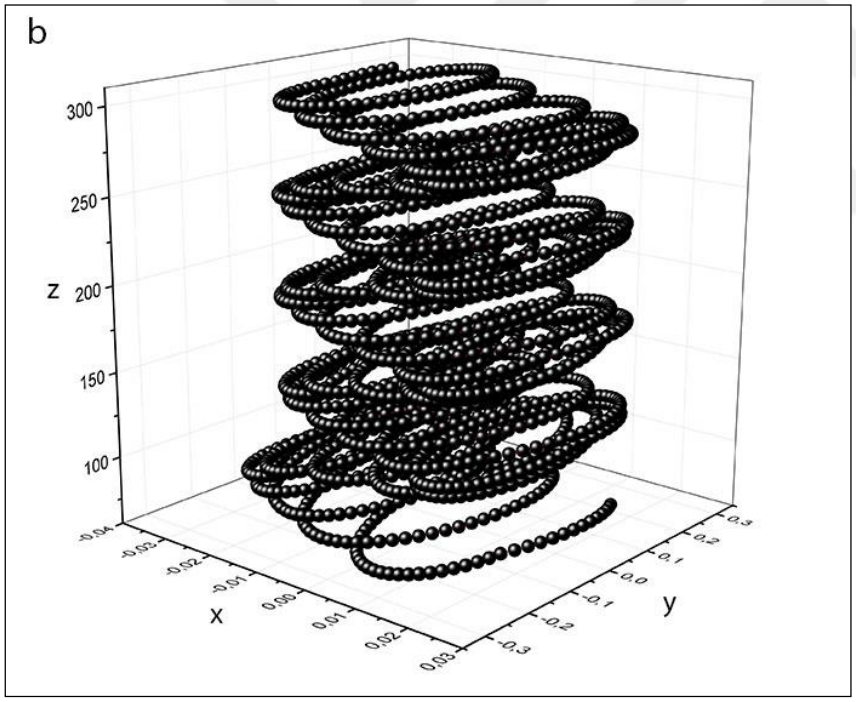

Şekil 3.14. Başlangıç parametreleri $a=-1{,}09, b=1{,}24, \beta=0{,}66, f=-0{,}49, \omega=1{,}33$ ve $\phi=0{,}09$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir.



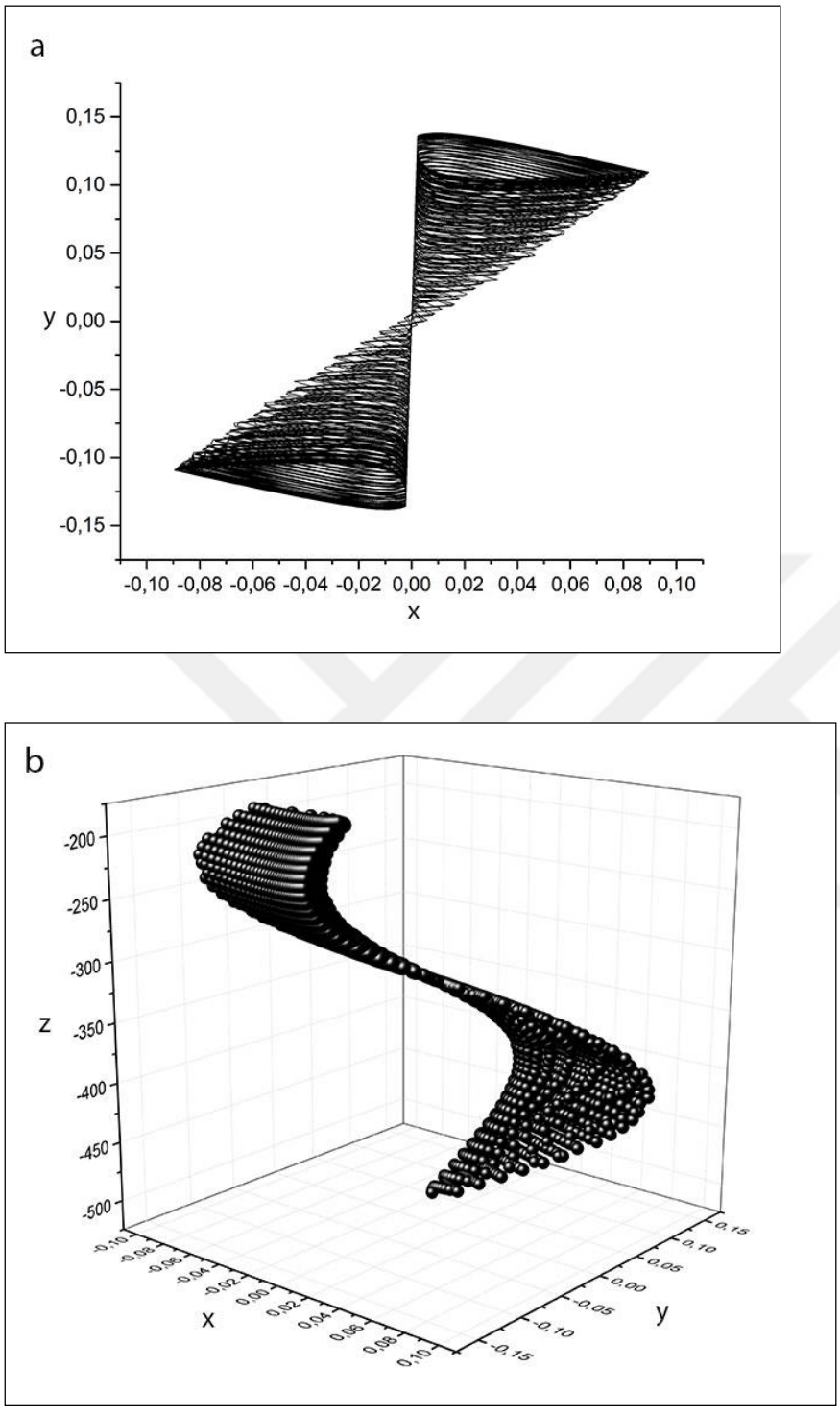




Şekil 3.15. Başlangıç parametreleri $a=-5{,}1, b=-0{,}19, \beta=9{,}71, f=4{,}19, \omega=3{,}9$ ve $\phi=6{,}7$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir

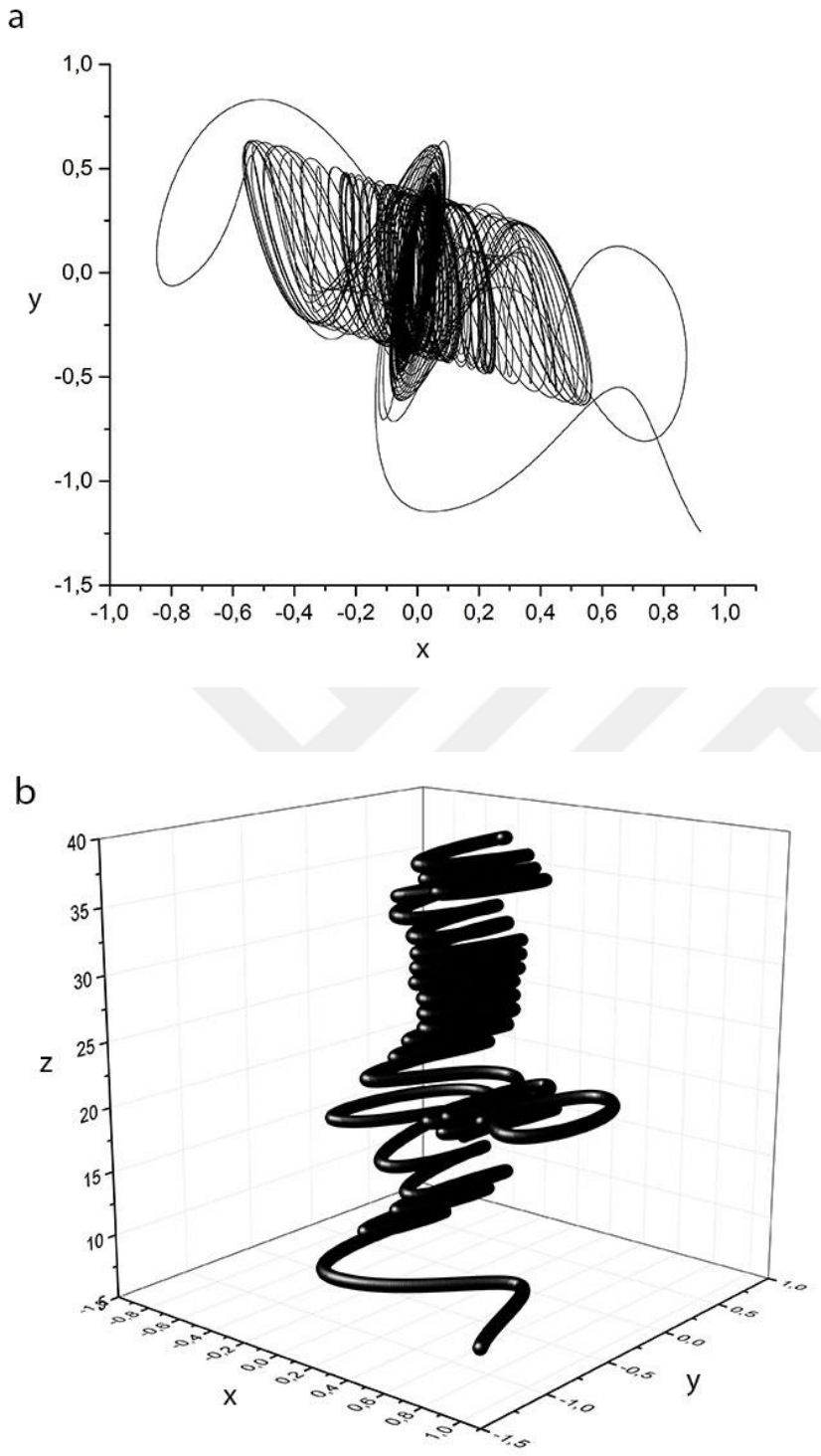


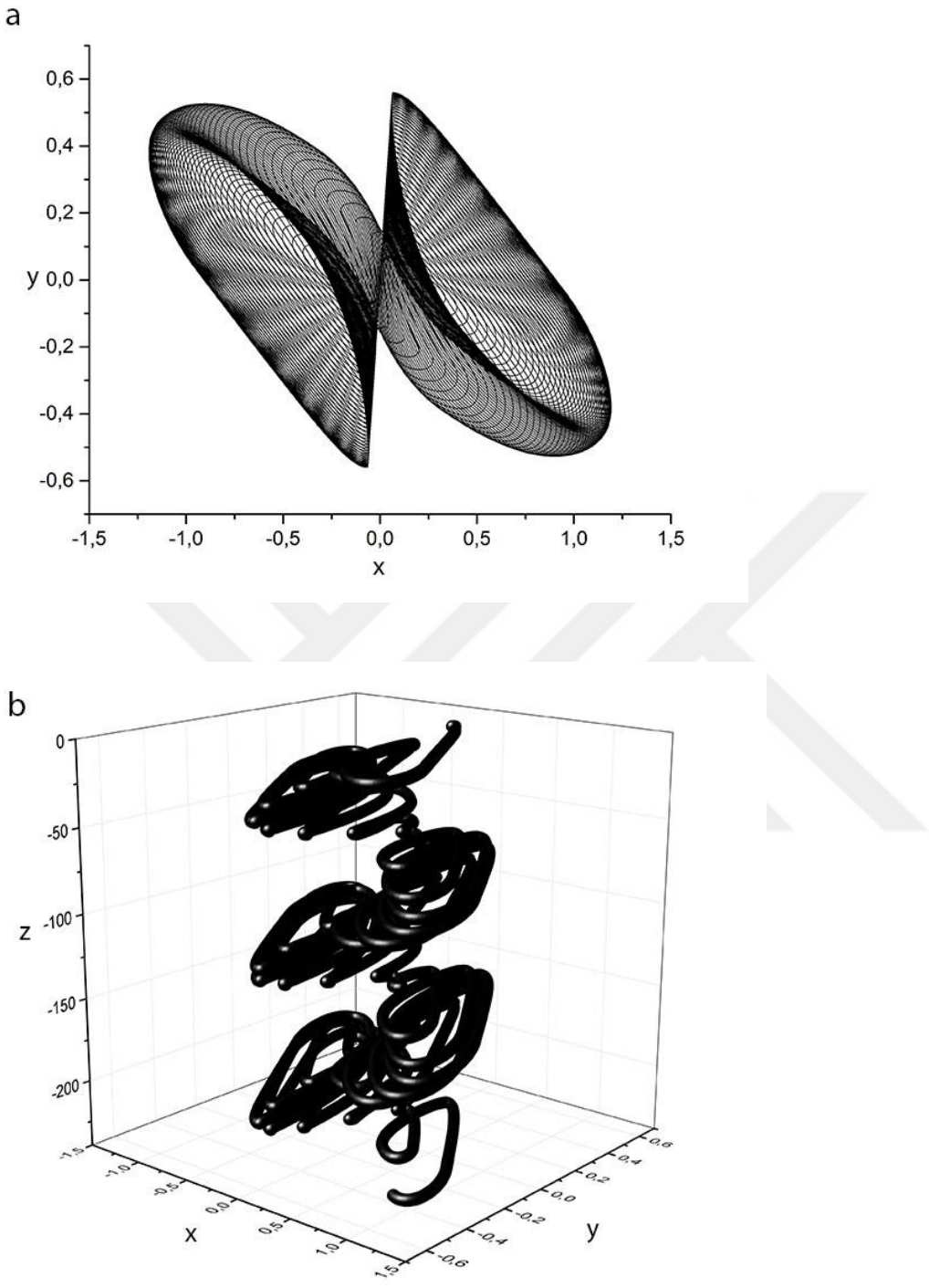

Şekil 3.16. Başlangıç parametreleri $a=-3{,}21, b=0{,}24, \beta=1{,}66, f=-5{,}17, \omega=21{,}33$ ve $\phi=19{,}11$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir



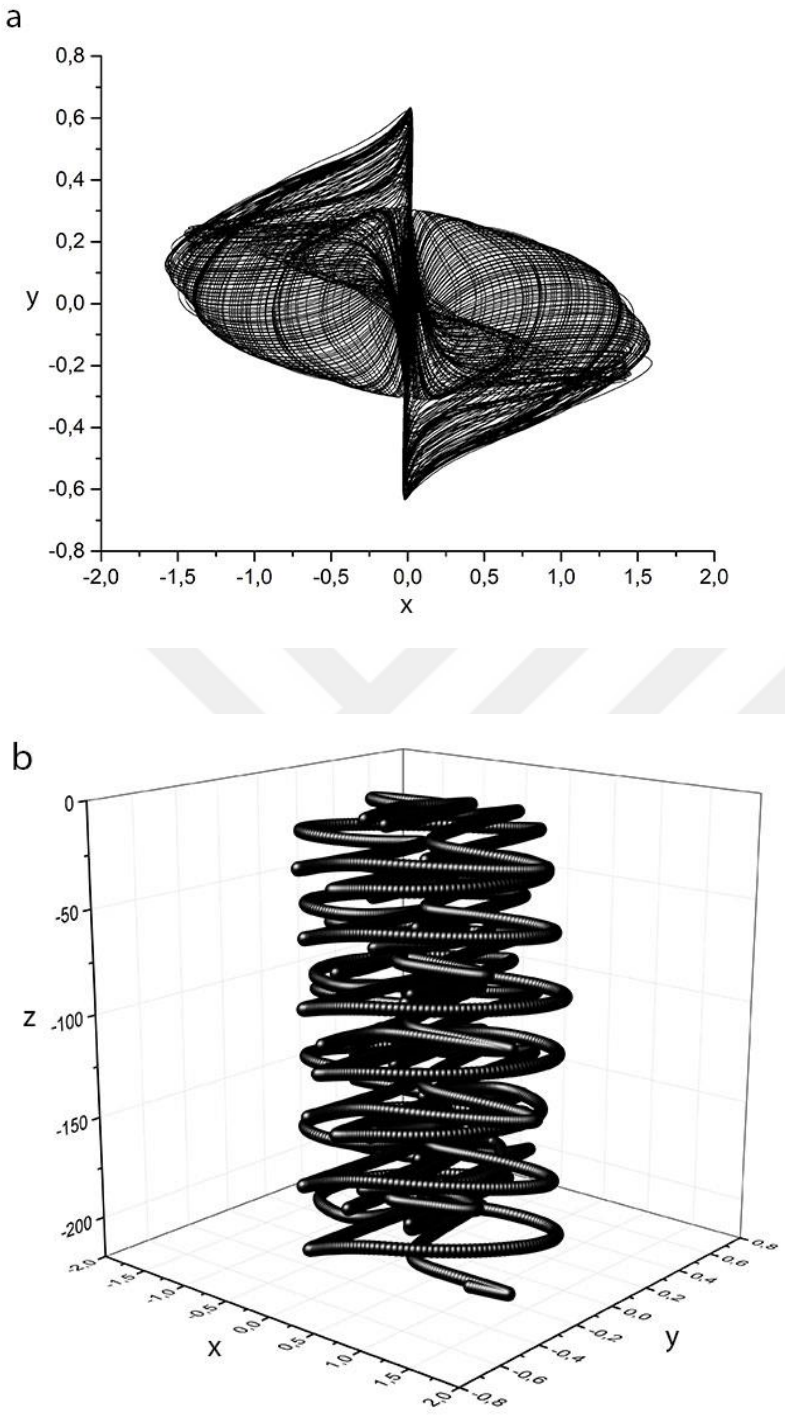

Şekil 3.17. Başlangıç parametreleri $a=-3{,}31, b=0{,}62, \beta=2{,}65, f=-1{,}86, \omega=19{,}36$ ve $\phi=0{,}37$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir



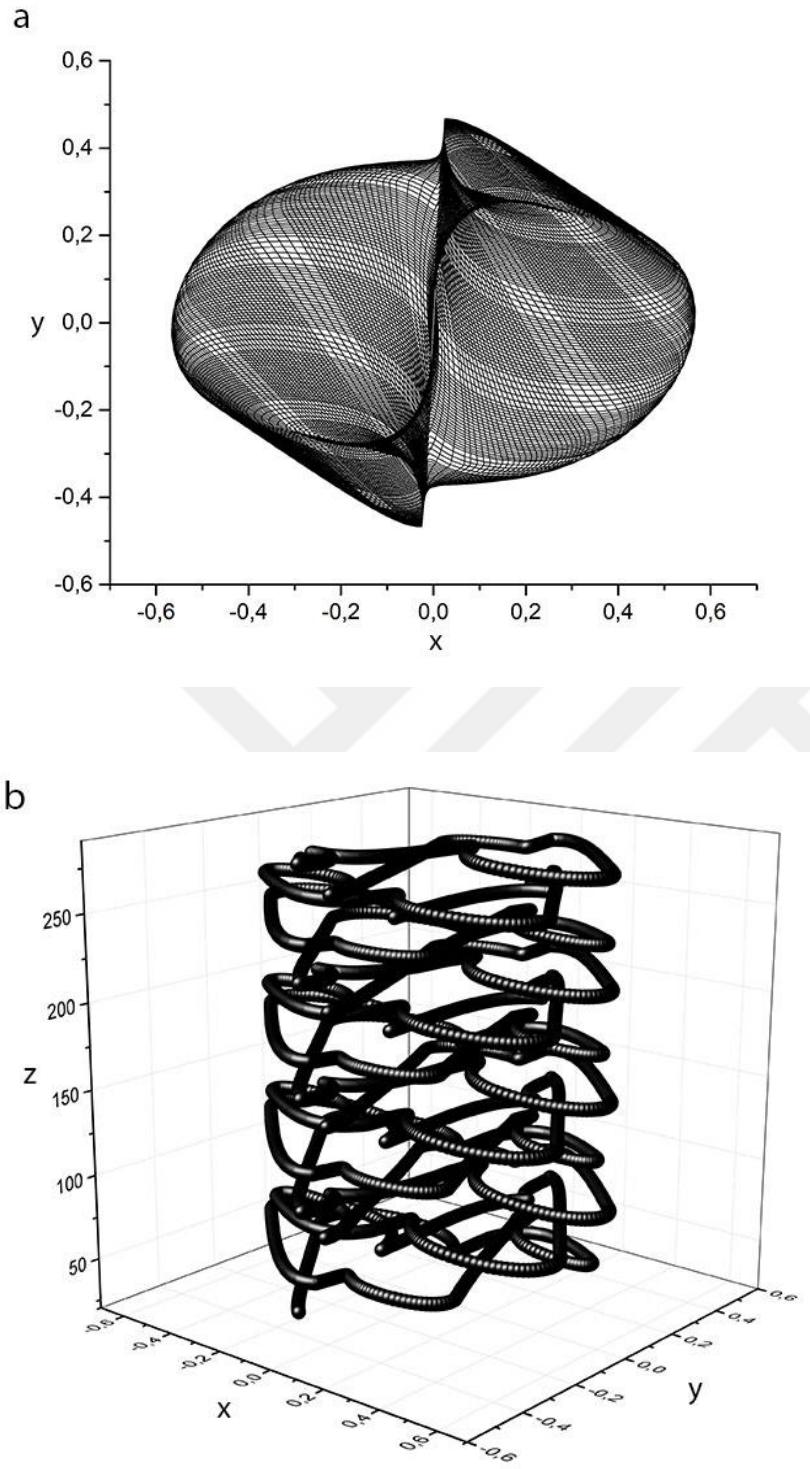

Şekil 3.18. Başlangıç parametreleri $a=-1{,}29, b=1{,}68, \beta=0{,}66, f=-2{,}19, \omega=-5{,}73$ ve $\phi=0{,}99$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir.



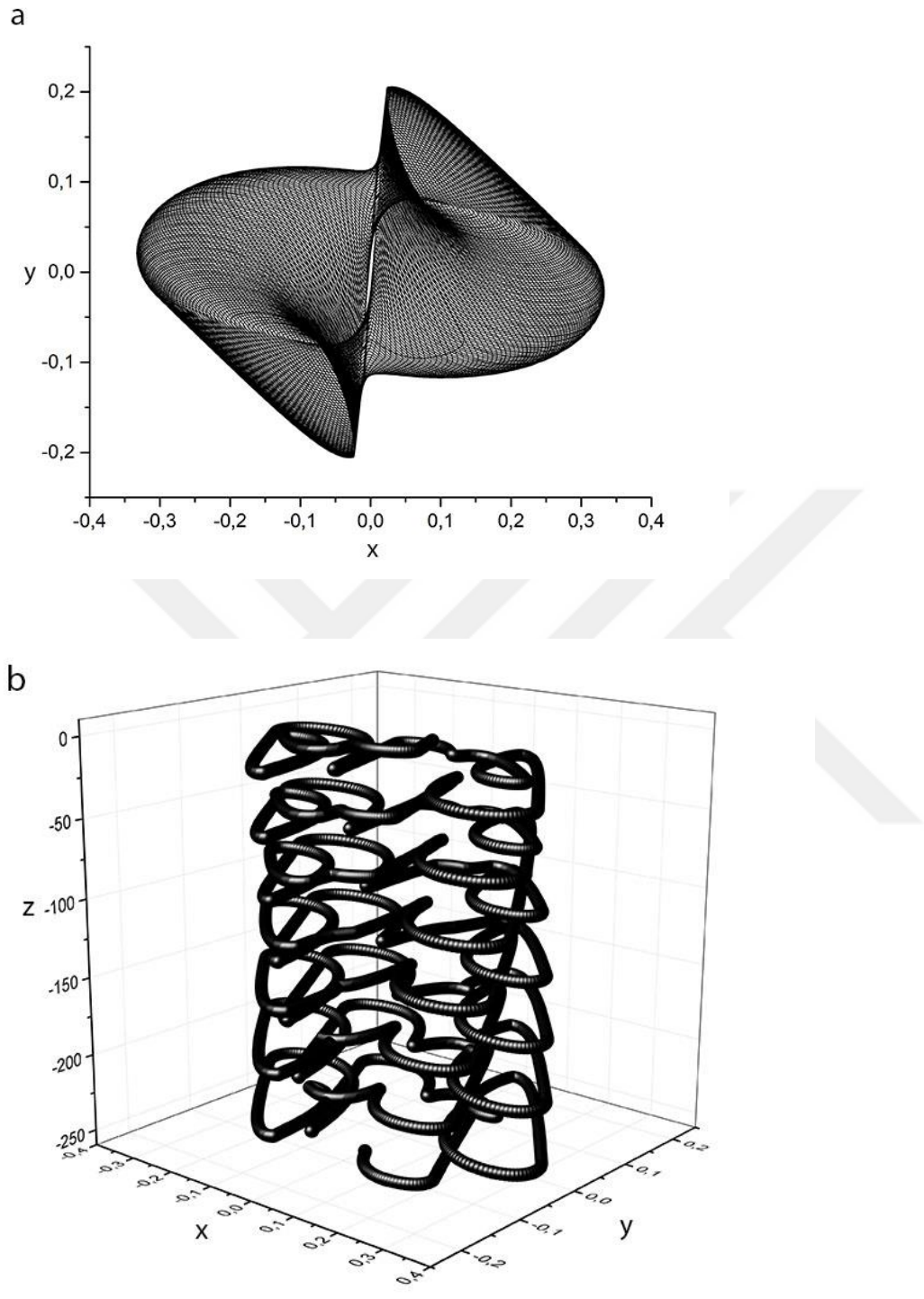

Şekil 3.19. Başlangıç parametreleri $a=-3{,}13, b=2{,}68, \beta=7{,}67, f=-4{,}81, \omega=-0{,}26$ ve $\phi=-3{,}52$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir



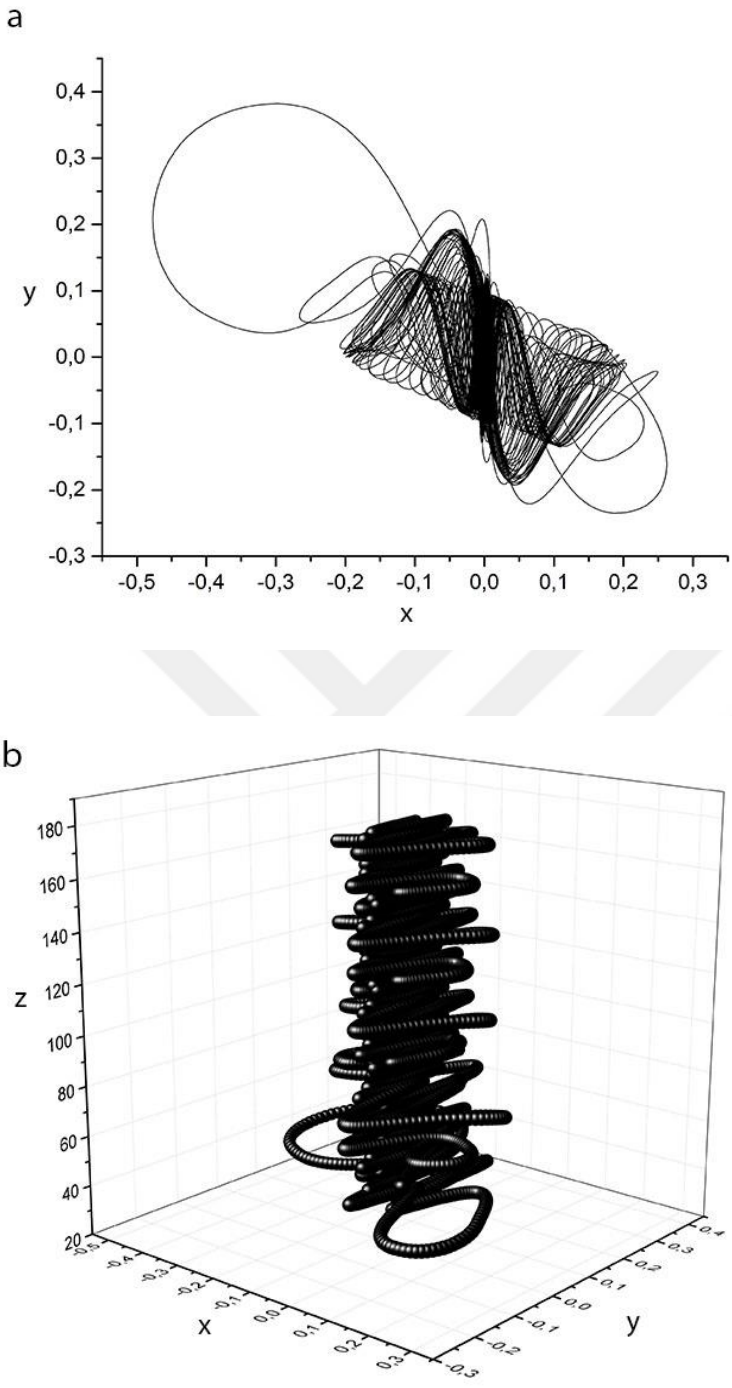

Şekil 3.20. Başlangıç parametreleri $a=-9{,}17, b=3{,}62, \beta=1{,}65, f=-1{,}86, \omega=8{,}36$ ve $\phi=-5{,}19$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir



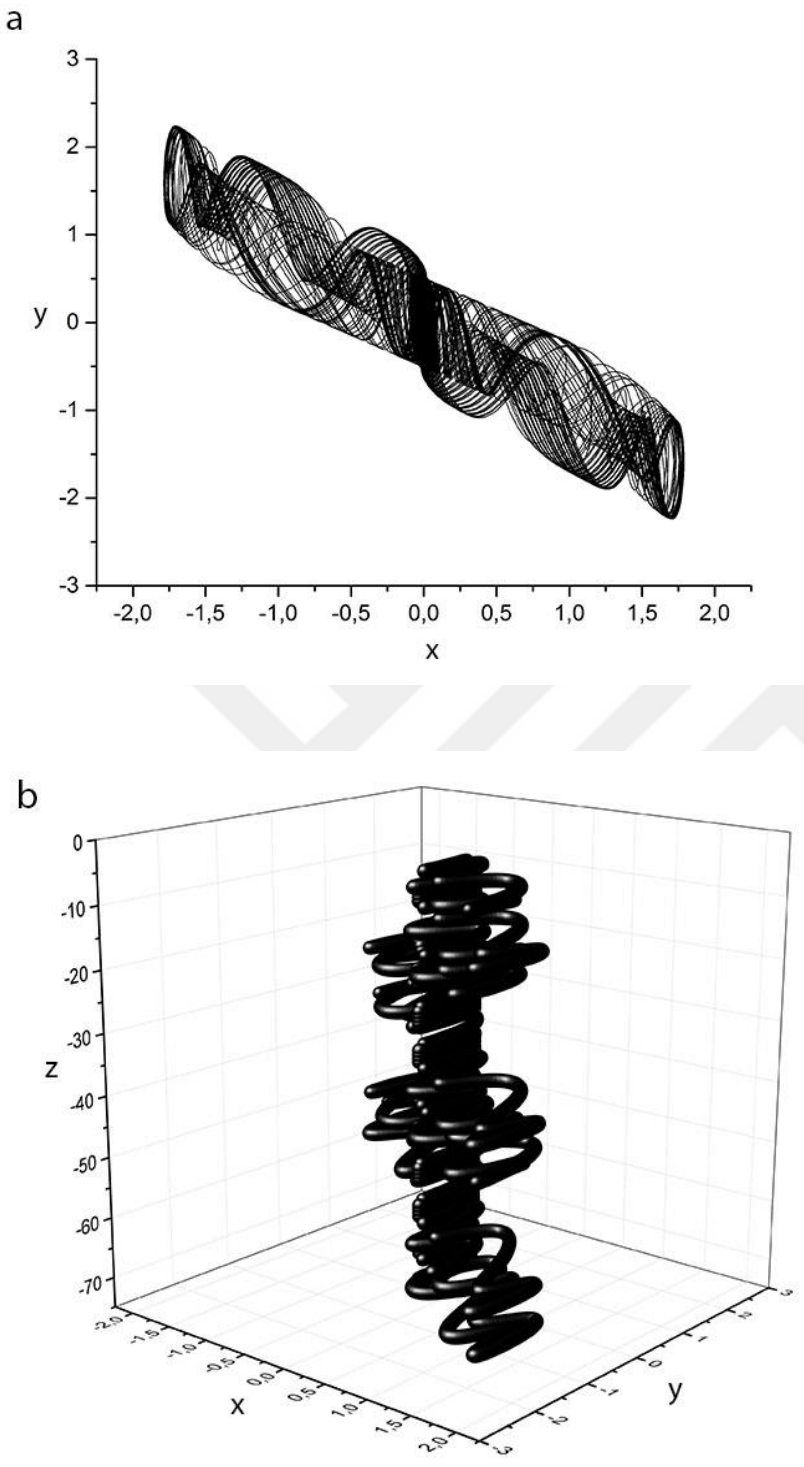

Şekil 3.21. Başlangıç parametreleri $a=-4{,}1, b=7{,}19, \beta=8{,}76, f=4{,}39, \omega=1{,}9$ ve $\phi=6{,}32$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir



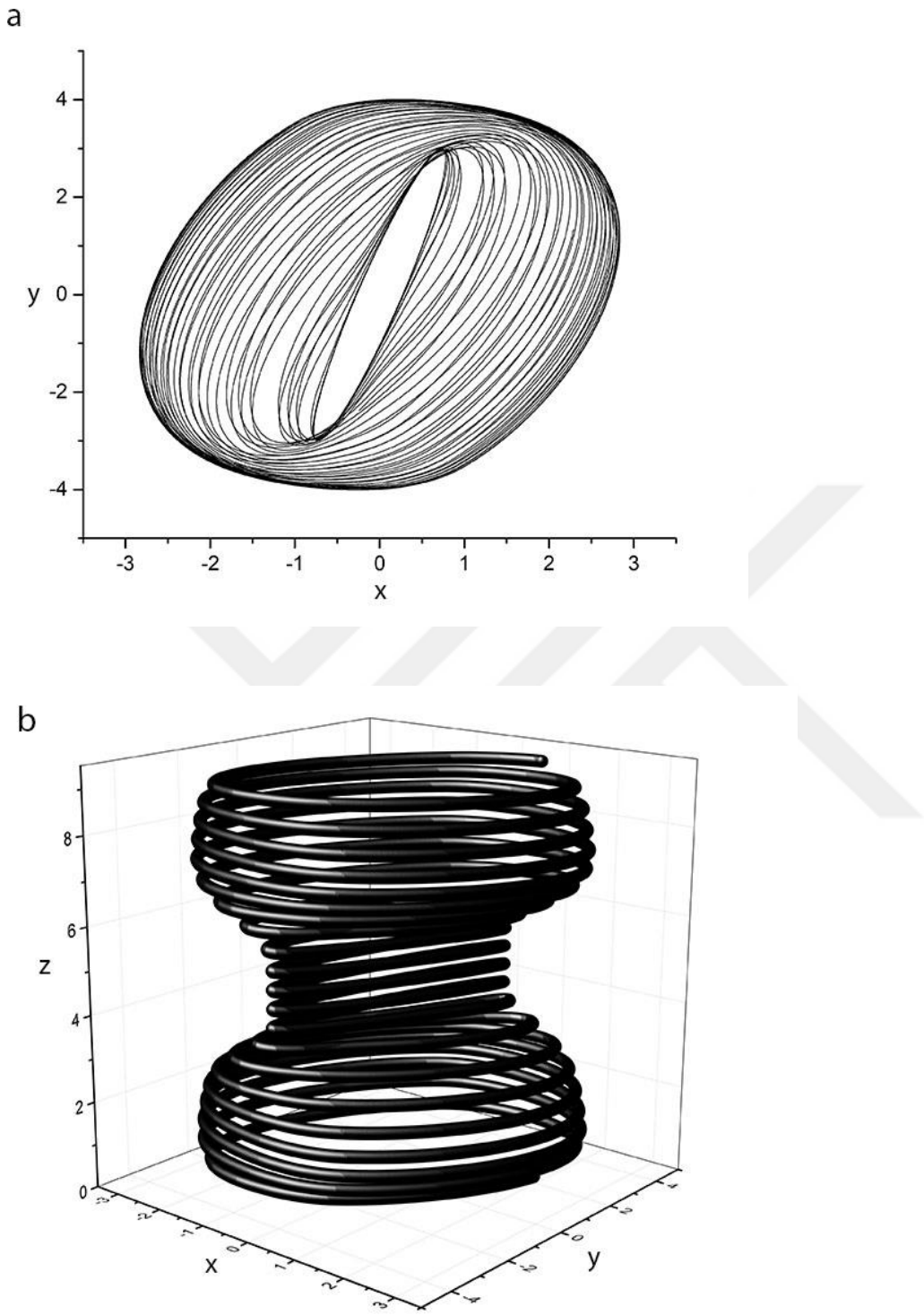

Şekil 3.22. Başlangıç parametreleri $a=-3{,}13, b=2{,}68, \beta=7{,}67, f=-1{,}81, \omega=-0{,}94$ ve $\phi=-5{,}52$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir



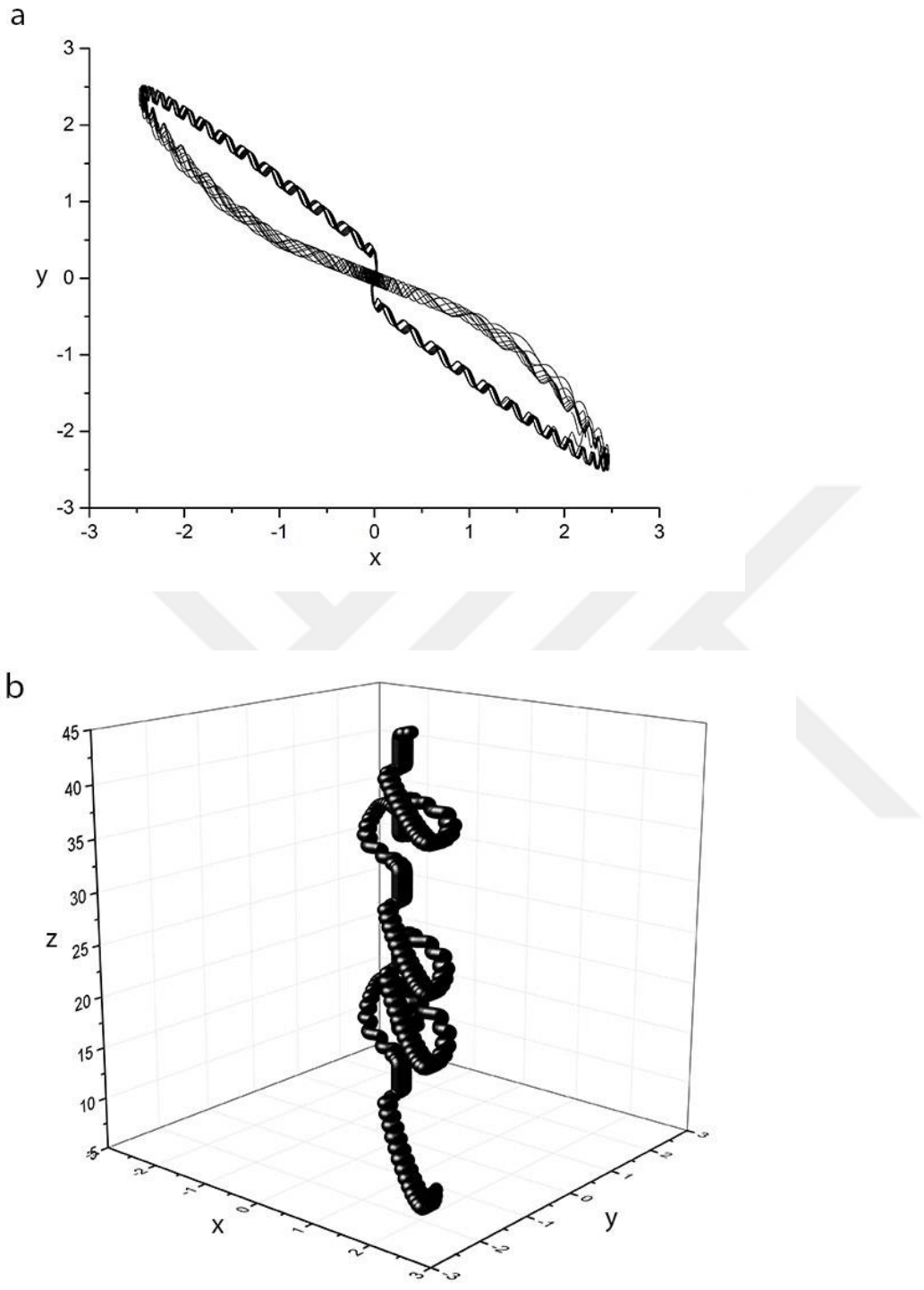

Şekil 3.23. Başlangıç parametreleri $a=-7{,}11, b=0{,}66, \beta=4{,}65, f=1{,}86, \omega=-19{,}93$ ve $\phi=5{,}53$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir



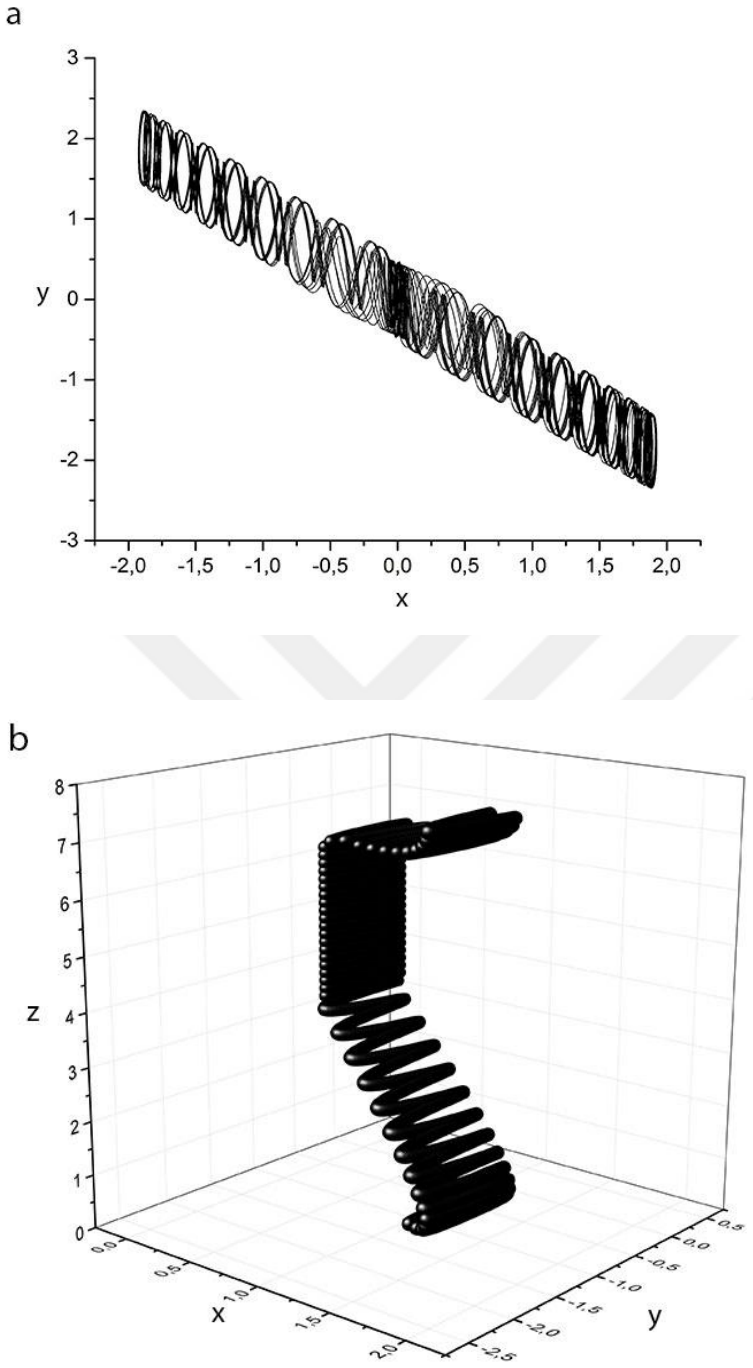

Şekil 3.24. Başlangıç parametreleri $a=-4{,}31, b=2{,}68, \beta=9{,}61, f=-8{,}17, \omega=-13{,}61$ ve $\phi=-1{,}33$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir.



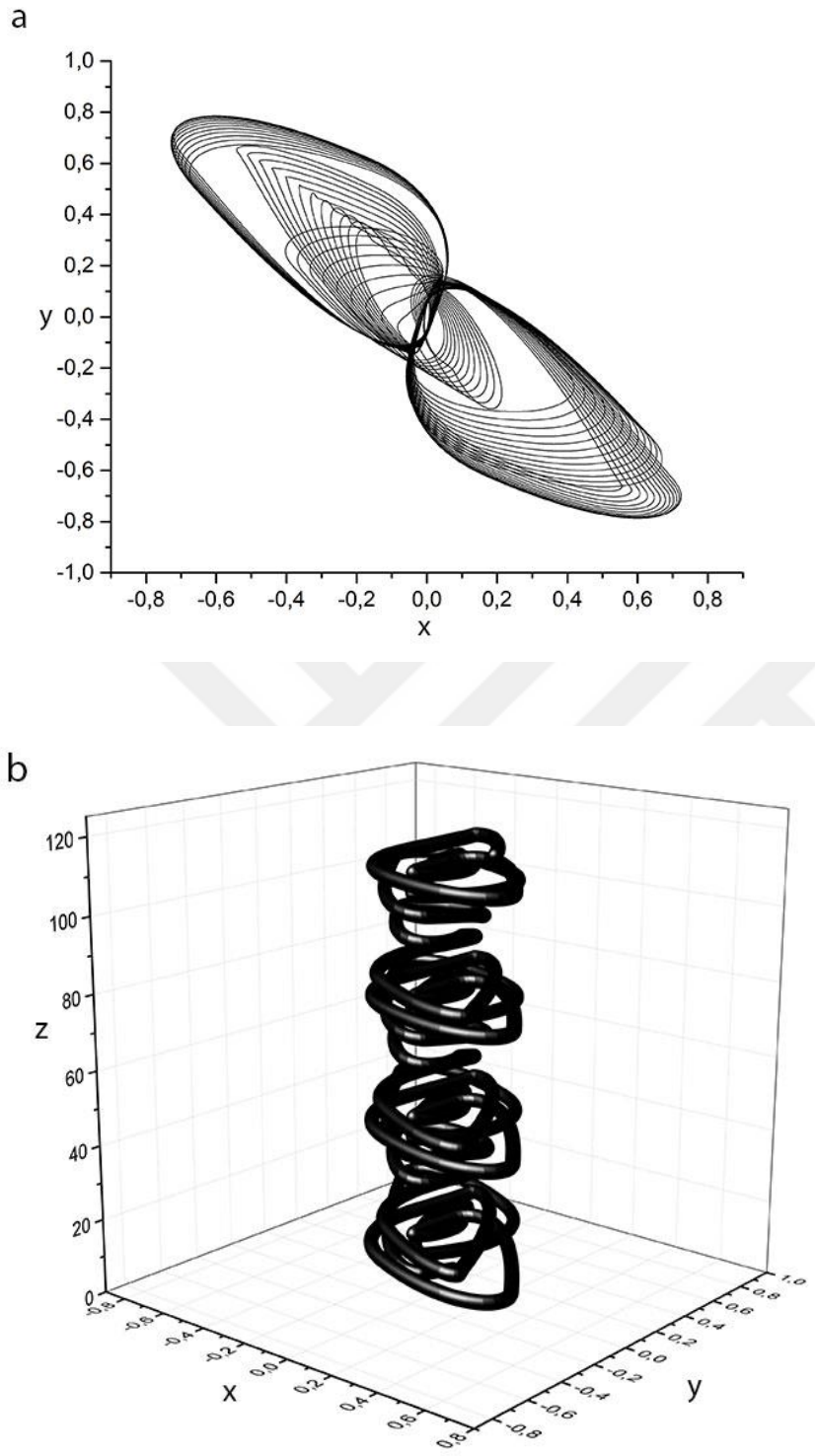

Şekil 3.25. Başlangıç parametreleri $a=-1{,}09, b=1{,}24, \beta=0{,}66, f=-4{,}49, \omega=1{,}33$ ve $\phi=0{,}09$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir.



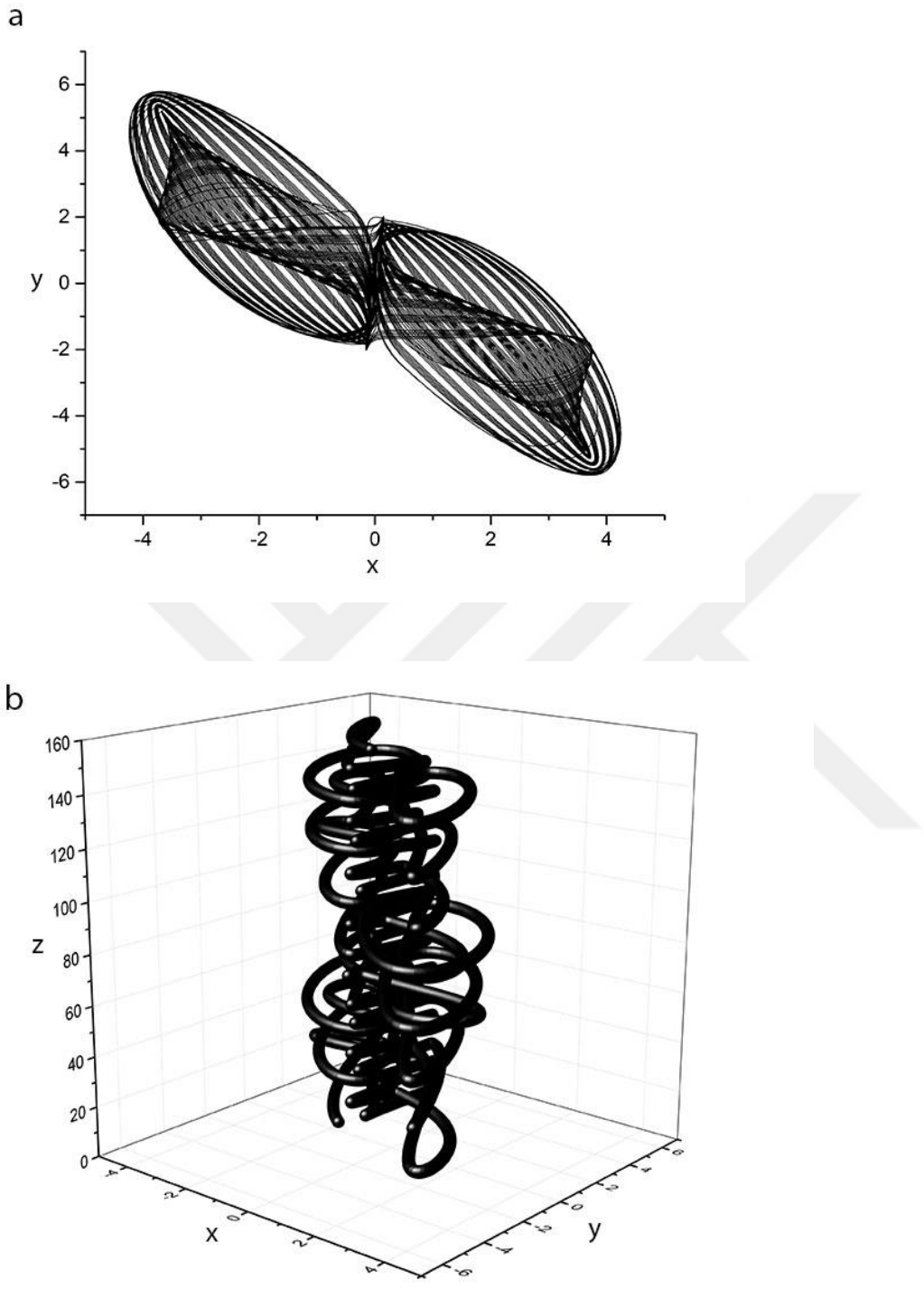

Şekil 3.26. Başlangıç parametreleri $a=-3{,}31, b=0{,}62, \beta=2{,}65, f=-1{,}86, \omega=19{,}36$ ve $\phi=0{,}37$ olan periyodik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir.



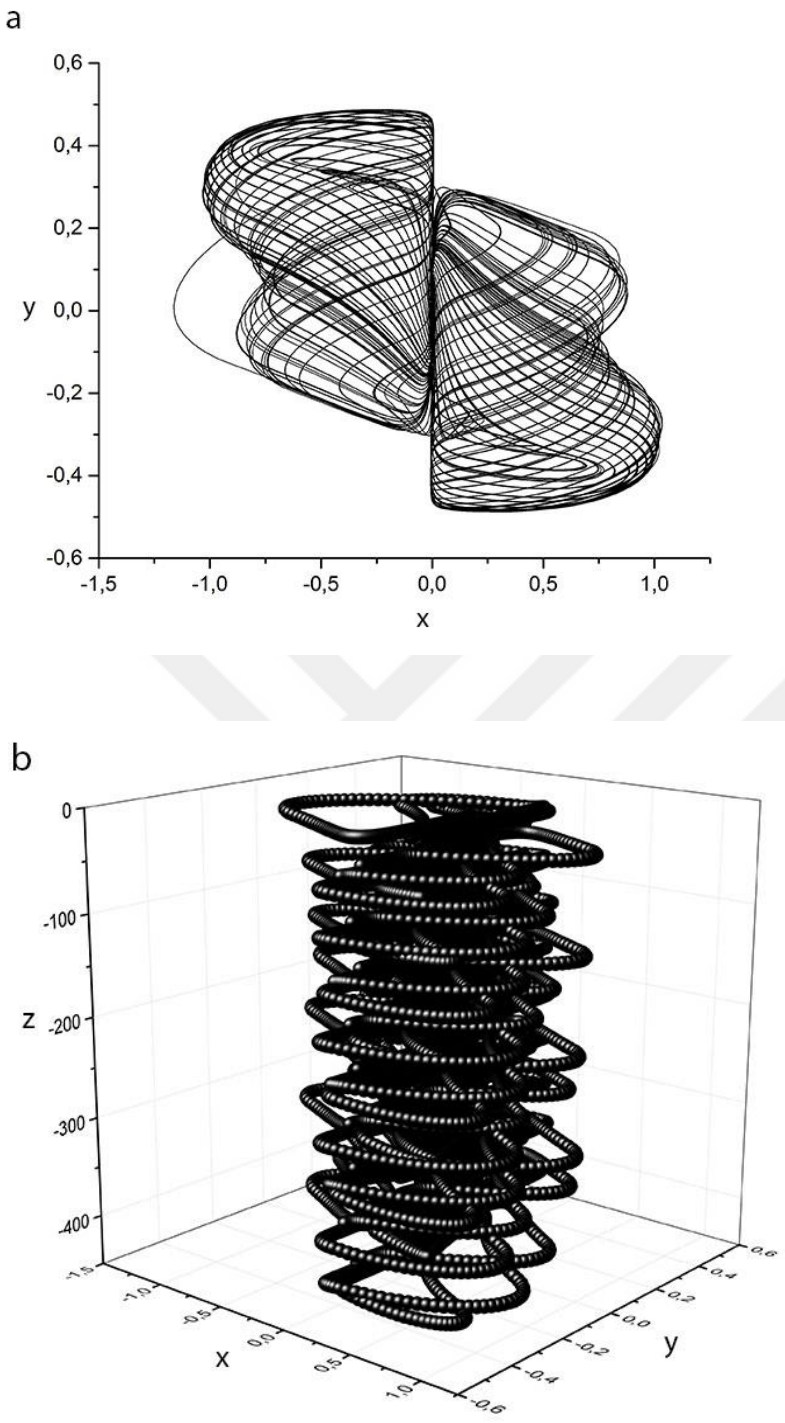

Şekil 3.27. Başlangıç parametreleri $a=-4{,}31, b=2{,}68, \beta=9{,}66, f=-7{,}27, \omega=-13{,}61$ ve $\phi=0{,}33$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir.



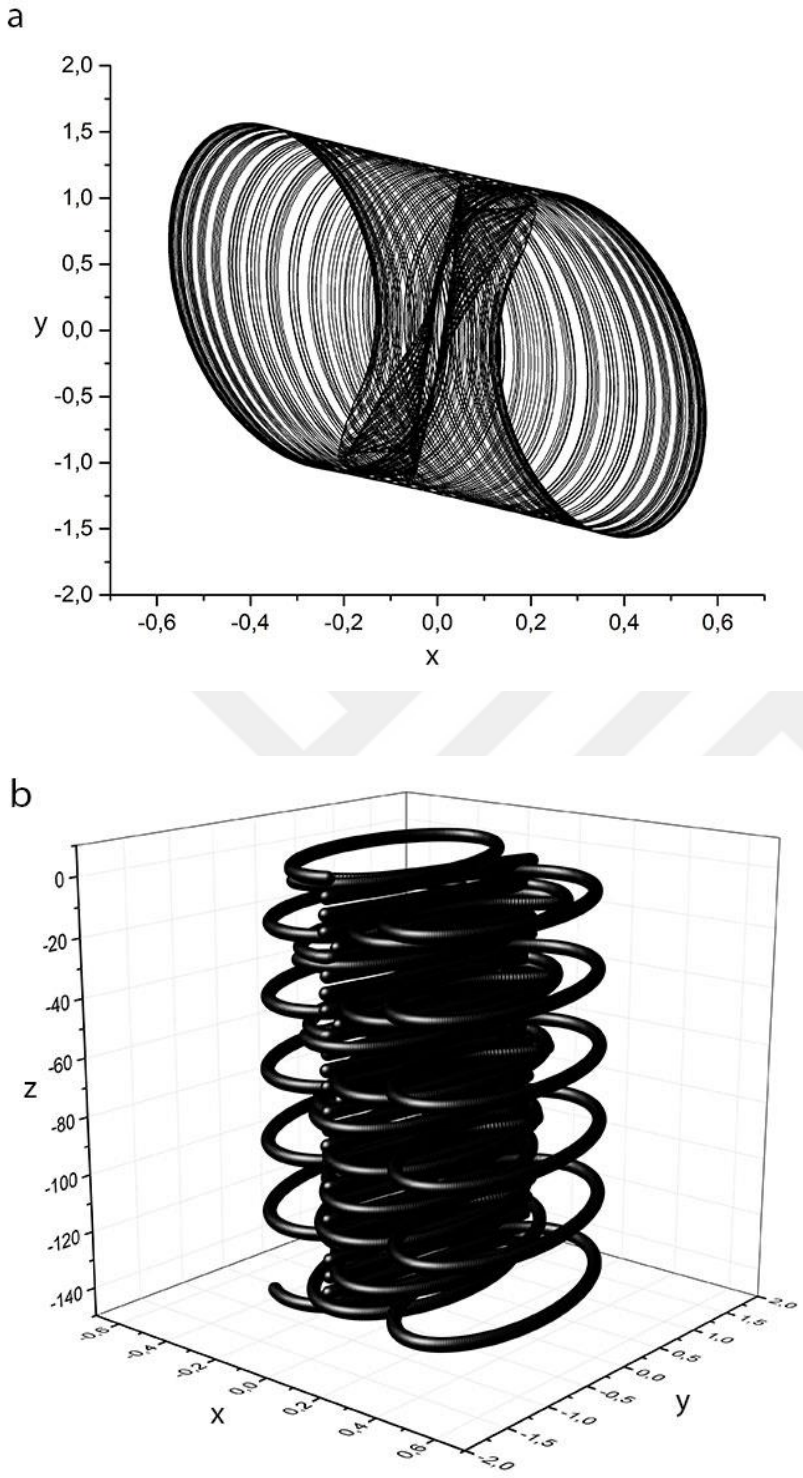

Şekil 3.28. Başlangıç parametreleri $a=-1{,}39, b=1{,}24, \beta=2{,}66,\ f=-0{,}49, \omega=1{,}33$ ve $\phi=1{,}11$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir



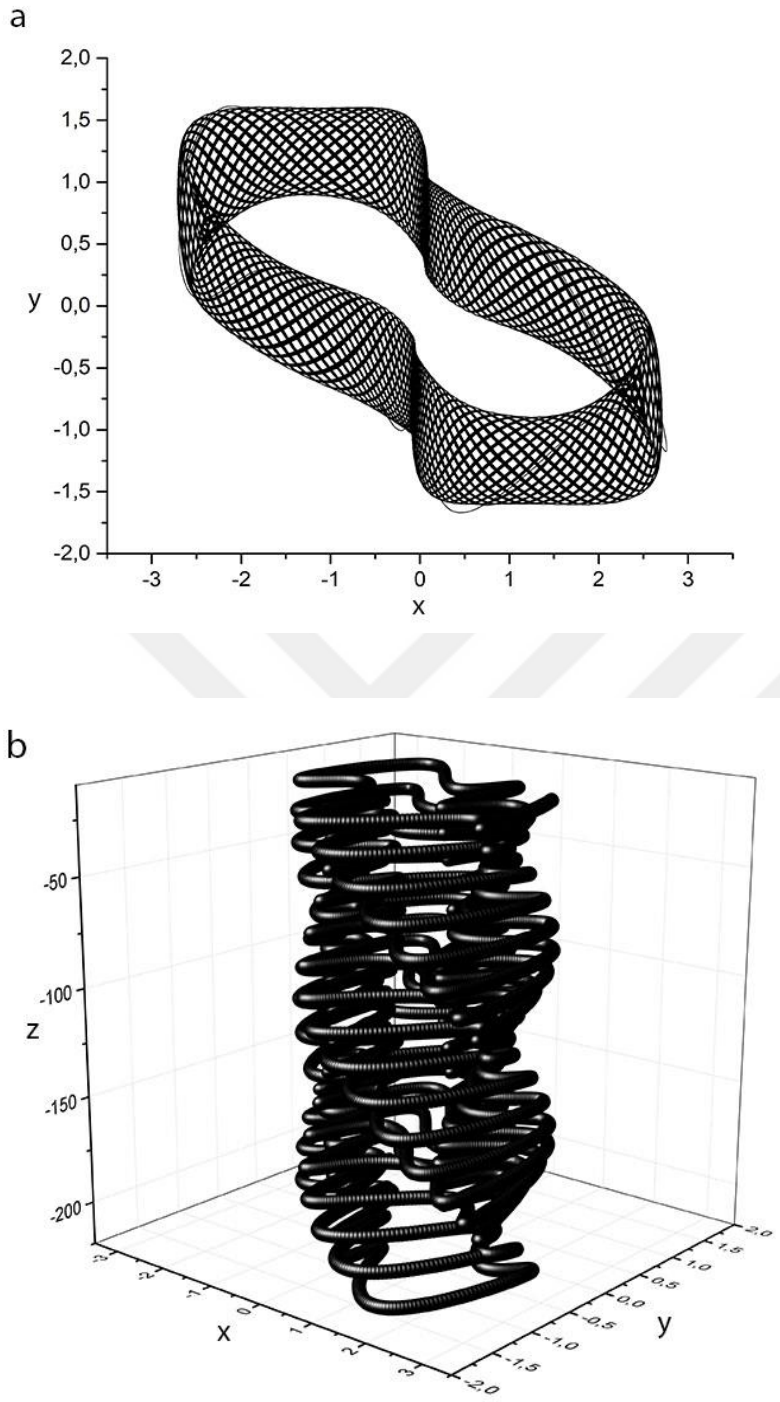

Şekil 3.29. Başlangıç parametreleri $a=-10{,}1, b=1{,}24, \beta=5{,}69, f=-13{,}17, \omega=3{,}92$ ve $\phi=2{,}39$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir



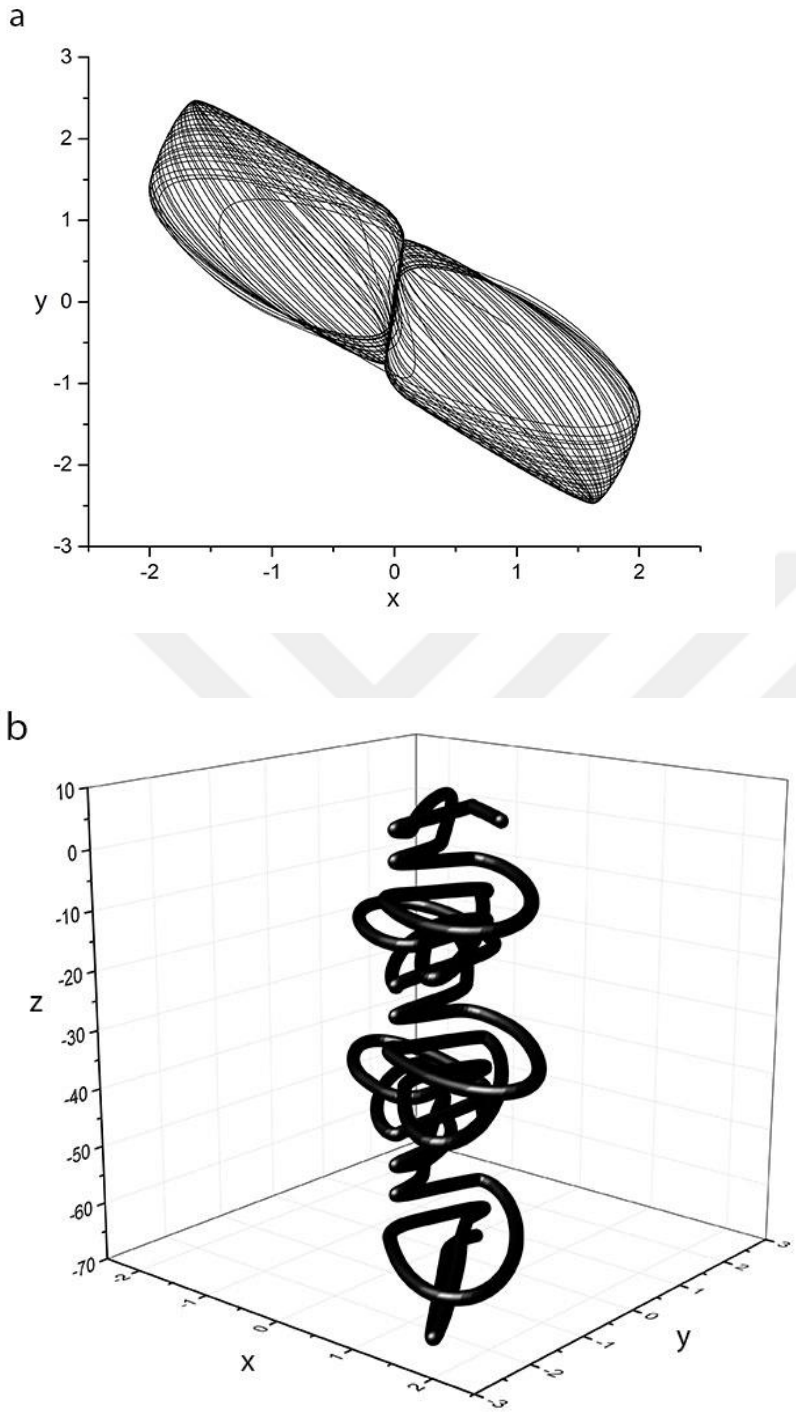

Şekil 3.30. Başlangıç parametreleri $a=-15{,}81, b=21{,}62, \beta=1{,}65, f=-1{,}86, \omega=-8{,}36$ ve $\phi=-7{,}37$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir



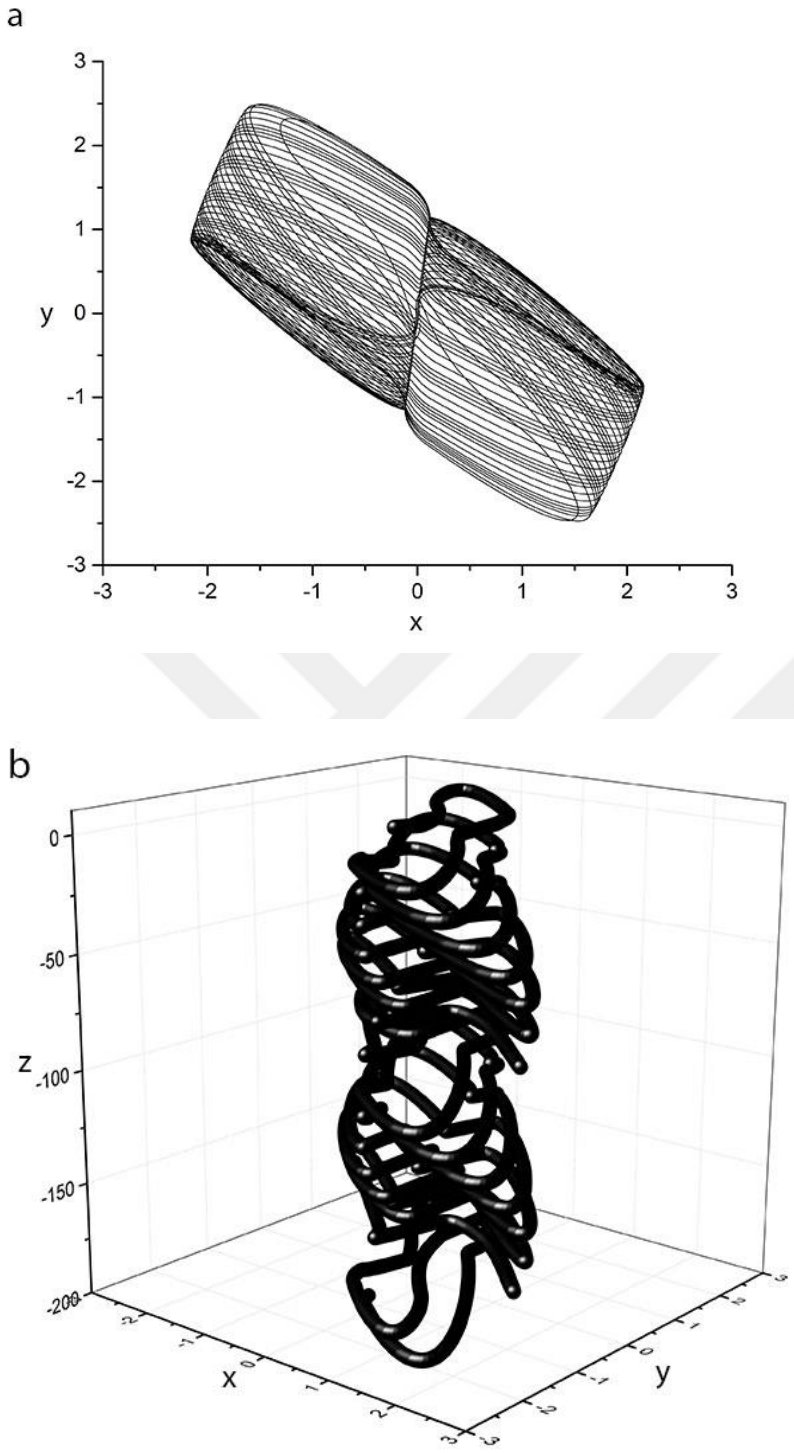

Şekil 3.31. Başlangıç parametreleri $a=-1{,}13, b=9{,}68, \beta=3{,}67, f=6{,}81, \omega=-4{,}94$ ve $\phi=-2{,}19$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir




Şekil 3.32. Başlangıç parametreleri $a=-7{,}11, b=0{,}62, \beta=1{,}65, f=-5{,}86, \omega=-13{,}93$ ve $\phi=-4{,}53$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir




Şekil 3.33. Başlangıç parametreleri $a=-4{,}31, b=2{,}68, \beta=9{,}61, f=-8{,}17, \omega=-1{,}61$ ve $\phi=-1{,}31$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir.




Şekil 3.34. Başlangıç parametreleri $a=-4{,}31, b=2{,}68, \beta=9{,}61, f=-12{,}17, \omega=-0{,}61$ ve $\phi=-1{,}31$ olan kaotik çekicinin 2 boyutlu (a) ve 3 boyutlu (b) gösterimleridir.

Kaotik çekicileri göstermek tek başına bir sistemin kaotik olduğunu göstermez. Bir sistemin kaotik olduğunu göstermek için literatürde birçok yöntem ileri sürülmüştür. Lyapunov üstelleri yöntemi kullanılarak sistemin kaotik davranışlar sergilediği gösterilebilir [84]. Sistemin kaotik davranışı, başlangıç parametrelerine bağlı olarak değişir. Dolayısıyla sistemin kaotik yapıda olmasını sağlamak için başlangıç parametreleri özel olarak belirlenmelidir. Belirli başlangıç parametreleri ile sistem hem periyodik özellik hem de kaotik özellik gösterebilir. $a=-1{,}05, b=-0{,}57, \beta=1{,}0, \phi=1{,}0, \omega=1{,}0$ ve $f=1{,}5$ başlangıç parametreleri için DCD periyodik özellik gösterirken $a=-1{,}05, b=-0{,}57, \beta=1{,}0, \phi=1{,}0, \omega=1{,}0$ ve $f=0{,}33$ için kaotik özellik gösterir [26]. Genel olarak sürüş genliği $f$'nin $0{,}24-0{,}84$ aralığında değerleri için sistem periyodik özellik gösterir. $0{,}84$'ün yukarısında ise sistemde kaotik davranışlar baskınlık gösterir.

# 4. KAOS TABANLI GÖRÜNTÜ ŞİFRELEME SİSTEMİ

## 4.1. Gizli Anahtar Üretimi

Şifreleme sistemleri genel olarak asimetrik şifreleme ve simetrik şifreleme olmak üzere 2' ye ayrılır. Asimetrik şifrelemede açık anahtarlı şifreleme yapılırken, simetrik şifreleme de gizli anahtar ile şifreleme yapılır. Bu gizli anahtarın haberleşen iki taraftan başka üçüncü herhangi bir şahsın eline geçmesi istenmez. Dolayısıyla simetrik şifreleme de gizli anahtar oldukça önemlidir.

SHA-256 geleneksel kriptografik karma algoritmasıdır ve 256 bitlik bir çıktı üretir [27, 28]. Bu değer SHA-256 algoritmasının girdisindeki en ufak bir değişiklik sonucu tamamen değişir. Dolayısıyla gizli anahtar üretimi için bu algoritma kullanılabilir. Bu sistem için gizli anahtar üretimi SHA-256 algoritması yardımıyla aşağıdaki gibi tasarlanır.

İlk olarak, orijinal görüntüden birtakım çıktılar üretilir. Bu çıktılar aşağıdaki algoritmalar yardımıyla yapılır:

*Resim-A* şifrelenecek herhangi bir renkli görüntü olacak şekilde aşağıdaki 3 algoritmanın da girdisini oluşturur.

Satır Toplama Algoritması

```
function satirToplam = satirToplama(Resim - A)
[r, n, k] = size(Resim – A)
for i = 1: r
    if i == 1
        satirToplam(i) = mod(sum(Resim – A(i,:)),256);
    else
        satirToplam(i) = bitxor(satirToplam(i – 1), mod(sum(Resim – A(i,:)),256));
    end
end
end
```

Sütun Toplama Algoritması

```
function sutunToplam = sutunToplama(Resim - A)
[r, n, k] = size(Resim – A)
for i = 1 : r
    if i == 1
        sutunToplam(i) = mod(sum(Resim – A(:, i)),256);
    else
        sutunToplam(i) = bitxor(sutunToplam(i – 1), mod(sum(Resim – A(:, i)),256));
    end
end
end
```

Renk Bileşenleri Toplama Algoritması

```
function [RGToplam, RBToplam, BGToplam, RGBToplam] = RGBToplamalar(Resim - A)
Resim – AR = Resim – A(:, :,1)
Resim – AG = Resim – A(:, :, 2)
Resim – AB = Resim – A(:, :, 3)
RGToplam = bitxor(mod(sum(Resim – AR(:)),256), mod(sum(Resim – AG(:)),256))
RBToplam = bitxor(mod(sum(Resim – AR(:)),256), mod(sum(Resim – AB(:)),256))
BGToplam = bitxor(mod(sum(Resim – AB(:)),256), mod(sum(Resim – AG(:)),256))
RGBToplam = bitxor(bitxor(mod(sum(Resim – AR(:)),256), mod(sum(Resim – AG(:)),256)),
                   mod(sum(Resim – AB(:)),256))
end
```

Yukarıdaki 3 algoritmanın kullanılmasındaki asıl amaç resmin herhangi bir yerinde meydana gelen en ufak bir değişikliğin gizli anahtar üretimini tamamen etkileyecek şekilde tüm anahtara yansımasını sağlamaktır. Yukarıda belirtilen fonksiyonlar MatLab'da oluşturulmuştur.

Gizli Anahtar Üretimi Algoritması

```
function gizliAnahtar = gizliAnahtarUretimi(Resim - A)
[r,n,k] = size(Resim - A)
satirToplamBin = de2bi(satirToplam(r),8)
sutunToplamBin = de2bi(sutunToplam(n),8)
RGToplamBin = de2bi(RGToplam,8)
RBToplamBin = de2bi(RBToplam,8)
BGToplamBin = de2bi(BGToplam,8)
RGBToplamBin = de2bi(RGBToplam,8)
gizliAnahtarBin = [satirToplamBin, sutunToplamBin, RGToplamBin, RBToplamBin,
                   BGToplamBin, RGBToplamBin]
gizliAnahtar = binaryVectorToHex(gizliAnahtarBin)
end
```

MatLab ortamında kodlanmış gizli anahtar üretimi algoritmasında, satır toplama, sütun toplama ve renk bileşenleri toplama algoritmaları ile açık görüntüden elde edilen çıktılar kullanılarak gizli anahtar oluşturulmuştur. Bu fonksiyonda öncelikle önceki fonksiyonlardan elde edilen çıktılar ikili sayı sistemine dönüştürülmüş ve sonrasında uç uca eklenerek birleştirilmiş ve ikili sistemde tek bir sayı üretilmiştir. Bu sayı 16'lık sisteme dönüştürülmüş ve gizli anahtar elde edilmiştir. Son olarak bu üretilen gizli anahtar aşağıdaki işlemden geçirilmiştir.

Tek Seferlik Gizli Anahtar Üretimi Algoritması

```
function tekSeferlikGizliAnahtar = tekSeferlikGizliAnahtarUretimi
rastgeleBinGurultu = randi([0 1],16,1)'
rastgeleGurultu = binaryVectorToHex(rastgeleBinGurultu)
tekSeferlikGizliAnahtar = strcat(gizliAnahtar, rastgeleGurultu)
end
```

Yukarıdaki algoritmada, üretilen gizli anahtara rastgele gürültü ekleyerek gizli anahtarın tek seferlik oluşturulmasını sağlıyoruz. Yani her şifreleme aşamasında bu gürültü anahtara

eklendiği zaman, şifrelenecek görüntü değişmese bile gizli anahtar her seferinde değişecektir.

SHA-256 gizli anahtar üretimi için yararlanılan elverişli bir algoritmadır. Bu algoritmanın girdisindeki en ufak değişiklik çıktısını tamamen değiştirir. Her şifreleme işlemi için yukarıda oluşturduğumuz tek seferlik anahtarı bu SHA-256 algoritmasına girdi olarak tanımlarsak elde ettiğimiz çıktı her seferinde bambaşka olacaktır. Böylelikle şifreleme sistemi, seçilmiş açık metin saldırısı, bilinen açık metin saldırısı gibi ataklara karşı dirençli olur.

Üretilen gizli anahtarın *GA* matematiksel gösterimi aşağıdaki şekilde yapılabilir:

$$GA = \left\lfloor h_1, h_2, \ldots, h_{64} \right\rfloor, \quad \exists i \in [1,2,\ldots,64] \quad \forall h_i \in [0-9], [A-F] \tag{4.1}$$

## 4.2. Gizli Anahtar Üzerinden Kaotik Üretecin Başlangıç Koşullarının Elde Edilmesi

Kaotik bir sistemin başlangıç koşullarına hassas biçimde bağlı olması bu sistemleri şifreleme için oldukça önemli kılıyor. Dolayısıyla şifreleme sistemine verilen gizli anahtardan kaotik sistemin başlangıç koşulları elde edilirken, anahtardaki en ufak değişikliğin başlangıç koşullarına mümkün olduğunca büyük yansımaları olması gerekmektedir. Böylelikle gizli anahtardaki en ufak bir değişikliğin sistemin başlangıç koşullarına büyük etkisi olacaktır. Bu da şifreleme sistemini bilinen açık metin saldırısı gibi ataklara karşı dirençli hale getirecektir.

Eş. 3.1 için başlangıç parametreleri $x_1, y_1, z_1, v_1$ ve başlangıç değeri $f$ aşağıdaki gibi üretilir:

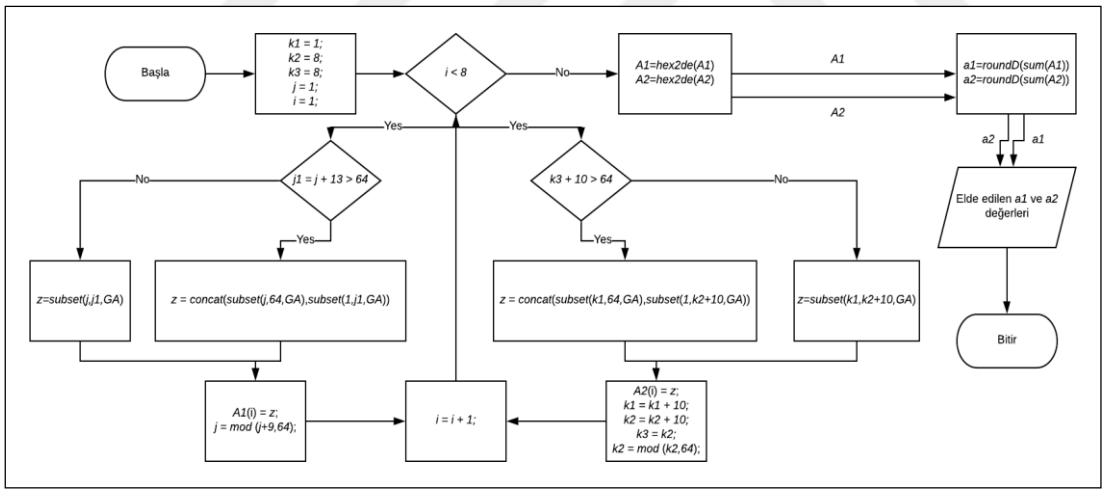
$$\begin{cases} x_1' = \left(hex2de\left(subset(1,10,GA)\right)x10^{-11}\right) + \left(hex2de\left(subset(11,16,GA)\right)x10^{-14}\right) \\ y_1' = \left(hex2de\left(subset(17,26,GA)\right)x10^{-11}\right) + \left(hex2de\left(subset(27,32,GA)\right)x10^{-14}\right) \\ z_1' = \left(hex2de\left(subset(33,42,GA)\right)x10^{-11}\right) + \left(hex2de\left(subset(43,48,GA)\right)x10^{-14}\right) \\ v_1' = \left(hex2de\left(subset(49,58,GA)\right)x10^{-11}\right) + \left(hex2de\left(subset(59,64,GA)\right)x10^{-14}\right) \end{cases} \tag{4.2}$$

Burada $subset\,(i, j, K)$ fonksiyonu *K* sayı dizisinin *i*. ve *j*. elemanları arasındaki sayı dizisini döndürür. Diğer yandan *hex2de* fonksiyonu girilen onaltılık sayıyı onluk tabana çevirir.

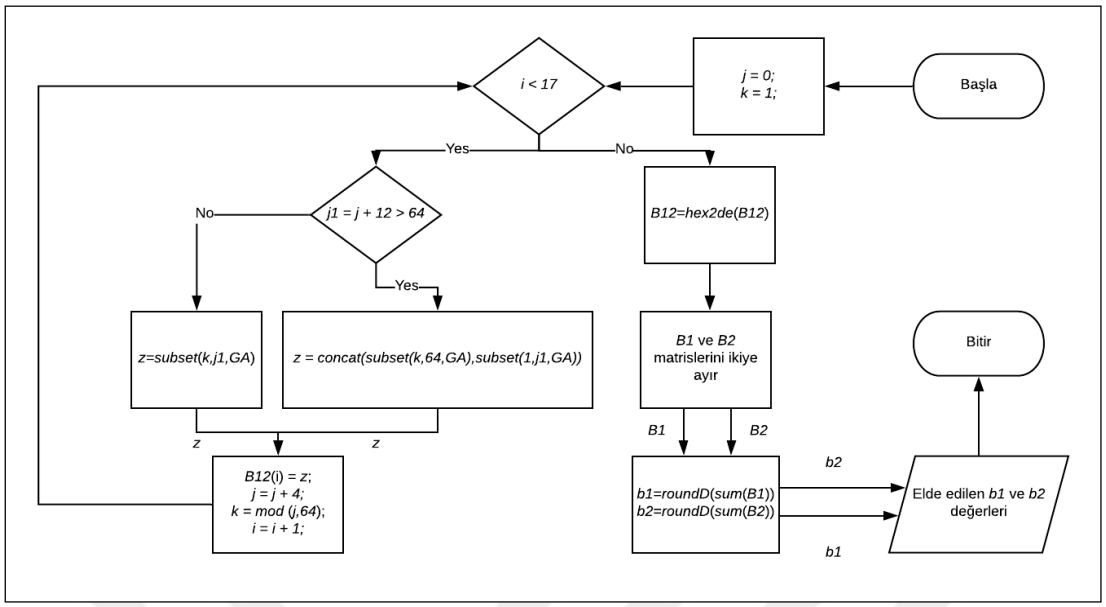
Eş. 4.2' de $10^{-11}$ ve $10^{-14}$ ile çarpma işlemini belirlerken $x_1', y_1', z_1', v_1'$ sayılarının ondalık kısımlarını ayarlamak göz önünde bulundurulmuştur.

$$\begin{cases} x_1 = x_1'(2 - a_1) \\ y_1 = y_1'(2 - a_2) \\ z_1 = z_1'(2 - b_1) \\ v_1 = v_1'(2 - b_2) \\ f = 0.84 + a_1 \end{cases} \tag{4.3}$$

Eş. 4.3' de $a_1, a_2, b_1, b_2$ değerleri 0 ile 1 arasında olacak şekilde aşağıdaki akış diyagramları yardımıyla elde edilir. Diğer yandan 0.84 değeri, Eş. 3.1' in kaotik özellik sergilediği en küçük *f* değeridir. Kaotik sistem *f* parametresine hassas bağlı olduğu için bu başlangıç değeri her şifreleme işlemi için 0.84 ile 1.84 arasında değişmektedir. $2 - a_{1,2}$ ve $2 - b_{1,2}$ değerleri ile çarpma işleminin yapılması, $x_1', y_1', z_1', v_1'$ değerlerinin çarpma işlemi ile küçültülmemesi içindir. Çünkü $a_{1,2} < 1$ ve $b_{1,2} < 1$ iken $2 - a_{1,2} > 1$ ve $2 - b_{1,2} > 1$ olur.




Şekil 4.1. $a_1, a_2 \in [0,1]$ reel sayılarının elde edildiği akış diyagramı



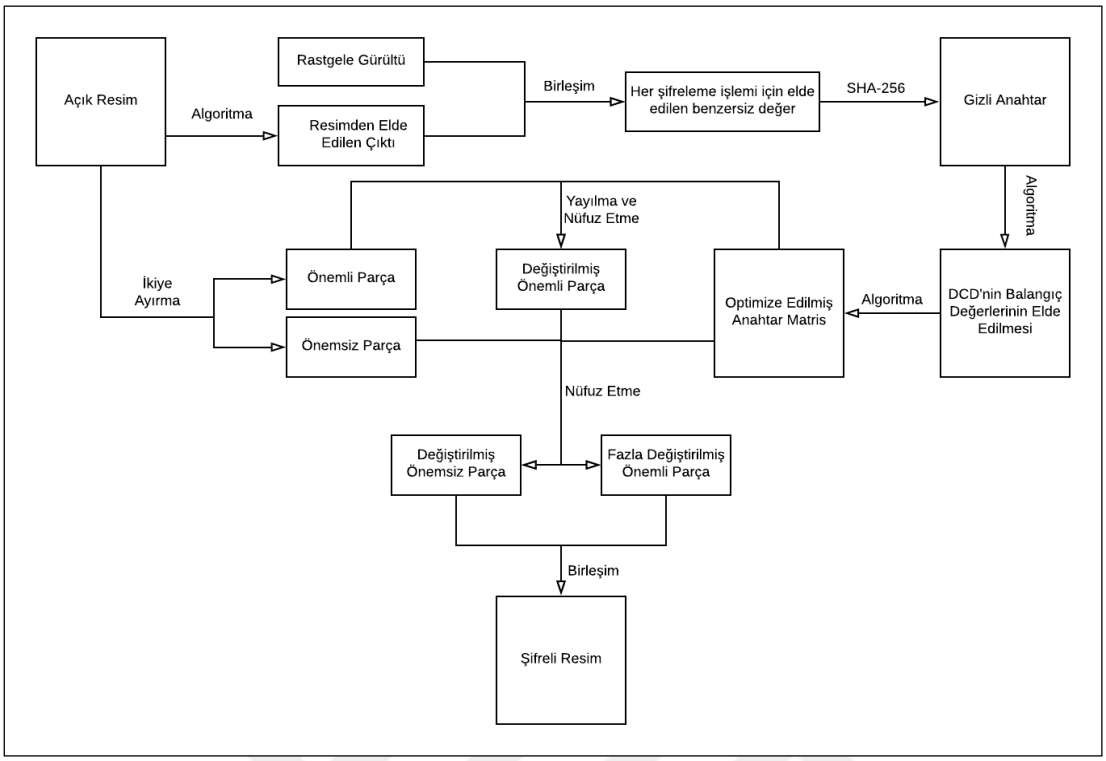

Şekil 4.2. $b_1, b_2 \in [0,1]$ reel sayılarının elde edildiği akış diyagramı

Yukarıda Şekil 4.1 ve Şekil 4.2 program şemalarında kullanılan *subset*, *hex2de* fonksiyonlarına yukarıda değinilmiştir. Burada, *concat* fonksiyonu verilen değerleri birleştirirken *roundD* fonksiyonu ise verilen reel sayının ondalık kısmını döndürür. Örnek olarak 3,9375 sayısı için *concat*(3,9375) = 0,9375 olur. Diğer yandan *sum* fonksiyonu girilen sayı dizisinin toplamını verir. Fonksiyon *mod* ise bilinen mod alma operatörüdür.

Burada $a_1, a_2, b_1, b_2$ değerlerinin üretilme sebebi, gizli anahtarda meydana gelecek en ufak değişikliğin Eş. 3.1 için üretilen başlangıç parametrelerine en iyi şekilde yansıyabilmesini sağlayabilmektir. Böylelikle gizli anahtar üzerinden yapılacak saldırılara karşı sisteme direnç kazandırılmış olur.

### 4.3. Şifreleme Algoritması

Tasarlanmak istenilen şifreleme sisteminde, belirli bir aşamaya kadar gizli anahtarın üretimi ve o anahtarın sisteme sağlanmasıyla üretilecek çıktılar için kaotik sistemin başlangıç parametrelerinin elde edilmesini gerçekleştirdik. Bu aşamada elde edilen kaotik dizilerin belirli işlemler altında geliştirilmesi ve açık resim ile belirli matematiksel işlemlere tabi tutulmasıyla şifrelenmiş görüntü elde edilir. Aşağıda şifreleme sisteminin akış diyagramı gösterilmektedir.




Şekil 4.3. Şifreleme işleminin akış diyagramı

Şekil 4.3’ de açık resimden şifreli resim elde edilene kadar geçen tüm aşamaların akış diyagramı gösterilmektedir. Yani şifreleme sisteminin genel bir görüntüsüdür. Bu sistemde şekilde görüldüğü gibi ilk olarak açık görüntüden bazı çıktılar elde edilir ve bu çıktılara rastgele gürültü eklenerek bir ön anahtar oluşturulur. Bu ön anahtar daha sonra SHA-256 algoritmasına tabi tutularak 16’ lık tabanda 64 basamaklı bir gizli anahtar üretilir. Daha sonra bu anahtardan kaotik sistemin başlangıç parametreleri elde edilir. Hem açık resimden elde edilen benzersiz bilgi, hem de SHA-256 sayesinde, orijinal görüntüde çok küçük bir değişiklik yaşansa bile, şifreleme için elde edilen anahtar bir öncekinden çok başka olur dolayısıyla üretilen başlangıç parametrelerinin oldukça farklılaşması sağlanır. Diğer yandan orijinal görüntü hiçbir değişiklik yapılmadan tekrar şifrelenmek istense bile, rastgele gürültü ve SHA-256 sayesinde anahtar tamamen değişecektir. Sonuç olarak, çok küçük bile olsa anahtardaki bu değişim, başlangıç parametrelerinin üretilmesi için kullanılan algoritma sayesinde, tüm başlangıç değerlerine tesir edecektir. Başlangıç değerlerine hassas bağlı olan kaotik sistem yardımıyla da, her seferinde bambaşka sayı dizileri elde edilecek ve böylelikle şifreleme sistemi güvenilir bir sistem haline gelecektir.

Şifreleme sisteminin tamamının ve tasarlanan şifreleme algoritmasının gösterimi şu şekildedir:

*Şifreleme Sistemi*

Girdi: Açık Resim *AR*

Çıktı: Şifrelenmiş Resim *SR*, Gizli Anahtar *GA*

Şifrelenecek görüntüdeki toplam piksel sayısı bizim kaotik üretecimizden sayı üretirken kullanacağımız bir referans olacaktır. Dolayısıyla ilk olarak piksel sayısını hesaplarız.

Şifrelenecek görüntünün (*AR*) dikey ve yatay büyüklükleri sırasıyla *D* ve *Y* olsun. Bu renkli görüntünün toplam boyutu $D\,x\,Y\,x3$ olur. Buna göre görüntüdeki toplam piksel sayısı *s* aşağıdaki gibi hesaplanır:

$$s = DxYx3 \tag{4.4}$$

*Gizli anahtar üretimi*:

1.Adım: Yukarıda tanımlanan algoritmaları kullanarak Eş. 4.1'i yani *GA* gizli anahtarını elde et.

Üretilen bu gizli anahtar *GA*, şifreleme sisteminin çıktılarından biridir.

*Şifreleme algoritması*:

Girdi: Açık Resim *AR*, Gizli Anahtar *GA*

Çıktı: Şifrelenmiş Resim *SR*

2.Adım (*Başlangıç parametrelerin edinimi*): Eş. 3.1' deki diferansiyel denklemlerin başlangıç değerleri $x_1, y_1, z_1, v_1, f$ , Eş. 4.2 ve Eş. 4.3'ü kullanarak elde et.

3.Adım: Belirlenen başlangıç değerlerini kullanarak iterasyon yöntemi yardımıyla Eş. 3.1'i çözdür ve $(4s)+5000$ adet kaotik sayı dizisi *KD*'yi üret. Bu üretilen sayı dizisinden şifreleme sistemine olumsuz etki yapabilecek ilk 1000 sayıyı kaldır.

$$\begin{aligned} &n = 4s \\ &ks = n + 4000 \\ &KD = kd_i, \ \ \exists i \in [1,2,...,ks], \ \forall kd_i \in IR \end{aligned} \tag{4.5}$$

4.Adım: Üretilen kaotik sayı dizisi *KD*'yi kullanarak, karıştırma ve nüfuz etme işlemleri için kullanılacak tek bir optimize edilmiş anahtar matris *OM*'yi üret.

| Anahtar Matris Üretme Algoritması |
|---|
| $for\, i = 1 : ks$<br>$\quad KD(i) = abs((KD(i) - round(KD(i),6) * 10\text{^}6));$<br>$end$<br>$KD' = unique(KD);$<br>$KD'' = subset(1, n, KD');$<br>$OM = sort(KD'')$ |

Burada $KD(i)$, *KD* sayı dizisinin *i*. elemanını temsil eder. Diğer yandan *round* fonksiyonu ilk parametresinde verilen sayıyı, ikinci parametresinde verilen ondalık basamağına göre en yakın sayıya yuvarlar. Fonksiyon *abs* mutlak değer operatörüyken, '^' ise bilinen üs alma operatörüdür. Fonksiyon *unique*, parametresi bir sayı dizisi olacak şekilde, bu sayı dizisinin tekrar eden elemanlarını siler. Fonksiyon *subset*, üçüncü parametresinde verilen sayı dizisini birinci ve ikinci parametresinde verilen indis numaraları aralığında döndürür. İndis numarası pozitif tam sayı olmalıdır. Son olarak *sort* fonksiyonu, girilen sayı dizisini küçükten büyüğe doğru sıralayarak bu sayı dizisinin elemanlarının yeni indis numaralarını döndürür. Böylelikle elde edilen *OM* optimize edilmiş anahtar matrisi 1 ile *n* arasında *n* adet tekrarsız tamsayıdan oluşur.

$$\begin{aligned} &\forall i, j \in [1,2,...,n], \\ &OM = [om_1, om_2, ...om_n], km_i \in [1,n], Z^+, \\ &\forall i \neq j \Rightarrow \forall om_i \neq om_j \end{aligned} \tag{4.6}$$

5.Adım: Açık renkli resmi (*AR),* bileşen K' dan başlayarak önce yukarıdan aşağıya sonra soldan sağa doğru tarayıp, sırasıyla Y ve M bileşenlerine de aynı işlemi uygulayarak resmi tek sütunlu bir matris olarak yeniden boyutlandır. Böylelikle elde edilen yeni boyutlandırılmış görüntü 1 adet sütun ve $s$ adet satırdan oluşur. Daha sonra her bir satırdaki pikseli 8-bitlik ikili sayı düzenine çevir. Sonuç olarak elde edilen yeniden boyutlandırılmış ikili düzende gösterilen resmin pikselleri 8 adet sütun ve $s$ adet satırdan meydana gelir.

| Dönüştürme Algoritması |
|---|
| $AR' = reshape(AR, n, 1)$<br>$for\ i = 1:n$<br>$IAR(i;1:8) = de2bi(AR'(i), 8)$<br>$end$ |

Burada *reshape* fonksiyonu girilen parametre değerlerine göre resmi yeniden boyutlandırırken *de2bi* fonksiyonu da ilk parametrede girilen onluk sistem tabanındaki değeri ikinci parametrede verilen uzunluk değerine göre ikilik sayı düzenine dönüştürür.

$AR'$ matrisindeki her bir piksel değerinin ayrı ayrı ikili düzende gösterimindeki ilk basamağı, $AR'$ ile aynı satır numarasına karşılık gelecek şekilde *IAR* matrisinin ilk sütununu oluşturur. Sırasıyla 2. basamak, *IAR* matrisinin 2. sütununu oluşturur ve mantık 8. basamağa kadar aynı şekilde ilerler.

6.Adım: *IAR* matrisini dikey biçimde ortadan ikiye ayır.

| Görüntünün Önemsiz Yarısını Ayırma Algoritması |
|---|
| $for\ j = 1:4$<br>  $for\ i = 1:n$<br>  $IAR_1(i, j) = IAR(i, j)$<br>  end<br>end |

| Görüntünün Önemli Yarısını Ayırma Algoritması |
|---|
| $for\ \ j = 5:8$<br>$\quad for\ i = 1:n$<br>$\quad\quad IAR_2(i,j) = IAR(i,j)$<br>$\quad end$<br>$end$ |

Yukarıdaki kod parçalarının çalıştırılmasıyla $IAR_1$ ve $IAR_2$ matrisleri oluşturulur. $IAR_1$, $IAR$ matrisinin ilk 4 sütunundan meydana gelirken, $IAR_2$ matrisi de son 4 sütunundan meydana gelir.

7.Adım(*Nüfuz etme ve yayılma*): Optimize edilmiş anahtar matris *OM*' yi kullanarak ikilik düzendeki $IAR_2$ matrisine yayılma metodunu uygula.

| Karıştırma Algoritması |
|---|
| $IAR_2' = reshape(IAR_2, n, 1)$<br>$for\ \ i = 1:n$<br>$\quad IAR_2''(i) = IAR_2'(OM(i))$<br>$end$<br>$IAR_2 = reshape(IAR_2'', s, 4)$ |

Burada *reshape* metodu, girilen ilk parametredeki matrisi, ikinci ve üçüncü parametrelerine göre sırasıyla yeni satır ve yeni sütun sayısı olacak şekilde yeniden boyutlandırır. Bu yeniden boyutlandırma işlemi önce yukarıdan aşağıya sonra soldan sağa olacak şekilde yapılır. *OM* matrisi kullanılarak yapılan yeniden indis numaralandırma işlemi ile ikili tabandaki sayıların birbiriyle tamamen karışması sağlanır ve bu karıştırma ikili tabanda yapıldığı için nüfuz etme işlemi de dolaylı olarak uygulanmış olur.

8.Adım(*Nüfuz etme*): *OM* optimize edilmiş anahtar matrisini kullanarak $IAR_1$ ve $IAR_2$ matrislerine nüfuz etme metodunu uygula.

Nüfuz Etme Algoritması

$OM' = reshape(OM, s, 4);$
$for \;\; i = 1:s$
$OAR_1(i) = bi2de(IAR_1(i;1:4));$
$OAR_2(i) = bi2de(IAR_2(i;1:4));$
$end$
$for \; i = 1:s$
$k_1 = \mathrm{mod}(OAR_1(i), 4);$
$if \; k_1 == 0$
$k_1 = 4;$
$end$
$OAR_2(i) = bitxor(OAR_2(i), \mathrm{mod}(OM'(i, k_1), 15));$
$k_2 = \mathrm{mod}(OAR\ (i), 4);$
$if \; k_2 == 0$
$k_2 = 4;$
$end$
$OAR_1(i) = bitxor(OAR_1(i), \mathrm{mod}(OM'(i, k_2), 15));$
$end$

Burada *bitxor*, bit düzeyinde mantıksal 'xor' operatörüdür. Diğer yandan *bi2de* fonksiyonu, girilen ikilik tabandaki sayıyı onluk tabana dönüştürür. Son olarak *mod*, bilinen mod alma operatörüdür.

9.Adım: Nüfuz etme algoritmasının uygulanması sonucu elde edilen $OAR_1$ ve $OAR_2$ matrislerine ikili formata dönüştürerek, aşağıdaki birleştirme algoritması ile bu matrisleri birleştir. Son olarak birleştirilerek elde edilen bu matrisi, açık resmin orijinal boyutlarına göre dönüştür.

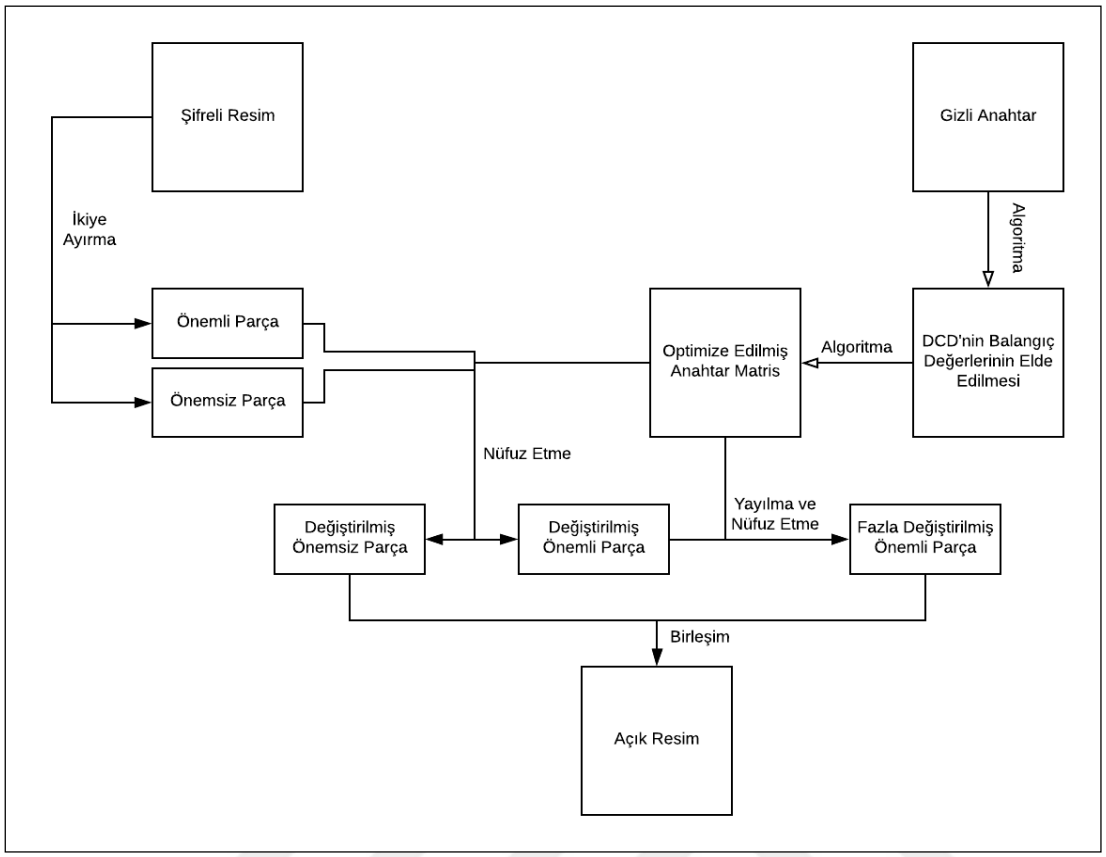
| Birleştirme Algoritması |
| --- |
| $for \;\; i = 1 : s$<br>$ISR(i;1:4) = de2bi(OAR_1(i),4);$<br>$ISR(i;5:8) = de2bi(OAR_2(i),4);$<br>$OSR(i) = bi2de(ISR(i;1:8))$<br>$end$<br>$SR = reshape(OSR, D, Y, 3)$ |

Burada, *de2bi* fonksiyonu ilk parametre olarak verilen onluk tabandaki sayıyı, ikinci parametre olarak verilen basamak sayısı uzunluğunda ikili tabana dönüştürür. Diğer metot *bi2de* ise *de2bi*'nin tam tersi olarak girilen ikili tabandaki sayıyı onluk tabana dönüştürür.

Birleştirme algoritmasının uygulanmasıyla elde edilen *SR*, şifrelenmiş görüntüdür ve şifreleme sistemi ile şifreleme algoritmasının çıktısıdır.

### 4.4. Şifre Çözme (Deşifre Etme) Algoritması

Tasarlanan şifreleme sisteminde öncelikle açık resimden matematiksel işlemler yardımıyla bazı bilgilerin çıkarılması sonucu gizli anahtar *GA* üretildi. Daha sonra bu gizli anahtardan kaotik üretecin başlangıç parametreleri üretildi ve şifreleme algoritmasıyla görüntü şifrelendi. Şimdi ise bu gizli anahtar kullanılarak yine kaotik sistemin başlangıç parametreleri elde edilecek ve sonrasında şifreleme algoritmasında uygulanan adımların tam tersi uygulanarak şifreli görüntü çözülecek. Deşifre etme algoritmasının akış diyagramı Şekil 4.4' de gösterilmektedir.




Şekil 4.4. Deşifre etme algoritmasının akış diyagramı

*Şifre Çözme Algoritması*

Girdi: Şifreli Resim *SR,* Gizli Anahtar *GA*

Çıktı: Açık Resim *AR*

1.Adım: Şifreleme sistemindeki 2,3 ve 4. adımları diğer bir değişle şifreleme algoritmasının ilk 3 adımını aynı şekilde uygulayarak optimize edilmiş anahtar matris *OM*'yi elde et.

2.Adım: Şifreleme sisteminin 5. adımını bu sefer şifreli resim *SR* için uygula.

| Dönüştürme Algoritması |
| --- |
| $SR' = reshape(SR, n, 1)$<br>$for\ i = 1:n$<br>$ISR(i;1:8) = de2bi(SR'(i), 8)$<br>$end$ |

Burada kullanılan fonksiyonların tamamına şifreleme sisteminde değinilmiştir.

3.Adım: Şifreleme sisteminin 6. adımını benzer şekilde bir önceki adımda elde edilen *ISR* matrisine uygula.

| Görüntünün Önemsiz Yarısını Ayırma Algoritması |
| --- |
| $for\ j = 1:4$<br>$for\ i = 1:n$<br>$ISR_1(i, j) = ISR(i, j)$<br>end<br>end |

| Görüntünün Önemli Yarısını Ayırma Algoritması |
| --- |
| $for\ j = 5:8$<br>$for\ i = 1:n$<br>$ISR_2(i, j) = ISR(i, j)$<br>end<br>end |

4.Adım: Şifreleme sistemindeki 8.adım olan nüfuz etme metodunun tersini uygulayarak şifreyi çözdürmek için ilk adımı uygula.

Ters Nüfuz Etme Algoritması

$OM' = reshape(OM, s, 4);$
$for \;\; i = 1:s$
$OSR_1(i) = bi2de(ISR_1(i;1:4));$
$OSR_2(i) = bi2de(ISR_2(i;1:4));$
$end$
$for \; i = 1:s$
$k_1 = \mathrm{mod}(OSR_2(i), 4);$
$if \; k_1 == 0$
$k_1 = 4;$
$end$
$OSR_1(i) = bitxor(OSR_1(i), \mathrm{mod}(OM'(i, k_1), 15));$
$k_2 = \mathrm{mod}(OSR_1(i), 4);$
$if \; k_2 == 0$
$k_2 = 4;$
$end$
$OSR_2(i) = bitxor(OSR_2(i), \mathrm{mod}(OM'(i, k_2), 15));$
$end$

Burada kullanılan metotların tanımı şifreleme sisteminin 8.adımında detaylı bir şekilde verilmiştir.

5.Adım: Şifreleme sisteminin 7. adımında uygulanan yayılma metodunun tam tersini elde edilen $OSR_2$ matrisine uygula.

Ters Karıştırma Algoritması

$for \;\; i = 1:s$
$ISR(i,1:4) = de2bi(OSR(i), 4)$
$ISR_2' = reshape(ISR_2, n, 1)$
$for \;\; i = 1:n$
$ISR_2''(OM(i)) = ISR_2'(i)$
$end$
$IAR_2 = reshape(ISR_2'', s, 4)$

Ters karıştırma algoritmasındaki yararlanılan fonksiyonlara şifreleme algoritmasında detaylı bir şekilde değinilmiştir.

6.Adım: Son olarak $OSR_1$ onluk düzende değerlere sahip olan matrisi ikilik tabana çevir. Daha sonra, şifreleme sisteminin 9. Adımına benzer şekilde bu ikilik düzendeki iki matrisi birleştir ve elde edilen matrisi şifreli resmin orijinal boyutlarına dönüştür.

| Matrisleri Birleştirme Algoritması |
|---|
| $for \;\; i = 1:s$<br>$IAR(i;1:4) = de2bi(OSR_1(i),4)$<br>$IAR(i;5:8) = IAR_2(i;1:4)$<br>$OAR(i) = bi2de(IAR(i;1:8))$<br>$end$<br>$AR = reshape(OAR, D, Y, 3)$ |

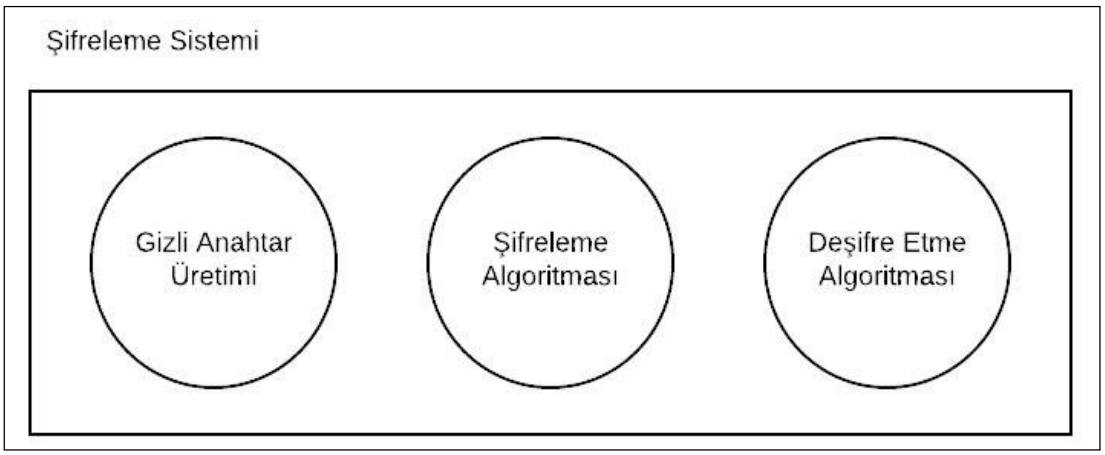
Burada kullanılan fonksiyonların detaylarına şifreleme sisteminde yer verilmiştir. Yukarıdaki program parçacığından elde edilen *AR* orijinal açık resimdir ve şifre çözme algoritmasının çıktısıdır.

### 4.5. Şifreleme Sisteminin Genel Analizi

Önceki bölümlerde kaos tabanlı gizli anahtarlı renkli resim şifreleme sisteminin tasarımının detaylı anlatımına yer verilmiştir. Bu bölümde, tasarlanan şifreleme sisteminin daha iyi kavranması açısından genel bir inceleme yapılmaktadır.

Öncelikle sistemin kaos tabanlı olması, şifreleme için kullanılan rastgele sayı üretecinin kaotik bir sistem olmasından kaynaklanmaktadır. Aynı zamanda şifreleme işleminin gizli anahtarla gerçekleştirilmesi bu sistemi simetrik bir şifreleme sistemi haline getirmektedir. Bu sistem renkli resim şifrelemek üzere tasarlanmışken gri düzey görüntülere de uyarlanabilir. Genel olarak sistemin özellikleri bu şekilde iken, detaylı incelemesi aşağıda yapılmaktadır

Tasarlanan sistemin genel görünümü Şekil 4.5'deki şema ile gösterilmiştir.




Şekil 4.5. Şifreleme sisteminin genel görünümü

Genel olarak tasarlanan bu şifreleme sistemi 3 ana bölümden oluşur. Bunlardan ilki gizli anahtarın üretimidir. Buradaki ana amaç her bir şifreleme işlemi için tek seferlik gizli anahtar üretmektir. Böylelikle dışarıdan gelecek seçilmiş açık metin saldırısı, bilinen açık metin saldırısı gibi ataklara karşı sisteme direnç kazandırılmış olur.

Bir diğeri ise şifreleme algoritmasının tasarımıdır. Bu algoritma tasarımında 2 önemli nokta öne çıkmaktadır. Bu öne çıkan noktalardan ilki başlangıç parametrelerinin üretimi konusudur. Kaos tabanlı bir şifreleme sisteminde kaotik üretecin başlangıç parametreleri şifrelemenin güvenilirliği açısından oldukça elzemdir. Dolayısıyla başlangıç değerlerinin hem sisteme kaotik özellik kazandırması hem de her şifreleme işleminde mümkün olduğunca farklı olması gerekir. Bu özellikleri sağlayacak şekilde gizli anahtardan kaotik sistemin başlangıç parametrelerinin üretimi sağlanmıştır. Gizli anahtarda çok ufak bir değişiklik bile olsa tasarlanan algoritma sayesinde bu değişiklik başlangıç parametrelerine en iyi şekilde yansımaktadır. Önemli olan diğer nokta ise, literatürde resim şifreleme standartları olarak kullanılan yayılma ve nüfuz etme metotlarının sistemde verimli bir şekilde uygulanmasıdır. Bu yolla, şifreleme sisteminin 7. ve 8. adımları uygulanmıştır. 7. adımda aslında bir yayılma işlemi uygulanıyor. Fakat bu işlem ikilik tabandaki sayılara uygulandığı için, ikilik düzende sadece sayıların yer değiştirmesi işlemi gerçekleşirken, onluk tabana göre değerlerin de değişmiş olduğu aşikârdır. Dikkat edilirse bu yayılma işlemi, piksel değerlerinin ikili formdaki önemli son 4 basamağına uygulanıyor. Bunun sebebi ilk 4 basamağın sayı hakkında önemli bilgiler taşımaması sonucu gereksiz işlem yoğunluğundan kaçınılmak

istenmesidir. 8. adımda da nüfuz etme işlemi uygulanıyor ve sistemin korelasyonu iyice azaltılıyor. Diğer yandan bu şifreleme işlemleri renkli görüntünün 3 bileşenine aynı anda uygulanıyor. Bu da renk bileşenleri arasındaki korelasyonu da değiştirerek şifreli görüntüyü daha da karmaşıklaştırıyor.

Şifreleme sisteminin son bölümü deşifre etme algoritmasıdır. Şifreleme sisteminde ilk adım olarak üretilen gizli anahtar bu algoritmaya girdi olarak sunulur ve genel olarak şifreleme algoritmasındaki adımların tam tersi uygulanarak orijinal görüntü elde edilir. Şifre çözme algoritmasında da ana prensip, olabildiğince orijinal resme yakın bir resim elde etmektir. Biz burada sisteme gürültü uygulanmadığı takdirde yüzde yüzlük bir geri dönüşüm elde ederek orijinal resmi tamamen yakalıyoruz. Diğer yandan literatürde şifre çözme algoritmalarının gürültü ataklarına karşı dayanıklı olması da önemli bir konudur. Bu hususta şifreleme algoritması tasarlanırken tersinir özelliğine de dikkat edilmiş ve şifrelenmiş görüntüdeki ufak bir bozulmanın deşifre etme algoritmasını tamamen etkisiz hale getirmemesi üzerinde önemle durulmuştur. Güvenlik analizleri bölümünde gürültü ataklarına karşı sistemin dayanıklılığı da test edilmiş ve tatmin edici sonuçlar elde edilmiştir.

# 5. DENEYSEL GÖSTERİMLER

Kaos tabanlı resim şifreleme sistemlerine literatürde geniş bir şekilde değinilmiş ve bununla alakalı birçok algoritma tasarlanmıştır. Bu sistemlerde, farklı kaotik üreteçler ile birçok farklı algoritma kullanılmıştır. Tasarlanan bu sistemlerin güvenlik testleri yapılmış ve diğer sistemlerle karşılaştırmalarda bulunulmuştur.

Bir şifreleme sistemi tasarımında deneysel gösterimler ve sayısal analiz sonuçları, sistemin durumu hakkında bize yol gösterici bilgiler sunar. Bu testler, geliştirilen şifreleme algoritmalarının verimliliğini tespit edebilmek için kritik öneme sahiptir. Bu açıdan bakıldığı zaman, şifreleme sisteminin uygulanabilirliğini arttırmak için bir araç tasarımı yapılmıştır. Bu araç yardımıyla tek bir platformda kaotik sürecin sonuçlarının görülebildiği, şifreleme ve deşifre etme işlemlerinin gerçekleştirilebildiği, sistemin güvenlik analizlerinin yapılabildiği ve birden fazla algoritmanın sayısal verilerle karşılaştırılabildiği bir yazılım geliştirilmiştir. Aslında bir kaotik şifreleme sistemi için gerekli olabilecek tüm işlemlerin gerçekleştirilebildiği komple bir kullanıcı arayüzü tasarlanmıştır.

## 5.1. Şifreleme Sistemi Arayüz Tasarımı

Yazılım genel olarak 7 menüden oluşmaktadır. Resim 5.1’ de tasarlanan arayüzün açılış sayfası mevcuttur.

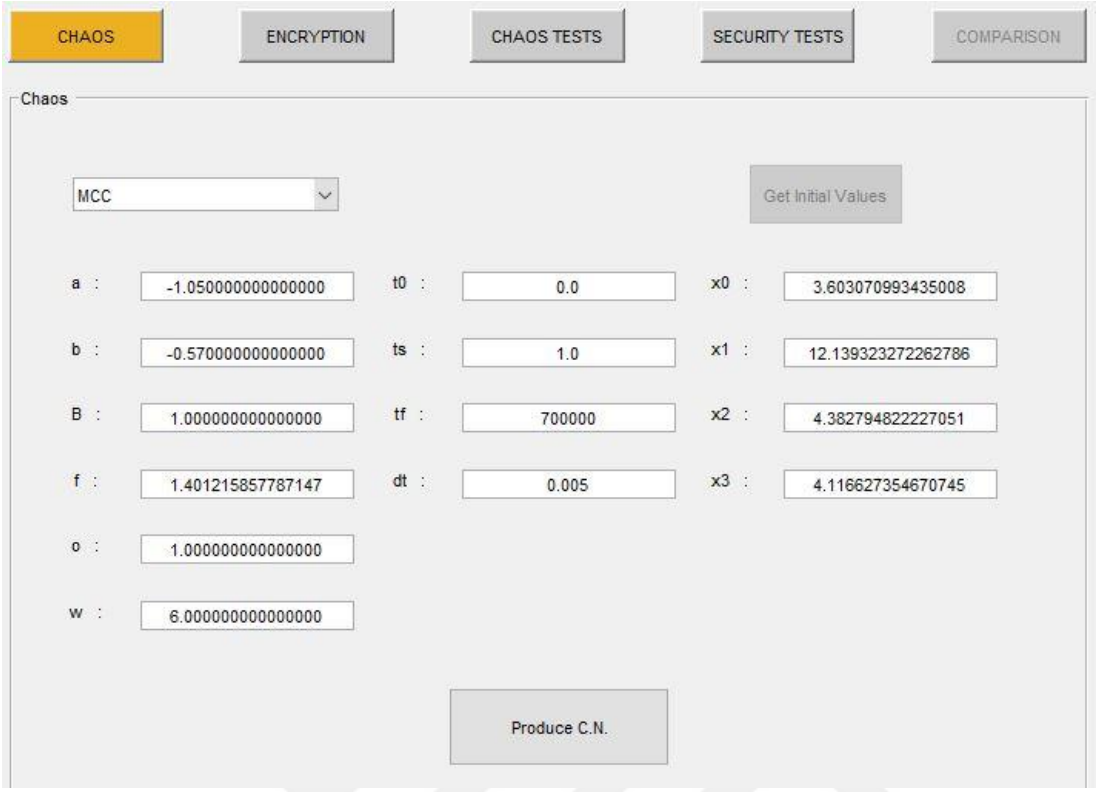

Resim 5.1. Resim şifreleme arayüzü açılış sayfası

Yukarıdaki Resim 5.1'e bakıldığında resmin üst bölümünde menü butonları yer alır. Bu butonlara basıldığında ilgili menüler arasında geçiş yapılabilir.

Yazılımın işleyiş mantığı soldan sağa doğrudur. İlk kullanılacak olan 'IMAGE' menüsüdür. Bu menüden öncelikle resim seçimi yapılır. Daha sonra gizli anahtar üretimi için kullanılacak algoritma seçimi yapılır ve gizli anahtar üretilir. Bu menü aşağıdaki Resim 5.2'de gösterilmektedir.

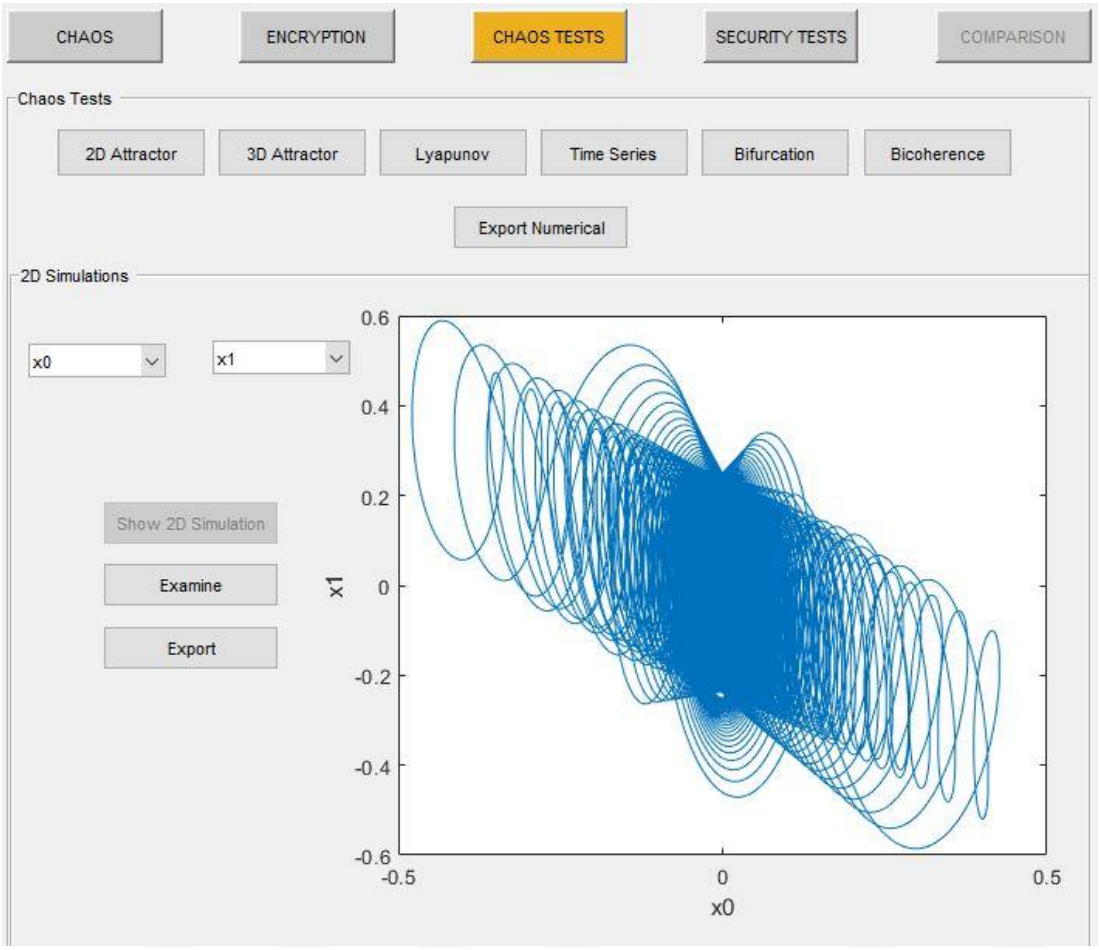

Resim 5.2. Resim şifreleme arayüzünün ‘IMAGE’ menüsü

Resim seçimi yapılıp şifreleme için kullanılacak olan gizli anahtar üretildikten sonra ikinci aşama olarak kaotik üreteç seçimi yapılır. Seçilen kaotik üretecin belirli başlangıç parametreleri gizli anahtardan üretilir. Son olarak şifreleme için yararlanılacak olan kaotik sayılar üretilir. Bu işlemler için Resim 5.3’ de gösterilen ‘CHAOS’ menüsü kullanılır.




Resim 5.3. Resim şifreleme arayüzünün ‘CHAOS’ menüsü

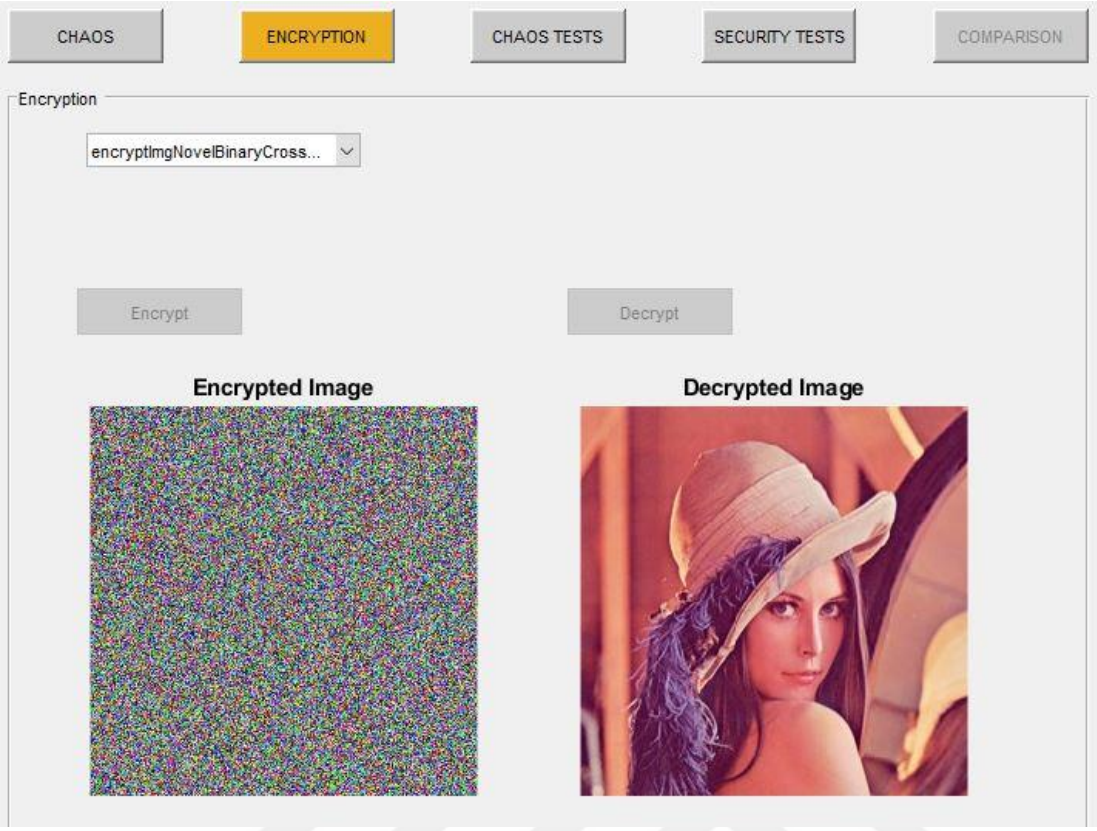
Kaotik sistemin çözümü sonucu elde edilen sayı dizilerinin kaotik olup olmadığının incelenmesi için ‘CHAOS TESTS’ menüsü mevcuttur. Bu menüde kaotik çekicilerin tespiti, Lyapunov üstellerinin belirlenmesi, zaman serileri analizi gibi birçok işlem yapılabilir.




Resim 5.4. Resim şifreleme arayüzünün ‘CHAOS TESTS’ menüsü, 2 boyutlu kaotik çekici analizi ‘2D Attractor’ alt menüsü

Resim 5.4’ de tasarlanan menü ile kaotik sistemin ilgili parametre değerleri sonucu kaotik özelliklerin irdelenebilmesi amaçlanmıştır. Ayrıca burada ‘.JPEG’ formatında grafiksel çıktılar, ‘EXCEL’ formatında sayısal çıktılar alınabilir.

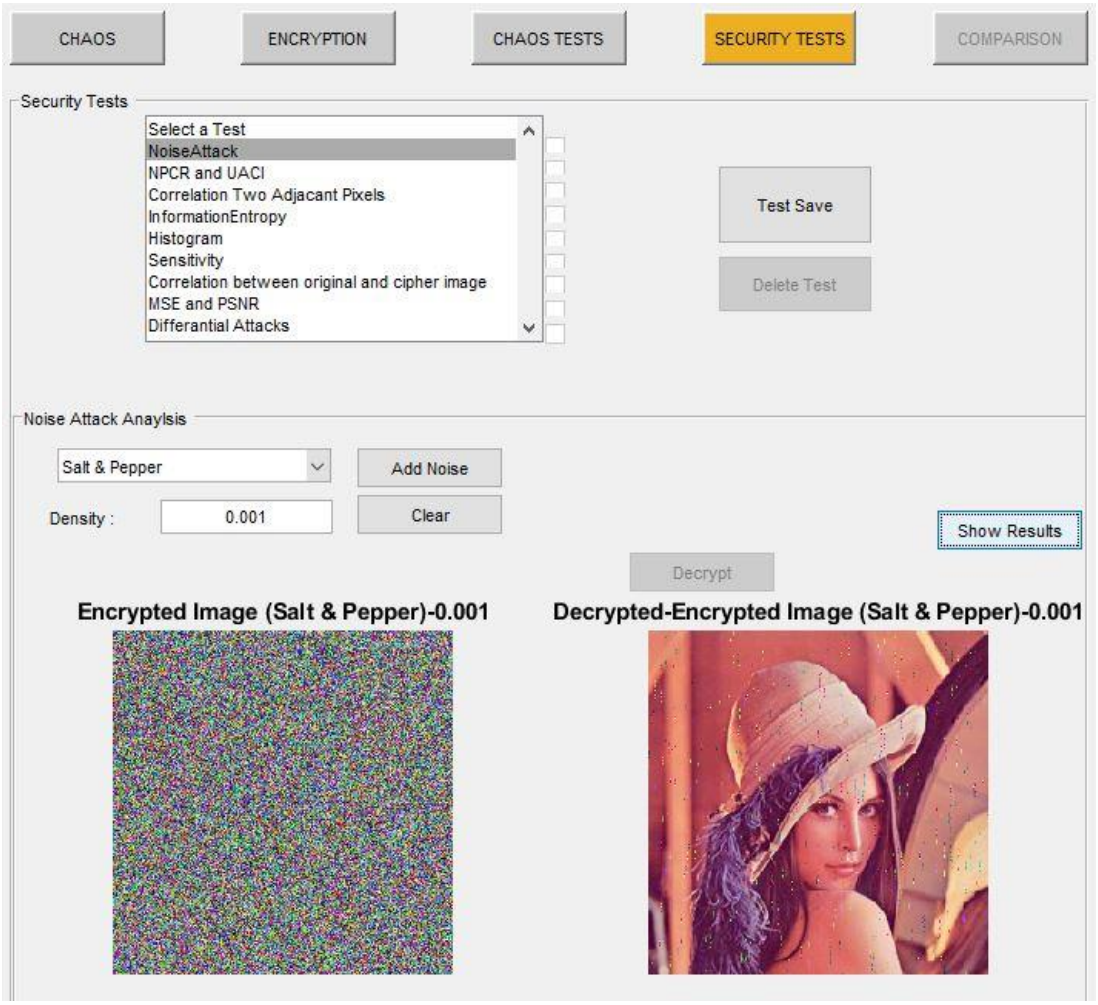
Üretecin kaotik özelliklerinin incelenmesinden sonra şifreleme algoritması seçilip şifreleme işlemi gerçekleştirilir. Daha sonra deşifre etme işlemi uygulanarak açık resim elde edilir.



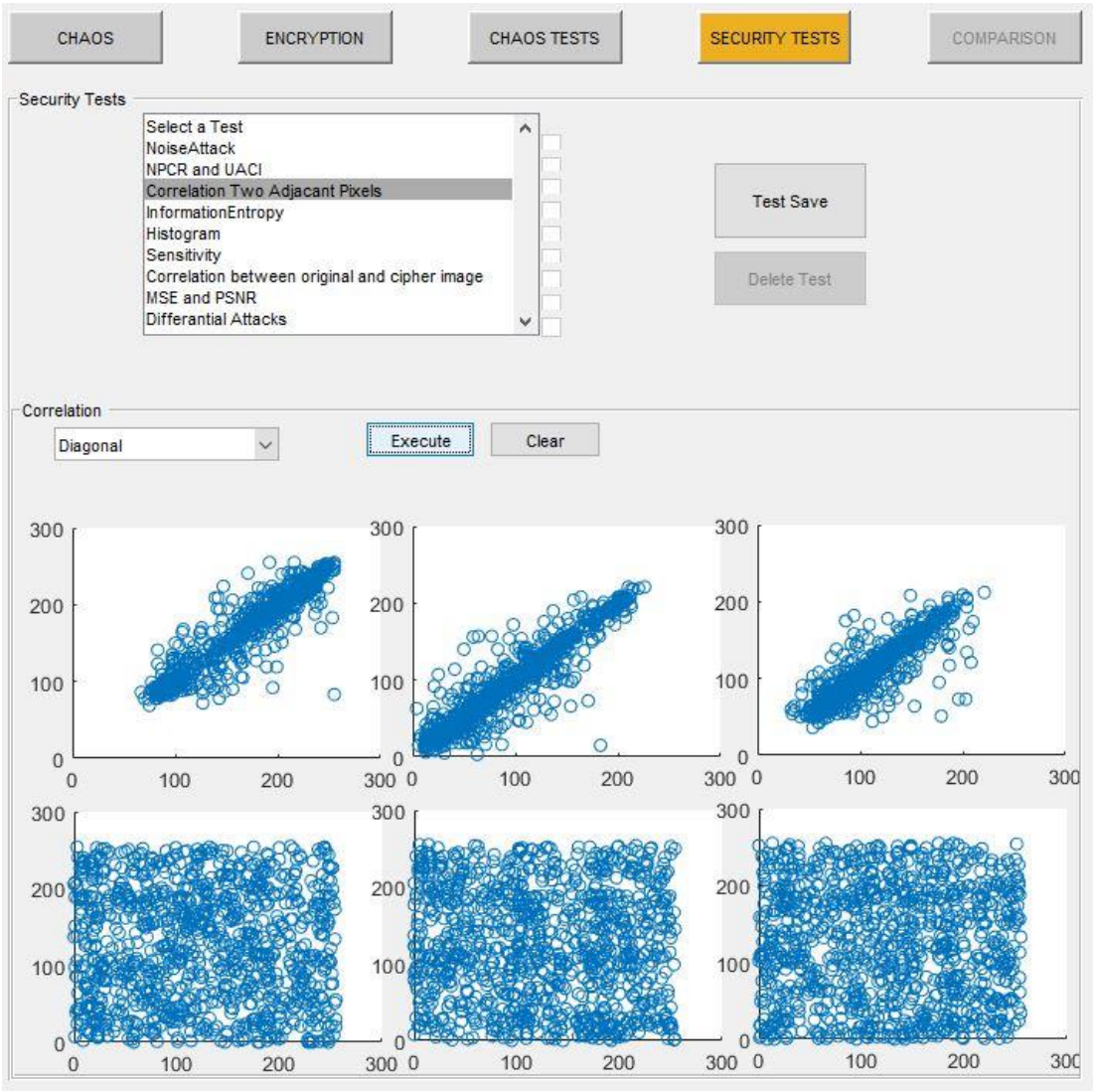

Resim 5.5. Resim şifreleme arayüzünün ‘ENCRYPTION’ menüsü

Yukarıda Resim 5.5’ de birden fazla şifreleme algoritmanın seçilebileceği bir alan mevcuttur. Sisteme birçok algoritma yazılabilir ve bu seçim ekranından yazılan algoritmalardan herhangi biri seçilip şifreleme işlemi gerçekleştirilebilir.

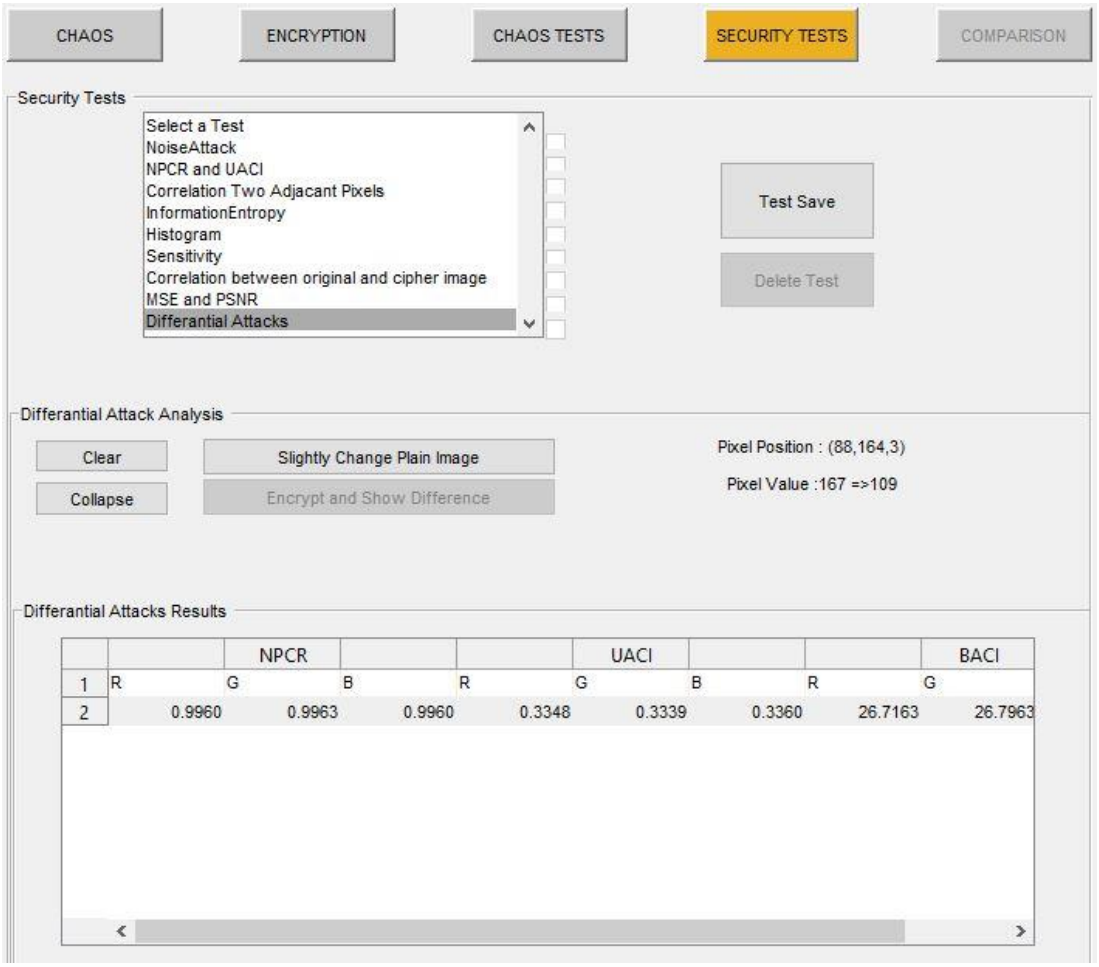
Şifreleme ve deşifre etme işlemlerini uyguladıktan sonra algoritmanın güvenilirliğinin test edilebilmesi için Resim [5.6-5.8]’deki ‘SECURITY TESTS’ menüsü kullanılır. Bu menü yardımıyla 9 farklı saldırının sayısal ve görsel verilerle test edilebilmesi sağlanır. Ayrıca bu testler kaydedilip farklı algoritmaların ilgili test sonuçlarıyla Resim 5.9’ da gösterilen ‘COMPARISON’ menüsünde karşılaştırılabilir.




Resim 5.6 Resim şifreleme arayüzünün ‘SECURITY TESTS’ menüsü, gürültü atağı analizi ‘Noise Attack Analysis’ alt menüsü

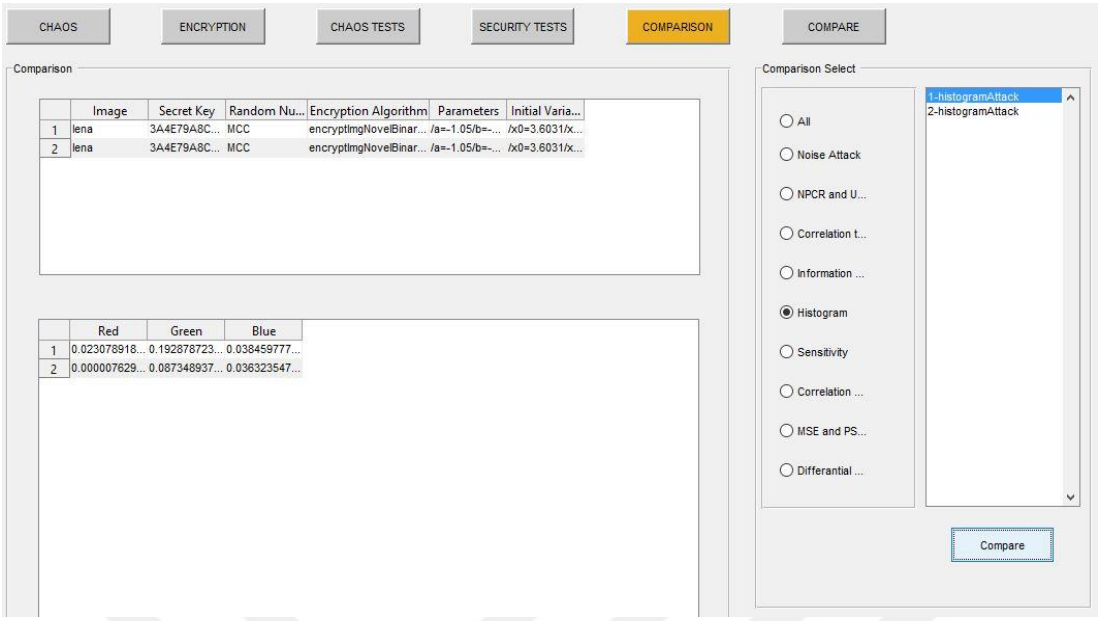



Resim 5.7. Resim şifreleme arayüzünün ‘SECURITY TESTS’ menüsü, korelasyon analizi ‘Correlation’ alt menüsü




Resim 5.8 Resim şifreleme arayüzünün ‘SECURITY TESTS’ menüsü, diferansiyel atak analizi ‘Differantial Attack Analysis’ alt menüsü

Seçilen şifreleme algoritmasının güvenlik testleri yapıldıktan sonra Resim [5.6-5.8] de sağ üst kısımlarda gösterilen ‘Test Save’ butonuna tıklayarak ilgili test kaydedilir. Sonra ‘ENCRYPTION’ menüsünden farklı bir algoritma seçerek tekrar şifreleme işlemi gerçekleştirilir ve sonrasında bu algoritmaya güvenlik testleri uygulanır. Ardından bu testlerde kaydedilerek Resim 5.9’ daki ‘COMPARISON’ menüsünde her iki algoritma için kaydedilmiş aynı güvenlik testleri karşılaştırılabilir.




Resim 5.9. Resim şifreleme arayüzünün ‘COMPARISON’ ve ‘COMPARE’ menüsü

Kaos tabanlı resim şifreleme sistemi tasarlarken, kaos gibi farklı bir disiplinin kriptoloji alanına uygulanabilmesi ve sistemin geçerliliğin verilerle doğrulanabilmesi için bu alanda bir uygulama geliştirmek önemli bir durum haline gelmektedir. Tasarlanan arayüz ile amaçlanan, bir kaos resim şifreleme sisteminin adımlarının daha net anlaşılabilmesi ve geliştiricinin daha etkili bir sistem tasarımı yapabilmesini sağlamaktır. Gerek kaos testleri, gerekse güvenlik testlerinin oldukça anlaşılır bir şekilde gerçekleştirilebilmesi sistemi bu iş için oldukça önemli hale getirir.

Bu arayüz yazılımı kapsamlı olarak tasarlanmıştır. Yeni algoritmaların ve yeni kaotik üreteçlerin sisteme eklenmesi oldukça kolaydır. Dolayısıyla farklı algoritmalarla farklı kaotik üreteçlerle çalışılıp optimize sistem rahatlıkla tasarlanabilir. Zaman açısından da geliştiriciye oldukça katkı sağlanmış olur. Yazılımın süreç şeklinde kurgulanması, yönlendirmelerle kullanıcı dostu olması ve işleyişinin basit olması gibi artılar geliştiriciye hız ve verimlilik açısından büyük bir imkân sağlar.

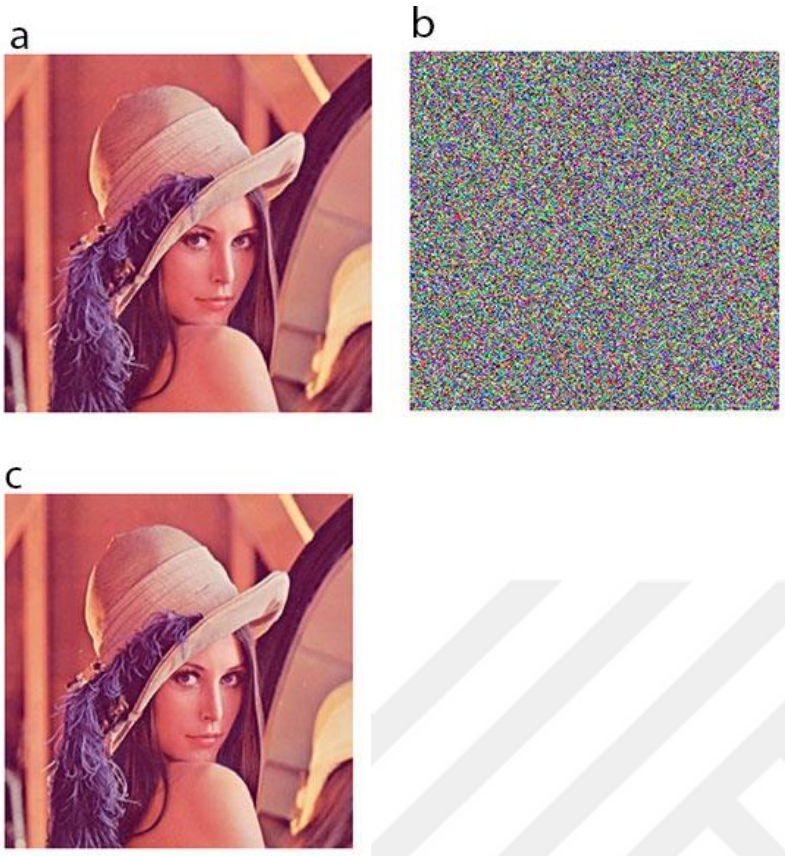
Bu arayüz yazılımı, MatLab platformunda gerçekleştirilmiş olup yaklaşık 7000 kod satırından ve bir arayüz tasarım dosyasından oluşmaktadır.

## 5.2. Deneysel Sonuçlar

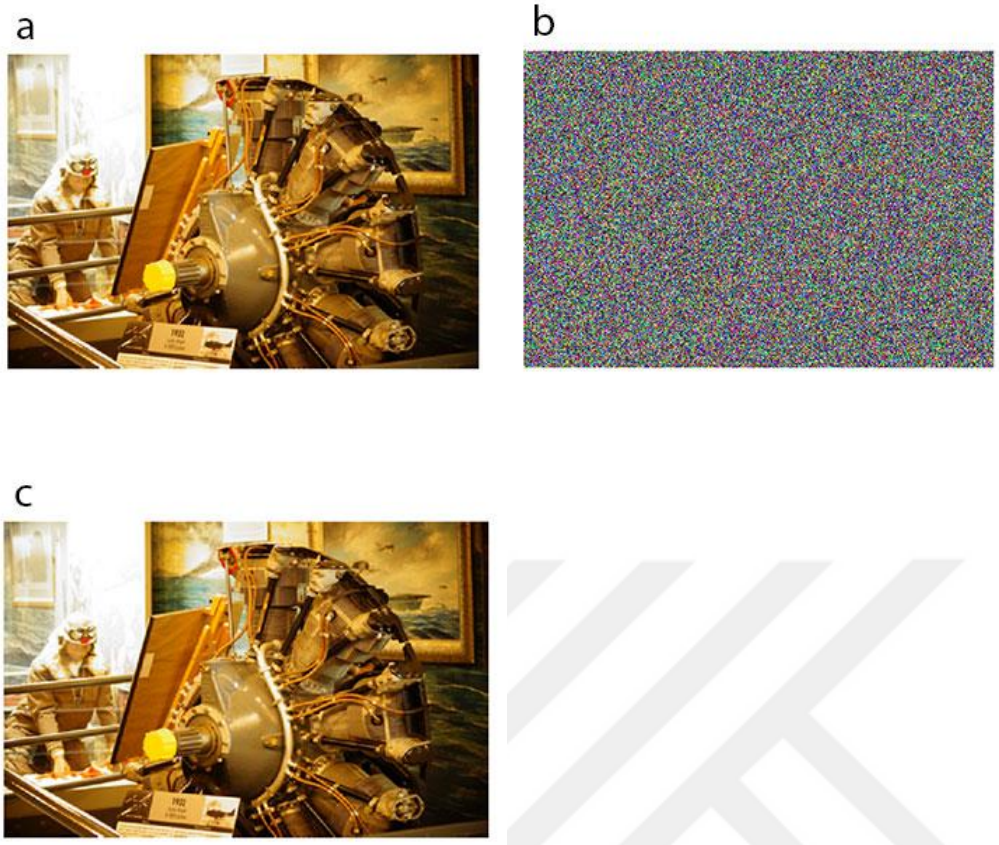
Şifreleme sisteminin Eş. 3.1'de tanımlı denklemlerle gösterilen üretecinin kaotik diziler üretmesi sağlanacak şekilde başlangıç parametreleri belirlenir. Parametrelerden sabit olanları $a=-1{,}05$, $b=-0{,}57$, $\beta=1{,}0$, $\phi=1$ ve $\omega=6$ olacak şekilde verilir [26]. Bu başlangıç parametreleri altında $f\geq 0{,}84$ şartı ile sistem kaotik davranış sergiler [26]. Yukarıda şifreleme sisteminin tasarımı anlatılırken her bir şifreleme işlemi için $0{,}84\geq f\geq 1{,}84$ sınırlaması getirilmiştir. Tüm bu şartlar altında sistem baskın bir şekilde kaotik davranış sergiler.

Diğer yandan her şifreleme işlemi için bir gizli anahtar üretilir ve bu anahtar eşsizdir. Dolayısıyla sabit bir gizli anahtar belirlenemez. Anahtardan kaotik üretecin başlangıç değerleri $x_1, y_1, z_1, v_1$ üretilir. Başlangıç parametresi $f$ ise 0,84-1,84 aralığında sistem tarafından belirlenir. Gizli anahtarın her şifreleme işleminde değişmesinden dolayı bu başlangıç değerleri de her seferinde değişir ve benzersizdir.

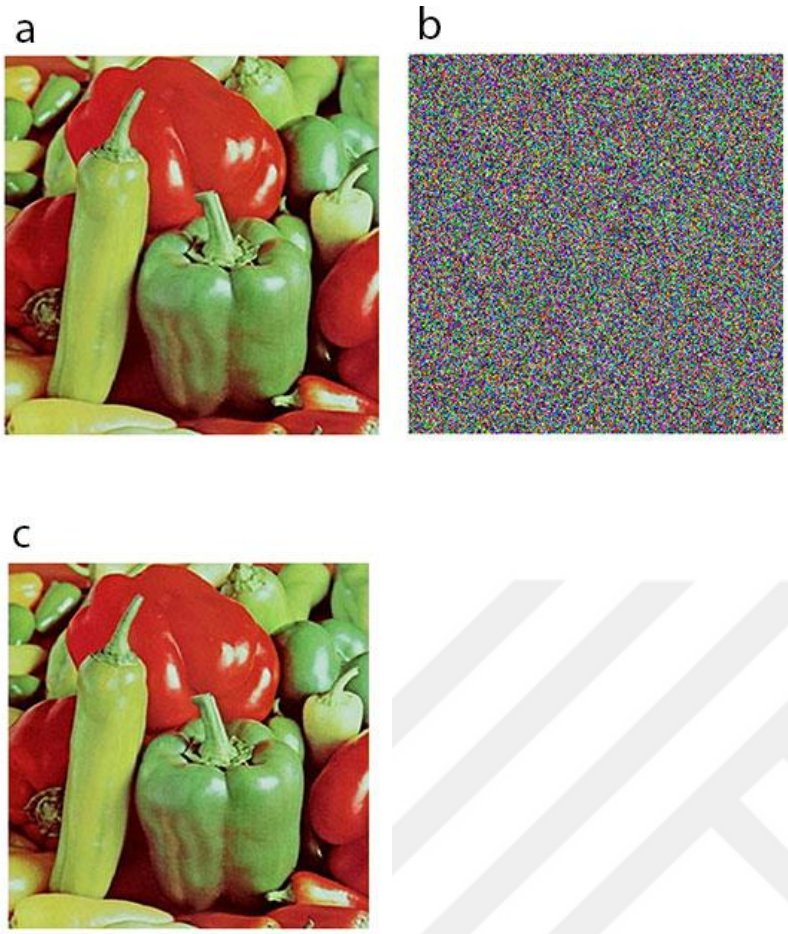
Boyutları 256x256x3 olan Lena görüntüsünün Resim 5.10'da, 282x424x3 olan Machine görüntüsünün Resim 5.11'de, 256x256x3 olan Peppers görüntüsünün Resim 5.12'de, 282x424x3 olan Asian Lady görüntüsünün Resim 5.13'de, 242x294x3 olan Vikings görüntüsünün Resim 5.14'de, 512x512x3 olan Airplane görüntüsünün Resim 5.15'de, 594x400x3 olan Arctichare görüntüsünün Resim 5.16'da, 512x512x3 olan Baboon görüntüsünün Resim 5.17' de, 490x733x3 olan Cat görüntüsünün Resim 5.18'de, 768x512x3 olan Monarch görüntüsünün Resim 5.19'da, 327x435x3 olan Paris görüntüsünün Resim 5.20'de sırasıyla orijinal (a), şifrelenmiş (b) ve deşifre edilmiş (c) durumları gösterilmektedir.



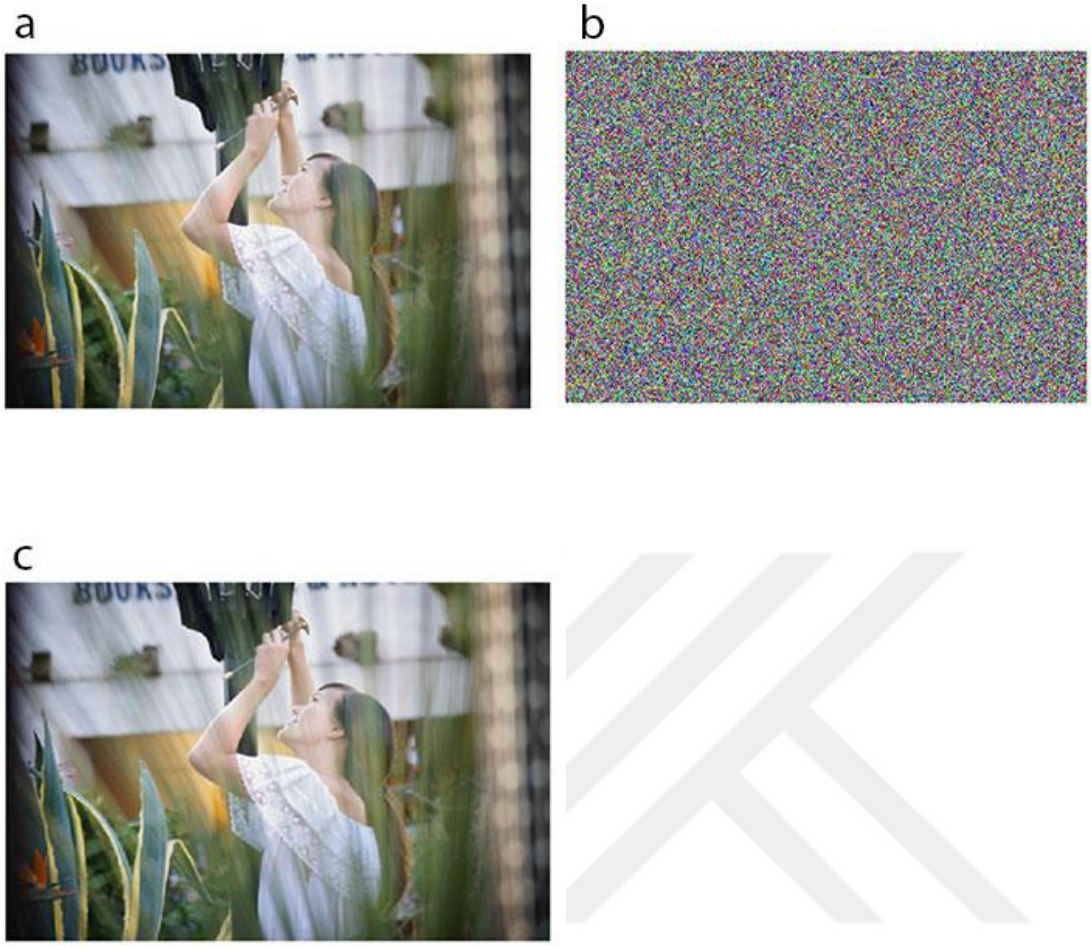

Resim 5.10. Lena (a) orijinal görüntüsünün ‘CEA17B64EDCD1C4DEADC25406 C19482DEC796D3A08E03D0BDB5BD9016934C7C2’ anahtarı ile şifrelenmiş (b) ve deşifre edilmiş (c) durumları



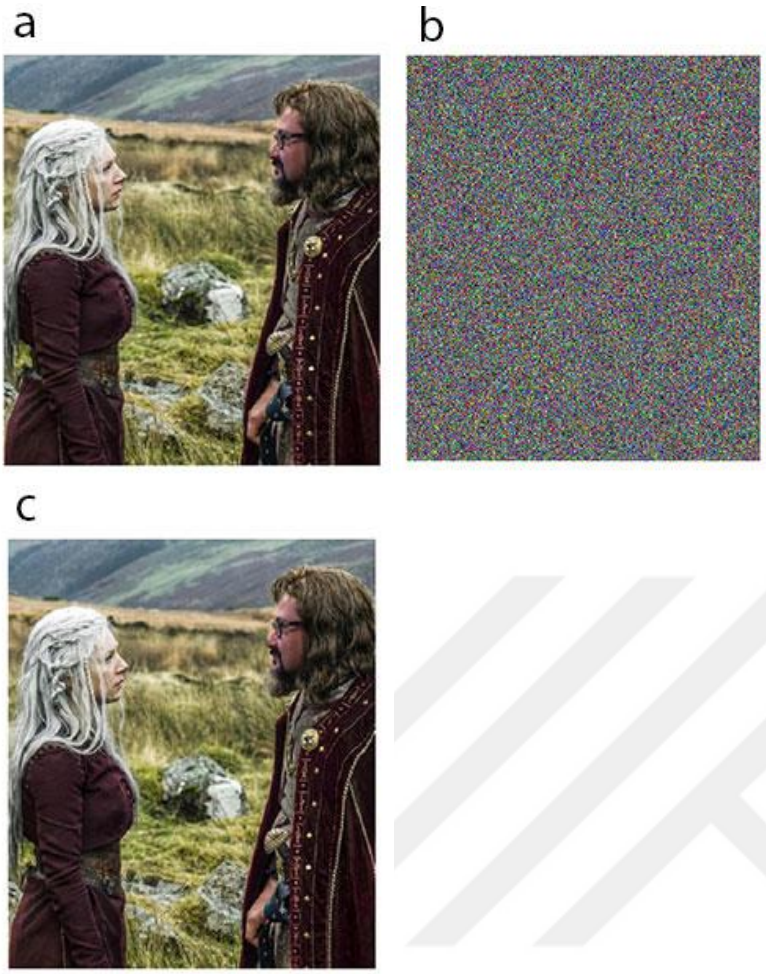

Resim 5.11. Machine (a) orijinal görüntüsünün ‘2A5D0D3F919A676C520E9A1 327FCA0CD9DAD3555CEB29A2889A7F016DCACD242’ anahtarı ile şifrelenmiş (b) ve deşifre edilmiş (c) durumları



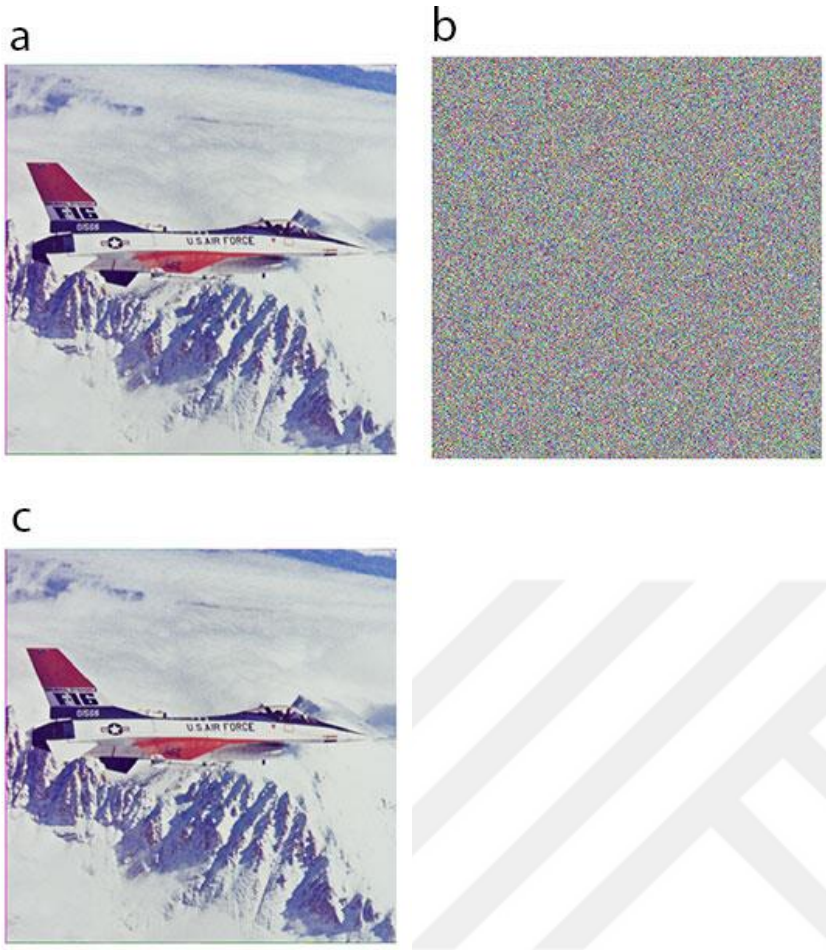

Resim 5.12. Peppers (a) orijinal görüntüsünün ‘B1B4D7A6B8F0F17CEF7DEA8 891FB111D61BEB28D0C59AFDA1D9D8E4E26A51686’ anahtarı ile şifrelenmiş (b) ve deşifre edilmiş (c) durumları



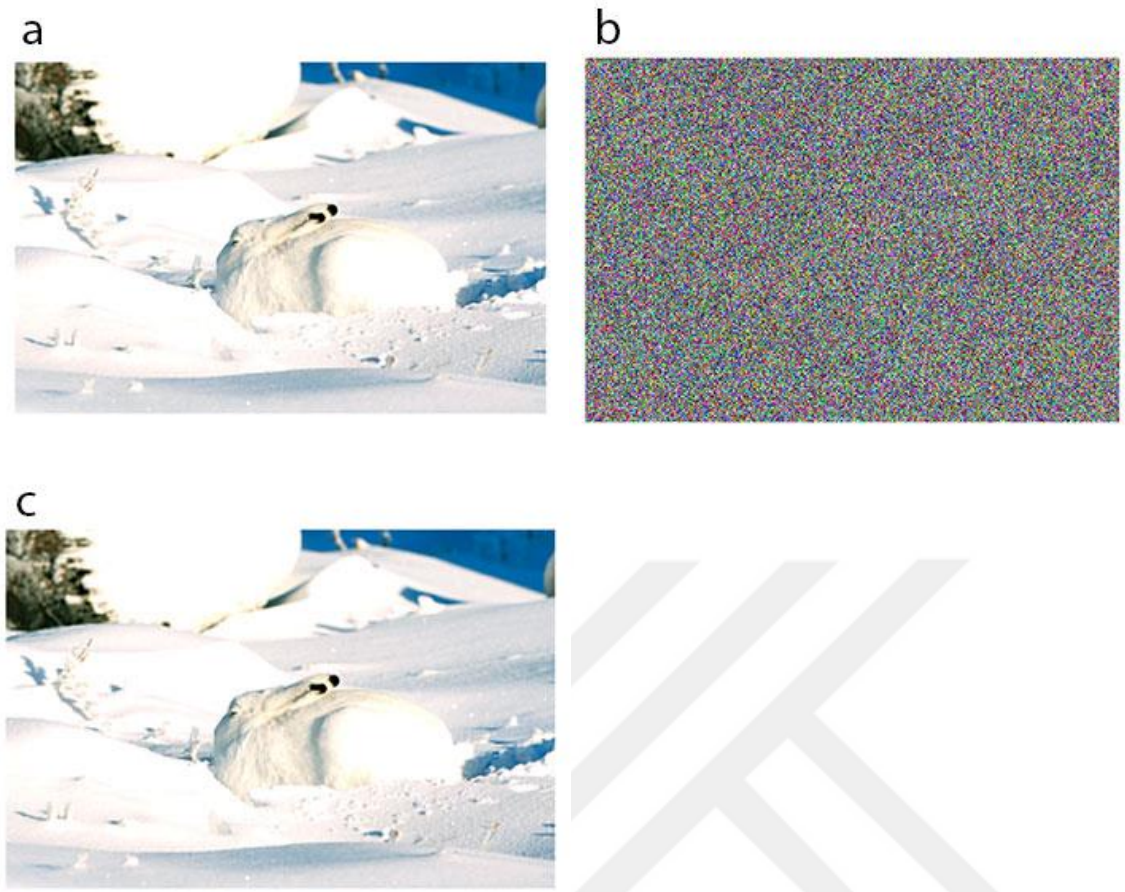

Resim 5.13. Asian Lady (a) orijinal görüntüsünün ‘58C5F8CCB657599DCBD A1E2C7341A886F3D668F144EDC3AFE31E438BEDCC0146’ anahtarı ile şifrelenmiş (b) ve deşifre edilmiş (c) durumları



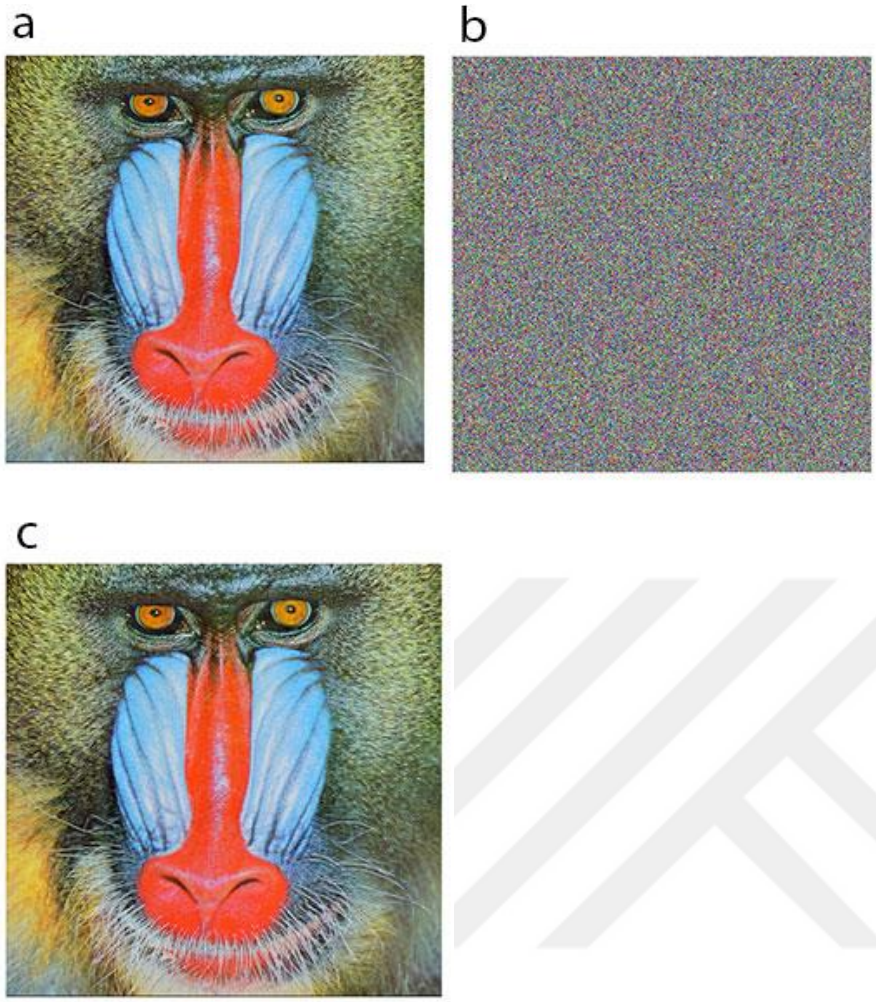

Resim 5.14. Vikings (a) orijinal görüntüsünün ‘3D3BB565F84885702E36 60EFAED22F2354C529F5C513778265ADBD0F446EB60E’ anahtarı ile şifrelenmiş (b) ve deşifre edilmiş (c) durumları



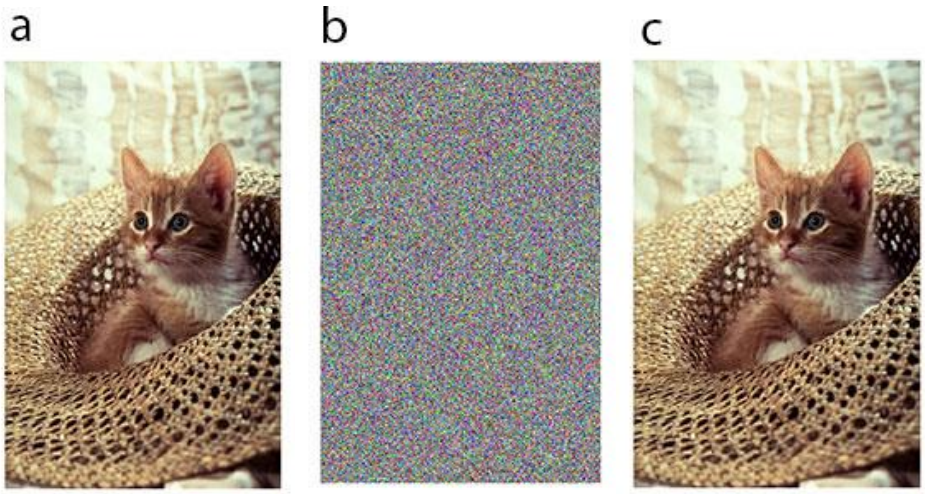

Resim 5.15. Airplane (a) orijinal görüntüsünün ‘AEF3221E82C21BF77510BAEA BB53C06340F02AF5DA1B7C0CFBEE29F15DB92464’ anahtarı ile şifrelenmiş (b) ve deşifre edilmiş (c) durumları




Resim 5.16. Arctichare (a) orijinal görüntüsünün ‘51BCF06CD9FE634A1DC 9C99D9DF6D99D90CF2D586DC85B8762CEB1F9A0DE8444’ anahtarı ile şifrelenmiş (b) ve deşifre edilmiş (c) durumları



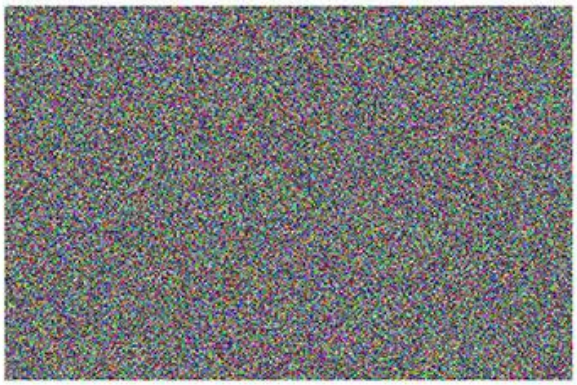

Resim 5.17. Baboon (a) orijinal görüntüsünün ‘265F4EC81BEF46AD34D 5B806B4661A42CD6F4DEB47600218619F38086AB0D3B5’ anahtarı ile şifrelenmiş (b) ve deşifre edilmiş (c) durumları




Resim 5.18. Cat (a) orijinal görüntüsünün ‘1A97836393A88B1E866 E6C06721CB176507BD9AED224CFDE258FEB46FC75CC8D’ anahtarı ile şifrelenmiş (b) ve deşifre edilmiş (c) durumları

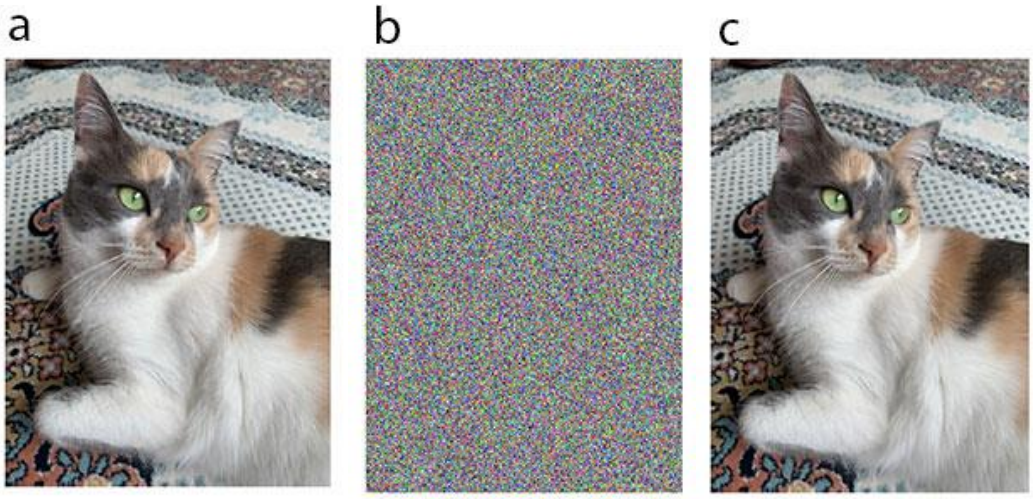
a

b



c

Resim 5.19. Monarch (a) orijinal görüntüsünün ‘415C89F624C1D16A12DAC64 5E29FB34B9920D3F1B472D216F1F081FD250A71E4’ anahtarı ile şifrelenmiş (b) ve deşifre edilmiş (c) durumları




Resim 5.20. Paris (a) orijinal görüntüsünün ‘6198E629294BB184AA6B 6A46E12D5675DB0EEA0FE50565970FDB65D026D4734D’ anahtarı ile şifrelenmiş (b) ve deşifre edilmiş (c) durumları

# 6. GÜVENLİK VE PERFORMANS ANALİZLERİ

## 6.1. Anahtar Uzayı Analizi

Başlangıç koşullarına hassas bağlılık, kaotik sistemlerin genel davranışıdır. Yüksek güvenilirliğe sahip olan bir şifreleme sistemi, kaba kuvvet saldırılarıyla başa çıkabilecek büyüklükte bir anahtar uzayına sahip olması gerekir. Bu şifreleme sisteminde ise kaotik üretecin başlangıç koşulları $x_1, y_1, z_1, v_1$ ve $f$ gizli anahtardan üretilir.

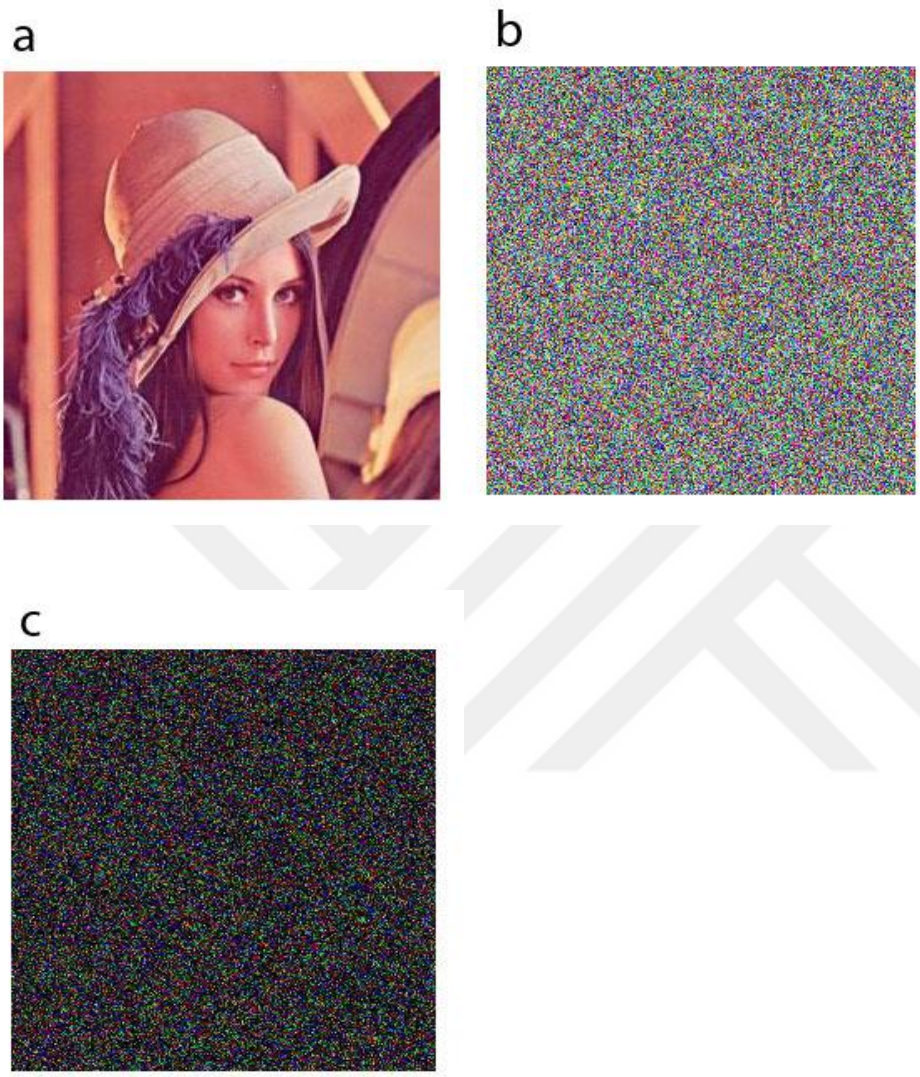
Kaotik özellik gösteren sistemler için genelde başlangıç koşullarının hassaslığı, başlangıç parametrelerinin virgülden sonraki 14 veya 15 hanesine kadar geçerlidir [15]. Bu kaotik sistem için üretilen başlangıç koşulu 5 adet olduğu için anahtar uzayı $10^{70}$'e erişebilir. Anahtar uzayı $10^{70} \cong 2^{232} > 2^{100}$ [75] şartını sağlandığı için sistem kaba kuvvet saldırılarıyla rahatlıkla başa çıkabilir.

## 6.2. Anahtar Hassasiyet ve Açık Resim Hassasiyet Analizi

Herhangi bir kaotik sistemin başlangıç koşullarında meydana gelen en ufak değişiklik, sistemin benzersiz çıktılar üretmesine sebep olur. Tasarlanan şifreleme sistemde kaotik üreteç olarak kullanılan DCD' nin başlangıç parametreleri, şifreleme algoritması için üretilen gizli anahtara bağlıdır. Gizli anahtar, şifrelenecek açık resimden elde edilen bilgiler ve rastgele gürültünün SHA-256 algoritmasına parametre olarak verilmesiyle üretilir. Karıştırma algoritması olan SHA-256, girdi değerlerine hassas şekilde bağlıdır. Dolayısıyla açık resimde meydana gelen küçük bir değişiklik, üretilen gizli anahtarın tamamına tesir eder. Açık resimde değişiklik olmasa bile, her seferde SHA-256 algoritmasının kullanacağı rastgele bir gürültü üretildiği için, algoritmanın ürettiği gizli anahtar tamamen değişecektir. Anahtarın her seferinde değişmesi, kaotik üretecin başlangıç parametrelerini de değiştireceğinden şifrelenmiş görüntü de bir öncekinden çok farklı olacaktır. Böylelikle tasarlanan şifreleme sistemi hem gizli anahtara hem de açık resme hassas şekilde bağlı olur. Bu da sistemin güvenilirliğini arttırır.

Resim 6.1 (a)'da, Resim 5.10 (a)'daki Lena resminin sadece bir pikselinin bir bit değeri değişmiş hali, 6.1 (b)' de (a)'nın şifrelenmiş hali gösterilmektedir. 6.1 (c)' de gösterilen ise orijinal Lena resminin şifrelenmiş hali ile bir bit değeri değişmiş Lena resminin şifrelenmiş

halinin matematiksel farkı gösterilmektedir. Farkın anlaşılamaz olduğu ve şifreli resimlerin birbirinden tamamen farklı olduğu görülmektedir.




Resim 6.1. (a) Resim 5.10 (a)'nın bir bit değiştirilmiş versiyonu, (a)'nın şifrelenmiş hali (b), (c) ise Resim 5.10 (b) ile (b)'nin matematiksel farkıdır.

### 6.3. Bilinen Açık Metin ve Seçilmiş Açık Metin Saldırılarına Karşı Direnç Analizi

Önerilen algoritmada gizli anahtar, resimden çıkarılan bilgi ile SHA-256 algoritmasının ürettiği karma değere bağlıdır. Dolayısıyla, şifrelenecek görüntünün değişmesi ile üretilen karma değer değişir ve gizli anahtar tamamen farklı oluşur. Saldırgan da herhangi bir görüntüden bir şekilde ele geçirdiği gizli anahtarı, başka bir görüntünün şifresini çözmek için kullanamaz. Sonuç olarak şifreleme sistemi, bilinen açık metin saldırılarına ve seçilmiş açık metin saldırılarına karşı güvenilir olur.

## 6.4. Diferansiyel Atak Analizi

Resim şifreleme sistemlerinden asıl beklenen iş, şifrelenmiş görüntünün orijinal halinden tamamen farklı olmasıdır. Literatürde bu farkın sayısal ölçümünün yapılabilmesi için NPCR [78], UACI [79] ve BACI [50] kıstasları kullanılabilir. Çizelge 6.1'de bazı orijinal görüntüler ve bunların şifrelenmiş halleri arasındaki NPCR, UACI ve BACI değerleri sunulmuştur.

Çizelge 6.1. Orijinal görüntülerden ve bu görüntülerin sunulan algoritma ile şifrelenmiş durumlarından elde edilen ortalama NPCR, UACI ve BACI değerleri

| | NPCR | | | UACI | | | BACI | | |
|---|---|---|---|---|---|---|---|---|---|
| Resim | K | Y | M | K | Y | M | K | Y | M |
| 5.10. (a)-(b) | 99,6139 | 99,6337 | 99,6261 | 32,3918 | 31,0319 | 28,0386 | 25,1694 | 23,1790 | 20,6677 |
| 5.11 (a)-(b) | 99,6253 | 99,5993 | 99,5232 | 35,6071 | 33,3809 | 38,2222 | 25,9815 | 24,9950 | 29,2798 |
| 5.12 (a)-(b) | 99,6398 | 99,5697 | 99,5269 | 30,1006 | 33,3664 | 30,8193 | 22,0046 | 25,7736 | 24,5989 |
| 5.15 (a)-(b) | 99,5914 | 99,5563 | 99,5719 | 28,2722 | 29,3665 | 27,8832 | 22,9594 | 23,9743 | 23,0763 |
| 5.17 (a)-(b) | 99,6341 | 99,6082 | 99,6170 | 29,8967 | 28,5737 | 31,3537 | 22,3557 | 21,5758 | 24,0221 |

Diğer yandan önerilen algoritma, birbirinden 1 bit farkı bulunan herhangi iki orijinal görüntünün şifrelenmiş durumlarının birbirinden tamamen farklı olduğunu garanti eder. Çizelge 6.2'de gösterilen NPCR, UACI ve BACI değerleri, ilgili görüntünün şifreli hali ile 1 bit değiştirilmiş durumunun şifreli hali arasındaki rastgele seçilmiş 1500 pikselin fark analizini temsil eder.

Çizelge 6.2. Orijinal görüntülerin şifrelenmiş halleri ile 1 bit farklı versiyonlarının şifrelenmiş halleri arasındaki NPCR, UACI ve BACI değerleri

| | NPCR | | | UACI | | | BACI | | |
|---|---|---|---|---|---|---|---|---|---|
| Resim | K | Y | B | K | Y | B | K | Y | B |
| lena | 99,63 | 99,59 | 99,62 | 33,41 | 33,39 | 33,55 | 26,6683 | 26,6847 | 26,8171 |
| baboon | 99,62 | 99,60 | 99,61 | 33,45 | 33,42 | 33,48 | 26,7341 | 26,7773 | 26,7798 |
| airplane | 99,54 | 99,56 | 99,58 | 32,63 | 32,69 | 32,66 | 26,5571 | 26,5920 | 26,5130 |
| artichare | 99,57 | 99,57 | 99,57 | 33,16 | 33,15 | 33,28 | 26,4663 | 26,5525 | 26,6193 |
| Asian lady | 99,63 | 99,61 | 99,60 | 33,38 | 33,53 | 33,61 | 26,7515 | 26,8055 | 26,8084 |
| Lena [25] | 99,64 | 99,61 | 99,62 | 33,39 | 33,56 | 33,48 | - | - | - |

## 6.5. Bilgi Entropisi Analizi

Bilgi entropisi, herhangi bir görüntüdeki keyfi dağılımın ne kadar olduğunu ölçmek için kullanılabilir. Bu ölçüt aşağıdaki formül ile uygulanır [80]:

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i) \log_2 \frac{1}{p(m_i)} \tag{6.1}$$

Şifrelenmiş bir görüntünün bilgi entropisi mümkün olduğunca, ideal değer olan 8' e yakın olmalıdır [81]. Bu durum görüntü bilgisinin ifşasını zorlaştırır. Çizelge 6.3' de bazı orijinal görüntülerin önerilen algoritma ile şifrelenmiş durumlarının bilgi entropi değerlerine bakılarak 8'e yakın olduğu görülebilir.

Çizelge 6.3. Şifreli görüntülerin bilgi entropi değerleri

| Resim | K | Y | M |
|---|---|---|---|
| lena | 7,9897 | 7,9895 | 7,9892 |
| monarch | 7,9898 | 7,9893 | 7,9899 |
| peppers | 7,9862 | 7,9873 | 7,9867 |
| baboon | 7,9892 | 7,9893 | 7,9884 |
| cat | 7,9907 | 7,9904 | 7,9911 |
| baboon [25] | 7,9701 | 7,9816 | 7,9724 |

## 6.6. Korelasyon Analizi

Orijinal bir görüntünün komşu pikselleri arasında bir ilişki vardır. İstatistiksel ataklara karşı koyabilmek için, şifreli görüntüde komşu pikseller arasındaki ilişki minimum olmalıdır. Aşağıdaki formüller komşu iki piksel arasındaki korelasyonu hesaplamak için kullanılır [82]:

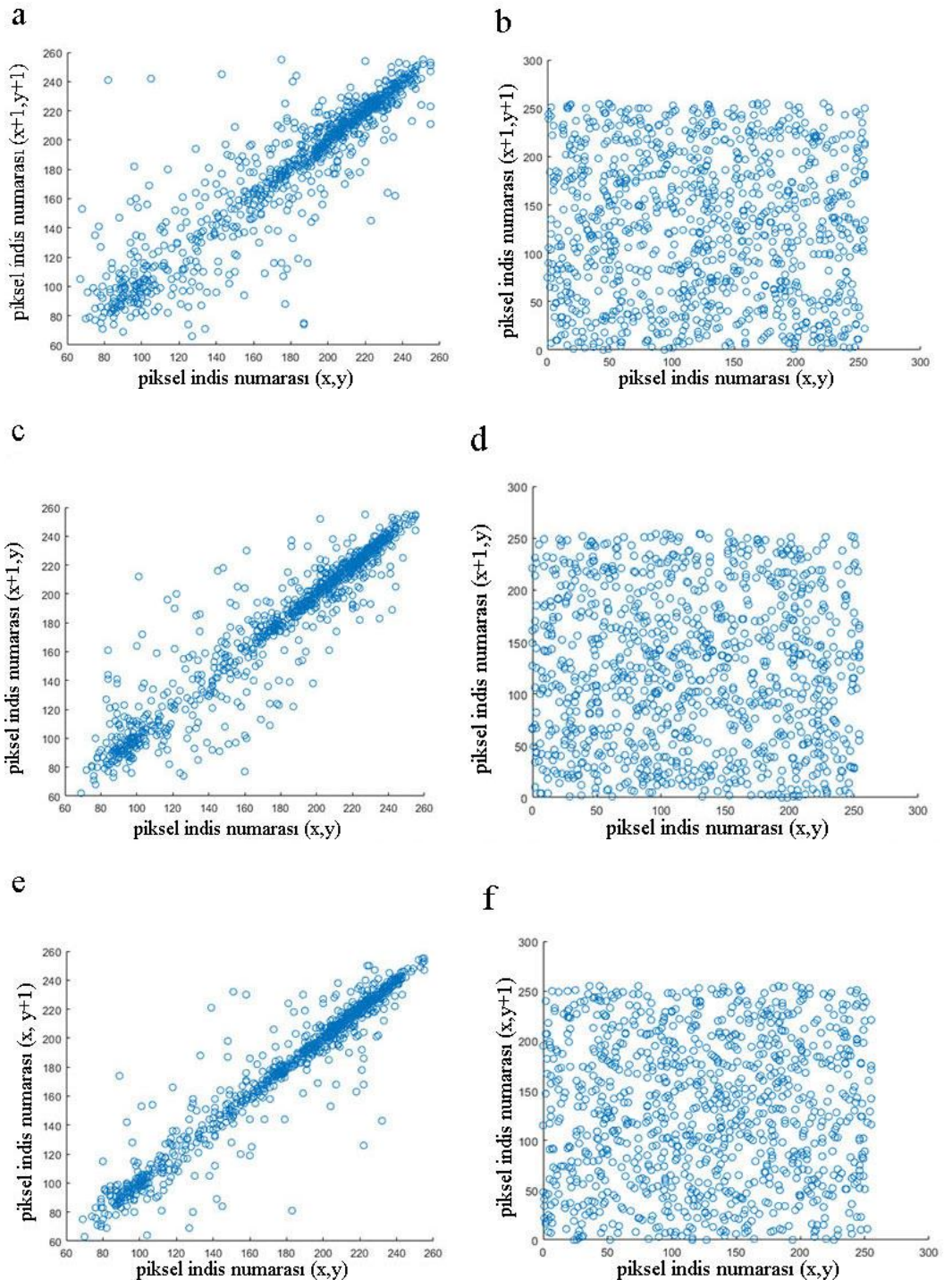
$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{6.2}$$

$$\operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{6.3}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{6.4}$$

Şekil 6.1’ de açık ve şifrelenmiş Lena görüntüsündeki, ayrı ayrı yatay, dikey ve çapraz olacak şekilde, bitişik herhangi iki pikselin korelasyon dağılımı gösterilmektedir. Buradan

şifrelenmiş görüntüde komşu pikseller arasındaki korelasyonun oldukça azaldığı görülmektedir.




Şekil 6.1. Şifreli ve açık Lena resminin komşu pikselleri arasındaki korelasyon dağılımını gösterir. (a),(c) ve (d) açık resmin, (b), (d) ve (f) açık resme karşılık gelen şifreli resmin sırasıyla çapraz, yatay ve dikey komşu piksellerin korelasyon dağılımıdır.

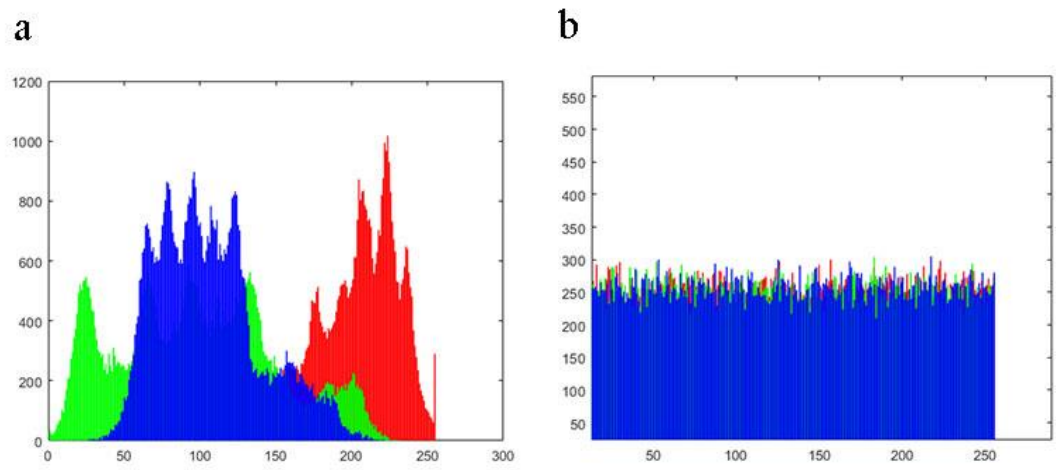
Çizelge 6.4’ de açık ve şifreli resimlerin bitişik pikselleri arasındaki korelasyonu gösterilmektedir. Sonuçlar şifreli resimlerin komşu pikselleri arasındaki bağlantının çok düşük olduğunu gösterirken açık resmin ilişkisinin de çok yüksek olduğunu gösterir.

Çizelge 6.4. Açık ve şifreli resimlerin komşu pikselleri arasındaki ortalama korelasyon değerleri

| | | Orijinal | | | Şifreli | | |
|---|---|---|---|---|---|---|---|
| Resim | Algoritma | Çapraz | Yatay | Dikey | Çapraz | Yatay | Dikey |
| Lena | Sunulan algoritma | 0,899669 | 0,968574 | 0,937493 | -0,016875 | 0,014745 | -0,007159 |
| Airplane | Sunulan algoritma | 0,945468 | 0,958525 | 0,976179 | 0,009973 | -0,003782 | -0,019320 |
| Paris | Sunulan algoritma | 0,951830 | 0,976494 | 0,965603 | -0,002965 | 0,013701 | 0,003254 |
| Artichare | Sunulan algoritma | 0,972995 | 0,984796 | 0,992501 | -0,022909 | 0,011009 | 0,014511 |
| Peppers | Sunulan algoritma | 0,901712 | 0,954639 | 0,944436 | 0,005042 | 0,006764 | 0,000393 |
| Lena | [85] | 0,9847 | 0,9271 | 0,9230 | 0,0578 | -0,0574 | -0,0035 |

## 6.7. Histogram Analizi

Bir görüntünün histogramı, piksel sayılarının dağılımı hakkında bilgi verir. Şekil 6.2’ de görüldüğü gibi orijinal resim bazı noktalar için tepe değerlere sahipken şifrelenmiş resim oldukça sabit bir dağılıma sahiptir.




Şekil 6.2. (a) Orijinal Lena görüntüsünün histogramı, (b) Şifrelenmiş Lena görüntüsünün histogramı

### 6.8. Gürültü Ataklarına Karşı Direnç Analizi

Şifrelenmiş bir resmin, gerçek iletişim kanallarından iletilirken çok çeşitli gürültülere maruz kalması kaçınılmazdır. Bu gürültü resmin orijinalinin elde edilmesi esnasında bazı problemlere yol açabilir ve orijinal görüntü net bir şekilde elde edilemez. Şifreleme sisteminin geçerli güvenilirlik düzeyine sahip olabilmesi için, tasarlanan algoritma gürültünün etkilerine karşı dirençli olmalıdır. PSNR (Peak Signal-to-Noise Ratio) ve MSE (Mean Square Error) kıstasları gürültünün etkisinden sonra şifresi çözülmüş resmin kalitesini ölçmek için kullanılır. Bu ölçütler aşağıdaki formülde gösterildiği gibidir [83]:

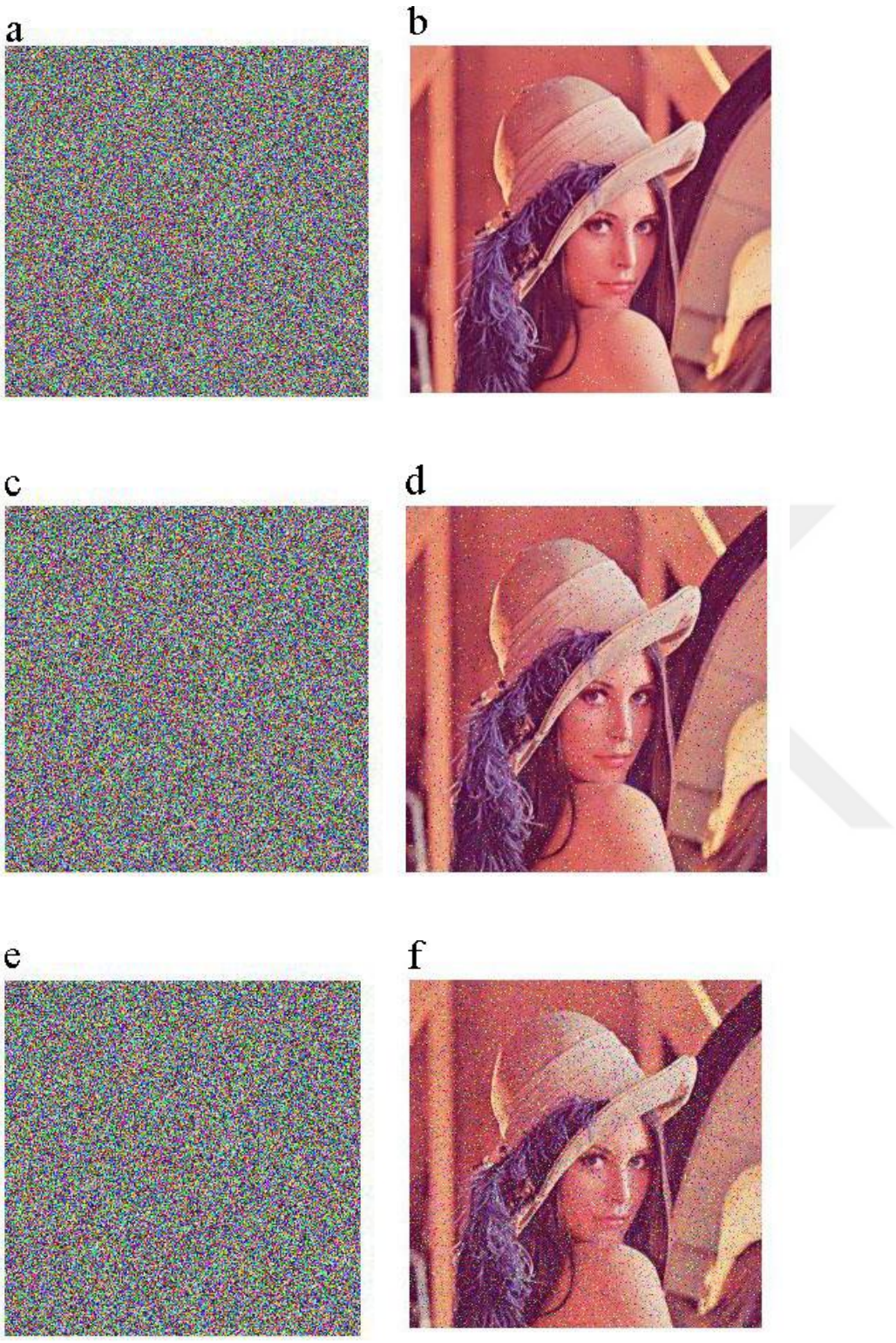
$$\mathrm{PSNR} = 10 \times \log_{10}\left(\frac{255 \times 255}{MSE}\right)(dB) \tag{6.5}$$

$$\mathrm{MSE} = \frac{1}{mn}\sum_{i=1}^{m}\sum_{i=1}^{n}\left\|I_1(i,j) - I_2(i,j)\right\|^2 \tag{6.6}$$

MSE, $I_1(i,j)$ ve $I_2(i,j)$ olarak temsil edilen ve gri seviye boyutları $mxn$ olan orijinal ve şifreli resim arasındaki ortalama kare hatasını hesaplar.

Aşağıda şifrelenmiş Lena görüntüsünün farklı şiddetlerde bir çeşit gürültüye maruz kaldıktan sonra deşifre edilebilme kalitesi gösterilmektedir (Resim 6.2). Şifreli Lena resminin gürültüye maruz bırakıldıktan sonraki deşifre edilmiş halleri Çizelge 6.5' de

gösterilmektedir. Bu analizlerden yola çıkarak, farklı şiddette gürültüye maruz bırakılan Lena şifreli resminin, orijinal haline çok yakın şekilde çözüldüğü görülmektedir. Çözülen görüntünün oldukça anlaşılabilir olması ve gürültü uygulanmadan çözülmüş Lena şifreli resmi ile arasındaki PSNR değerinin yaklaşık 30 $dB$ olması çözümün iyi yapılabildiğinin kanıtıdır. Sonuç olarak, önerilen algoritmanın belli derecede gürültü ataklarına karşı dirençli olduğu söylenebilir.




Resim 6.2. (a), (c) ve (e) sırasıyla şiddeti 0,01, 0,05 ve 0,1 olarak salt & pepper gürültüsüne maruz bırakılmış şifreli Lena resmi ve (b), (d) ve (f) sırasıyla bu görüntülerin deşifre edilmiş durumları.

Çizelge 6.5. Farklı şiddetlerde salt & pepper gürültüsüne maruz kalan şifreli Baboon görüntüsünün geri elde edinim başarısının sayısal sonuçları

| | MSE | | | | PSNR | | | |
|---|---|---|---|---|---|---|---|---|
| Gürültü Şiddeti | K | Y | M | K,Y,M Ortalama | K | Y | M | K,Y,M Ortalama |
| 0,01 | 102 | 99 | 100 | 100 | 28,0299 | 28,1526 | 28,1318 | 28,1047 |
| 0,05 | 532 | 527 | 542 | 533 | 20,8692 | 20,9129 | 20,7939 | 20,8586 |
| 0,1 | 1081 | 1070 | 1042 | 1064 | 17,7923 | 17,8376 | 17,9516 | 17,8605 |
| 0,01 [86] | | | | 107 | | | | 27,8245 |
| 0,05 [86] | | | | 538 | | | | 20,8155 |
| 0,1 [86] | | | | 1060 | | | | 17,8748 |

## 6.9. Hız Analizi

Şifreleme hızı sistemin uygulanabilirliğini yansıtır. Sistemde şifreleme ve deşifre etme işlemlerinin hızlı olabilmesi için bazı önlemler alınmıştır. Bunlardan ilki algoritmada, çok zaman tüketen işlemler yerine bit düzeyinde yapılan ayrıcalıklı veya vb. mümkün olduğunca az zaman tüketen işlemlerin kullanılmasıdır. Diğer yandan kaotik sistemden elde edilen veriler hem yayılma hem de nüfuz etme işlemi için kullanılarak tek seferlik üretim sağlanmıştır. Yine yayılma ve nüfuz etme işlemleri birleştirilerek görüntünün sadece önemli yarısına tek sefer uygulanması ve ayrıyeten nüfuz etme işleminin görüntünün tamamına tek sefer uygulanmasıyla 3 adımda gerçekleştirilecek işlem 1,5 adımda yapılmıştır. Alınan tüm bu önlemler, şifreleme hızının arttırılmasına yardımcı olabilir.

Aritmetik ve nicel operasyonlar fazla zaman tüketen işlemlerdir. Bu yüzden, şifreleme hızını değerlendirmek için piksel başına düşen nicel işlem sayısı ve piksel başına üretilen kaotik durum değişkeni sayısı bir ölçüt olarak kullanılabilir. Sunulan algoritmaya göre şifreleme için piksel başına düşen nicel işlem sayısı 1,5'dir. Diğer yandan şifreleme için piksel başına üretilen kaotik durum değişkeni sayısı 4'tür (Bkz. Eş. 4.10). Aşağıda diğer algoritmalarla şifreleme hız testi karşılaştırılmaları yapılmıştır (Çizelge 6.6). Çizelge 6.6'dan anlaşılacağı üzere, şifreleme sistemi yeterince hızlıdır.

Çizelge 6.6. Geçerli güvenilirlik düzeyine sahip şifreleme için performans ve hız analizi

| Algoritma | Piksel başına üretilen kaotik durum değişkeni sayısı | Piksel başına düşen nicel operasyon sayısı | Ortalama hız (MB/s) |
|---|---|---|---|
| Sunulan algoritma | 4 | 1,5 | 0,61 |
| [87] | 9 | 3 | - |
| [88] | 7 | 2 | - |
| [89] | - | - | 0,39 |

# 7. SONUÇ

Tasarlanan sistem için ilk olarak tek seferlik gizli anahtar üretildi. Bu anahtar, görüntüden çıkarılan benzersiz bilgi yardımıyla SHA-256 algoritması kullanılarak oluşturuldu. Böylelikle anahtarın her şifreleme işlemi için olabildiğince değişmesi garanti altına alındı.

Geniş parametre uzayına sahip kaotik davranışlar sergileyen DCD sisteminden, şifrelemede yararlanılacak bazı kaotik seriler elde edildi. Kaos üreten bu elektronik devre ailesinden DCD sistemi, başlangıç koşullarına hassas bağlılığı, basit kurulumu, geniş parametre uzayı ve hiper kaotik yapısıyla şifreleme için oldukça uygundur. Bu kaotik üretecin başlangıç parametrelerinin gizli anahtar üzerinden elde edinimi işlemi için bir algoritma tasarlandı. Bu algoritma sayesinde gizli anahtardaki küçük bir değişiklik, DCD'nin başlangıç parametrelerine olabildiğince çok tesir edecektir. Tüm bu yapılanlar sayesinde, simetrik şifreleme mantığına göre tasarlanan sistemin en önemli ögesi olan gizli anahtarın güvenliği de garanti altına alındı.

Belirli başlangıç parametreleri ile kaotik DCD sisteminin farklı kaotik çekicileri gösterildi. Bu kaotik sistemin çözümünün benzersiz çıktıları olduğu ve başlangıç parametrelerindeki ufak değişikliklerle çözümün de tamamen değiştiği gözlendi. Bu zengin kaotik sonuçlar, DCD sisteminin kriptoloji için uygunluğunu kaotik çekiciler ile gözler önüne sermektedir.

Tasarlanan şifreleme algoritmasıyla, görüntü şifreleme standartları olan yayılma ve nüfuz etme yönteminin etkili bir şekilde uygulanması sağlandı. Bu işlemler, görüntüye bit düzeyinde uygulanarak iki yöntem pratikte birleştirilerek gerçekleştirildi. Diğer yandan karıştırma metodu sadece resmin bit haritasına göre en büyük 4 değerine uygulanarak bir nevi sistem performansının olumsuz etkilenmesinin önüne geçildi. Ayrıca şifreleme işlemi için tasarlanan algoritma tamamen tersinir olduğu için orijinal görüntünün, hiçbir dış etkiye maruz kalınmadığı takdirde, geri elde ediniminde kayıp oluşmaması garanti altına alındı.

Sistemin kolaylıkla gösterimi, denenmesi, analiz edilmesi, güvenlik testlerinin yapılması için bir yazılım aracı tasarlandı. Bu araç ile şifreleme işleminin her bir adımı rahatlıkla gerçekleştirildi. Farklı algoritmaların farklı kaotik üreteçler yardımıyla hızlı bir şekilde denenmesi sağlandı. Geliştirilen bu arayüz sayesinde zamana bağlı herhangi bir kaotik üreteç rahatlıkla sisteme eklenebilir, buna bağlı üretilen diziler için yeni algoritmalar oluşturulup

hızlı bir şekilde sisteme adapte edilebilir. Bu arayüz geliştirilerek, zaman bağımsız kaotik üreteçlerin de sisteme adapte edilip çalıştırılması sağlanabilir. Tasarlanacak herhangi bir şifreleme sistemi için rahatlıkla kullanılabilir. Geliştirilmeye açık olup, literatürde resim şifreleme için kullanılabilecek önemli bir araç olarak standartlaşabilir.

Tasarlanan şifreleme sistemi renkli resimler için tasarlandı. Fakat gri seviye görüntüler için uyarlaması yapılabilir. Diğer yandan, görüntünün boyutu, şifreleme sisteminin performansının ölçülmesi için bir referans olabilir. Farklı boyutlarda farklı renkli görüntüler şifrelenerek denenmiş ve performans açısından literatüre kıyasla oldukça tatmin edici sonuçlar çıkmıştır. Dolayısıyla her türlü boyut ve formattaki resim, 256'lık düzende dijital görüntüye dönüştürüldüğü takdirde bu şifreleme sistemi için kullanılabilir.

Sistemin performansının ölçülebilmesi için birçok güvenlik testi uygulandı. Bu testler anahtar uzayı analizi, anahtar hassasiyeti ve açık resim hassasiyeti analizi, korelasyon analizi, bilgi entropisi analizi, histogram analizi, gürültü saldırılarına karşı direnç analizi, diferansiyel atak analizi, seçilmiş açık metin ve bilinen açık metin saldırılarına karşı direnç analizi ve hız analizi olacak şekilde 9 adettir. Her bir testten, şifreleme işleminin geçerli sayılabilmesi için gerekli sonuçlar alınmıştır. Sistemin özellikle anahtar hassasiyeti ve açık resim hassasiyeti oldukça iyi tasarlanmış olduğu testlerle aşikârdır. Diferansiyel ataklar, seçilmiş açık metin saldırıları ve bilinen açık metin saldırıları ve gürültü ataklarına karcı direnç sağlama literatürle de karşılaştırıldığında sistemin en güçlü yanları olarak öne çıkmaktadır.

İlerleyen zamanlarda bu tasarlanan şifreleme sistemi uygulamasının gerçek zamanlı gerçekleştirimi yapılabilir. Bu sistem için tasarlanan ve kapsamlı bir içeriğe sahip olan şifreleme arayüz yazılımı geliştirilip yeni özellikler eklenebilir. Yeni güvenlik testleri ve kaotik üreteçler sisteme eklenebilir. Sistem şu an sadece zamana bağlı kaotik sistemler için çalışmaktadır. Geliştirme yapılarak zaman bağımsız sistemler içinde uygun hale getirilebilir. Tasarlanan algoritma mantığı farklı şifreleme sistemleri için denenebilir. Yine bu algoritma farklı kaotik üreteçler ile kullanılabilir.

Sonuç olarak literatüre, DCD kaotik sisteminin benzersiz kaotik çekicilerinin varlığı ve şifreleme alanında uygulanabilirliği, görüntü şifreleme işlemleri için kullanılabilecek bir

şifreleme sistemi ve bu işlemlerin geliştiriciler tarafından gerçekleştirilip incelenebilmesini sağlayan bir kullanıcı arayüzü kazandırılmıştır.

# KAYNAKLAR


1. Alvarez, G., and Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. ***International journal of bifurcation and chaos***, *16*(08), 2129-2151

2. Liu, H., Kadir, A., and Niu, Y. (2014). Chaos-based color image block encryption scheme using S-box. ***AEU-international Journal of Electronics and Communications,*** *68*(7), 676-686

3. Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. ***International Journal of Bifurcation and chaos***, *8*(06), 1259-1284

4. Kiraz, M. S., and Uzunkol, O. (2016). Efficient and verifiable algorithms for secure outsourcing of cryptographic computations. ***International Journal of Information Security***, *15*(5), 519-537

5. Stinson, D. R. (2005). Cryptography: theory and practice. ***Chapman and Hall/CRC***

6. Fu, C., Lin, B. B., Miao, Y. S., Liu, X., and Chen, J. J. (2011). A novel chaos-based bit-level permutation scheme for digital image encryption. ***Optics communications***, *284*(23), 5415-5423

7. Murillo-Escobar, M. A., Cruz-Hernández, C., Abundiz-Pérez, F., López-Gutiérrez, R. M., and Del Campo, O. A. (2015). A RGB image encryption algorithm based on total plain image characteristics and chaos. ***Signal Processing***, *109*, 119-131

8. Liu, H., and Wang, X. (2010). Color image encryption based on one-time keys and robust chaotic maps. ***Computers & Mathematics with Applications***, *59*(10), 3320-3327

9. Parvaz, R., and Zarebnia, M. (2018). A combination chaotic system and application in color image encryption. ***Optics & Laser Technology***, *101*, 30-41

10. Chai, X., Gan, Z., Yuan, K., Chen, Y., and Liu, X. (2019). A novel image encryption scheme based on DNA sequence operations and chaotic systems. ***Neural Computing and Applications***, *31*(1), 219-237

11. Wang, Y., Quan, C., and Tay, C. J. (2016). Asymmetric optical image encryption based on an improved amplitude–phase retrieval algorithm. ***Optics and Lasers in Engineering***, *78*, 8-16

12. Luo, Y., Yu, J., Lai, W., and Liu, L. (2019). A novel chaotic image encryption algorithm based on improved baker map and logistic map. ***Multimedia Tools and Applications***, 1-21

13. Jiang, N., Dong, X., Hu, H., Ji, Z., and Zhang, W. (2019). Quantum Image Encryption Based on Henon Mapping. ***International Journal of Theoretical Physics***, *58*(3), 979-991

14. Zhou, S., Zhang, Q., Wei, X., and Zhou, C. (2010). A summarization on image encryption. ***IETE Technical Review***, *27*(6), 503-510

15. Guan, Z. H., Huang, F., and Guan, W. (2005). Chaos-based image encryption algorithm. ***Physics Letters A***, *346*(1-3), 153-157

16. Gao, H., Zhang, Y., Liang, S., and Li, D. (2006). A new chaotic algorithm for image encryption. ***Chaos, Solitons & Fractals***, *29*(2), 393-399

17. Zhou, Y., Bao, L., and Chen, C. P. (2014). A new 1D chaotic system for image encryption. ***Signal processing***, *97*, 172-182

18. Chiaraluce, F., Ciccarelli, L., Gambi, E., Pierleoni, P., and Reginelli, M. (2002). A new chaotic algorithm for video encryption. ***IEEE Transactions on Consumer Electronics***, *48*(4), 838-844

19. Behnia, S., Akhshani, A., Mahmodi, H., and Akhavan, A. (2008). A novel algorithm for image encryption based on mixture of chaotic maps. ***Chaos, Solitons & Fractals***, *35*(2), 408-419

20. Pan, H., Lei, Y., & Jian, C. (2018). Research on digital image encryption algorithm based on double logistic chaotic map. ***EURASIP Journal on Image and Video Processing***, *2018*(1), 142

21. Sharma, S., Kumar, T., Dhaundiyal, R., Mishra, A. K., Duklan, N., & Maithani, A. (2019). Improved method for image security based on chaotic-shuffle and chaotic-diffusion algorithms. ***International Journal of Electrical and Computer Engineering***, *9*(1), 273

22. Ye, R. (2011). A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism. ***Optics Communications***, *284*(22), 5290-5298

23. Mazloom, S., and Eftekhari-Moghadam, A. M. (2009). Color image encryption based on coupled nonlinear chaotic map. ***Chaos, Solitons & Fractals***, *42*(3), 1745-1754

24. Zhu, Z. L., Zhang, W., Wong, K. W., and Yu, H. (2011). A chaos-based symmetric image encryption scheme using a bit-level permutation. ***Information Sciences***, *181*(6), 1171-1186

25. Teng, L., Wang, X., and Meng, J. (2018). A chaotic color image encryption using integrated bit-level permutation. ***Multimedia Tools and Applications***, *77*(6), 6883-6896

26. Kurt, E. (2006). Nonlinearities from a non-autonomous chaotic circuit with a non-autonomous model of Chua's diode. ***Physica Scripta***, *74*(1), 22

27. Gilbert, H., & Handschuh, H. (2003, August). Security analysis of SHA-256 and sisters. ***International workshop on selected areas in cryptography*** (175-193). Springer, Berlin, Heidelberg.

28. Chai, X. (2017). An image encryption algorithm based on bit level Brownian motion and new chaotic systems. ***Multimedia Tools and Applications***, *76*(1), 1159-1175

29. Semmlow, J. (2017). Circuits, Signals and Systems for Bioengineers: A MATLAB-based Introduction (Third edition). London: Academic Press, 1-792.

30. Pecora, L. M., and Carroll, T. L. (1990). Synchronization in chaotic systems. ***Physical review letters***, *64*(8), 821.

31. Boccaletti, S., Kurths, J., Osipov, G., Valladares, D. L., and Zhou, C. S. (2002). The synchronization of chaotic systems. ***Physics reports***, *366*(1-2), 1-101

32. Kurt, E., Ve Kasap, R. (2011). Karmaşanın Bilimi Kaos. Ankara: Nobel Akademik Yayıncılık, 1-214.

33. Pamuk, N. (2013). Dinamik Sistemlerde Kaotik Zaman Dizilerinin Tespiti. ***Balıkesir Üniversitesi Fen Bilimleri Enstitüsü Dergisi***, *15*(1), 78-92

34. Zou, F., and Nossek, J. A. (1993). Bifurcation and chaos in cellular neural networks. ***IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications***, *40*(3), 166-173

35. Vaidyanathan, S., and Volos, C. (Eds.). (2016). Advances and applications in chaotic systems, (Vol. 636, p. 445). ***Springer***, Berlin, Germany

36. Tucker, W. (1999). The Lorenz attractor exists. ***Comptes Rendus de l'Académie des Sciences-Series I-Mathematics***, *328*(12), 1197-1202

37. Ioana-Elena, E. N. E. (2018). Chaos theory, a modern approach of nonlinear dynamic systems. ***Romanian Journal of Information Technology and Automatic Control***, *28*(4), 89-96

38. İnternet: Brain Corporation, Chua Circuit, URL: http://www.scholarpedia.org/article/Chua's_circuit, Son Erişim Tarihi: 17.05.2019

39. Cafagna, D., and Grassi, G. (2008). Fractional-order Chua's circuit: time-domain analysis, bifurcation, chaotic behavior and test for chaos. ***International Journal of Bifurcation and Chaos***, *18*(03), 615-639

40. Csiszár, I., and Narayan, P. (1997, June). *Common randomness and secret key generation with a helper*. In Proceedings of IEEE International Symposium on Information Theory (157). Germany, UIm

41. Gabidulin, E. M., Paramonov, A. V., and Tretjakov, O. V. (1991, April). Ideals over a non-commutative ring and their application in cryptology. **In *Workshop on the Theory and Application of Cryptographic Techniques*** (pp. 482-489). Springer, Berlin, Heidelberg

42. Macq, B. M., and Quisquater, J. J. (1995). Cryptology for digital TV broadcasting. ***Proceedings of the IEEE***, *83*(6), 944-957

43. Damgård, I., and Jurik, M. (2001, February). A generalisation, a simpli. cation and some applications of paillier's probabilistic public-key system. **In *International Workshop on Public Key Cryptography*** (119-136), Springer, Berlin, Heidelberg

44. Singh, G. (2013). A study of encryption algorithms (RSA, DES, 3DES and AES) for information security. ***International Journal of Computer Applications***, *67*(19), 33-37.

45. Michalski, A., Gaj, K., and El-Ghazawi, T. (2003, September). An implementation comparison of an IDEA encryption cryptosystem on two general-purpose reconfigurable computers. **In *International Conference on Field Programmable Logic and Applications*** (204-219). Springer, Berlin, Heidelberg

46. Chen, G., Mao, Y., & Chui, C. K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. ***Chaos, Solitons & Fractals***, *21*(3), 749-761

47. Lian, S., Sun, J., & Wang, Z. (2005). A block cipher based on a suitable use of the chaotic standard map. ***Chaos, Solitons & Fractals***, *26*(1), 117-129

48. Xiao, D., Liao, X., & Wei, P. (2009). Analysis and improvement of a chaos-based image encryption algorithm. ***Chaos, Solitons & Fractals***, *40*(5), 2191-2199

49. Wang, Y., Wong, K. W., Liao, X., & Chen, G., (2011). A new chaos-based fast image encryption algorithm. ***Applied soft computing***, *11*(1), 514-522

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

51. Daemen, J., and Rijmen, V, (2013). The design of Rijndael: AES-the advanced encryption standard. ***Springer Science & Business Media***, 1-38.

52. Huang, X., & Ye, G. (2014). An efficient self-adaptive model for chaotic image encryption algorithm. ***Communications in Nonlinear Science and Numerical Simulation***, *19*(12), 4094-4104

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

54. Unnikrishnan, G., Joseph, J., and Singh, K. (2000). Optical encryption by double-random phase encoding in the fractional Fourier domain. ***Optics letters***, *25*(12), 887-889

55. UbaidurRahman, N. H., Balamurugan, C., and Mariappan, R. (2015). A novel DNA computing based encryption and decryption algorithm. ***Procedia Computer Science***, *46*, 463-475

56. Lu, X., Lei, J., Li, W., Lai, K., & Pan, Z. (2019). Physical Layer Encryption Algorithm Based on Polar Codes and Chaotic Sequences. ***IEEE Access***, *7*, 4380-4390

57. Patel, K. D., & Belani, S. (2011). Image encryption using different techniques: A review. ***International Journal of Emerging Technology and Advanced Engineering***, *1*(1), 30-34

58. Bu, S., & Wang, B. H. Improving the security of chaotic encryption by using a simple modulating method. ***Chaos, Solitons & Fractals***, *19*(4), 919-924.

59. Nichat, S. P., & Sikchi, S. S. (2013). Image encryption using hybrid genetic algorithm. ***International Journal of Advanced Research in Computer Science and Software Engineering***, *3*(1), 427-431.

60. Matthews, R. (1984). On the derivation of a "Chaotic" encryption algorithm. ***Cryptologia***, *8*(1), 29-41

61. Fridrich, J. (1997, October). Image encryption based on chaotic maps. ***In 1997 IEEE International Conference on Systems, Man, and Cybernetics. Computational Cybernetics and Simulation***(1105-1110). USA, Orlando.

62. Pareek, N. K., Patidar, V., & Sud, K. K. (2006). Image encryption using chaotic logistic map. ***Image and vision computing***, *24*(9), 926-934

63. Peng, J., Zhang, D., & Liao, X. (2009). A digital image encryption algorithm based on hyper-chaotic cellular neural network. ***Fundamenta Informaticae***, *90*(3), 269-282

64. LI, P., & TIAN, D. P. (2008). Digital Image Encryption Algorithm Based on Hyperchaotic Sequence [J]. ***Microelectronics & Computer***, 3, 1-10.

65. HU, Y. F., & ZHU, S. A. (2008). Research of Chaos Scrambling in Image Watermarking System [J]. ***Chinese Journal of Electron Devices***, 5, 1-10

66. Chen, J. X., Zhu, Z. L., Fu, C., Yu, H., & Zhang, L. B. (2015). A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. ***Communications in Nonlinear Science and Numerical Simulation***, *20*(3), 846-860

67. Wei-Bin, C., & Xin, Z. (2009, April). Image encryption algorithm based on Henon chaotic system. **In *2009 International Conference on Image Analysis and Signal Processing*** (94-97), China, Taizhou.

68. Marotto, F. R. (1979). Chaotic behavior in the Hénon mapping. ***Communications in Mathematical Physics***, *68*(2), 187-194

69. Li, C., & Chen, G. (2004). Chaos and hyperchaos in the fractional-order Rössler equations. ***Physica A: Statistical Mechanics and its Applications***, *341*, 55-61

70. Liu, H., Zhu, Z., Jiang, H., & Wang, B. (2008, November). A novel image encryption algorithm based on improved 3D chaotic cat map. **In *2008 The 9th International Conference for Young Computer Scientists*** (3016-3021). China, Hunan.

71. Zhen, W., Xia, H., Yu-Xia, L., & Xiao-Na, S. (2013). A new image encryption algorithm based on the fractional-order hyperchaotic Lorenz system. ***Chinese Physics B***, *22*(1), 1-7.

72. Gong-bin, Q., Qing-feng, J., & Shui-sheng, Q. (2009, May). A new image encryption scheme based on DES algorithm and Chua's circuit. **In *2009 IEEE International Workshop on Imaging Systems and Techniques*** (168-172). China, Shenzhen.

73. Alvarez, G., Montoya, F., Romera, M., & Pastor, G. (2004). Cryptanalyzing a discrete-time chaos synchronization secure communication system. ***Chaos, Solitons & Fractals***, *21*(3), 689-694

74. Zhang, H., & Cai, R. (2010, October). Image encryption algorithm based on bit-plane scrambling and multiple chaotic systems combination. **In *2010 International Conference on Intelligent Computing and Integrated Systems*** (113-117). China, Guilin.

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

76. Deepan, B., Quan, C., Wang, Y., & Tay, C. J. (2014). Multiple-image encryption by space multiplexing based on compressive sensing and the double-random phase-encoding technique. ***Applied optics***, *53*(20), 4539-4547.

77. Biham, E. (1994, May). On Matsui's linear cryptanalysis. **In *Workshop on the Theory and Application of Cryptographic Techniques*** (pp. 341-355). Springer, Berlin, Heidelberg.

78. Zhang, Y., & Xiao, D. (2014). Self-adaptive permutation and combined global diffusion for chaotic color image encryption. ***AEU-International Journal of Electronics and Communications***, *68*(4), 361-368.

79. Seyedzadeh, S. M., & Mirzakuchaki, S. (2012). A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map. ***Signal processing***, *92*(5), 1202-1215.

80. Wang, X. Y., Chen, F., & Wang, T. (2010). A new compound mode of confusion and diffusion for block encryption of image based on chaos. ***Communications in Nonlinear Science and Numerical Simulation***, *15*(9), 2479-2485.

81. Mirzaei, O., Yaghoobi, M., & Irani, H. (2012). A new image encryption method: parallel sub-image encryption with hyper chaos. ***Nonlinear Dynamics***, *67*(1), 557-566.

82. Rhouma, R., Meherzi, S., & Belghith, S. (2009). OCML-based colour image encryption. ***Chaos, Solitons & Fractals***, *40*(1), 309-318.

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

84. Wolf, A., Swift, J. B., Swinney, H. L., & Vastano, J. A. (1985). Determining Lyapunov exponents from a time series. ***Physica D: Nonlinear Phenomena***, *16*(3), 285-317.

85. Liu, H., And Wang, X. (2011). Color image encryption using spatial bit-level permutation and high-dimension chaotic system. ***Optics Communications***, *284*(16-17), 3895-3903.

86. Xiong, Z., Wu, Y., Ye, C., Zhang, X., and Xu, F. (2019). Color image chaos encryption algorithm combining CRC and nine palace map. ***Multimedia Tools and Applications***, 1-21.

87. Mao, Y., Chen, G., & Lian, S. (2004). A novel fast image encryption scheme based on 3D chaotic baker maps. ***International Journal of Bifurcation and chaos***, *14*(10), 3613-3624.

88. Wang, Y., Wong, K. W., Liao, X., Xiang, T., and Chen, G. (2009). A chaos-based image encryption algorithm with variable control parameters. ***Chaos, Solitons & Fractals***, *41*(4), 1773-1783.

89. Chai, X., Zheng, X., Gan, Z., Han, D., and Chen, Y. (2018). An image encryption algorithm based on chaotic system and compressive sensing. ***Signal Processing***, *148*, 124-144.

# ÖZGEÇMİŞ

## Kişisel Bilgiler


Soyadı, adı : ARPACI, Batuhan

Uyruğu : T.C.

Doğum tarihi ve yeri : 05.11.1992 / Ankara

Medeni hali : Evli

Telefon : 0 (534) 938 68 79

e-mail : bthnrpc@gmail.com


## Eğitim

| Derece | Eğitim Birimi | Mezuniyet Tarihi |
|---|---|---|
| Lise | Çağrıbey Anadolu Lisesi | 2010 |
| Lisans | Hacettepe Üniversitesi/ Matematik Bölümü | 2014 |

## İş Tecrübesi

| Tarih | Yer | Görev |
|---|---|---|
| 2015 Ekim- 2016 Mart | Küresel Yazılım | Yazılım Geliştirici |
| 2016 Ekim- Günümüz | Türkiye Belediyeler Birliği | Yazılım Mühendisi |

## Yabancı Dil

İngilizce

## Konferanslar

**1.** Arpacı, B., Kurt, E., And Çelik, K., "A New Algorithm for the Colored Image Encryption via the Modified Chua's Circuit", ***International Conferance on Cyber Security and Computer Science***", Karabük, 58-66, (October 2018).

## Hobiler

Yüzme, Futbol, Doğa yürüyüşü, Popüler bilim

**GAZİLİ OLMAK AYRICALIKTIR.**