T.C.
YOZGAT BOZOK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ
ANABİLİM DALI

KESİR-DERECELİ KAOTİK SİSTEMLER İLE GÖMÜLÜ SİSTEM TABANLI KRİPTOLOJİ VE STEGANOGRAFİ UYGULAMASI

BERKAY EMİN

DOKTORA TEZİ

Danışman: Dr. Öğr. Üyesi Mustafa YAZ

İkinci Danışman: Prof. Dr. Akif AKGÜL

EYLÜL – 2024

YOZGAT

T.C.
YOZGAT BOZOK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI

KESİR-DERECELİ KAOTİK SİSTEMLER İLE GÖMÜLÜ SİSTEM TABANLI KRİPTOLOJİ VE STEGANOGRAFİ UYGULAMASI

BERKAY EMİN

DOKTORA TEZİ

Danışman: Dr. Öğr. Üyesi Mustafa YAZ

İkinci Danışman: Prof. Dr. Akif AKGÜL

EYLÜL – 2024

YOZGAT

	YOZGAT BOZOK ÜNİVERSİTESİ **LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ** **LİSANSÜSTÜ TEZ ONAY FORMU**

T.C.

YOZGAT BOZOK ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Enstitümüzün Elektrik Elektronik Mühendisliği Anabilim Dalı Doktora Programı öğrencisi Berkay EMİN'in hazırladığı "**Kesir-Dereceli Kaotik Sistemler ile Gömülü Sistem Tabanlı Kriptoloji ve Steganografi Uygulaması**" başlıklı tezi ile ilgili tez savunma sınavı, Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliği'nin ilgili maddeleri gereğince 03/09/2024 Salı günü saat 14:00'da yapılmış, tezin onayına oy birliği ile karar verilmiştir.

Başkan : Doç. Dr. Mehmet EKİCİ

Jüri Üyesi : Dr. Öğr. Üyesi Mustafa YAZ (Danışman)

Jüri Üyesi : Prof. Dr. Akif AKGÜL (İkinci Danışman)

Jüri Üyesi : Dr. Öğr. Üyesi Cemil ALTIN

Jüri Üyesi : Dr. Öğr. Üyesi Yusuf ALACA

Jüri Üyesi : Dr. Öğr. Üyesi Emre DENİZ

ONAY:

Bu tezin kabulü, Enstitü Yönetim Kurulu'nun ……../……../….. tarih ve …… sayılı Enstitü Yönetim Kurulu Kararı ile onaylanmıştır.

…...../……../……..

Prof. Dr. Ümit BUDAK

Lisansüstü Eğitim Enstitüsü Müdürü

TEZ BEYANI

Tez yazım kurallarına uygun olarak hazırlanan bu tezin yazılmasında bilimsel ahlak kurallarına uyulduğunu, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, tezin içerdiği yenilik ve sonuçların başka bir yerden alınmadığını, kullanılan verilerde herhangi bir tahrifat yapılmadığını, tezin herhangi bir kısmının bu üniversite veya başka bir üniversitedeki başka bir tez çalışması olarak sunulmadığını beyan eder, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Berkay EMİN

03/09/2024

ÖN SÖZ

Doktora eğitimim süresince, kıymetli bilgi ve tecrübeleriyle bana her zaman destek olan, araştırmamın planlanmasından yazılmasına kadar her aşamada yardımlarını esirgemeyen, teşvik eden ve yönlendiren değerli ortak danışman hocam Prof. Dr. Akif AKGÜL'e ve danışman hocam Dr. Öğr. Üyesi Mustafa YAZ'a en derin şükranlarımı sunarım.

Tez izleme komitemde bulunarak değerli bilgi ve fikirleriyle beni yönlendiren kıymetli hocalarım Doç. Dr. Mehmet EKİCİ ve Dr. Öğr. Üyesi Cemil ALTIN'a en içten teşekkürlerimi sunarım.

Bu süreçte, bilgi ve deneyimlerinden yararlanma fırsatı bulduğum değerli hocalarım Doç. Dr. Zabit MUSAYEV, Doç. Dr. Abdullah GÖKYILDIRIM, Doç. Dr. Haris ÇALGAN, Dr. Öğr. Üyesi Fahrettin HORASAN, Prasina ALEXANDER, Isidore Komofor NGONGIAH, Chandra Sekhar DEVARAPU, Rameshbabu RAMAR, Sundarapandian VAIDYANATHAN, Christos VOLOS, Rajeshkanna SUBRAMANI ve Sifeu Takougang KINGNI hocalarıma en içten teşekkürlerimi sunarım.

Tez çalışmam ve hayatım boyunca daima yanımda olan, emeklerinin karşılığını asla tam olarak ödeyemeyeceğim kıymetli anneme, babama ve ağabeyime en derin minnet ve teşekkürlerimi sunarım.

Sabırları, anlayışı ve sonsuz desteğiyle her zaman yanımda olan sevgili eşim Eda Hanım'a sonsuz şükranlarımı sunarım.

Berkay EMİN

03/09/2024

ÖZET

DOKTORA TEZİ

KESİR-DERECELİ KAOTİK SİSTEMLER İLE GÖMÜLÜ SİSTEM TABANLI KRİPTOLOJİ VE STEGANOGRAFİ UYGULAMASI

BERKAY EMİN

YOZGAT BOZOK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
ELEKTRİK ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI

TEZ DANIŞMANI: DR. ÖĞR. ÜYESİ MUSTAFA YAZ
İKİNCİ DANIŞMAN: PROF. DR. AKİF AKGÜL

Bu tez çalışmasında, Arneodo ve Sprott B kaotik sistemleri Incommensurate kesir-dereceli olarak tasarlanmıştır. Sistemlerin denge noktaları bulunmuş, zaman serileri ve faz portreleri elde edilmiş ve Lyapunov üstel değerleri hesaplanmıştır. Parametre değişimlerine göre Lyapunov üstel spektrumları ve çatallaşma diyagramları çizilmiştir. Incommensurate kesir-dereceli sistemler Nvidia Jetson AGX Orin üzerinde modellenerek simülasyonlar yapılmış ve tasarlanan elektronik kart aracılığıyla devre uygulamaları gerçekleştirilmiştir.

Bu kaotik denklemler Grünwald–Letnikov yöntemiyle ayrıklaştırılmış ve tez kapsamında önerilen RSÜ algoritması kullanılarak gömülü sistem tabanlı, özgün RSÜ tasarımı yapılmıştır. Tasarlanan RSÜ'ler, uluslararası alanda kabul gören NIST 800-22, FIPS 140-1 ve ENT istatistiksel testlerinden başarıyla geçerek şifreleme ve steganografi algoritmalarının geliştirilmesinde temel alınmıştır. Incommensurate kesir-dereceli kaotik RSÜ kullanılarak gömülü sistem tabanlı özgün bir görüntü şifreleme algoritması geliştirilmiştir. Her iki kaotik sistem temelli şifreleme algoritmasının başarımı, şifrelenen görüntülerin güvenlik analizleri yapılarak ölçülmüştür. Bu sayede hem Incommensurate kesir dereceli Arneodo (IKA) hem de Incommensurate kesir dereceli Sprott B (IKSB) kaotik sistemlerinin gömülü sistem tabanlı şifreleme uygulamalarında başarıyla kullanılabileceği gösterilmiştir.

Ayrıca, tasarlanan RSÜ kullanılarak gömülü sistem tabanlı bir görüntü steganografi algoritması geliştirilmiştir. Geliştirilen steganografi uygulaması, iki seviyeli güvenliğe sahiptir. Her iki kaotik sistem temelli steganografi algoritmasının başarımı, stego görüntülerin güvenlik analizleri yapılarak ölçülmüştür. Bu sayede hem IKA hem de IKSB kaotik sistemlerinin, gömülü sistem tabanlı steganografi uygulamalarında başarıyla kullanılabileceği gösterilmiştir.

2024, xvii + 138 Sayfa

Anahtar Kelimeler: Incommensurate Kesir Dereceli Kaotik Sistemler, Rastgele Sayı Üretici, Rasgelelik Testleri, Kaos Tabanlı Şifreleme, Kaos Tabanlı Steganografi, Güvenlik Analizleri

ABSTRACT

DOCTORATE THESIS

EMBEDDED SYSTEM BASED CRYPTOLOGY AND STEGANOGRAPHY APPLICATION WITH FRACTIONAL-ORDER CHAOTIC SYSTEMS

BERKAY EMIN

YOZGAT BOZOK UNIVERSITY

SCHOOL OF GRADUATE STUDIES

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING

SUPERVISOR: ASSOC. PROF. DR. MUSTAFA YAZ

CO-SUPERVISOR: PROF. DR. AKIF AKGUL

In this thesis, the Arneodo and Sprott B chaotic systems have been designed as incommensurate fractional-order systems. The equilibrium points of the systems were identified, time series and phase portraits were obtained, and Lyapunov exponents were calculated. Lyapunov exponent spectra and bifurcation diagrams were plotted according to parameter variations. The incommensurate fractional-order systems were modeled on the Nvidia Jetson AGX Orin, and simulations were performed, followed by circuit implementations through a custom-designed electronic board.

These chaotic equations were discretized using the Grünwald–Letnikov method, and an original Pseudorandom Number Generator (PRNG) design, based on the embedded system and using the proposed PRNG algorithm within this thesis, was realized. The designed PRNGs successfully passed internationally recognized statistical tests, including NIST 800-22, FIPS 140-1, and ENT, serving as the foundation for encryption and steganography algorithms. An original image encryption algorithm based on an embedded system was developed using the incommensurate fractional-order chaotic PRNG. The performance of both chaotic system-based encryption algorithms was evaluated by conducting security analyses of the encrypted images, demonstrating the successful application of both the Incommensurate Fractional-Order Arneodo (IKA) and Incommensurate Fractional-Order Sprott B (IKSB) chaotic systems in embedded system-based encryption.

Additionally, an embedded system-based image steganography algorithm was developed using the designed PRNG. The developed steganography application features a two-level security mechanism. The performance of both chaotic system-based steganography algorithms was evaluated by conducting security analyses of the stego images, demonstrating the successful application of both IKA and IKSB chaotic systems in embedded system-based steganography.

2024, xvii + 138 Pages
Keywords: Incommensurate Fractional Order Chaotic Systems, Random Number Generators, Randomness Tests, Chaos Based Encryption, Chaos Based Steganography, Security Analysis

İÇİNDEKİLER

Sayfa

TABLOLAR LİSTESİ

Tablo **Sayfa**

ŞEKİLLER LİSTESİ

Şekil **Sayfa**

SİMGELER ve KISALTMALAR LİSTESİ

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

Simgeler	**Açıklamalar**
χ^2	**:** Ki-Kare
dB	**:** Desibel
s	**:** Saniye
Kısaltmalar	**Açıklamalar**
RSÜ	**:** Rastgele Sayı Üreteci
RBD	**:** Rastgele Bit Dizisi
ORS	**:** Ondalık Rastgele Sayılar
FIPS	**:** Federal Bilgi İşleme Standartları
NIST	**:** Ulusal Standartlar ve Teknoloji Enstitüsü
IEEE-754	**:** IEEE Kayan noktalı sayı formatı
P-değeri	**:** NIST 800-22 testinde rasgelelik ölçütü
PRN	**:** Sahte Rastgele Sayı
LSB	**:** En Az Anlamlı Bit
MSB	**:** En Anlamlı Bit
DSP	**:** Dijital Sinyal İşlemcisi
FPGA	**:** Alan Programlanabilir Kapı Dizisi
AES	**:** Gelişmiş Şifreleme Standardı
DES	**:** Veri Şifreleme Standardı
RSA	**:** Rivest-Shamir-Adleman
ECC	**:** Eliptik Eğri Kriptografisi
HMAC	**:** Hash Tabanlı Mesaj Doğrulama Kodu

MD : Mesaj Özeti Algoritması

SHA : Güvenli Hash Algoritması

PNG : Taşınabilir Ağ Grafikleri

BPCS : Bit Düzlemi Karmaşıklık Segmentasyonu

TOPS : Saniyede Tera İşlem

SRSÜ : Sözde Rastgele Sayı Üreteçleri

GRSÜ : Gerçek Rastgele Sayı Üreteçleri

NPCR : Piksel Değişim Oranı

UACI : Birleştirilmiş Ortalama Değişim Yoğunluğu

GLCM : Gri Düzey Birlikte Oluşum Matrisi

MSE : Ortalama Karesel Hata

PSNR : Tepe Sinyal-Gürültü Oranı

UIQI : Evrensel Görüntü Kalitesi Endeksi

IF : Görüntü Doğruluğu

TI : Texas Instruments

IKA : Incommensurate kesir dereceli Arneodo

IKSB : Incommensurate kesir dereceli Sprott B

DAC : Dijital Analog Dönüştürücü

SPI : Seri Çevresel Arayüz

XOR : Exclusive Or (Özel veya)

RDB : Rastgele Bit Dizisi

ORS : Ondalıklı Rastgele Sayılar

GP : Görüntü Pikselleri

KGP : Karıştırılmış Görüntü Pikselleri

ŞGP : Şifrelenmiş Görüntü Pikselleri

ÇGP : Çözülmüş Görüntü Pikseller

1. GİRİŞ

Son yıllarda dijital dönüşüm; internetin yaygınlaşması, sosyal medya kullanımının artması ve mobil cihazların günlük yaşamın ayrılmaz bir parçası haline gelmesiyle hız kazanmıştır. COVID-19 pandemisi sırasında dijital verilerde büyük bir artış yaşanmış, eğitimde dijital ders içerikleri ve çevrimiçi sınavlar, sağlıkta ise elektronik sağlık kayıtları ve tele tıp uygulamaları öne çıkmıştır. Bu gelişmeler, dijital verilerin güvenli bir şekilde yönetilmesi ve saklanması gerekliliğini artırmıştır. Özellikle savunma sanayii bağlamında, ülkemizin jeopolitik riskleri ve stratejik coğrafi konumu dikkate alındığında, veri güvenliği kritik öneme sahiptir.

Kaotik sistemler, son yıllarda bilim ve mühendislik dünyasında geniş bir araştırma konusu haline gelmiştir. Teknolojinin ilerlemesiyle birlikte kaos bilimi; haberleşme, görüntü işleme, bulanık mantık, kontrol, fizik, optimizasyon ve mekatronik gibi birçok alanın yanı sıra başlangıç değerlerine duyarlılıkları, ergodiklikleri ve karmaşık davranışları gibi avantajları nedeniyle özellikle bilgi güvenliği çalışmalarında da sıklıkla kullanılmaya başlanmıştır. Kesir dereceli kaotik sistemlerin, tamsayı mertebesindeki sistemlere kıyasla daha fazla karmaşıklık sunarak, şifrelemenin güvenliğini artırmak mümkündür. Özellikle incommensurate kesir dereceli kaotik sistemlerin, kesir dereceli sistemlere göre yüksek karmaşıklık, genişletilmiş parametre alanı, artan güvenlik seviyesi, gelişmiş performans ve çok yönlülük gibi özelliklerinden dolayı ek avantajlar sağlamaktadır.

Kaotik dinamiklerin özelliklerinden faydalanmak ve bu özellikleri gerçek dünyada uygulayabilmek için öncelikle dinamiklerin gerçek anlamda oluşturulması gerekmektedir. Bu doğrultuda ise literatürde, çeşitli kaotik denklemlerin kaotik sinyal üreten devre modelleri tasarlanmıştır. Gömülü sistem tabanlı üretilen kaotik sinyalleri ise gerçek anlamda oluşturabilmek için harici kartlar kullanılmaktadır.

Kaos tabanlı yöntemlerle şifrelenen bir veriyi deşifre edebilmek için, kaotik sistemin tüm denklemlerini, parametrelerini ve başlangıç koşullarını eksiksiz olarak bilmek gereklidir. Şifre çözme sürecinde yapılacak en küçük bir hata, şifreli verinin doğru bir şekilde çözümlenmesini engeller. Bu duyarlılıklar nedeniyle kaotik dinamikler kriptografi ve steganografi uygulamalarında sıklıkla tercih edilmektedir.

Kriptografik uygulamalarda kullanılan Rasgele Sayı Üreteçlerinin (RSÜ) ürettiği sayıların rastgeleliği, şifreleme uygulamalarının güvenliğini doğrudan etkilediği için kritik öneme

sahiptir. Üretilen rastgele sayılar, FIPS 140-1, NIST 800-22 ve ENT gibi uluslararası kabul görmüş testlerden başarıyla geçtikten sonra şifreleme uygulamalarında kullanılabilmektedir.

Kesir dereceli kaotik sistemler, Riemann-Liouville, Caputo ve Grünwald - Letnikov gibi yöntemler ile sayısal olarak çözümlenerek elde edilen veriler kriptografi ve steganografi uygulamalarında kullanılabilmektedir. Verilerin şifrelenmesi ve gizlenmesi tek başına yeterli değildir. Bu sistemlerin güvenilirliğin üst seviyede olduğunu göstermek için çeşitli güvenlik analizlerinin yapılması gerekmektedir.

Gömülü sistemler, kompakt ve taşınabilir yapıları sayesinde güvenlik çözümlerinin çeşitli fiziksel ortamlarda kolaylıkla kullanılabilmesini sağlar. Ayrıca, bu sistemler şifreleme ve steganografi işlemlerini yüksek hızda gerçekleştirebildikleri için literatürde son zamanlarda tercih edilmektedir.

Sonuç olarak kaotik sistemler, özellikle de kesir dereceli kaotik sistemler, bilgi güvenliği alanında önemli bir potansiyele sahip umut vadeden bir araştırma alanıdır. Literatürde kaotik sistemlerin kullanımıyla ilgili olarak kaos tabanlı rastgele sayı üretimi, şifreleme ve steganografi çalışmalarında çeşitli ortamlarda ve farklı multimedya verileriyle gerçekleştirilen uygulamalar bulunmaktadır. Şifreleme ve steganografi bağlamında kaotik sistemlerin kullanımına dair aşağıdaki bilimsel çalışmalar örnek olarak gösterilebilir:

1963 yılında Edward Lorenz'in öncülüğünde gelişmeye başlayan "Kaos Bilimi" (Lorenz, 1963), Rössler (Rössler, 1976) ve Chua (Chua et al., 1986) gibi bilim insanlarının katkılarıyla hızla ilerlemiş ve günümüzde de birçok alanda gelişmeye devam etmektedir.

Son yıllarda birçok alanda kullanılmak üzere farklı kaotik ve hiperkaotik sistemler literatüre sunulmuştur (P. Li et al., 2024; C. Xu et al., 2023; Zhao et al., 2024; Shuang Zhou et al., 2023). Kesir dereceli kaotik sistemlerin, tamsayı dereceli sistemlere kıyasla uygulamalarda daha fazla avantaj sunmasından dolayı kesir dereceli kaotik sistemler üzerine araştırmalar devam etmektedir. Literatürde, tamsayı dereceli kaotik sistemler üzerinde değişiklik yaparak veya tamamen yeni kesir dereceli sistemler geliştirilmiştir. Yu ve arkadaşları (2009) kesir dereceli Lorenz kaotik sisteminin dinamiklerini kapsamlı şekilde incelemişler ve kesirli dereceden Lorenz sisteminin tamsayı mertebeden muadili ile benzer denge ve kararlılığa sahip olduğunu göstermişlerdir (Yu et al., 2009). Petráš (2022) yapmış olduğu çalışmada; Chen, Lü, Yang, Liu, Shimizu-Morioka, Burke-Shaw, Lorenz tipi sistemlerin kesirli dereceli formlarını incelemiştir (Petráš, 2022). Sene (2022) ise yapmış olduğu çalışmada Caputo

türevi ile tanımlanan yeni bir kesirli mertebeden kaotik sistemin özelliklerini ve davranışlarını incelemiştir. Ayrıca çalışmada önerilen sistemin kaotik davranışları, Lyapunov üsleri ve faz portre analizleri gerçekleştirilmiştir. Sistem elektrik devresi olarak modellenmiş ve simülasyonu gerçekleştirilmiştir (Sene, 2022). Pacheco ve arkadaşları (2018) ise tek parametreli ve dört doğrusal olmayan özelliğe sahip yeni bir kesirli dereceden kaotik sistem tanıtmışlarıdır. Önerdikleri kesirli dereceli sisteminin düşük kesirli türevli değerde (0.95) bile gizli çekiciler üretebildiğini göstermişlerdir (Munoz-Pacheco et al., 2018). Liu ve arkadaşları (2023) ise yeni bir 3 boyutlu kesirli dereceli sistemin küresel dinamiklerini incelemiştir. Bu doğrultuda ise sistemin dinamik davranış, bifurkasyon diyagramları, faz portreleri ve en büyük Lyapunov üssü (LE) kullanılarak analiz etmiştir. Çeşitli teorik bulguları göstermek için ise sayısal simülasyonlar yapmışlardır (P. Liu et al., 2023). Gökyıldırım ve arkadaşları (2024), yapmış oldukları çalışmada kesirli dereceli Arneodo kaotik sisteminin parametre analizini tartışmışlardır. Yazarlar güvenli iletişim uygulamalarında kullanılmak üzere minimum uygulanabilir kesirli dereceli değerin araştırılmasına odaklanmışlardır. Sistemin 0.55 ile 1 arasındaki parametre analizi sonucunda neredeyse tüm kesirli dereceli değerlerinde kaotik durumlarının varlığını ispatlamışlardır. Bu çalışma, kaotik sistemlerin güvenli iletişimdeki potansiyelini artırmak amacıyla Arneodo kaotik sistemini kesirli dereceli analizlerle daha karmaşık ve öngörülemez hale getirmektedir. Bu sayede, veri güvenliği için daha güçlü ve dinamik sistemler elde edilmiştir (Gokyildirim, Akgul, et al., 2024).

Literatürde kaotik dinamiklerin gerçek dünyadaki uygulamalarını gerçekleştirebilmek amacıyla çeşitli elektronik devreler tasarlanmıştır. Bu devreler, kaotik sistemlerin öngörülemez ve düzensiz davranışlarını elektronik ortamda üretmek ve analiz etmek için kullanılmaktadır. Kaotik devreler, güvenlik ve şifreleme, sensör teknolojileri, radar sistemleri, kontrol mühendisliği, tıbbi uygulamalar ve optik kaos gibi birçok alanda yenilikçi çözümler sunmaktadır. Jia ve arkadaşları (2014) ise kesirli dereceli kaotik sisteminin karakteristiklerinin analizini ve analog devre uygulamasını gerçekleştirmişlerdir (Jia et al., 2014). Borah ve arkadaşları ise (2016), yeni bir kesirli dereceli kaotik sistem önermişlerdir. Bu sistem, operasyonel amplifikatörler, dirençler ve kondansatörler kullanılarak analog devrelerle tasarlanmıştır. Elde ettikleri sonuçları, sayısal simülasyonlar ve osiloskop ölçümleriyle doğrulamışlardır (Borah et al., 2016). Sayed ve ekibi (2020), FPGA kartında gecikmeli kesirli dereceli kaotik sistem uygulamasını gerçekleştirmişlerdir. Bu sistem,

Grünwald-Letnikov yaklaşım yöntemi kullanılarak sayısal olarak çözülmüş ve Nexys 4 Artix-7 FPGA XC7A100T kartı üzerinde hayata geçirilmiştir. Çalışmalarında, FPGA'yı osiloskopa bağlamak için bir Pmod DAC 2 kullanmışlardır (Sayed et al., 2020).

Kaotik rastgele sayı üreteci, özellikle kriptografi, güvenli iletişim ve bilimsel simülasyonlar gibi alanlarda kritik öneme sahiptir. Üretilen sayıların rastgeleliği, kriptoloji ve steeganografi uygulamalarının güvenilirliğini doğrudan belirlemektedir. Bu doğrultuda Özkaynak (2020) yapmış olduğu çalışmada, kesirli dereceli kaotik Chua sistem temelli rastgele sayı üreteci geliştirmiştir. Üretecin rastgelelik özellikleri ki-kare ve monobit testleri ile test etmiştir. Elde edilen analiz sonuçlarına göre, üretecin rastgelelik gereksinimlerini başarılı bir şekilde karşıladığını göstermiştir (Ozkaynak, 2020). Artuğer ve Özkaynak (2024), çalışmalarında yeni bir kaotik sistem önermiştir. Bu sistemi, S-Box tasarımı ve rastgele sayı üretiminde kullanmışlardır. Önerilen haritayı kullanarak 1 milyon bit uzunluğunda üç farklı rastgele dizi üretmişlerdir. Bu dizilere NIST SP 800-22 testi uygulanmış ve tüm dizilerin başarılı olduğu belirlenmiştir (Artuğer et al., 2024). Çalgan (2024), DMDE *(dark matter and dark energy)* kaotik sisteminin, incommensurate kesirli dereceli formunda kaotik davranışı tetiklediği ortaya koymuştur. Aynı zamanda, belirli incommensurate kesirli dereceler ve sistem parametreleri asimptotik olarak kararlı denge durumlarına yol açtığında, gizli bir çekici keşfetmiştir. Bu durum, IFODMDE *(incommensurate fractional-order dark matter and dark energy)* kaotik sistemine dayalı yeni bir rastgele sayı üreteci (RNG) tasarımına yol açmıştır. Tasarlanmış olduğu RNG, uluslararası kabul görmüş NIST 800-22 rastgelelik testleri ile de doğrulamıştır (Calgan, 2024).

İlk yıllarda, kaotik maskeleme, kaotik modülasyon ve kaotik anahtarlama gibi şifreleme yöntemleri analog olarak uygulanmıştır. Ancak günümüzde, kaos tabanlı şifreleme işlemleri genellikle dijital olarak yapılmaktadır. Dijital kaos tabanlı şifrelemenin analog kaos tabanlı şifrelemeye göre bazı temel avantajları bulunmaktadır. Bunlar arasında, şifre çözme işlemi için yalnızca şifreleme algoritmasının tersinin alınmasının yeterli olması, şifreleme algoritmalarının kolayca değiştirilip güncellenebilmesi, analog şifrelemede sıkça karşılaşılan senkronizasyon sorunlarının olmaması, gürültü, sıcaklık ve nem gibi dış etkenlerden etkilenmemesi sayılabilir. Kesir dereceli kaotik sistemler, şifreleme alanında tam sayılı kaotik sistemlere göre daha karmaşık dinamikler, daha yüksek rastgelelik ve güvenlik gibi birçok avantaj sunmasından dolayı literatürde son yıllarda araştırma konusu

olmuştur. Bu doğrultuda, Gökyıldırım ve arkadaşları (2024), tıbbi görüntülerin şifrelenmesi için kesirli dereceli Sprott K kaotik sistemini kullanan yeni bir yöntem sunmuşlardır. Ayrıca Kaotik sistemlerin, özellikle kesirli dereceli olanların, tıbbi görüntü şifrelemesinde büyük potansiyele sahip olduğunu vurgulamışlardır (Gokyildirim, Çiçek, et al., 2024). Xu ve arkadaşları (2022) 4 nöron tabanlı yeni bir kesirli dereceden HNN modeli önermişlerdir. Önerilen sistem tarafından oluşturulan PRN'ler (Pseudo-Random Number - Sahte Rastgele Sayı) ile, çoklu Hash kullanan yeni bir şifreleme algoritması tasarlayarak görüntüleri şifreleme uygulaması gerçekleştirmişlerdir (S. Xu et al., 2022). Zhang ve arkadaşları (2020) kesirli dereceli lojistik sisteme dayalı etkin bir S-kutusu oluşturma şeması önermişlerdir. Aynı zamanda kesirli dereceli Lojistik sistem, S-kutuları ve Güvenli Hash Algoritması MD2 kullanarak bir görüntü şifreleme şeması sunmuşlardır. Şifreleme şeması; anahtar alanı analizi, histogram analizi ve NIST testi gibi çeşitli performans analiz metrikleri kullanılarak test edilmiştir ve sonuçlar şemanın güvenli ve verimli olduğunu göstermişlerdir (Y.-Q. Zhang et al., 2020). Liu ve arkadaşları (2023) altı dereceli ayrık kaotik haritayı (SODCM) kesirli olarak genelleştirmiş ve bilgi güvenliği için görüntü şifreleme uygulamıştır. Daha sonra ilgili testlerle şifreleme verimliliğini kanıtlamışlardır (Z. Liu et al., 2023).

Steganografi, bilgi güvenliği ve gizliliği açısından çok önemli bir araçtır. Öncelikle steganografinin temel amacı, bir mesajın varlığını gizleyerek iletişimin gizliliğini artırmaktır. Steganografi özellikle gizli veya hassas bilgilerin iletiminde büyük bir rol oynar; ticari sırlar, askeri bilgiler veya kişisel veriler gibi hassas bilgilerin korunmasını sağlamaktadır. Şifreleme ile birlikte kullanıldığında, steganografi yalnızca mesajın içeriğini değil aynı zamanda mesajın varlığını da gizler, bu da bilgiyi çifte güvence altına almaktadır. Kaos tabanlı steganografi ise karmaşık ve öngörülemez yapısı sayesinde bilgi güvenliği ve gizliliği sağlama konusunda önemli avantajlar sunmaktadır. Son yıllarda, kaos tabanlı steganografi önemli ölçüde ilgi görmektedir. Hameed (2015) yapmış olduğu çalışmada, konuşma gizleme yönteminin geliştirilmesi için kaotik steganografi ve kriptografi tekniklerini birleştirmiştir. İlk olarak konuşma sinyalini ön işleme tabi tutmuştur. Daha sonra konuşma bit akışı, lorenz ve Chua'nın kesirli dereceli kaotik sistemlerden elde edilen anahtar ile XOR edilmiş ve şifrelenmiştir. Ek olarak şifrelenmiş konuşma mesajı, dijital bir resimde gizlemek için Modified Arnold Cat Map (MACM) kullanmıştır (A. Hameed, 2015). Bader ve arkadaşları (2024), kaotik sistemler ve Bloom filtrelerini kullanarak görüntü steganografisi uygulaması gerçekleştirmişlerdir. Çalışmada lorenz kaotik sistemi kullanarak

kapak resimlerinde gizli veri saklamak için rastgele görüntü konumlarını oluşturmuşlardır. Bloom filtresini ise aynı pikselde veri tekrarını ve kaybını önlemek için kullanmışlardır. Önerdikleri yaklaşım ile geleneksel LSB tekniklerinin zayıflıklarını aşarak şifreli verilerin rastgele konumlarına gömülmesini sağlamışlardır (Bader et al., 2024). Thenmozhi ve Chandrasekaran'ın (2013) yapmış oldukları çalışmada kaotik haritalar kullanılarak gizli verileri şifrelemiş ve dalgacık dönüşüm yöntemi kullanılarak gizli verileri, kapak görselline gömmüşlerdir (Thenmozhi et al., 2013). Gömülü kartlar temelli kaotik sistemler modellenerek şifreleme ve steganografi uygulamasının avantajları, yüksek hesaplama gücü ve enerji verimliliği ile birleşerek etkili ve güvenilir bilgi güvenliği çözümleri sunmaktadır. Ayrıca gömülü sistemlerin düşük güç tüketimi, bu çözümleri taşınabilir ve güç kısıtlamalı uygulamalar için ideal hale getirmektedir. Literatürde, şifreleme ve steganografi uygulamaları FPGA, DSP ve çeşitli mikrodenetleyiciler üzerinde gerçekleştirilmiştir. Kiran ve arkadaşları (2023), Nvidia Jetson Orin geliştirme kartı üzerinde büyük ölçekli verilerin (görüntüler ve videolar) verimli bir şekilde şifrelenmesi için yeni bir ayrık zamanlı kaotik şifreleme mekanizması önermiştir (Kiran et al., 2023). Megherbi ve arkadaşları (2024), kesirli dereceli kaotik sistemlerin dürtüsel kontrolüne dayalı bir kablosuz metin verisi iletimini ESP32 mikrodenetleyici kartları kullanarak başarıyla uygulamışlardır (Megherbi et al., 2024). Yang ve arkadaşları (2020) dijital sinyal işlemcisi (DSP) platformunda improper kesir dereceli lazer kaotik sistemin dinamik özelliklerini incelemiştir. İlgili kaotik harita kullanılarak görüntü şifreleme uygulaması gerçekleştirmişlerdir (Yang et al., 2020). Jing-yu ve arkadaşları (2023) çizgi denge noktalarına sahip yeni bir dört boyutlu kaotik sistem önermişlerdir. Sistem, kaotik bir dizinin kullanıldığı bir şifreleme algoritması ve PVD-LSB steganografi sistemi ile birlikte çalışmaktadır. Şifreleme yöntemi ve PVD-LSB steganografi FPGA üzerine uygulanmış ve performans analizlerini gerçekleştirmişlerdir (Jing-yu et al., 2023). Janakiraman ve arkadaşları (2018) ise gri tonlamalı resimlerin şifrelenmesi için Lightweight kaotik resim şifreleme algoritması önermişlerdir. Uygulamayı 32-bit mikrodenetleyici üzerinde gerçekleştirmişlerdir. Algoritma, kaotik haritalar ve bit düzeyinde işlemleri kullanarak resmi şifrelemekte ve yüksek güvenlik sağlamaktadır (Janakiraman et al., 2018).

Bu tez çalışmasının amacı ise, literatürde mevcut olan Arneodo ve Sprott kaotik sistemlerini incommensurate kesir dereceli olarak ifade edip bu sistemlerin kaotik davranışlarını analiz etmektir. Elde edilen incommensurate kaotik sistemleri kullanarak, önerilen algoritmanın

Python dili ile Nvidia Jetson AGX Orin gömülü kartı ve Jupiter programlama ortamında RSÜ tasarımı gerçekleştirilmesi hedeflenmektedir. Üretilen rastgele sayıların rastgeleliğini test etmek amacıyla NIST 800-22, FIPS 140-1 ve ENT istatistiksel testlerinden başarıyla geçtiği ispatlanacaktır. Ayrıca, üretilen rastgele sayılar kullanılarak Nvidia Jetson AGX Orin üzerinde, önerilen görüntü şifreleme ve steganografi algoritmaları gerçekleştirilecek; son olarak, bu şifreleme ve steganografi uygulamalarının güvenlik analizleri yapılarak önerilen algoritmaların güvenilirliği ispatlanacaktır.

Bu amaçlar doğrultusunda tezin ikinci bölümünde; kriptoloji, steganogtrafi, gömülü sistemler, rastgele sayı üreteçleri ve testleri, güvenlik analizleri, kaotik sistemler ve kesir dereceli türevlerin sayısal analizleri hakkında temel bilgiler verilmiştir.

Tezin üçüncü bölümünde ise incommensurate kesir dereceli kaotik sistemler tanıtılarak kaotik sistemlerin denge nokta analizi, faz portresi, Lyapunov üstelleri, zaman serilerinde başlangıç değerlerine duyarlılık analizi ve çatallaşma diyagram analizleri gerçekleştirilmiştir. Bu sayede incommensurate kesir dereceli sistemlerin kaotik olup olmadığı kanıtlanarak dinamik özellikleri ortaya çıkarılmıştır. Daha sonra incommensurate kesir dereceli kaotik sistemler, gömülü sistem tabanlı modellenerek tasarlanan elektronik kart ile faz portreleri elde edilmiştir. Tez kapsamında önerilen rastgele sayı üreteç algoritması tanıtılarak gömülü sistem tabanlı rastgele sayı üretimi gerçekleştirilmiştir. Üretilen rastgele bitlerin istatiksel analizleri yapılarak bu rastgele sayıların şifreleme ve steganografi çalışmalarında kullanılabileceği gösterilmiştir. Ayrıca, önerilen şifreleme ve steganografi algoritmaları tanıtılmış ve gömülü sistem tabanlı görüntü şifreleme ve steganografi uygulamaları gerçekleştirilmiştir. Bu uygulamaların güvenlik analizleri yapılarak etkinlikleri kanıtlanmıştır.

Dördüncü bölümde ise tez kapsamında elde edilen bulgular, literatürdeki benzer çalışmalarla kıyaslanmış olup çalışmanın literatüre katkıları ve yenilikçi yönleri vurgulanmıştır.

Son bölümde ise tez kapsamında elde edilen sonuçlar bahsedilerek ileride yapılacak çalışmalar hakkında öneriler sunulmuştur.

2. GENEL BİLGİLER

İnsanlık tarihi boyunca güvenlik, Maslow'un ihtiyaçlar hiyerarşisinde de yer aldığı üzere, en temel gereksinimlerden biri olmuştur. Maslow'un piramidinde, güvenlik ihtiyaçları, fizyolojik ihtiyaçlardan hemen sonra gelmektedir. Bireylerin huzur ve emniyet içinde yaşamalarını sağlayacak unsurları içermektedir. Bu durum, eski zamanlardan günümüze kadar insanların, fiziksel ve bilgisel güvenliği sağlamak için çeşitli önlemler almasına neden olmuştur.

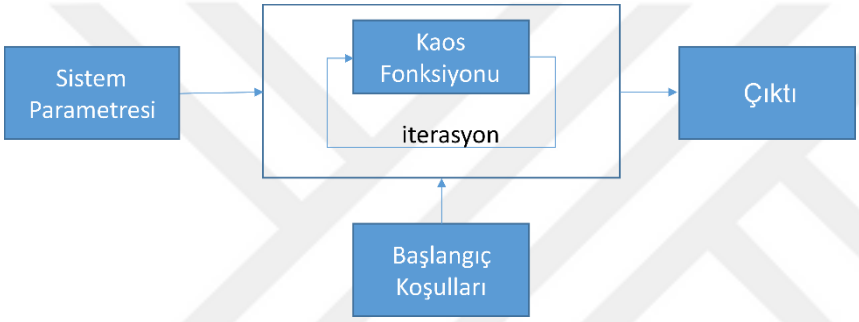
Kriptoloji ise güvenlik kavramlarının merkezinde yer almaktadır. Kriptolojinin bilinen en eski tarihi Antik Mısır'a kadar uzanmaktadır. Mısırlı kâtipler, kil tabletleri yazarken genellikle standart dışı hiyeroglifler kullanmışlardır; bu, yazılı kriptografinin belgelenmiş ilk örneğidir (Whitman et al., 2011). Büyük Roma İmparatoru Julius Caesar ise komutanlarına ve müttefiklerine gizli mesaj göndermek amacıyla Caesar şifrelemesini kullanmıştır (Santos et al., 2021). IX. yüzyılda İslam dünyasında kriptoloji alanında önemli gelişmeler yaşanmıştır. Bağdat'ta yaşayan El-Kindi tek alfabeli yerine koyma şifreleme yöntemini geliştirerek frekans analizini bulan ilk kişidir (Broemeling, 2011). Modern kriptolojinin temelleri ise XX. yüzyılda atılmıştır. İkinci Dünya Savaşı sırasında, Müttefik ve Mihver Devletleri arasındaki mücadelede kriptoloji büyük bir rol oynamıştır. Özellikle Enigma makinesi, Nazi Almanya'sı tarafından gizli mesajları şifrelemek ve tekrar çözmek amacıyla kullanılan bir şifreleme cihazıdır. Bu cihazın şifresini çözmek için yapılan çalışmalar, modern bilgisayar biliminin ve kriptolojinin gelişimine büyük katkı sağlamıştır. Alan Turing ve ekibinin Bletchley Park'ta yaptığı çalışmalar, Enigma şifrelerinin çözülmesi ve savaşın seyrinin değişmesinde önemli bir rol oynamıştır (da Silva et al., 2024). Günümüzde ise, teknolojinin gelişmesiyle beraber veri güvenliği ve gizliliğinin önemi daha da artmıştır. Bilgisayar ağları üzerinden sürekli veri akışı gerçekleşmektedir. Verilerin üçüncü kişilerin eline geçmeden iletilmesi büyük önem taşımaktadır. Bu doğrultuda araştırmacılar ise bilgilerin gizliliğini, güvenliğini ve bütünlüğünü korumak amacıyla sürekli şifreleme algoritmaları, protokoller ve güvenlik mekanizmaları geliştirmektedir.

Güvenlik tehditlerini önlemek için şifreleme yöntemleri kullanılmaktadır. Genel olarak şifreleme, verinin içerdiği bilgileri belirli bir yöntem kullanarak anlaşılmaz bir hale dönüştürülmesi olarak tanımlanabilmektedir. Verilerin içerdiği bilgileri şifrelemek amacıyla genellikle kriptoloji ve stenografi olarak adlandırılan yöntemler kullanılmaktadır.

2.1. Kaotik Sistemler

2.1.1. Kaos Kuramı

Kaos kavramı, Amerikalı meteorolog Edward Norton Lorenz tarafından keşfedilmiştir. Lorenz, olaylardaki küçük değişikliklerin büyük etkiler yaratabileceğini gözlemlemiştir. 1963 yılında bu kavram, bilim camiasına tanıtılmıştır (Lorenz, 1963). Halk arasında 'Düzensizlik-Kargaşa' olarak bilinen kaos, aslında kendi iç düzeni ve sınırları olan karmaşık bir süreçtir. Kaotik bir sistem, başlangıç koşullarına son derece duyarlı ve ölçülemeyecek derecede karmaşık olan sistemler olarak tanımlanabilmektedir (Yardım et al., 2013). Şekil 2.1'de temel bir kaotik sistemin çalışma yapısı verilmiştir.



Şekil 2.1. Temel bir kaotik sistemin çalışma yapısı

Yapı incelendiğinde kaotik sistemlerin her iterasyonda giriş değerine ve sistem parametrelerine bağlı olarak yeni bir çıktı ürettiği görülmektedir. Kaotik sistemin doğası gereği, üretilen çıktı değerinin önceki değerden doğrusal olarak bağımsız olması beklenir.

Kaotik sistemler ayrık ve sürekli zamanlı olmak üzere iki ana başlık altında incelenebilir. Dinamik sistemler kuralına göre kaotik sistemler ayrık işaretler olarak incelendiğinde ayrık zamanlı, sürekli işaretler olarak incelendiğinde ise sürekli zamanlı dinamik sistemler olarak adlandırılır.

2.1.1.1. Ayrık Zamanlı Sistemler

Ayrık zamanlı kaotik sistemler kendi arasında tek boyutlu ve çok boyutlu kaotik sistemler olarak iki gruba ayrılabilir. Ayrık zamanlı kaotik sistemler ayrıklaştırma algoritmaları işlemlerine tabi tutulmadan doğrudan sayısal uygulamalarda kullanılabilmektedir (Akgül, 2015). Literatürde bulunan Logistic Map, Cubic Map, Tent Map, Sine Map, Pinchers Map ve Cusp Map tek boyutlu ayrık zamanlı kaotik sistemlerdir. Logistic Map kaotik sistemlerin anlaşılmasında ve incelenmesinde sıkça kullanılan basit ancak güçlü bir ayrık zamanlı kaotik

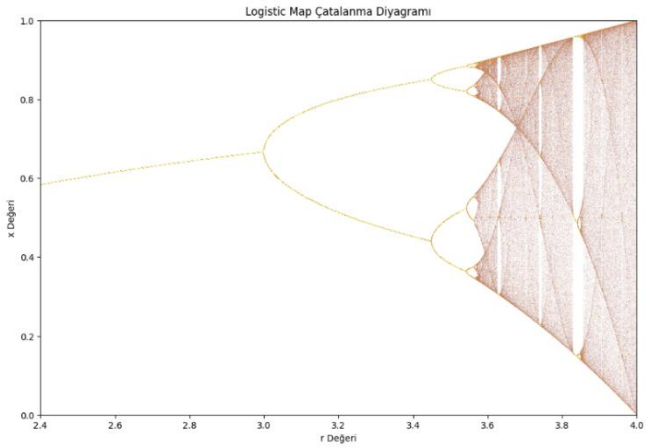
sistem modeldir. İlk olarak Pierre François Verhulst tarafından XIX. yüzyılın ortalarında popülasyon dinamiklerini modellemek için geliştirilmiştir. Logistic Map'in, popülasyon büyümesini sınırlayan kaynak kısıtlamalarını dikkate alarak popülasyon dinamiklerini modellemektedir (Verhulst et al., 1838). Denklem 2.1'de Logistic Map'in matematiksel denklemi verilmiştir.

$$x_{n+1} = r x_n (1 - x_n)$$

Denklem 2.1. Logistic map denklemi

Burada, sistem değişkeni x ve yineleme sayısı n olarak ifade edilmektedir.

Şekil 2.2'deki çatallaşma diyagramı incelenerek, Logistic Map'in kaotik olma durumu irdelenmiştir.



Şekil 2.2. Logistic Map çatallaşma diyagramı

Denklem 2.1'de verilen r parametresi 2.4-4 değeri arasında incelenmiştir. Bu değer 2.4-3 arasında bir, 3-3.4 arasında iki, 3.5 civarı dört, kaosa yakın değerde sekiz sonuç üretmektedir. 3.56995'ten büyük değerler için sistemin kaosa girdiği görülmektedir. Ayrıca $0 < r < 3.56995$ arasında sistem pozitif Lyapunov üsteline sahip değildir. Sistem, Lyapunov üstelinin pozitif olmaması nedeniyle kaotik davranış sergileyemez (Nurhan Yavuz, 2006).

Ayrıca iki denklemden meydana gelen, iki boyutlu ayrık zamanlı kaotik sistemlere ise, Hénon Map, Lozi Map, Tinkerball Map ve Holmes Cubic Map gibi haritalar örnek verilebilir. Bu haritalardan Hénon Map incelenecek olursa,

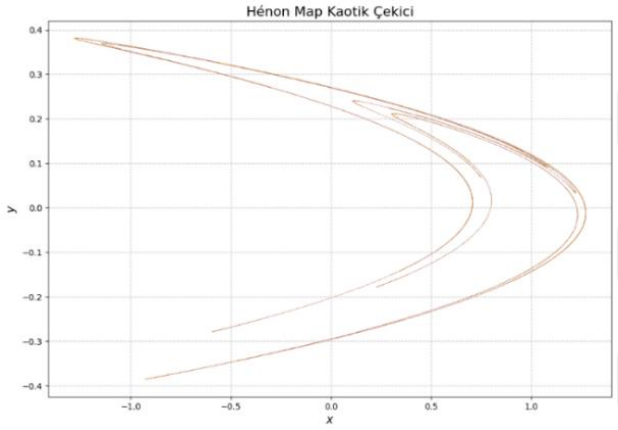
Hénon Map, ilk olarak Michel Hénon tarafından tanımlanmıştır (Hénon, 1976). Hénon Map'in matematiksel modeli Denklem 2.2'de verildiği gibidir.

$$x_{n+1} = 1 - ax_n^2 + y_n$$

$$y_{n+1} = bx_n$$

Denklem 2.2. Hénon map denklemi

Burada $a = 1.4$ ve $b = 0.3$ sistem parametreleri ve $x[0] = 0.1, y[0] = 0.1$ başlangıç şartları için elde edilen x-y kaotik çekicisi Şekil 2.3'te verildiği gibidir.



Şekil 2.3. Henon Map kaotik çekicisi

Üç denklemden meydana gelen, üç boyutlu ayrık zamanlı kaotik sistemlere ise, Generalized Hénon Map, Coupled Logistic Maps, 3D Baker's Map ve Lorenz Chaotic Map örnek verilebilir. Bu haritalardan Lorenz Chaotic Map incelenecek olursa;

Lorenz Chaotic Map'in matematiksel modeli Denklem 2.3'te verildiği gibidir.

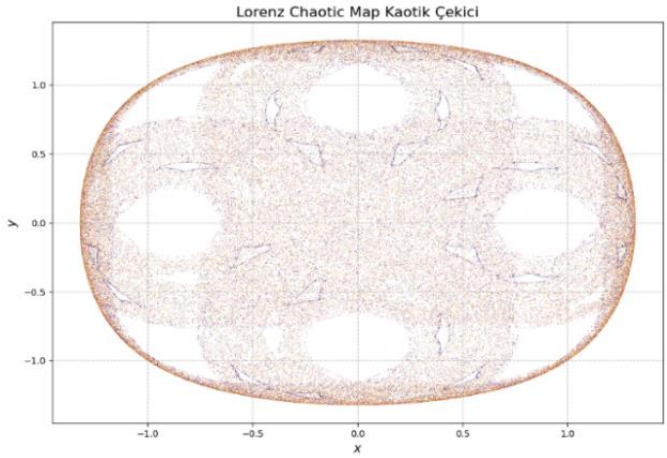
$$x_{n+1=}x_n y_n - z_n$$

$$y_{n+1} = x_n$$

$$z_{n+1} = y_n$$

Denklem 2.3. Lorenz chaotic map denklemi

Burada, $x[0] = 0.5, y[0] = 0.5$ ve $z[0] = -1.0$ başlangıç değeri için elde edilen kaotik çekici Şekil 2.4'te verilmiştir.



Şekil 2.4. Lorenz Chaotic Map kaotik çekicisi

2.1.1.2. Sürekli Zamanlı Sistemler

Sürekli zamanlı kaotik sistemler adi diferansiyel denklemlerle ifade edilirler. Sürekli zamanlı sistemler, $i = 1,2,3,\dots,n$ olmak üzere n adet birinci dereceden adi diferansiyel denklemden oluşur ve Denklem 2.4 ile tanımlanabilir (Butcher, 1997).

$$\left.\begin{aligned} \frac{dx^{(i)}}{dt} &= f_1\left(x^{(i)}, x^{(i+1)}, \dots \dots x^{(n)}\right) \\ \frac{dx^{(i+1)}}{dt} &= f_2\left(x^{(i)}, x^{(i+1)}, \dots \dots x^{(n)}\right) \\ &\cdot\cdot \\ \frac{dx^{(n)}}{dt} &= f_n\left(x^{(i)}, x^{(i+1)}, \dots \dots x^{(n)}\right) \end{aligned}\right\}$$

Denklem 2.4. Sürekli zamanlı sistemler

Yukarıdaki ifadeler yeniden düzenlendiğinde, adi diferansiyel denklemler vektörel formda Denklem 2.5'te gösterildiği şekilde ifade edilebilir.

$$\frac{dx(t)}{dt} = F[x(t)]$$

$$x(t_0) = x_0$$

Denklem 2.5. Vektörel adi diferansiyel denklem sistemi

Burada x, n boyutlu vektördür. Ayrıca $x \in R^m$ durum vektörüdür. x_0 başlangıç durum vektörüdür. t ise zamanı ifade etmektedir.

Ayrık zamanlı kaotik sistemler, doğrusal olmayan tek boyutlu basit denklemlerle tanımlanırken, sürekli zamanlı kaotik sistemlerin en az üç boyutlu olmalıdır (Akgül, 2015).

Ayrıca sürekli zamanlı kaotik sistemlerde, eğer sistemin boyutu üçten fazla ise, bu sistemler hiperkaotik sistemler olarak adlandırılmaktadır.

Lorenz, Rössler, Chen, Chua, Arneodo ve Sprott (1994) gibi sistemler sürekli zamanlı kaotik sistemlere örnek olarak verilebilir.

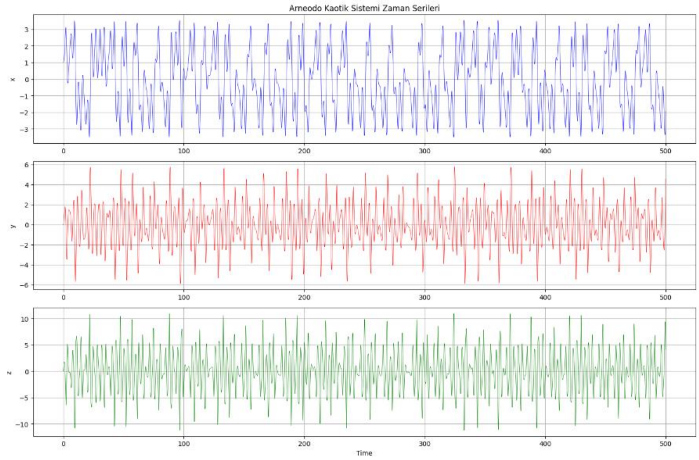
İlk olarak sürekli zamanlı kaotik sistemlerden Arneodo sistemi incelendiğinde, bu sistemin üçüncü dereceden diferansiyel denklemlerle tanımlandığı görülmektedir. Arneodo kaotik sistemi, Lorenz sisteminin bir genellemesi olarak ortaya çıkmıştır ve doğrusal olmayan dinamik sistemler alanında önemli bir yer tutar. 1985 yılında A. Arneodo, ve arkadaşlarının tanıttığı (Arneodo et al., 1985) doğrusal olmayan denklem sistemi Denklem 2.6'da verilmiştir.

$$\left.\begin{aligned} \frac{dx}{dt} &= y \\ \frac{dy}{dt} &= z \\ \frac{dz}{dt} &= -ax - by - cz + x^3 \end{aligned}\right\}$$

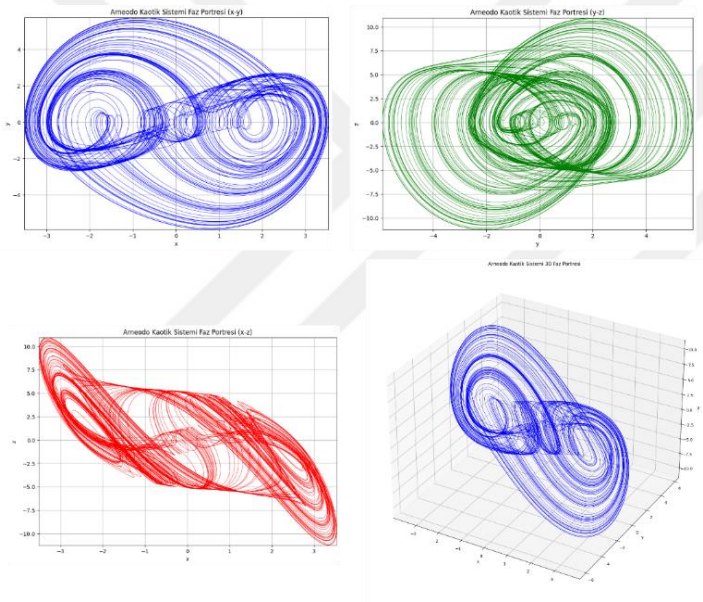
Denklem 2.6. Arneodo kaotik sistemi

Burada x, y ve z sistemin durum değişkenlerini a, b ve c ise sistem parametrelerini ifade etmektedir. Sistem parametreleri ve durum değişkenleri, sistemin davranışını belirlemede kritik bir öneme sahiptir. Parametrelerdeki ve başlangıç koşullarındaki küçük değişiklikler, büyük sonuçlara neden olabilmektedir.

Denklem 2.6'da verilen Arneodo sisteminin, kaotik davranış sergileyebilmesi için, sistem parametrelerinin $a = 5.5, b = 3.5$ ve $c = 1.0$, başlangıç şartlarının ise $x(0) = 0.1, y(0) = 0.1, z(0) = 0.1$ olmalıdır. Arneodo sistemi için verilen parametre ve başlangıç değerlerine göre elde edilen zaman seri ve faz portreleri sırasıyla Şekil 2.5 ve Şekil 2.6'da verilmiştir.



Şekil 2.5. Arneodo kaotik sisteminin zaman serileri



Şekil 2.6. Arneodo kaotik sisteminin x-y, y-z, x-z için faz portreleri

2.1.2. Kaotik Sistemlerin Analizi

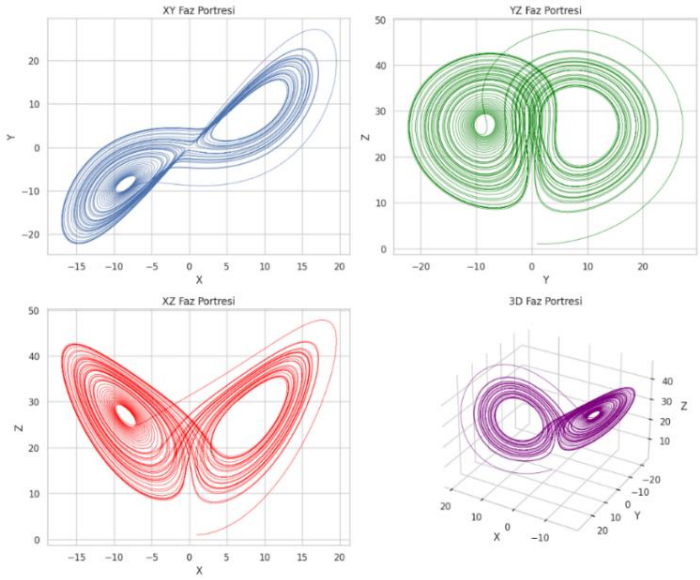
Bir sistemin kaotik özellikler taşıyıp taşımadığını belirlemek için çeşitli analiz yöntemleri kullanılmaktadır. Kaotik bir sistemin davranışını belirlemek için kullanılan yöntemler arasında denge nokta analizi, faz portreleri, Lyapunov üsleri, zaman serilerinde başlangıç değerlerine duyarlılık analizi ve çatallaşma diyagramları bunlardan bazılarıdır. Bu analiz yöntemlerinden birkaçının kullanılması, sistemin kaotik olup olmadığını anlamak için yeterli olabilir. Tez çalışmasında ilgili analizler Google Colaboratory (Google, 2024) ve Matlab R2021b (The MathWorks Inc., 2021) platformlarında gerçekleştirilmiştir.

2.1.2.1. Denge Nokta Analizi

Kaotik sistemler basit fonksiyonlarla tanımlanamadığından, bu sistemler hakkında doğrudan çıkarımlar yapmak zordur. Bu nedenle doğrusal olmayan dinamik sistemler olan kaotik sistemlerin davranışını anlamak için sistemin denge noktalarının, yani $F[x(t)] = 0$ durumundaki denge noktalarının, bulunup analiz edilmesi gerekmektedir (Pehlivan, 2007). Kaotik sistem analizi için öncelikle sistemin denge noktaları belirlenir. Denge noktalarını bulmak için denklemler sıfıra eşitlenerek çözümlenir ve elde edilen ifadeler reel sayılar ise sistemin denge noktaları mevcut kabul edilir. Ancak bazı kaotik sistemler yalnızca sanal denge noktalarına sahip olup reel denge noktaları bulunmamaktadır, hatta bazı sistemlerin hiç denge noktası olmayabilir. Bu sistemler denge noktasız kaotik sistemler olarak isimlendirilir. Denge noktaları belirlendikten sonra, sistemin Jacobian matrisi bu noktalarda hesaplanır ve $|J - \lambda I| = 0$ karakteristik denge çözümünden özdeğerler bulunur. Denge noktalarının kararsız olup olmadığı, yani sistemin kaotik davranış sergileyip sergilemediği, özdeğerler aracılığıyla belirlenebilir. Eğer özdeğerlerin reel kısmından en az biri pozitif ise, bu denge noktasının kararsız olduğunu ve sistemin kaotik olduğunu gösterir (Akgül, 2015). Sistemin kaotik özellikler sergilediğinden emin olmak için sonraki bölümlerde anlatılan diğer analizlerin de yapılması faydalı olacaktır.

2.1.2.2. Faz Portresi

Faz portresi, bir dinamik sistemin davranışını faz uzayında görselleştiren grafiksel bir temsildir. Sistemin durum değişkenlerinin zaman içindeki hareketlerini göstererek sistemin kararlı, periyodik veya kaotik olup olmadığını belirlenmesine yardımcı olmaktadır. Üç boyutlu kaotik bir sistem için x-y, y-z, x-z ve x-y-z olmak üzere dört farklı şekilde faz portreleri incelenebilmektedir. Faz portreleri çeşitli Python kütüphaneleri kullanılarak rahatlıkla elde edilebilmektedir. Ayrıca faz portreleri çeşitli elektronik devre gerçekleştirme simülasyon programları veya tasarlanan elektronik devrelerinin osiloskop çıktıları olarak da elde edilebilmektedir. Şekil 2.7'de Lorenz sistemine ait faz portresi örnek olarak verilmiştir.



Şekil 2.7. Lorenz sistemine ait faz portresi

2.1.2.3. Lyapunov Üstelleri

Lyapunov üstelleri, bir sistemin dinamik davranışının belirlenmesinde kritik bir ölçüt olarak kullanılmaktadır. Bu üsteller, bir deterministik kaotik sistemin faz uzayındaki boyut sayısına eşittir ve her bir üstel, ayrılma veya yakınlaşmanın ölçüsünü ifade eder. Lyapunov üstellerinin hesaplanması, 1980'li yıllarda Wolf ve arkadaşları tarafından gerçekleştirilmiştir (Wolf et al., 1985) İki başlangıç noktası arasındaki başlangıç uzaklığı d_0 olmak üzere, belirli bir zaman sonrasında bu uzaklık;

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

Denklem 2.7. Zamanla başlangıç uzaklığı değişim denklemi

şeklinde verilir ve birinci Lyapunov üstelini (λ) hesaplamak için Denklem 2.8'de verilen formül kullanılır (Arslan, 2019) :

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

Denklem 2.8. Lyapunov üsteli denklemi

Bir dinamik sistem, toplamları sıfırdan küçük olmak üzere, sıfırdan büyük en az bir Lyapunov üsteline sahipse kaotik olarak tanımlanır. Üç boyutlu bir sistemde, Lyapunov üstelleri için tek mümkün durum (+, 0, -) tipidir. Bu durumda $\lambda_1 > 0, \lambda_2 = 0, ve\ \lambda_3 < 0\ olur$ (Bolotin et al., 2017; Sandri, 1996). Dinamik sistemlerde Lyapunov üstelleri,

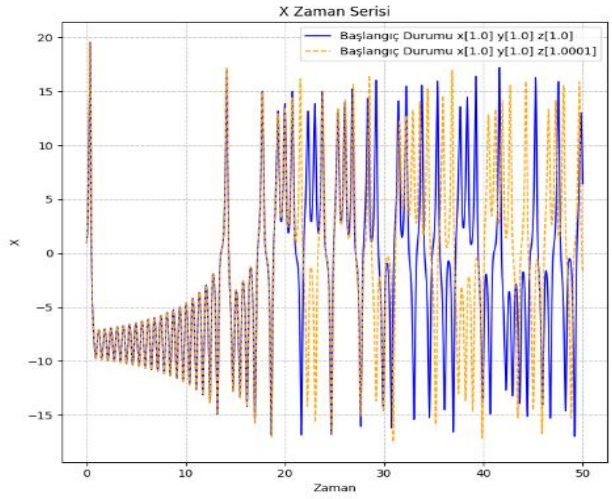
çekicilerin tiplerini karakterize etmeye yardımcı olur. Lyapunov üstellerine göre sistem durumları Tablo 2.1'de gösterildiği gibidir (Arslan, 2019).

Tablo 2.1. Lyapunov üstellerinin işaretlerine göre değişimi

Sistem Türü	Sistem Durumları	Lyapunov Üstelinin İşaretleri
3 Boyutlu Sistemler	Sabit Nokta	(-, -, -)
	Limit Döngü	(0,-,-)
	Torus	(0,0,-)
	Tuhaf Çekici	(+,0,-)
4 Boyutlu Sistemler	Sabit Nokta	(-,-,-,-)
	Limit Döngü	(0,-,-,-)
	Torus	(+,0,-,-)
	Tuhaf Çekici	(+,+,0,-)

2.1.2.4. Zaman Serilerinde Başlangıç Değerlerine Duyarlılık Analizi

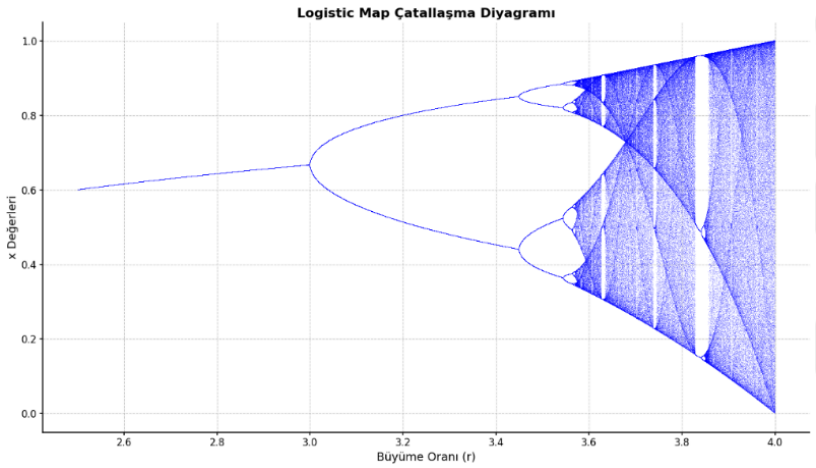
Bir sistemin kaotik olabilmesi için başlangıç koşullarına son derece duyarlı olması gerekmektedir. Sistemin başlangıç değerlerinde yapılan küçük değişikliklerin, sistemin çıkışında büyük farklılıklar yaratması, sistemin kaotik olup olmadığına dair önemli bir bilgi sağlar. Kaotik işaretleri farklı başlangıç değerleriyle en iyi gözlemleme yöntemlerinden biri, sistemin zaman serilerini aynı ekranda incelemektir (Akgül, 2015). Şekil 2.8'de örnek olarak Lorenz sistemi için farklı başlangıç değerleri ile elde edilen zaman serisi verilmiştir.



Şekil 2.8. Lorenz kaotik sisteminde başlangıç değerlerine duyarlılık analizi

2.1.2.5. Çatallaşma Diyagramı

Çatallaşma diyagramı, bir sistemin parametrelerinde meydana gelen küçük değişikliklerin faz uzayında yapısal değişiklikler yaratıp yaratmadığını inceleyerek, sistemin kaotik davranış sergileyip sergilemediğini belirlemek için kullanılır. Bir sistemin kaotik özellik göstermesi, parametrelerdeki küçük değişimlerin çatallaşmalar yaratmasına bağlıdır. Çatallaşma meydana gelmiyorsa, sistem periyodik bir davranış sergiler (Pehlivan, 2007). Bir sistemin çatallaşma diyagramı incelenerek kaotik olup olmadığına veya hangi parametre aralıklarında kaotik davranışlar sergilediğine karar verilebilir. Şekil 2.9'da Logistic Map'e ait örnek çatallaşma diyagramı verilmiştir.



Şekil 2.9. Logistic Map'e ait örnek çatallaşma diyagramı

2.1.3. Kesir Dereceli Kaotik Sistemler

Fiziksel sistemlerin matematiksel modellerini oluşturmak ve bu sistemlerdeki değişimleri tanımlayabilmek için türev kavramına ihtiyaç duyulur. Bu sistemler genellikle mevcut durumları ve değişimleri ile ifade edilebilir. Bu konudaki ilk çalışmalar Newton, L'Hospital, Abel, Euler ve Riemann gibi isimler tarafından yapılmıştır. Özetle bu bilim insanları, sistemlerin matematiksel modellerini oluşturan fonksiyonların asimptotik davranışlarını inceleyerek, bağımsız değişkenlerdeki en küçük değişikliklere karşı fonksiyonların tepkisini araştırmışlardır (Karcı, 2015).

Türev kavramı, yaklaşık 300 yıldır bilimsel araştırmaların merkezinde yer almış olup Newton, L'Hospital ve Leibniz gibi bilim insanları tarafından derece 1 olarak ele alınmıştır. 1695 yılında L'Hospital'in Leibniz'e, *"Bir f fonksiyonunun n tam sayı mertebesinden*

türevini tanımladın, peki $n = \frac{1}{2}$ *olduğunda* $\frac{d^n f}{dx^n}$ *kavramının bir anlamı var mı?"* sorusunu yöneltmesi, kesirli analizin başlangıcı olarak kabul edilmektedir. Bu alanda çalışan önemli matematikçiler arasında Newton, L'Hospital, Leibniz, Euler, Abel, Caputo, Riemann, Grünwald, Miller ve Ross bulunmaktadır. Bu bilim insanlarının yaptığı çalışmalar, kesir dereceli türev kavramının ortaya çıkmasını sağlamıştır.

Aşağıda $f(x)$ fonksiyonu ve türev tanımını ele aldığımızda;

$$H^2 f(x) = Df(x) = \frac{d}{dx} f(x) = f'(x)$$

Denklem 2.9. Birinci türev denklemi

$$f(x) = x^k$$

Denklem 2.10. Üstel fonksiyon denklemi

şeklinde tanımlanan fonksiyonun türevi aşağıdaki gibi hesaplanır:

$$f'(x) = \frac{d}{dx} f(x) = kx^{k-1}$$

Denklem 2.11. Türev kuralı

Bu işlem tekrarlanarak Denklem 2.12'de verilen genel bir türev formülü elde edilir.

$$\frac{d^a}{dx^a} x^k = \frac{k!}{(k-a)!} x^{k-a}$$

Denklem 2.12. Genel türev formülü

Faktöriyel fonksiyonunun karmaşık sayılar ve tam sayı olmayan reel sayılar için genelleştirilmesi, aşağıda verilen gamma fonksiyonu Γ kullanılarak yapılabilir.

$$(n-1)! = \Gamma(\mathrm{n})$$

Denklem 2.13. Gamma fonksiyonu ile faktöriyel ilişkisi

$$\Gamma(\mathrm{z}) = \int_0^\infty t^{z-1} e^{-t}\, dt$$

Denklem 2.14. Gamma fonksiyonu tanım integrali

Kompleks düzlemde analitik devamlılığın sağlanabilmesi için n negatif tam sayı olmamalı, pozitif tam sayı olmalıdır.

Gamma fonksiyonu Denklem 2.12'de yerine yazılırsa,

$$\frac{d^a}{dx^a}x^k = \frac{\Gamma(\mathrm{k}+1)}{\Gamma(\mathrm{k}-\mathrm{a}+1)}x^{k-a},\ \ \mathrm{k} \geq 0$$

Denklem 2.15. Gamma fonksiyonu tabanlı kesirli türev formülü

$k = 1$ ve $a = 1/2$ için;

$$\frac{d^{\frac{1}{2}}}{dx^{\frac{1}{2}}}x = \frac{\Gamma(1+1)}{\Gamma(1-\frac{1}{2}+1)}x^{1-\frac{1}{2}} = \frac{1!}{\Gamma(\frac{3}{2})}x^{\frac{1}{2}} = \frac{2x^{\frac{1}{2}}}{\sqrt{\pi}}$$

Denklem 2.16. Gamma fonksiyonu ile kesirli türev hesabı ($k = 1$ ve $a = ½$)

bu şekilde x fonksiyonunun yarı türevi elde edilir.

Kesirli dereceli türevler üzerine yapılan araştırmalar, 1730'lardan bu yana farklı şekillerde tanımlanmış ve günümüzde de yoğun bir şekilde devam etmektedir. Matematiksel tarihi oldukça eski olan bu alan, türev ve integral derecelerinin tam sayı olmayan (reel, irrasyonel, kompleks) değerler alabilmesi ile dikkat çekmektedir. L'Hospital ve Leibniz arasındaki mektuplaşmada ortaya çıkan kesirli türev kavramı üzerine, 1819 yılında Lacroix tarafından ilk makale yayımlanmıştır (Ross, 1974). Daha sonra Abel'in çalışmaları bu alanda önemli gelişmeler sağlamıştır (Cafagna, 2007). Literatürde kesirli türev ve integrallerin ortak gösterimi olarak kullanılan ve *D* simgesi ile ifade edilen "integrodiferansiyel" operatörünün farklı durumları için türev ve integral kavramları tanımlanır. Denklem 2.17'de görüleceği üzere, üs derecesi α negatif olduğunda integral, pozitif olduğunda ise türev anlamına gelmektedir (Korkmaz, 2013; Petráš, 2011).

$${}_aD_x^a = \begin{cases} \dfrac{d^a}{dx^a}, & a > 0 \\ 1, & a = 0 \\ \displaystyle\int_a^x (d\tau)^{-a}, & a < 0 \end{cases}$$

Denklem 2.17. İntegrodiferansiyel operatör

Literatürde yapılan çalışmalar incelendiğinde kesirli dereceden türevler üzerinde çok sayıda araştırma yapıldığı ve bu araştırmaların günümüzde de aktif bir şekilde sürdüğü anlaşılmaktadır. Kesirli türevler, 1730'lu yıllardan bu yana çeşitli yöntemlerle

tanımlanmıştır. Bu tanımlar ve yaklaşımlar kısaca aşağıdaki başlıklarda verilmiştir (Karcı, 2015);

2.1.3.1. L. Euler (1730) Tanımı

$$\frac{d^n x^m}{dx^n} = m(m-1)\ldots\ldots(m-n+1)x^{m-n}$$

Denklem 2.18. L. Euler (1730) tanım formülü

Formülünü gamma fonksiyonu kullanarak;

$$\frac{d^n x^m}{dx^n} = \frac{\Gamma(\mathrm{m}+1)}{\Gamma(\mathrm{m}-\mathrm{n}+1)} x^{m-n}$$

Denklem 2.19. L. Euler (1730) tanım formülünün Gamma fonksiyonu ile ifadesi

şeklinde ifade edilebilir.

2.1.3.2. Riemann-Liouville Tanımı

$${}_aD_t^a f(t) = \frac{1}{\Gamma(\mathrm{n}-\mathrm{a})}\left(\frac{d}{dt}\right)^n \int_a^t \frac{f(v)dv}{(t-v)^{a-n+1}}$$

Denklem 2.20. Riemann-Liouville tanım formülü

şeklinde tanımlanmıştır.

2.1.3.3. Caputo (1967) Tanımı

$${}_a^C D_t^a f(t) = \frac{1}{\Gamma(a-n)} \int_a^t \frac{f^{(n)}(v)dv}{(t-v)^{a+1-n}}$$

Denklem 2.21. Caputo (1967) tanım formülü

şeklinde tanımlanmıştır.

2.1.3.4. Grünwald - Letnikov Tanımı

$${}_aD_t^a f(t) = \lim_{h\to 0} h^{-a} \sum_{j=0}^{\frac{t-a}{h}} (-1)^j \binom{a}{j} f(t-jh)$$

Denklem 2.22. Grünwald-Letnikov tanım formülü

Burada, $m-1<a<m$ şeklinde olmalıdır. $\binom{a}{j}$ ise genelleştirilmiş binom katsayısıdır.

Denklem 2.23'teki gibi ifade edilir.

$$\binom{a}{j}=\frac{a!}{j!\,(a-j)!}=\frac{\Gamma(a+1)}{\Gamma(\mathrm{j}+1)\Gamma(a-j+1)}$$

Denklem 2.23. Genelleştirilmiş binom katsayısı

2.1.4. Kesir Dereceli Türevlerin Sayısal Analizi

Kesir dereceli türevlerin sayısal analizi için, Denklem 2.22'de belirtilen Grünwald-Letnikov tanımından faydalanılarak Denklem 2.24'te verilen tanımlama oluşturulabilir (Arslan, 2019).

$$k-\frac{L_m}{h}D_{t_k}^{a}f(t)\approx\lim_{h\to 0}h^{-q}\sum_{j=0}^{\frac{t-a}{h}}(-1)^j\binom{q}{j}f(t_k-j)$$

Denklem 2.24. Grünwald-Letnikov yaklaşımı

Burada L_m hafıza uzunluğunu, $t_k=kh$, h adım aralığını temsil ederken, $(-1)^j\binom{q}{j}$ binominal katsayıları da $c_j^{(q)}(j=0,1,2\ldots)$ olarak tanımlanır. Bu katsayılar aşağıdaki şekilde hesaplanır.

$$c_0^{(q)}=1$$

Denklem 2.25. Binom katsayısı başlangıç koşulu

$$c_j^{(q)}=\left(1-\frac{1+q}{j}\right)c_{j-1}^{q}$$

Denklem 2.26. İteratif binom katsayı denklemi

Daha sonra, kesirli diferansiyel denklemlerin genel sayısal çözümü aşağıdaki şekilde tanımlanır.

$${}_aD_t^q y(t)=f(y(t),t)$$

Denklem 2.27. Kesirli diferansiyel denklem

$$y(t_k) = f(y(t), t)h^q - \sum_{j=v}^{k} c_j^{(q)} y(t_{k-j})$$

Denklem 2.28. Kesirli diferansiyel denklem için sayısal çözüm denklemi

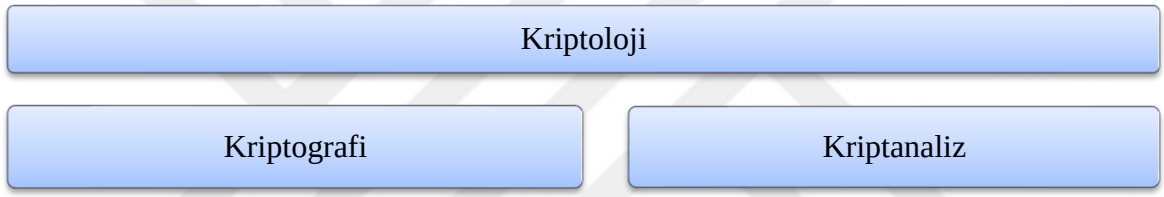
2.2. Kriptoloji

Gizli bilgi anlamına gelen kriptoloji Yunanca kökenli olup gizli anlamına gelen krypto(κρυπτός) ve bilgi anlamına gelen logos (λόγος) kelimelerinden türetilmiştir. Kriptolojinin temel amacı bilgi güvenliğini sağlamak ve gizliğini korumaktır (Simmons, 1983). Diğer bir ifadeyle kriptoloji, anlamlı olan verileri şifreleme türleri kullanarak üçüncü kişiler için anlamsız hale getirilmesini sağlayan bilim dalıdır. Günümüzde kriptoloji devletlerarası iletişimde, askeri alanlarda, bankacılık sistemlerinde vb. birçok sistemde kullanılmaktadır. Şifreleme süreçlerinde kullanılan algoritmaların tasarımı, geliştirilmesi ve analiz edilmesi kriptoloji biliminin ana bileşenlerindendir. Kriptoloji sistemlerinin, güvenliği sağlamak için belirli gereksinimleri karşılaması zorunludur. Bu temel gereksinimler aşağıdaki ilkeleri içermektedir:

- Veri Bütünlüğü (Data Integrity): Veri bütünlüğü, iletişim sürecinde verinin yetkisiz kişiler tarafından değiştirilmediğini garanti etmektedir. Verinin iletim sırasında ekleme, silme veya değiştirme gibi müdahalelere karşı korunmasını sağlar. Özetleme gibi teknikler kullanılarak, verinin alıcıya herhangi bir değişiklik yapılmadan ulaştığını doğrulamak için kullanılır (William, 2017; Zajac, 1994).
- Kimlik Doğrulama (Authentication): Kimlik doğrulama, iletişimde bulunan tarafların birbirlerinin kimlik bilgilerini doğrulamasını sağlamaktadır. Alıcının, gelen verinin gerçekten belirtilen gönderici tarafından gönderildiğinden emin olmasını temin eder. Böylece güvenilir bir kimlik doğrulamayla, sahtecilik ve kimlik hırsızlığını önlenebilir (Al-Shabi, 2019).
- Gizlilik (Confidentiality): İletişimde iletilen verinin yetkisiz kişiler tarafından okunmasını engelleyen gereksinimdir. Bu güvenlik ilkesi, iletişim araçlarının fiziksel korunması ve güvenlik protokolleri, şifreleme algoritmaları gibi yöntemlerle sağlanmaktadır. Gizlilik, bilgi güvenliğinin temel taşlarından biridir(Yassein et al., 2017).

- Reddedilemezlik (Non-repudiation): Gönderilen verinin kaynağının doğrulanmasını ve göndericinin gönderdiği veriyi reddedememesini temin etmektedir. Dijital imza gibi teknikler bu gereksinimi karşılamak için kullanılmaktadır (Delfs et al., 2002).

Şifreleme işlemleri için birçok farklı algoritma tasarlanmıştır. Tasarlanan bazı karmaşık algoritmalar, performans açısından tatmin edici olmayabilir ve istenmeyen hatalara yol açabilmektedir. Şifre çözme sürecindeki küçük bir hata, orijinal verinin elde edilememesine neden olabilir. Bu nedenle, algoritma tasarımında yukarıda verilen temel gereksinimlere dikkat edilmelidir. Şifreleme algoritmalarının etkinliği, karıştırma ve dağıtma özelliklerinin ne kadar iyi olduğuna bağlıdır. Kaos tabanlı yöntemler, bu özelliklerin sağlanmasında oldukça etkilidir. Kriptoloji, kriptografi ve kriptanaliz arasındaki ilişki Şekil 2.10'da özetlenmiştir.



Şekil 2.10. Kriptoloji, kriptografi, kriptanaliz arasındaki ilişki

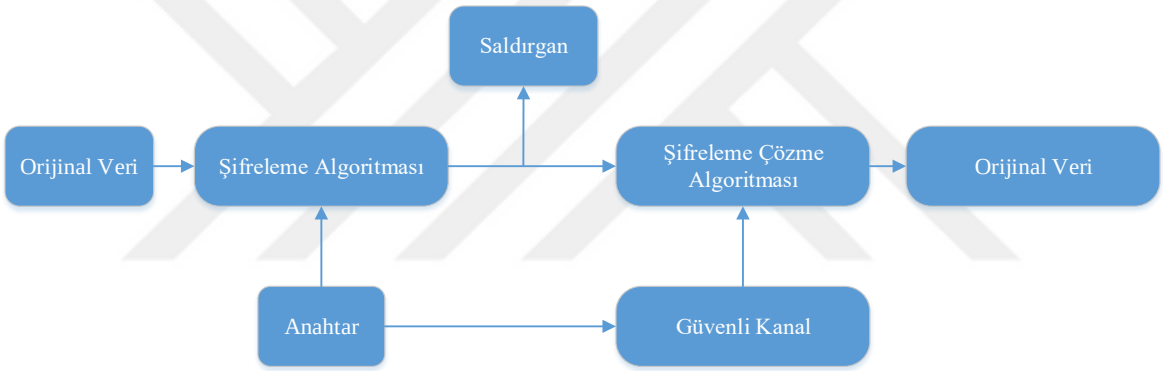
Kriptografi, bilgi güvenliğini sağlamak amacıyla, algoritma tasarımı ve geliştirilmesine yönelik çözümler sunarak, bilgiyi gönderici ve alıcı dışında kimsenin anlayamayacağı biçime dönüştürmeyi amaçlar. Bu doğrultuda şifreleme, şifre çözme, dijital imza vb. gibi teknikler kullanarak bilgi güvenliği sağlamaktadır (Gautam et al., 2018). Kriptanaliz ise şifrelenmiş veriyi çözmek ve şifreleme sistemlerini analiz etmekle ilgilenen bir bilim dalıdır. Kriptoanaliz, şifrelenmiş metni çözmek ve şifreleme sistemlerini analiz etmek için kullanılan bir süreçtir. Bu süreç, gizli bilgiyi anlamaya çalışarak şifreleme sistemlerinin güvenliğini test etmeyi amaçlamaktadır (Carter et al., 2007). Kriptoanaliz, kriptografik sistemlerin güvenlik zaaflarını anlamak ve ortaya çıkarmak açısından oldukça önemlidir.

Kaotik sistemlerin başlangıç değerlerine duyarlılık, ergodisite ve karmaşık davranışlar gibi avantajlardan dolayı kaotik sistem tabanlı algoritmaların, özellikle modern kriptografide önemli bir rol oynamaktadır. Kaotik sistemler şifreleme biliminin temel unsurları olan karıştırma ve yayılma özelliklerini iyi bir şekilde sağladıkları için, son zamanlarda şifreleme çalışmalarında giderek daha fazla tercih edilmektedir. Literatürde, rastgele sayı üretimi, süre

ve bellek gibi avantajlarından dolayı kaotik sistem tabanlı birçok şifreleme uygulaması gerçekleştirilmiştir. Literatürde ayrık ve sürekli zamanlı olarak tek boyutlu veya çok boyutlu biçimlerde birçok kaotik sistem bulunmaktadır. Kesir dereceli kaotik sistemler ise genellikle daha karmaşık dinamikler ve bellek etkileri sergilerler. Bundan dolayı kesir dereceli sistemlerin kullanılması özellikle güvenlik uygulamalarında daha avantajlı olacaktır.

2.2.1. Kriptoloji Türleri

Şifreleme temel olarak bilginin gizliliğini, bütünlüğünü ve güvenliğini sağlamak amacıyla kullanılan matematiksel ve mantıksal yöntemlerin bütünleşik bir dizisidir. Literatürde çeşitli şifreleme teknikleri geliştirilmiş olup bu teknikler bilgiyi yetkisiz erişimden koruma ve iletişim süreçlerinde gizliliği muhafaza etme amacı taşımaktadır. (Por et al., 2023). Şekil 2.11'de şifreleme ve şifre çözme sisteminin genel yapısı verilmiştir.



Şekil 2.11. Şifreleme sisteminin genel yapısı

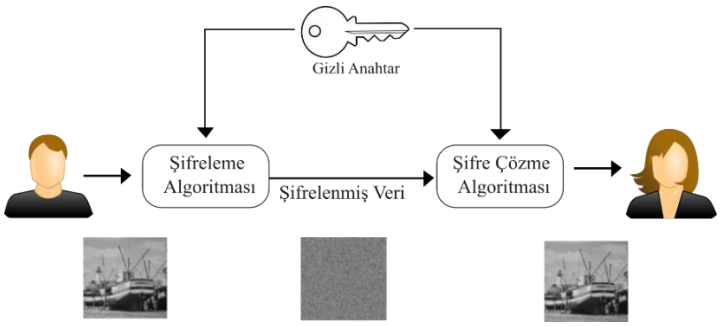
Şifreleme sisteminin temel amacı güvensiz bir kanal üzerinden veri iletişimi sırasında, saldırgan tarafından erişilemeyen biçimde iletişim sağlayabilmektir. Sistemde var olan, orijinal veri metin, ses, fotoğraf, video gibi multimedya verilerini ifade etmektedir. Anahtar, şifreleme ve şifre çözme işlemlerinde kullanılan gizli bilgiyi ifade etmektedir. Anahtarın güvenliği, tüm şifreleme sisteminin güvenliğini belirler. Anahtar, şifreleme algoritması ile birlikte çalışarak veriyi anlaşılmaz hale getirmektedir. Bir şifreleme işleminde anahtar uzunluğunun artması, şifreleme algoritmalarının güvenliğini önemli ölçüde artırmaktadır. Çünkü uzun anahtarlar, saldırganların kaba kuvvet (brute force) saldırılarıyla doğru anahtarı bulma olasılığını düşürmektedir. Ancak, bu durum aynı zamanda şifreleme ve şifre çözme işlemlerinin daha fazla hesaplama gücü ve süre gerektirmesi anlamına gelmektedir. Ayrıca, donanımsal ve yazılımsal gerçeklemelerde uzun anahtarların kullanımı, performans üzerinde olumsuz etkilere neden olmaktadır. Donanım tabanlı uygulamalarda, uzun anahtarlar için

gerekli olan ek hesaplamalar, işlemcinin daha fazla enerji tüketmesine ve daha fazla ısınmasına yol açabilmektedir. Yazılım tabanlı uygulamalarda ise, uzun anahtarlar bellekte daha fazla yer kaplar ve işlem sürelerini uzatabilmektedirler. Kaos tabanlı teknikler kullanılarak gerçekleştirilen şifreleme çalışmalarında, doğru yöntem seçildiğinde anahtar uzunluğu fazla olsa bile, kaos tabanlı olmayan sistemlere kıyasla süre açısından önemli avantajlar elde edilebilir. Bellek harcaması genellikle süre ile doğru orantılı olduğundan, süre avantajları ve dezavantajları bellek kullanımı için de geçerli olacaktır (Akgül, 2015). Şifreleme algoritması ise orijinal veriyi, belirli bir anahtar kullanarak şifreli hale getiren matematiksel işlemler bütünüdür. Saldırganlar ise şifrelenmiş veriyi ele geçirmeye çalışan yetkisiz kişiler veya sistemleri ifade etmektedir. Şifreleme işlemindeki temel amaç veriyi saldırganlardan korumaktır. Güvenli kanal ise, anahtarın şifreleme ve şifre çözme işlemlerini gerçekleştirecek taraflar arasında güvenli bir şekilde iletilmesini sağlayan yapıdır. Şifre çözme algoritması ise şifrelenmiş veriyi, orijinal haline geri döndüren matematiksel işlemler bütünüdür. Bu işlem, şifreleme algoritmasıyla ters yönde çalışır ve doğru anahtar kullanılarak gerçekleştirilir.

Literatürde bulunan şifreleme algoritmaları kendi içerisinde anahtar dağıtımına göre genel olarak iki ana sınıfa ayrılmaktadır (Dahat et al., 2016).

2.2.1.1.Simetrik Kriptoloji

Simetrik şifreleme, aynı anahtarı hem şifreleme hem de şifre çözme algoritmalarında kullanıldığı bir kriptoloji türüdür. Bu şifreleme türünde anahtarın kesinlikle gizli tutulması gerekmektedir. Gizli anahtarın, alıcı-verici tarafından önceden bilinmesi gerekmektedir. Şekil 2.12'de simetrik şifreleme modeli verilmiştir.



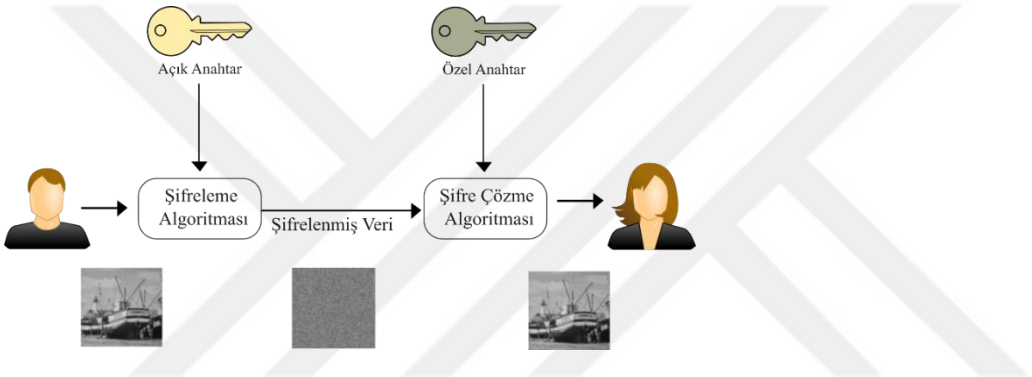
Şekil 2.12. Simetrik şifreleme modeli

Simetrik şifreleme algoritmaları, asimetrik şifreleme algoritmalarına göre hızlıdırlar. Genellikle şifrelenecek verinin türüne göre blok ve akış şifreleme algoritmaları olmak üzere

iki ana kategoriye ayrılır. Blok şifreleri, veriyi sabit boyutlu bloklar halinde işlerken, akış şifreleri veriyi bit veya byte seviyesinde işlemektedir. Blok şifrelemesine örnek olarak AES ve DES algoritmaları verilebilirken akış şifrelemesine ise örnek olarak RC4 algoritması gösterilebilir (Cui et al., 2023; Dash et al., 2023).

2.2.1.2.Asimetrik Kriptoloji

Asimetrik şifreleme, diğer adıyla açık anahtarlı şifreleme sistemleri genel olarak iki farklı anahtarların kullanıldığı sistemdir. Bu yöntemdeki anahtarlardan birisi genel olarak bilinen açık anahtarken, diğeri ise sahibi tarafından gizlenen özel anahtardır. Şekil 2.13'te asimetrik şifreleme modeli verilmiştir.



Şekil 2.13. Asimetrik şifreleme modeli

Asimetrik şifreleme sistemlerinde açık anahtara sahip olan kişi veriyi sadece şifreleyebilir, şifre çözme işlemini gerçekleştirmez. Şifreli veriyi çözme yeteneği sadece özel anahtara sahip olan kişilerde bulunmaktadır. Açık anahtar genel olarak paylaşılarak veri şifrelemesi yapılırken özel anahtar gizli tutulur ve şifre çözme işlemi için kullanılmaktadır. Bu yöntem, veri güvenliğini sağlamak ve izinsiz erişimi önlemek için etkili bir yol sunmaktadır (Fujisaki et al., 2013). En bilinen asimetrik şifreleme algoritmalarına RSA, Diffie-Hellman, ElGamal ve ECC örnek olarak verilebilir.

2.2.1.3.Özet (Hash) Kriptoloji

Özetleme fonksiyonları, girdiyi sabit uzunlukta bir dizeye dönüştürür. Bu dönüşüm tek yönlüdür. Özetleme fonksiyonlarında anahtar kullanılmaz. Kriptografik özet fonksiyonları, kullanıcıların verilerde yetkisiz değişiklikleri tespit etmesine olanak tanıyan mesaj özetleri oluşturur. Bu işlevler, özellikle kritik sistemler ve hassas veri tabanları için oldukça önemlidir. Verinin kaynağını doğrulamak amacıyla özet fonksiyonları, diğer kriptografik yöntemlerle entegre edilebilir. Özet algoritmaları, şifreleme ile birleştirildiğinde, verilerin

kaynağını tanımlayan özel mesaj özetleri üretebilirler. Bu tür özetler, Özet Tabanlı Mesaj Doğrulama Kodu (Hash-based Message Authentication Code-HMAC) olarak bilinir ve günümüzde yaygın olarak kullanılan standart bir algoritmadır. HMAC, veri kaynağının doğrulanmasını sağlar ve saldırganların müdahalelerini önler (Krawczyk et al., 1997). Literatürde MD5, SHA-1, SHA-2, SHA-3 ve Merkle Ağacı yaygın olarak kullanılan özetleme algoritmalarıdır.

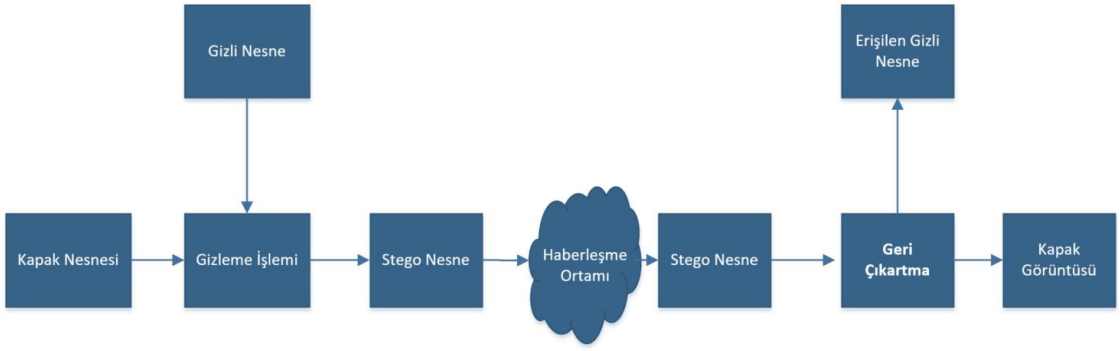
Kriptoloji türlerinin kıyaslanması Tablo 2.2'de verilmiştir.

Tablo 2.2. Kriptoloji türlerinin kıyaslanması

Özellik	Simetrik Kriptoloji	Asimetrik Kriptoloji	Özet (Hash) Kriptoloji
Anahtar Kullanımı	Aynı anahtar hem şifreleme hem de şifre çözme için kullanılmaktadır.	Bir açık anahtar ve bir gizli anahtar kullanılmaktadır.	Anahtar kullanılmaz, sadece hash fonksiyonları kullanılmaktadır.
Güvenlik	Anahtar dağıtımı güvenli olmalıdır.	Açık anahtar herkesle paylaşılabilir, gizli anahtar saklanır.	Tek yönlüdür, geri dönüşü yoktur.
Hız	Genellikle hızlıdır.	Daha yavaştır.	Çok hızlı, sadece özet hesaplama yapar.
Örnek Algoritmalar	AES, DES, 3DES	RSA, ECC, DSA	MD5, SHA-1, SHA-256
Anahtar Uzunluğu	Kısa (128-256 bit)	Uzun (2048-4096 bit veya daha fazla)	-
Kullanım Alanları	Büyük veri şifreleme, veri aktarımı	Dijital imzalar, anahtar değişimi, küçük veri blokları	Veri bütünlüğü, dijital imzalar, parola saklama
Avantajlar	Hızlı ve verimli	Güvenli anahtar dağıtımı, dijital imza ve kimlik doğrulama	Veri bütünlüğünü sağlama, kolay uygulama
Dezavantajlar	Anahtar dağıtımı zor ve riskli	Daha yavaş işlem süresi	Çakışma riski, bazı eski algoritmaların güvenlik sorunları
Kritik Uygulamalar	VPN, disk şifreleme	SSL/TLS, PGP, e-posta şifreleme	Veri bütünlüğü kontrolü, dijital imzalar, blockchain

2.3. Steganografi

Steganografi, tarihsel süreçte iletişim güvenliğini sağlamak amacıyla önemli bir rol oynamış eski bir sanattır. Bu terim, Yunanca kökenli "Steganos" (saklanmış, gizli veya korunmuş) ve "Graphtein" (yazı) kelimelerinden türetilmiştir, bu nedenle "gizli yazı" anlamına gelmektedir (M. Uzun, 2023). Genel olarak steganografi, hassas veya gizli bilgileri gizlemek ve bu bilgileri yetkisiz erişimden korumak amacıyla kullanılan bir dizi teknik ve metodolojiyi ifade etmektedir. Bu teknikler veriyi fark edilmeden başka bir veri içine gizleme, dosya boyutlarını değiştirme veya veri içeriğini manipüle etme gibi yöntemlerle gerçekleştirilir. Bu sayede, bilgilerin gizliliği korunur ve yetkisiz kişilerin erişimine karşı koruma sağlanır. Modern steganografi uygulamaları, gizli bilgileri fark edilmez bir şekilde taşıyıcı medya dosyalarına gizlemeyi hedefler. Steganografi, bilginin iletimini gizli olarak sağladığı için şifrelemeye göre daha az dikkat çeken bir yöntemdir. Bu yüzden birçok uygulamada bazı taraflarca şifreleme yerine tercih edilmektedir. Steganografi, özellikle dijital görüntüler, ses dosyaları ve video dosyaları gibi medya dosyalarında yaygın olarak kullanılır (Petitcolas et al., 1999). Steganografik sistemin genel çalışma mantığını özetleyen bir diyagram Şekil 2.14'te sunulmaktadır (Kadhim et al., 2019). Şekilden de anlaşılacağı üzere, gizlenmesi gereken hassas veriler, bir veri gizleme algoritması kullanılarak taşıyıcı bir nesne olan "kapak" dosyasında küçük değişiklikler yapılarak saklanır. Bu taşıyıcı dosyalar, dijital görüntüler, ses dosyaları veya video dosyaları gibi çeşitli formatlarda olabilir. Gizleme işlemi sonucunda oluşturulan, gizli veriyi içeren dijital nesne "stego" olarak adlandırılır. Stego nesnesinden veri çıkarma algoritması kullanılarak gizli nesne tekrar ortaya çıkarılabilir.



Şekil 2.14. Steganografik sistemin blok diyagramı

Steganografik işlemler, gizli bilgileri taşıyıcı medya dosyasının içine yerleştirirken bu medya dosyasının görsel veya akustik özelliklerini korumayı ve bu şekilde gizli bilgilerin

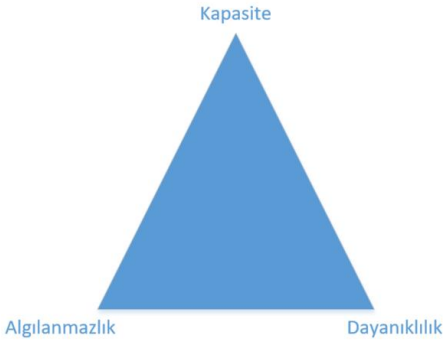
yetkisiz kişiler tarafından tespit edilememesini amaçlamaktadır. Bu işlem, gizli bilgilerin saklandığı stego nesnesinin dışarıdan bakıldığında normal ve doğal görünmesini sağlar, böylece gizli bilginin varlığı fark edilemez. Steganografi, kriptografi birlikte kullanılarak dijital iletişim güvenliği ve veri saklama alanlarında kritik bir öneme sahiptir. Bu tekniklerin bir arada kullanılması, bilgilerin güvenli bir şekilde saklanması ve iletilmesini sağlamak için etkili bir yaklaşım sunar. Steganografi ayrıca geniş bir uygulama yelpazesi sunar ve farklı medya dosyalarında (görüntü, ses, video vb.) gizli bilgilerin saklanmasına olanak tanır. Bu da bilgi güvenliği açısından çok çeşitli kullanım alanlarına sahip olduğunu göstermektedir.

Steganografik sistemlerin üç temel özelliği vardır: algılanamazlık, veri kapasitesi ve dayanıklılıktır. Bu özellikler, gizli bilgilerin etkili bir şekilde saklanmasını ve iletilmesini sağlayarak steganografinin temel amacına hizmet etmektedir.

Algılanamazlık, steganografik tekniklerin başarısının en önemli göstergelerinden biridir ve steganografinin temel amacı olan gizliliği korumakla doğrudan ilişkilidir. Bu kavram, verinin taşıyıcı ortama gizlenmesi sonucu oluşabilecek herhangi bir kalite düşüşünü veya gözle görülür değişikliği en aza indirgeyerek kapak nesnesinin doğal görünümünü ve işlevselliğini korumasını ifade etmektedir (VenkatramanS et al., 2004).

Veri kapasitesi, steganografik işlem sırasında taşıyıcı medya içine gömülecek gizli verinin miktarını tanımlar. Daha fazla gizli veri gizleme kapasitesi, daha fazla bilgiyi taşıyıcı nesne içine entegre etme olanağı sağlar. Ancak, bu kapasitenin artırılması, taşıyıcı medya üzerinde yapılan değişikliklerin algılanma riskini de artırabilir. Bu nedenle, steganografi uygulamalarında veri kapasitesi ile değişiklik algılanabilirliği arasında önemli bir denge bulunur. Etkili bir steganografik sistemin temel amacı, en fazla miktarda bilgiyi kapak nesnesinde en az değişikliğe sebep olacak şekilde iletmektir. Veri kapasitesi, gizli bilginin bit cinsinden ölçülen miktarının kapak medyasının boyutuna oranı olarak tanımlanabilir (Mandal et al., 2022).

Dayanıklılık kavramı ise, steganografik işlemin stego nesnesi üzerinde yapılan dışsal değişikliklere karşı etkinliğini sürdürebilme yeteneğini ifade eder. Bu özellik, steganografi uygulamalarının güvenilirliğini artırmaktadır çünkü stego nesnesinin dışsal değişikliklere karşı dayanıklılığı, gizli verinin bütünlüğünü korur ve kaybolmasını veya bozulmasını engeller (Altaay et al., 2012).



Şekil 2.15. Veri gizleme özellikleri arasındaki denge üçgeni (Kaynak: Wang ve ark., 2023)

Şekil 2.15'te veri gizleme özellikleri arasındaki denge gösterilmektedir. Her steganografi yöntemi, bu özellikler arasında bir denge sağlamaya çalışır ve kullanım senaryosuna göre tercih edilen özellikler değişebilir. Herhangi bir steganografik yöntemi seçerken, belirli bir uygulama veya senaryo için en uygun dengeyi sağlamak önemlidir.

Steganografi teknikleri, kullanılan kapak nesnesinin türüne göre, metin steganografisi, ses steganografisi ve görüntü steganografisi olmak üzere üç ana kategorilere ayrılmaktadır. Tez çalışmasında görüntü steganografisi gerçekleştirilecektir. Görüntü steganografisi hakkında temel bilgiler bir sonraki bölümde verilecektir.

2.3.1. Görüntü Steganografisi Yöntemleri ve Özellikleri

Görüntü steganografisi, genel olarak kapak nesnesinin bir resim olarak seçildiği steganografi uygulamalarını ifade etmektedir. Gizlenen veriler, kapak resminde olduğu gibi farklı formatlarda kullanılabilmektedirler. Ancak görüntü steganografisi, steganografinin temel unsurudur ve bu durumun temel nedenleri şöyle özetlenebilir:

1. Erişilebilirlik ve Paylaşım Kolaylığı: Görüntüler, taşınabilir ve internet üzerinden kolayca paylaşılabilir. Bu, diğer formatlara kıyasla daha rahat erişim ve paylaşım sağlar.
2. Yüksek Kapasite: Görüntüler, büyük miktarda veriyi saklama kapasitesine sahiptir. Her piksel veya renk kanalı, gizli veriler için kullanılabilir. Diğer taraftan, metin tabanlı kapak nesneleri daha az veri saklama kapasitesine sahiptir.
3. Görsel Algıya Dayanıklılık: İnsan gözü, küçük değişiklikleri algılamada sınırlıdır. Görüntü steganografisinde yapılan küçük değişiklikler genellikle gözle fark edilmez, bu da gizli verilerin etkili bir şekilde gizlenmesini sağlar.
4. Çoklu Uygulama Alanları: Görüntü steganografisi, telif hakkı koruma, kimlik doğrulama, gizli iletişim ve veri güvenliği gibi çeşitli alanlarda kullanılabilir.

5. Teknolojik Gelişmelere Uyumluluk: Görüntü işleme teknolojilerindeki ilerlemeler, daha karmaşık ve etkili görüntü steganografi yöntemlerinin geliştirilmesine olanak sağlar. Yapay zekâ ve makine öğrenimi gibi teknolojiler, görüntü steganografisini daha da geliştirir ve daha sofistike hale getirir.

Görüntü steganografisi için kullanılan birçok yöntem bulunmaktadır ve bu yöntemler iki ana kategoriye ayrılır: uzaysal/görüntü alan teknikleri ve frekans/dönüşüm alan teknikleridir. Uzaysal alan teknikleri, gizli verilerin doğrudan piksel değerlerine yerleştirilmesini içerirken, frekans alan teknikleri, verilerin görüntünün frekans bileşenlerine gömülmesini içermektedir (Morkel et al., 2005).

2.3.2. Uzaysal/Görüntü Steganografi Tekniği

Uzaysal alan teknikleri, gizli bilgiyi doğrudan kapak görüntüsünün piksellerine yerleştirir. Bu teknikler arasında en yaygın olarak kullanılan yöntem, piksellerin en az anlamlı bitlerini (LSB) değiştirme yöntemidir. Bu teknik, görüntüdeki her pikselin en düşük anlamlı bitini değiştirerek veri saklar. Kayıpsız görüntü formatları olan Bitmap, PNG ve 8 bit gri tonlamalı GIF, LSB teknikleri için uygundur. LSB, basitliği ve kolay uygulanabilirliği nedeniyle yaygın olarak tercih edilen bir yöntemdir (Cheddad et al., 2010; Provos et al., 2003). Bir diğer uzaysal alan tekniği ise Bit Düzlem Karmaşıklık Segmentasyonu (BPCS) yöntemidir. Bu yöntem, 1997 yılında Richard O. Eason ve Eiji Kawaguchi tarafından tanıtılmıştır. BPCS, her bit düzleminin hesaplama karmaşıklığını kullanarak veri ekler. Bu teknik, taşıyıcı ortamı karmaşıklık derecelerine göre segmentlere ayırır ve verileri yüksek karmaşıklığa sahip segmentlere yerleştirir. BPCS, sadece en düşük değerlikli bitleri değil; tüm bit düzlemini kullanarak işlem yapmaktadır (Kawaguchi, 1997).

Dijital sistemlerde, bilgiler bit dizisi formunda ifade edilir. Örneğin, desimal formdaki 123 sayısı, binary notasyonla 01111011 olarak ifade edilir. Bu notasyonda, en anlamlı bit (Most Significant Bit, MSB) ve en anlamsız bit (Least Significant Bit, LSB) kavramları kullanılır. MSB, sayının en solundaki ve 2 tabanında en büyük üstel değeri temsil eden bittir. LSB ise, sayının en sağındaki ve 2 tabanında en küçük üstel değeri temsil eden bittir. Temsil edilen en anlamlı ve en anlamsız dijitleri Şekil 2.16'da gösterilmiştir.

MSB LSB

0	1	1	1	1	0	1	1

Şekil 2.16. "123" sayısının LSB-MSB gösterimi

Örneğin, 123 sayısının MSB'si değiştirilmesiyle, sayı 128 artarak 251 olurken, LSB'si değiştirilmesiyle, sayı sadece 1 azalarak 122 olur. Bu, MSB'nin değiştirilmesinin büyük, LSB'nin değiştirilmesinin ise küçük bir değişime neden olduğunu gösterilmektedir (Chan et al., 2004). LSB steganografi tekniği, bu prensibe dayanmaktadır. Kapak resmin piksellerindeki LSB bitleri değiştirilerek gizli bilgiler saklanır. Piksel değerlerinin LSB bitlerinde yapılan değişiklikler, görüntü kalitesinde çıplak gözle fark edilemeyen bozulmalara neden olur ve bu bozulmalar genellikle gürültü olarak değerlendirilir. Bu nedenle stego görüntü, orijinal görüntüden çıplak gözle ayırt edilemez ve gizli mesajın ortaya çıkarılması zor olmaktadır.

LSB (Least Significant Bit) yönteminde verilerin eklenme modu, kullanılan kapak resmin 8 bit veya 24 bit olmasına bağlı olarak değişmektedir. Gri tonlamalı 8 bitlik görüntülerde, her piksele yalnızca bir bit gizlenebilir. Bu tür görüntülerde, her piksel 256 farklı ton değerinden birini temsil eder ve bu ton değeri içerisinde yalnızca en az anlamlı bit değiştirilerek veri saklanmaktadır. 24 bit derinlikli renkli görüntüler ise her pikselde kırmızı (Red, R), yeşil (Green, G) ve mavi (Blue, B) olmak üzere üç ayrı renk bileşenini içerir. Her bir bileşen 8 bitlik bir değeri temsil eder ve bu sayede her piksel 24 bitlik bir veri içerir. Bu yapı, her bir renk bileşenine bir bitlik veri yerleştirilmesine olanak tanır, böylece her pikselde toplamda 3 bitlik gizli bilgi saklanabilir. Dolayısıyla, 24 bitlik renkli görüntüler, 8 bitlik gri tonlamalı görüntülere kıyasla daha fazla veri saklama kapasitesine sahiptir (Chan et al., 2004; Kharrazi et al., 2004).

Tablo 2.3'te kriptoloji ve steganografi yöntemlerinin kıyaslaması verilmiştir.

Tablo 2.3. Kriptoloji ve Steganografi kıyaslaması

	Kriptoloji	Steganografi
Anlamı	Kriptografi terimi "gizli yazı" anlamına gelmektedir.	Steganografi terimi Yunanca "örtülü yazı" anlamına gelmektedir.
Amaç	Verilerin formunu anlaşılmaz hale getirir.	Gizli veriyi algılanamayacak şekilde saklar.

Tablo 2.3. (devam) Kriptoloji ve Steganografi kıyaslaması

Kapak(Cover)	Gerek yoktur. Direk veri üzerine uygulanmaktadır.	Kapak seçimi serbesttir.
Geçersiz Olma Durumu	Şifrenin çözülmesi	Gizli verinin fark edilmesi
Saldırı Türü	Kriptoanaliz	Steganaliz
İşlem Çıktısı	Şifreli dosya	Stego dosya

Steganografi ve kriptografi, temel hedeflerinde benzerlik gösterirken, yaklaşımları farklıdır. Steganografi, verinin formatını değiştirmeden asıl veriyi korurken, kriptografi veriyi okunamaz bir forma dönüştürerek gizliliği sağlar. Ayrıca, kriptografik sistem üçüncü bir tarafın verilere eriştiğinde kırılmış olarak kabul edilirken, steganografi sistemi üçüncü bir tarafın gizli verinin varlığını tespit ettiğinde kırılmış sayılır (Johnson et al., 1998).

2.4. Gömülü Sistemler

2.4.1. NVIDIA Jetson AGX Orin

NVIDIA Corporation tarafından geliştirilen, NVIDIA Jetson AGX Orin, yapay zekâ ve yüksek performanslı bilgi işlem uygulamaları için tasarlanmış gelişmiş bir platformdur. AGX Orin, yüksek işlem gücü ve paralel işlem yetenekleri sayesinde kaotik sistemlerin karmaşık hesaplamalarını, veri şifreleme ve deşifreleme işlemlerini, ayrıca steganografi gibi kriptoloji uygulamalarını hızlı ve etkili bir şekilde gerçekleştirebilmektedir. NVIDIA Jetson AGX Orin'e ait görsel Şekil 2.17'de verilmiştir.

Şekil 2.17. NVIDIA Jetson AGX Orin

NVIDIA Jetson AGX Orin gömülü sistem, güçlü, düşük maliyetli ve taşınabilir olmasından dolayı, tez çalışmasında tercih edilmiştir. Jetson AGX Orin'in teknik özellikleri Tablo 2.4' te verilmiştir (NVIDIA, 2024).

Tablo 2.4. Nvidia Jetson AGX Orin Gömülü Kartının Temel Özellikleri

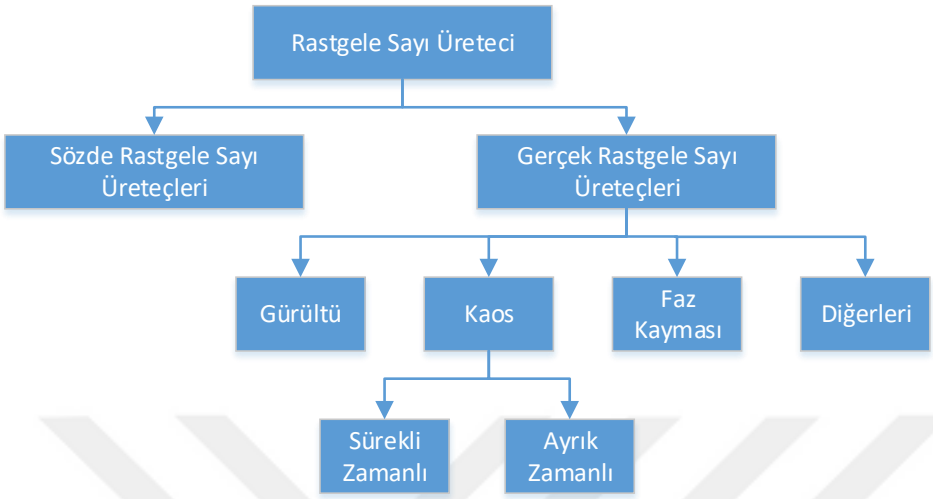
Özellik	Detaylar
GPU	NVIDIA Ampere Mimarisi 2048 NVIDIA® CUDA® çekirdekli ve 64 tensör çekirdekli
CPU	12 çekirdekli Arm® Cortex®-A78AE v8.2 64 bit CPU 3 MB L2 + 6 MB L3
Bellek	64 GB 256 bit LPDDR5
Depolama	64 GB eMMC 5.1
Güç Tüketimi	15W-60W
Boyutlar	110 mm x 110 mm x 71,65 mm
Hesaplama Gücü	275 TOPS (Trillion Operations Per Second)

NVIDIA Jetson AGX Orin'in özellikle hesaplama gücünün 275 TOPS olması, saniyede 275 trilyon işlem gerçekleştirebilme kapasitesine sahip olduğu anlamına gelmektedir. Bu durum, NVIDIA Jetson AGX Orin'in yoğun ve karmaşık matematiksel işlemlerin gerektiği şifreleme-şifre çözme ve steganografi süreçleri gibi veri işlemlerinin gerçekleştirilmesine olanak tanımaktadır.

2.5. Rastgele Sayı Üreteçleri ve Testleri

Rastgele sayılar, aralarında herhangi bir bağlantı bulunmayan sayılardır (Hasanbayli et al., 2021). Günümüzde rastgelelik kavramı birçok uygulamada yaygın bir şekilde kullanılmaktadır. İstatistik, nümerik analiz, şans oyunları gibi alanların yanı sıra, kriptolojik uygulamaların çoğunda da rastgele sayılardan yararlanılmaktadır (Akçay et al., 2017; B. Li et al., 2019; Schindler, 2009). Güvenli haberleşme uygulamalarında, iletilecek veya alınacak verinin sadece alıcı ve iletici tarafından bilinmesi gerektiğinde rastgele sayılar kullanılır. Bankamatik kullanıcı erişimi, oturum erişimi ve kimlik doğrulama gibi çeşitli şifreleme alanları rastgele sayıların kullanımına örnek olarak verilebilir. Rastgele Sayı Üreteçleri,

Şekil 2.18'de görüldüğü gibi temel olarak sözde Rastgele Sayı Üreteçleri ve Gerçek Rastgele Sayı Üreteçleri olmak üzere iki başlık altında incelenmektedirler.



Şekil 2.18. Rastgele sayı üreteçlerinin sınıflandırılması (Kaynak: Yu ve ark., 2019)

2.5.1. Sözde Rastgele Sayı Üreteçleri

Sözde Rastgele Sayı Üreteçleri (SRSÜ'ler), başlangıçta belirlenen bir "tohum" (seed) değeriyle başlatıldığında matematiksel algoritmalar kullanarak rastgele sayı dizileri oluşturmaktadır. SRSÜ deterministik yapıda oldukları için aynı tohum değeriyle başlatıldıklarında her seferinde aynı sayı dizisini üretirler. Bu özellik SRSÜ'lerin simülasyonlar, modellemeler için öngörülebilir ve tekrarlanabilir sonuçlar sağlamasını mümkün kılmaktadır (L'Ecuyer, 1994).

2.5.2. Gerçek Rastgele Sayı Üreteçleri

Gerçek Rastgele Sayı Üreteçleri (GRSÜ'ler), fiziksel süreçlerden elde edilen rastgelelik üzerine kurulmuştur ve bu süreçlerin öngörülemez doğası nedeniyle gerçekten rastgele sayı dizileri üretirler. Kuantum mekaniksel olaylar; termal gürültü, radyoaktif bozunma, kaotik davranışlar ve diğer çevresel gürültü kaynakları gibi doğal olaylardan yararlanabilir. GRSÜ'lerin temel avantajı deterministik olmayan yapılarıdır, yani aynı başlangıç koşullarından bile farklı sonuçlar üretebilirler, bu da onları kriptografi ve yüksek güvenlik gerektiren diğer uygulamalar için ideal kılmaktadır (Ferguson et al., 2010).

GRSÜ'lerin ürettiği rastgele sayılar, kriptografik uygulamalar için özellikle değerlidir çünkü bu sayılar öngörülemezdir ve herhangi bir matematiksel algoritma tarafından tekrar

üretilemez. Özellikle güvenli şifreleme anahtarları oluşturmak ve hassas verilerin şifrelenmesi işlemlerinde kritik öneme sahiptir (Kocher, 1995). Tablo 2.5'te Sözde Rastgele Sayı Üreteçleri ile Gerçek Rastgele Sayı Üreteçleri karşılaştırılmıştır.

Tablo 2.5. Sözde ve Gerçek rastgele sayı üreteçlerinin karşılaştırılması

Özellik	Sözde Rastgele Sayı Üreteçleri (SRSÜ'ler)	Gerçek Rastgele Sayı Üreteçleri (GRSÜ'ler)
Temel İlke	Matematiksel algoritmalar kullanarak deterministik rastgele sayılar üretir.	Fiziksel olaylardan kaynaklanan öngörülemez süreçlerle rastgele sayılar üretir.
Başlangıç Koşulu	Tohum (seed) değeriyle başlar; aynı tohum aynı sayı dizisini üretir.	Tohum değeri kullanmaz; fiziksel olayların rastgele doğasıyla çalışır.
Öngörülebilirlik	Deterministik oldukları için öngörülebilirdir.	Öngörülemezdir ve herhangi bir matematiksel modelle tekrar üretilemez.
Hız	Çok hızlıdır, büyük miktarda sayıyı hızla üretebilir.	Genellikle SRSÜ'lere göre daha yavaştır, çünkü fiziksel süreçlerin ölçümü gereklidir.
Uygulama Alanları	Simülasyonlar, istatistiksel modelleme, bilgisayar oyunları ve kriptografik olmayan uygulamalar.	Kriptografi, yüksek güvenlik gerektiren iletişim ve finansal işlemler.
Güvenlik	Kriptografik uygulamalar için uygun değildir.	Kriptografik uygulamalar için idealdir, çünkü ürettiği sayılar öngörülemezdir.
Maliyet	Düşük maliyetlidir, yazılım tabanlı olarak kolayca uygulanabilir.	Donanım tabanlı olması nedeniyle maliyeti daha yüksektir.
Avantajları	Yeniden üretilebilir ve test edilebilir; yüksek hızda çalışır.	Yüksek güvenlik sunar; tamamen rastgele ve öngörülemez sayılar üretir.
Dezavantajları	Öngörülebilirlik nedeniyle güvenlik açısından zayıftır.	Üretim hızı ve maliyeti nedeniyle bazı uygulamalar için pratik olmayabilir.

Kriptoloji uygulamalarında kullanılacak olan rastgele sayı üreteci (RSÜ) tasarımlarında, kaotik sistemler, başlangıç koşullarına ve kontrol parametrelerine olan duyarlılıkları nedeniyle yaygın şekilde kullanılmaktadır. Bu sistemler, yüksek düzeyde rastgele bit dizileri üreterek daha güçlü bir şifreleme sağlayabilirler. Kaotik sistemlerin ürettiği değerleri

rastgele bit dizilerine dönüştürebilmek için sistemin detaylı bir şekilde analiz edilmesi ve algoritmik işlemlerden geçirilmesi gerekmektedir. Rastgele sayı üretecinin (RSÜ) oluşturduğu rastgele bit dizilerinin kriptolojik uygulamalarda kullanılabilmesi için bu dizilerin çeşitli rastgelelik testlerinden geçirilmesi ve tüm testleri başarıyla geçmesi gerekmektedir. Bu kapsamda uygulanacak testlerle ilgili detaylı bilgiler, bir sonraki bölümde ayrıntılı olarak ele alınacaktır.

2.5.3. İstatiksel Testler

Rastgele sayı üreteçleri, kriptografik sistemlerde ve güvenlik protokollerinde son derece kritik bir role sahiptir. Bu üreteçler tarafından sağlanan rastgele sayılar; şifreleme, anahtar oluşturma, kimlik doğrulama gibi pek çok alanda kullanılmaktadır. Ancak; bilgisayar korsanları tarafından güvenlik önlemlerini aşmak, şifrelenmiş verileri çözmek veya sistemlere zarar vermek amacıyla rastgele sayı üreteçlerine saldırılar gerçekleştirilebilir. Bu nedenle, güvenliğin sağlanması ve saldırılardan korunma konusunda rastgelelik özelliklerinin istatistiksel olarak doğrulanması büyük önem taşmaktadır.

2.5.3.1.FIPS 140-1

Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından yayınlanan Federal Bilgi İşleme Standartları (FIPS) kapsamında, FIPS 140-1, kriptografik modüllerin güvenlik gereksinimlerini kapsamakla beraber rasgele sayı üreteçleri için istatistiksel testleri önermektedir. FIPS 140-1 testi, monobit, poker, run ve long term test olmak üzere dört farklı testten oluşmaktadır. Bu testlerin ayrıntısı aşağıda verilmiştir (NIST, 1994).

- Monobit Testi: 20.000 bitlik bir örnek dizisi üzerinde gerçekleştirilir ve bu dizideki “1” bitlerinin sayısının belirli bir aralıkta olup olmadığını inceler. Spesifik olarak “1” bitlerinin sayısı 9.654 ile 10.346 arasında olmalıdır. Bu aralık, ideal bir rastgele dağılımda beklenen “0” ve “1” bitlerinin yaklaşık olarak eşit sayıda olması gerektiği prensibine dayanmaktadır.
- Poker Testi: Bu alt test, 20.000 bitlik bir örnek dizisini 5.000 adet 4 bitlik segmente ayırarak başlar. Ardından her bir 4 bitlik değerin (0’dan 15’e kadar) kaç kez oluştuğunu sayar ve bu sayılar $f(i)$ olarak ifade edilir. Daha sonra Denklem 2.29’da verilen matematiksel formül uygulanır.

$$X = \frac{2^{16}}{5000}\left(\sum_{i=0}^{15} f(i)^2\right) - 5000$$

Denklem 2.29. Poker testi istatistiksel hesaplama formülü

Elde edilen sonucun 1.03 ile 57.4 arasında olması beklenir. Bu aralık, ideal bir rastgele dağılımda 4 bitlik grupların uniform bir şekilde dağılması gerektiği prensibine dayanmaktadır.

- Koşu Testi (Run Test): 20.000 bitlik bir örnek dizide ardışık olarak tekrar eden "0" ve "1" dizilerinin (run'ların) dağılımını incelemektedir. Bir "run", kesintisiz olarak devam eden aynı değerli (ya tümü "0" ya da tümü "1") bit dizisi olarak tanımlanır. Test prosedürü, farklı uzunluktaki run'ların (1'den 6'ya kadar, 6'dan uzun olanlar 6 olarak kabul edilir) sayısını belirler. Sayı dizilerinin koşu testinden başarılı sayılabilmesi için gerekli olan aralık Tablo 2.6'da verilmiştir.
- Uzun Koşu Testi (Long Runs Test): 20.000 bitlik bir örnek dizide 34 veya daha fazla ardışık bitten oluşan, tamamı "0" veya tamamı "1" olan bit dizilerinin (uzun koşuların) varlığını inceler. Testin temel prensibi, örnek akışta hiçbir uzun koşunun bulunmaması gerektiğidir.

FIPS 140-1 testinde, 20 Kbit'lik bit dizisi bu dört farklı testte tabi tutulmaktadır. RNG çıkışından elde edilen bit dizisinin rastgele sayılması için tanımlı dört testten geçmesi gerekmektedir (F. Sun et al., 2009).

Verilen FIPS 140-1 alt testlerinin ayrıntılarına göre, bir rastgele dizinin testleri başarıyla geçebilmesi için elde edilen test sonuçlarının belirli aralıklar içinde yer alması gerekmektedir. Bu aralıklar, Tablo 2.6'da ayrıntılı olarak sunulmuştur.

Tablo 2.6. FIPS140-1 testinin kabul edilebilir aralıkları

FIPS 140-1 Test Adı		Kabul Edilebilir Aralık
Monobit Testi		9654 -10346
Poker Testi		1.03 - 57.4
Run Testi		
	Run Test (1)	2267 - 2733
	Run Test (2)	1079 - 1421

Tablo 2.6. (devam) FIPS140-1 testinin kabul edilebilir aralıkları

	Run Test (3)	502 - 748
	Run Test (4)	223 - 402
	Run Test (5)	90 - 223
	Koşu Testi (6)	90 - 223
Long Run Test		34 Run

2.5.3.2.NIST 800-22

NIST 800-22, Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından geliştirilen ve rastgele sayı üreteçlerinin istatistiksel testlerini içeren bir standart test bataryasıdır. Bu test bataryası, rastgele sayı üreteçlerinin güvenilirliğini değerlendirmek ve doğrulamak amacıyla kullanılan en yaygın standartlardan biridir. NIST 800-22, toplamda 16 adet istatistiksel test içermektedir ve en az 1Mbit veri serisine ihtiyaç duymaktadır. Bu testlerin ayrıntısı aşağıda verilmiştir (Bassham et al., 2010).

- Frequency (Monobit) Test (Frekans (monobit) testi): Bir bit dizisindeki 0 ve 1 sayılarının oranını inceleyerek dizinin rastgeleliğini değerlendiren temel bir istatistiksel testtir. Bu test, rastgele bir dizide 0 ve 1 bitlerinin yaklaşık olarak eşit sayıda olması gerektiği prensibine dayanmaktadır. Bu test, diğer tüm testlerin geçerliliği için temel bir adım olarak kabul edilir ve test edilecek dizinin minimum 100 bit uzunluğunda olması önerilmektedir.
- Frequency Test within a Block (Bir blok içindeki frekans testi): Bu test, uzun bir bit dizisini eşit uzunlukta bloklara böler ve her blok içindeki 1'lerin oranını incelemektedir. Testin amacı, her blokta 1'lerin oranının, ideal bir rastgele dizide beklenen ½ oranına ne kadar yakın olduğunu belirlemektir. Test süreci, bit dizisini M-bit uzunluğunda N adet bloğa ayırır ve her blok için 1'lerin oranını hesaplanır. Daha sonra, bu oranların dağılımının ki-kare dağılımına uygunluğu değerlendirilir. Eğer hesaplanan ki-kare istatistiği, belirli bir anlamlılık düzeyinde kabul edilebilir aralıkta ise dizi o blok boyutu için rastgele kabul edilmektedir. Testin uygulanabilmesi için dizinin en az 100 bit uzunluğunda olması ve blok boyutunun en az 20 olması önerilmektedir.
- Run Test (Akış testi): Bu testte, “akış” terimi, ardışık ve aynı bitlerin oluşturduğu alt dizileri ifade etmektedir. Testin amacı, dizideki sıfır ve birlerin çeşitli uzunluktaki

akışlarının sayısının, rastgele bir dizide beklenenle uyumlu olup olmadığını belirlemektir. Özellikle, sıfırlar ve birler arasındaki salınımın çok hızlı veya çok yavaş olup olmadığını tespit etmektedir. Test sürecinde ise öncelikle, dizideki "1" oranı hesaplanır ve bu oran Frekans (Monobit) Testi ile doğrulanır. Eğer ön test geçilirse, dizideki toplam akış sayısı hesaplanır. Bu sayı, sıfır ve bir akışlarının toplamıdır. Hesaplanan akış sayısı, beklenen akış sayısıyla karşılaştırılır ve $\chi 2$ istatistiği ile değerlendirilir. Elde edilen $P - değeri$ anlamlılık düzeyinden büyükse dizi rastgele kabul edilmektedir.

- Longest Run of Ones in a Block (Bir blok içerisinde en uzun birler akış testi): Bir blok içerisinde en uzun birler akış testi: Bu test, diziyi belirli uzunluklarda bloklara böler ve her blok içindeki en uzun "1" akışlarının sıklığını analiz eder. Elde edilen akış uzunlukları kategorilere ayrılarak tablolandırılır ve gözlemlenen değerler beklenen değerlerle karşılaştırılır. Bu karşılaştırma χ^2 istatistiği ile yapılır ve sonuçlar, $P - değeri$ hesaplanarak değerlendirilir.
- Binary Matrix Rank Test (İkili matris rankı testi): Bu test, bit dizisini ardışık sıfır ve birlerden oluşan matrislere dönüştürür ve oluşturulan matrislerin satır veya sütunları arasındaki doğrusal bağımlılığı inceler. Matrislerin derecesinin teorik olarak beklenen değerden sapması, test istatistiğini oluşturur. Test sürecinde ise, Dizi ardışık $M \times Q$ bitlik bloklara bölünür. Her blok, Q bitlik alt bloklara ayrılır ve bu alt bloklar $M \times Q$ boyutunda matrisler oluşturur. Her matrisin rankı hesaplanır ve bu rankların frekansları hesaplanır, beklenen değerlerle karşılaştırılır ve χ^2 istatistiği kullanılarak değerlendirilir.
- Discrete Fourier Transform (Spectral) Test (Ayrık fourier dönüşüm testi): Bir bit dizisindeki periyodik özellikleri tespit ederek rastgelelik değerlendirmesi yapmayı amaçlar. Bu test, bit dizisinin Fourier dönüşümünü kullanarak, dizideki periyodik bileşenlerin varlığını incelemektedir.
- Non-Overlapping Template Matching Test (Örtüşmeyen şablon eşleştirme testi): Bir bit dizisinde belirli bir aperiodik örüntünün (şablonun) beklenen sayıda görülüp görülmediğini inceleyerek rastgelelik değerlendirmesi yapmayı amaçlamaktadır. Bu test, önceden belirlenmiş bir m-bit şablonun bit dizisi içinde kaç kez göründüğünü saymaktadır.
- Overlapping Template Matching Test (Örtüşen şablon eşleştirme testi): Bir bit dizisinde belirli bir hedef desenin örtüşen tekrarlarının sayısını tespit ederek dizinin rastgele olup

olmadığını değerlendiren bir testtir. Bu testte, bit dizisi belirli uzunluklarda bloklara ayrılır ve her blok içinde belirli bir $m - bit$ hedef desen aranmaktadır.

- Maurer's Universal Statistical test (Maurer'in "Evrensel İstatistik" testi): Eşleşen örüntüler arasındaki bit sayısını inceleyerek, dizinin bilgi kaybı olmadan önemli ölçüde sıkıştırılıp sıkıştırılamayacağını tespit etmeye çalışır. Önemli ölçüde sıkıştırılabilen bir dizi, rastgele olmayan olarak kabul edilmektedir.
- Linear Complexity Test (Doğrusal karmaşıklık testi): Bir bit dizisinin doğrusal geri besleme kaydırma registeri (LFSR) kullanılarak üretilen en kısa yinelemeli diziyi belirlemek suretiyle dizinin doğrusal karmaşıklığını ölçer ve rastgele olup olmadığını değerlendirmektedir. Bu test, bit dizisini belirli uzunlukta bloklara ayırarak her blok için Berlekamp-Massey algoritması yardımıyla doğrusal karmaşıklık değerini hesaplar. Rastgele bir dizinin yüksek doğrusal karmaşıklığa sahip olması beklenir çünkü düşük doğrusal karmaşıklık, dizinin öngörülebilir olduğunu göstermektedir. Her blok için elde edilen doğrusal karmaşıklık değerleri, teorik olarak beklenen değerlerle karşılaştırılır ve gözlemlenen değerlerle beklenen değerler arasındaki farklar kullanılarak χ^2 istatistiği ile değerlendirilmektedir.
- Serial test (Seri testi): Bu test, verilen bit dizisindeki her m bitlik örneğin, dizideki diğer m bitlik örneklerle benzer değişim ve tekdüzelik seviyesini incelemektedir. Seri testi sonucunda, $P - değeri\ 1$ ve $P - değeri\ 2$ olmak üzere iki ayrı test sonucu elde edilmektedir.
- Approximate Entropy Test (Yaklaşık entropi testi): Bu test, bir dizideki m uzunluğundaki blokların frekanslarını inceler ve bu blokların $m + 1$ uzunluğundaki bloklarla olan ilişkisini değerlendirmektedir. Testin amacı, dizideki bitlerin ne kadar düzenli veya düzensiz olduğunu belirlemektir. Yaklaşık entropi, m uzunluğundaki blokların birbirine ne kadar benzediğini ve bir pozisyon artırılarak oluşturulan $m + 1$ uzunluğundaki bloklarda bu benzerliğin ne kadar devam ettiğini ölçer. Düşük entropi değerleri; dizinin yüksek düzeyde düzenli olduğunu, yüksek entropi değerleri ise dizinin düzensiz olduğunu göstermektedir.
- Cummulative Sums test (Kümülatif toplamlar testi): Bu test, incelenen bit dizisinin kümülatif toplamlarının maksimum sapmasını analiz ederek dizinin rastgelelik özelliklerini değerlendirir. Testin temel prensibi, bit dizisini -1 ve $+1$ değerlerine dönüştürerek bir rastgele yürüyüş (random walk) oluşturmak ve bu yürüyüşün sıfırdan

maksimum sapmasını hesaplamaktır. Rastgele bir dizi için bu sapmaların küçük olması beklenmektedir. Test istatistiği, normal dağılıma göre değerlendirilir ve elde edilen P-değeri, dizinin rastgeleliği hakkında nicel bir ölçü sağlar. Bu test, dizideki sapmaların beklenen sınırlar içinde olup olmadığını belirleyerek dizinin rastgele olup olmadığını tespit edilmektedir.

- Random Excursions Test (Rasgele gezinimler testi): Bu test, kümülatif toplam rastgele yürüyüşünde belirli bir durumun tam olarak K kez ziyaret edildiği döngü sayısına odaklanır. Bu test, aslında sekiz testin bir serisidir ve her biri $-4, -3, -2, -1$ ve $+1, +2, +3, +4$ durumları için ayrı bir test ve sonuç içermektedir. Testin amacı, bir döngü içinde belirli bir duruma yapılan ziyaret sayısının, rastgele bir dizi için beklenenden sapma gösterip göstermediğini belirlemektir. Test sürecinde, giriş dizisi önce normalize edilmiş $(-1, +1)$ bir diziye dönüştürülür ve ardından kısmi toplamlar hesaplanır. Bu kısmi toplamlar kullanılarak sıfır değerlerine göre döngüler tanımlanır ve her durum için ziyaret sayıları belirlenir. İstatistiksel analiz, gözlemlenen ziyaret sayılarını teorik beklentilerle karşılaştırır. Her durum için bir χ^2 istatistiği hesaplanır ve buna karşılık gelen $P - değeri$ elde edilir. Eğer hesaplanan $P - değeri$ belirli bir eşik değerinin altında ise dizinin rastgele olmadığı sonucuna varılmaktadır. Aksi takdirde, dizinin rastgele olduğu kabul edilir. Test, minimum 1.000.000 bitlik bir dizi uzunluğu için önerilmektedir.
- Random Excursions Variant Test (Rasgele gezinimler değişken testi): Bu son test ise, kümülatif toplam rastgele yürüyüşü sırasında belirli bir durumun kaç kez ziyaret edildiğini analiz eden bir testtir. Bu test, -9'dan +9'a kadar olan on sekiz farklı durumu inceler ve her biri için ayrı değerlendirmeler yapmaktadır. Test sürecinde, giriş dizisi normalize edilmiş $(-1$ ve $+1)$ bir diziye dönüştürülür ve ardından kısmi toplamlar hesaplanır. Bu kısmi toplamlar kullanılarak sıfırdan başlayan ve sıfırda biten döngüler tanımlanır. Her döngüdeki belirli bir duruma yapılan ziyaretlerin sayısı hesaplanır ve her bir durum için gözlemlenen ziyaret sayıları teorik beklentilerle karşılaştırılır. İstatistiksel analiz, her durum için bir χ^2 istatistiği hesaplar ve buna karşılık gelen P-değeri elde edilmektedir. Elde edilen P-değerleri, belirli bir eşik değerinin altında ise, dizinin rastgele olmadığı sonucuna varılmaktadır. Aksi takdirde, dizinin rastgele olduğu kabul edilmektedir. Bu test, minimum 1.000.000 bitlik bir dizi uzunluğu için önerilmektedir.

Rastgele sayı dizisinin istatistiksel olarak güvenilir kabul edilmesi için NIST 800-22'nin içerdiği 16 testin tamamını geçmesi gerekmektedir. Bu testlerde $P - değeri$, anlamlılık düzeyi olan $\alpha = 0{,}001$'den büyük veya eşit olmalıdır.

2.5.3.3. ENT

ENT testi bit dizilerinin rastgelelik özelliklerini değerlendirmek amacıyla istatiksel analizler uygulamaktadır. John Walker tarafından geliştirilen bu test bilgisayar bilimi ve kriptoloji alanında önemli rol oynamaktadır. ENT testi, bit dizilerinin rastgeleliğini tanımlamak amacıyla Aritmetik Ortalama, Entropi, Korelasyon, Ki-Kare ve Monte Carlo değerleri olmak üzere 5 farklı testi içermektedir (Walker, 2008). Bu testlerin ayrıntısı aşağıda verilmiştir (Hernandez-Castro et al., 2017).

- Aritmetik Ortalama: Adından da anlaşılacağı gibi, bu sadece dizideki sayıların aritmetik ortalamasıdır. Gerçek bir rastgele dizi için beklenen istatistik değeri ikili modda 0.5 ve bayt modunda 127.5'tir.
- Entropi: Bu test, klasik Bilgi Teorisi'nde tanımlandığı gibi, incelenen dizinin entropisini hesaplar. Rastgele bir dizinin yüksek entropiye sahip olması beklenir. Bayt modunda, uzun bir dizinin teorik olarak ulaşabileceği maksimum entropi bayt başına 8 bittir, ikili modda ise bit başına 1 bittir.
- Korelasyon: Bu test, dizideki ardışık iki sembol (bit veya bayt) arasındaki korelasyon derecesini ölçer. İdeal bir rastgele dizide korelasyon düşük olmalı ve sıfıra çok yakın değerler göstermelidir. Buna karşılık, kötü bir rastgele dizide korelasyon daha yüksek mutlak değerlere sahip olur.
- Ki-kare: Ki-kare testi, sayıların frekansını belirler ve bunu uniform bir dağılımda beklenen frekanslarla karşılaştırır. Bu karşılaştırmayı gerçekleştirmek için ki-kare istatistiği kullanılır.
- Monte Carlo: Bu test, diziyi bir karedeki koordinatlar olarak değerlendirir ve karenin içine yerleştirilen bir çemberin içine düşen noktaların sayısını sayar. Bu sayı, pi değerini tahmin etmek için kullanılır. Gerçekten rastgele bir dizi, pi'yi yüksek doğrulukla tahmin ederken rastgele olmayan bir dizinin pi'yi doğru şekilde tahmin etmesi beklenmez. Test, pi'nin tahmin edilmesindeki yüzde hatayı ölçen pierror istatistiğini kullanmaktadır.

Yukarıda ayrıntıları verilen alt testlerin, başarılı sayılabilmesi için gerekli kabul edilebilir aralıklar özet olarak Tablo 2.7'de sunulmuştur.

Tablo 2.7. ENT testinin kabul edilebilir aralıkları

ENT Test Adı	Kabul Edilebilir Aralık
Aritmetik Ortalama	127.5
Entropi Testi	8
Korelasyon	0
Chi-Kare Testi	%10 ve %90 Aralığında
Monte Carlo	Pi Sayısı

2.6. Analizler

2.6.1. Kriptoloji Analizi

Görüntü şifreleme işleminin güvenirliliği şifreleme algoritmasının performansına bağlıdır. Görüntü şifreleme algoritması kaba kuvvet (brute force), yan kanal saldırıları ve kriptanaliz ataklarına karşı dirençli olmalıdır. Görüntü şifreleme sürecinin performansını ölçmek için literatürde çeşitli istatistiksel testler kullanılmaktadır (Akgul et al., 2016; Zhu et al., 2023). Bu testler, şifrelenmiş görüntünün istatistiksel özelliklerini değerlendirerek şifreleme algoritmasının güvenlik seviyesinin belirlenmesine yardımcı olmaktadır. Literatürde görüntü şifreleme uygulamalarında yaygın olarak kullanılan analizlerin her biri, diğer bölümde ayrıntılı bir şekilde ele alınacaktır.

2.6.1.1. Histogram Analizi

Histogram grafiği, görüntünün piksellerinin yoğunluk dağılımını göstermektedir. İlk olarak Karl Pearson tarafından önerilmiştir. Orijinal görüntülerinin histogram grafiği dengeli bir dağılım sergilemesi beklenmektedir. Şifreli görüntülerin histogram dağılımı ise istatiksel saldırıları önlemek amacıyla tek düze bir dağılım sergilemesi gerekmektedir (Thiyagarajan et al., 2019). Etkili bir şifreleme algoritması, şifrelenmiş görüntünün histogramını orijinal görüntünün histogramından belirgin şekilde farklılaştırmalıdır. Şifrelenmiş görüntünün histogramı incelenerek, şifreleme algoritmasının etkinliği temel olarak değerlendirilmektedir. Düzgün dağılıma sahip bir histogram, şifreleme işleminin başarılı olduğunu ve şifrelenmiş görüntünün saldırılara karşı dirençli olduğunu göstermektedir (Ye, 2010). Histogram analizinin bazı avantajları ve sınırlamaları bulunmaktadır. Basit ve hızlı bir yöntem olması, histogram analizinin önemli bir avantajıdır. Ayrıca, şifreleme algoritmasının temel güvenlik özelliklerini görsel olarak değerlendirme imkanı sunmaktadır

(H. Liu et al., 2010). Ancak, histogram analizi sadece yüzeysel bir değerlendirme sağlar ve şifreleme algoritmasının tüm güvenlik özelliklerini kapsamlı bir şekilde değerlendiremez. Daha sofistike saldırılara karşı güvenliği tam olarak değerlendiremediği için diğer güvenlik analizleri ile birlikte kullanılması gereklidir (Y. Zhang et al., 2013). Bu nedenle histogram analizi, şifrelenmiş görüntülerin güvenliğini değerlendirmek için önemli bir ilk adım olmasına rağmen kapsamlı bir güvenlik değerlendirmesi için ek analiz yöntemleriyle desteklenmelidir.

Ayrıca şifreleme işleminin neden olduğu tekdüze ve homojenliği doğrulamak amacıyla $variance(var)$ ve χ^2 testleri gerçekleştirilmektedir. Varyans, bir gri tonlamalı görüntünün histogramındaki piksel frekanslarının dağılımını analiz ederek istatistiksel saldırılara karşı direnç gösteren bir niceliksel ölçüdür. χ^2 ise gri tonlamalı görüntülerin histogramındaki piksel dağılımının homojenliğini nicel olarak ölçmektedir. $variance(var)$ ve χ^2 testlerine ait formüller sırasıyla Denklem 2.30 ve Denklem 2.31'de verilmiştir.

$$var(x) = \frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{n_i - n_j}{2}$$

Denklem 2.30. Varyans test formülü

Denklem 2.30'da n gri tonlamalı pikselin yoğunluk değerini gösterirken n_i ve n_j parametreleri, sırasıyla i ve j yoğunluk değerlerine sahip piksellerin sayısını ifade etmektedir. Düşük varyans değerleri, histogramın piksel dağılımının daha homojen olduğunu ifade etmektedir.

$$\chi^2 = \sum_{i=0}^{255}\frac{(v_i - e_i)^2}{e_i}$$

Denklem 2.31. Ki-Kare testi formülü (χ^2)

Denklem 2.31'de i gri seviye sayısını, v_i gözlenen frekansı ve e_i ise beklenen frekansı temsil etmektedir. 255 serbestlik derecesi ve %5 kritik seviye düzeyinde χ testinin ideal değeri $\chi^2\,(255{,}0{,}05) = 293.2478$ dir (Parida et al., 2021). $\chi^2_{test} < \chi^2(255{,}0{,}05)$ olması histogramdaki piksel dağılımının dengeli ve homojen olduğunu göstermektedir.

2.6.1.2. Korelasyon Analizi

Korelasyon analizi, görüntünün pikselleri arasındaki ilişkiyi değerlendirmek için kullanılır. Orijinal görüntüde, pikseller arasında yüksek bir korelasyon gözlenmektedir. Ancak güvenli bir şifreleme işlemi sonrasında elde edilen şifrelenmiş görüntü de ise bitişik pikseller arasındaki korelasyon değeri teorik olarak sıfıra yakın bir düzeye indirilmesi beklenmektedir (Gupta et al., 2023). Korelasyon katsayısı Denklem 2.32'de verilen ifade ile hesaplanır (Ahmad et al., 2017).

$$cor = \frac{\frac{1}{N} \times \sum_{l=0}^{N} \left(i_l - E(l)\right)\left(j_l - E(l)\right)}{\sqrt{\frac{1}{N} \times \sum_{l=0}^{N} \left(i_l - E(l)\right)^2} \times \sqrt{\frac{1}{N} \times \sum_{l=0}^{N} \left(j_l - E(l)\right)^2}}$$

Denklem 2.32. Korelasyon katsayısı formülü

Burada N piksel sayısını E ise beklenen değer operatörünü ifade etmektedir. Korelasyon katsayısı değerinin ideal olarak sıfıra yakın olması, bir şifreleme sistemini istatistiksel saldırılara karşı daha güçlü olduğunu göstermektedir.

2.6.1.3. Diferansiyel Atak Analizi

Diferansiyel saldırılar, şifreli verilerdeki küçük değişikliklerin düz verilerdeki farklılıkları izleyerek gizli anahtarı keşfetmeye çalıştığı bir kripto analiz yöntemidir. Algoritmaların bu tip saldırılara karşı dayanıklılığını ölçmek amacıyla The Number of Changing Pixel Rate (NPCR) ve Unified Average Changed Intensity (UACI) değerleri hesaplanır. NPCR orijinal görüntüsünde bir piksel değiştiğinde, şifreli görüntüdeki piksellerin değişim oranını göstermektedir. UACI ise, orijinal görüntüsü ile şifreli görüntü arasındaki farkların ortalama yoğunluğunu ölçer. NPCR ve UACI Denklem 2.33-2.35'te verilen formüller ile hesaplanmaktadır.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{T} \times 100\%$$

Denklem 2.33. NPCR formülü

$$D(i,j) = \begin{cases} 0 & if\ C(i,j) = C'(i,j) \\ 1 & if\ C(i,j) \neq C'(i,j) \end{cases}$$

Denklem 2.34. Değişim gösterge fonksiyonu

$$UACI = \frac{\sum_{i,j}|C(i,j) - C'(i,j)|}{I_{max} \times T} \times 100\%$$

Denklem 2.35. UACI formülü

Burada T toplam piksel sayısını, C ve C' ise iki şifreli görüntüyü ve I_{max} ise toplam piksel yoğunluğunu ifade eder. Literatürde ideal $NPCR$ ve $UACI$ değerleri, sırasıyla >99% ve ≈33% değeri başarı kriteri olarak kabul edilmektedir (M. Khan et al., 2019).

2.6.1.4. Bilgi Entropi Analizi

Bilgi entropi analizi, bir veri kümesindeki düzensizlik veya rastgelelik derecesini ölçen istatistiksel bir yöntem olarak kullanılmaktadır. Entropi, bir veri kümesinin tahmin edilebilirliği veya bilgi içeriği hakkında bilgi sağlamaktadır. Yüksek entropi değeri, veri kümesinin daha rastgele ve tahmin edilemez olduğunu gösterirken düşük entropi değeri, veri kümesinin daha düzenli ve tahmin edilebilir olduğunu göstermektedir. Ayrıca entropi analizi; genellikle veri sıkıştırma, rastgele sayı üreteçleri, şifreleme algoritmaları ve veri gizliliği gibi alanlarda kullanılmaktadır. Aynı şekilde rastgele sayı üreteçleri için entropi analizi, üretilen sayıların rastgelelik seviyesini ve istatistiksel dağılımlarını değerlendirmek için kullanılmaktadır. Matematiksel olarak entropi Denklem 2.36'da verilen formül ile hesaplanmaktadır (J. Khan et al., 2015).

$$H(m) = -\sum_{i=0}^{2^N-1} p(m_i) \times \log_2\big(p(m_i)\big)$$

Denklem 2.36. Bilgi entropisi formülü

Burada N her bir sembol için kullanılan bit sayısını temsil eder ve $p(m)$ sembol m_i'nin olasılığını ifade eder. Şifrelenmiş görüntülerde ideal entropi değeri $H(m) = 8$'dir (G. Zhou et al., 2015).

2.6.1.5. MSE-PSNR

Görüntü şifreleme işleminin performansının değerlendirilebilmesi için şifrelenmiş görüntü ve orijinal görüntü arasındaki benzerlik ölçümlerinin yapılması gerekmektedir. Görüntülerin benzerlik ölçütlerini hesaplamak için kullanılan ölçüm metrikleri bulunmaktadır. Söz konusu metriklerden yaygın olarak kullanılanlardan biri ortalama kare hatası (MSE)'dır. MSE Denklem 2.37'de verilen formülle hesaplanmaktadır.

$$MSE = \frac{1}{M \times N} \sum_{x=1}^{M} \sum_{y=1}^{N} \left[C_{1_{i,j}} - C_{2_{i,j}} \right]^2$$

Denklem 2.37. Ortalama kare hatası (MSE) formülü

Burada C_1 ve C_2 boyutları $M \times N$ olan iki görüntü olup, hataların ortalama toplamı her (i, j) pikseli için ölçülür. MSE değerinin yüksek olması, farklılığın daha yüksek olduğunu gösterir. Tam olarak benzer görüntülerde ise MSE için ideal değer sıfırdır (Kaur et al., 2020).

Öte yandan, tepe sinyal gürültü oranı (PSNR) da yaygın olarak kullanılan başka bir karşılaştırma metriğidir. PSNR Denklem 2.38'de verilen formülle hesaplanmaktadır.

$$PSNR = 10 \log_{10}(\frac{MAX^2}{MSE})$$

Denklem 2.38. Tepe sinyal gürültü oranı (PSNR) formülü

Burada MAX görüntünün maksimum piksel değerini ifade etmektedir. 8 bit renk değeri için $MAX = 2^8 - 1 = 255$'dir. İdeal durumda, benzer görüntüler için PSNR değeri sonsuz olurken tamamen farklı görüntüler için bu değer sıfırdır (Kaur et al., 2020).

2.6.1.6. Anahtar Uzayı Analizi

Güvenli bir şifreleme yöntemi, kaba kuvvet saldırılarına karşı koyabilmek için yeterince geniş bir anahtar alanına sahip olmalıdır. İyi bir kripto sistemin kaba kuvvet saldırısını etkisiz hale getirmesi için anahtar uzayının en az 2^{100} olması önerilmektedir (Hu ve ark., 2017). Kesir dereceli kaotik sistemler, kesir dereceleri, başlangıç koşulları ve sistem parametrelerine hassasiyetlerinden dolayı genellikle kaotik şifreleme sistemlerinde anahtar olarak kullanılmaktadır. Kaotik şifrelemede anahtar uzunluğunun analizinde, kesir derece, kaotik sistem boyutu ve sistem parametrelerinin sayısı anahtar alanının genişliğini belirlemektedir (Meng ve Gu, 2023).

2.6.1.7. Saldırı Analizleri

Şifrelenmiş görüntülerin güvenliğini ve dayanıklılığını değerlendirmek amacıyla gürültü ekleme ve kesme gibi saldırı analizleri de yapılmalıdır. Gürültü analizinde, şifrelenmiş bir görüntüye rastgele gürültü ekleyerek şifreleme algoritmasının bu tür saldırılara karşı ne kadar dirençli olduğunu test edilmektedir. Gürültü saldırısı, genellikle Gauss, tuz biber veya Poisson gibi farklı türlerde uygulanmaktadır. Şifreleme algoritmasının etkinliği, gürültü

eklenmiş şifreli görüntünün çözüldükten sonra orijinal görüntüye ne kadar yakın olduğuna göre değerlendirilmektedir. Tez çalışmasında farklı oranlarda tuz-biber saldırıları gerçekleştirilecektir. Kesme atak analizinde ise, şifrelenmiş görüntülerin belirli bölgelerinin kesilmesini ve ardından bu bozulmuş görüntünün çözümlenmesi sürecini içermektedir. Kesilmiş bölgeler nedeniyle veri kaybı meydana gelir ve şifreleme algoritmasının bu veri kaybına karşı ne kadar dayanıklı olduğu ölçülür. Bu analiz, kesilmiş şifreli görüntünün çözülmesi sonucu elde edilen görüntünün orijinal görüntüye olan benzerliği ile değerlendirilmektedir.

2.6.2. Steganografi Analizi

2.6.2.1. İstatiksel Analizler

İyi bir steganografi yöntemi, gizli bilgiyi başarılı bir şekilde saklarken aynı zamanda bu bilginin tespit edilmesini zorlaştıran özelliklere sahip olmalıdır. Bu bağlamda, tez çalışmasında önerilen yöntemin güvenilirliğini değerlendirmek amacıyla kullanılan ve tanımları verilen istatistiksel metrik değerleri şunlardır:

- Korelasyon analizi, iki görüntü arasındaki benzerliği belirlemek için kullanılan bir kriterdir. Korelasyon, Denklem 2.39'da verilen formülle hesaplanır:

$$corr = \sum_{ij}^{MN} (i - v_i)\big(j - v_j\big)p_{ij}/\sigma_i \times \sigma_j$$

Denklem 2.39. Korelasyon katsayısı formülü

Burada, $i\ ve\ j$ görüntünün satır ve sütunlarını, p_{ij} ise (i,j) pozisyonundaki piksel değerini, v görüntü varyansını ve σ ise standart sapmayı ifade etmektedir.

Korelasyonun yüksek olması, görüntülerin birbirine çok benzediğini gösterirken düşük olması ise görüntülerin birbirinden farklı olduğunu göstermektedir.

- Bilgi Entropisi, bir sistemin rastgelelik miktarını ölçmek için kullanılan bir metriktir. Denklem 2.40'ta verilen formülle hesaplanmaktadır.

$$I(R) = \sum_{i=0}^{F-1} P(R = i) \times \log_2 P(R = i)$$

Denklem 2.40. Bilgi entropisi formülü

Burada P ayrık bir olasılık yoğunluk fonksiyonunu, F ise olası sonuçların sayısını ifade etmektedir.

- Homojenlik, Gri Düzey Birlikte Oluşum Matrisi, (GDBOM) üzerinde eleman dağılımlarının diyagonal üzerindeki yakınlığını ölçen bir metriktir. Denklem 2.41'de verilen formülle hesaplanmaktadır.

$$Hom = \sum_{ij}^{MN} \frac{p_{ij}}{1 - |i - j|}$$

Denklem 2.41. Homojenlik formülü

- Kontrast, görüntüdeki tüm pikseller için bir piksel ile komşuları arasındaki yoğunluk farkını ölçen bir metriktir. Denklem 2.42'de verilen formülle hesaplanmaktadır.

$$Kont = \sum_{i,j}^{MN} |i - j|^2 p_{ij}$$

Denklem 2.42. Kontrast formülü

- Enerji, GDBOM elemanların karelerinin toplamını hesaplayan bir metriktir. Denklem 2.43'te verilen formülle hesaplanmaktadır.

$$E = \sum_{ij}^{MN} p_{ij}^2$$

Denklem 2.43. Enerji formülü

2.6.2.2. Sapma Ölçüm Metrikleri

Sapma ölçüm metrikleri, bir görüntünün özelliklerinin değişim derecesini nicel olarak değerlendirmek amacıyla kullanılmaktadır. Literatürde bazı yaygın sapma ölçüm metrikleri şunlardır;

- Ortalama karesel hata (MSE, Mean Squared Error), iki görüntü arasındaki farkların karesinin ortalamasını hesaplayan bir metriktir. Denklem 2.44'te verilen formülle hesaplanmaktadır.

$$MSE = \sum_{i,j}^{MN} \left(cp_{ij} - sp_{ij}\right)^2 / (M \times N)$$

Denklem 2.44. Ortalama kare hatası (MSE) formülü

Burada, cp_{ij} kapak görüntüsünün, sp_{ij} ise stego görüntüsünün i, j konumlarınındaki piksel değerlerini temsil etmektedir.

- Tepe sinyal gürültü oranı (PSNR, Peak Signal to Noise Ratio), kapak ve gizli görüntüler arasındaki benzerlik derecesini analiz eden bir görüntü kalite ölçütüdür. Yüksek bir PSNR değeri iyi bir görüntü kalitesini göstermektedir (Awadh et al., 2022). PSNR değerinin 30 dB'den yüksek olduğunda, 30 dB'den yüksek olduğunda orijinal ve stego görüntülerin görsel olarak ayırt edilemez olduğu kabul edilmektedir (Y.-X. Liu et al., 2019). Denklem 2.45'te verilen formülle hesaplanmaktadır.

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} \ (dB)$$

Denklem 2.45. Tepe sinyal gürültü oranı (PSNR) formülü

2.6.2.3. Görüntü Kalitesinin Değerlendirilmesi

Görüntü kalitesinin değerlendirilmesi amacıyla gerçekleştirilen bazı analizler şunlardır;

- UIQI (Universal Image Quality Index- Evrensel Görüntü Kalitesi Endeksi), bir görüntünün kalitesini değerlendiren ve [-1, 1] aralığında değere sahip olan bir metriktir. Değerin -1' e yakın olması karşılaştırılan iki görüntünün tamamen farklı olduğunu, 1 olması ise iki görüntünün tamamen aynı olduğunu ifade eder (Z. Wang et al., 2002). UIQI, Denklem 2.46'da verilen formülle hesaplanmaktadır.

$$\text{UIQI} = 4 \times \sigma_{cs} \times \frac{\overline{cp} \times \overline{cs}}{(\sigma_c^2 + \sigma_s^2)[\overline{cp}^2 + \overline{cs}^2]}$$

Denklem 2.46. Evrensel görüntü kalitesi endeksi formülü

Burada,

$$\overline{cp} = \sum_{ij}^{MN} \frac{cp_{ij}}{M \times N}$$

Denklem 2.47. Orijinal görüntünün tüm piksellerinin ortalama değeri

$$\overline{cs} = \sum_{ij}^{MN} \frac{sp_{ij}}{M \times N}$$

Denklem 2.48. Stego görüntünün tüm piksellerinin ortalama değeri

$$\sigma_c^2 = \sum_{ij}^{MN} \frac{\left(cp_{ij} - \overline{cp}\right)^2}{M \times N - 1}$$

Denklem 2.49. Orijinal görüntünün varyansı

$$\sigma_s^2 = \sum_{ij}^{MN} \frac{\left(sp_{ij} - \overline{sp}\right)^2}{M \times N - 1}$$

Denklem 2.50. Stego görüntünün varyansı

$$\sigma_{cs} = \sum_{ij}^{MN} \frac{\left(cp_{ij} - \overline{cp}\right)\left(sp_{ij} - \overline{sp}\right)}{M \times N - 1}$$

Denklem 2.51. Orijinal ve stego görüntüler arasındaki kovaryans

değerleri yukarıda verilen denklemlere göre hesaplanmaktadır.

- Görüntü Doğruluğu (Image Fidelity-IF) ise bir görüntünün kalitesini değerlendiren ve değeri 1'e ne kadar yakınsa, iki görüntünün o kadar benzer olduğunu gösteren bir indekstir. Denklem 2.52'de verilen formülle hesaplanmaktadır.

$$IF = 1 - \frac{\sum_{ij}^{MN}\left(cp_{ij} - sp_{ij}\right)^2}{\sum_{ij}^{MN}(cp_{ij} \times sp_{ij})}$$

Denklem 2.52. Görüntü doğruluğu formülü

3. GEREÇ VE YÖNTEM

3.1. Incommensurate Kesir Dereceli Arneodo Kaotik Sistemi

Arneodo ve arkadaşları, 1981 yılında üçüncü derece modellerinin genel yapısını tanıtmışlardır (Arneodo et al., 1981). Üç adet adi diferansiyel denklem olarak formüle edilen Arneodo kaotik sisteminin genelleştirilmiş hali Denklem 3.1'de verildiği gibi tanımlanabilmektedir.

$$\dot{x} = y$$

$$\dot{y} = z$$

$$\dot{z} = ax - by + cz - x^3$$

Denklem 3.1. Genelleştirilmiş Arneodo kaotik sistemi

Burada, $x, y\ ve\ z$ durum değişkenini, $a, b\ ve\ c$ ise sistem parametresini temsil etmektedir.

Arneodo sisteminin dinamik karmaşıklığını, kesirli dereceli analizler yoluyla artırılabilir. Bu doğrultuda Sistem 3.1 aşağıdaki gibi kesirli diferansiyel denklemlerle formüle edilebilir.

$$D^{q_1}x = y$$

$$D^{q_2}y = z$$

$$D^{q_3}z = ax - by + cz - x^3$$

Denklem 3.2. Kesirli dereceli Arneodo kaotik sistemi

Burada, D^q kesirli derece operatörünü ifade etmektedir. Pozitif veya negatif q derecesi seçilerek, bu operatör kesirli bir türev alma veya integratör işlevi görebilir. Bu tez çalışmasında $0 \leq q_i \leq 1$ $(i = 1,2,3)$ olacak şekilde her dinamik denklem için farklı kesirli mertebe değerleri seçilmiştir. Böylece sistemin karmaşıklığını ve tahmin edilemezliği daha da artıracak olup güvenli kriptoloji uygulamaları için daha kullanışlı hale getirecektir.

Incommensurate kesir dereceli Arneodo (IKA) sisteminin sayısal çözümü aşağıdaki gibidir:

$$x(i) = y(i-1).h^{q_1} - \sum_{j=1}^{i-1} c_1^{(q1)}(j).x(i-j)$$

$$y(i) = z(i-1).h^{q_2} - \sum_{j=1}^{i-1} c_2^{(q2)}(j).y(i-j)$$

$$z(i) = (a.x(i) - b.y(i) + c.z(i-1) + x(i)^3).h^{q_3} - \sum_{j=1}^{i-1} c_3^{(q3)}(j).z(i-j)$$

Denklem 3.3. IKA sisteminin sayısal çözümü

T_{sim} simülasyon zamanı olmak üzere, $i = 1,2,3 \ldots N$ ve $N = [T_{sim}/h]$'ı ifade etmektedir. Başlangıç koşulu $x(0), y(0)\ ve\ z(0)$'tır. $c_j^{(q_i)}$ ise binominal katsayıyı ifade etmektedir.

3.1.1. IKA Kaotik Sisteminin Analizi

3.1.1.1. Denge Nokta Analizi

$y = 0$

$z = 0$

$ax - by + cz - d = 0$

Denklem 3.4. Denge noktası denklemi

Denklem 3.1'e bakıldığında IKA sisteminin dengeleri $E_1 = (0,0,0)$ ve $E_2 = (\pm\sqrt{a}, 0,0)$ olarak hesaplanmaktadır. Denklem 3.2 için Jacobian matrisi aşağıdaki gibi ifade edilebilir;

$$J = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ a - 3x^2 & -b & c \end{bmatrix}$$

Denklem 3.5. Jacobian matris

Genel olarak kabul edildiği üzere, Denklem 3.2'deki incommensurate kesirli mertebeden sistemin sıfır çözümü, $\det(\Delta(\lambda)) = 0$ denkleminin tüm kökleri $|\arg(\lambda)| > \pi/2M$ artını sağladığında, global asimptotik kararlılık elde edilir (Tavazoei et al., 2008). Burada $\lambda(s)$ karakteristik matris olup, $\det(\Delta(s))$ ise Denklem 3.1'in karakteristik polinomu olarak adlandırılır. IKA sistemi için karakteristik matris aşağıdaki gibi hesaplanır;

$$J_{E_1} = \begin{bmatrix} \lambda^{M_{q1}} & -1 & 0 \\ 0 & \lambda^{M_{q2}} & -1 \\ -a + 3x^2 & b & \lambda^{M_{q3}} - c \end{bmatrix}$$

Denklem 3.6. Karakteristik matris

Burada M, incommensurate kesirli derecelerin ($q_{1,2,3}$) paydalarının en küçük ortak katıdır. $a = 5.7\ , b = 3.5, c = 2.468, q_1 = 0.54, q_2 = 0.55\ ve\ q_3 = 0.56$ değerlerini alarak denge noktalarını $E_1 = (0,0,0), E_{2,3} = (\pm 2.3875,0,0)$ olarak Denklem 3.6'da ayrı ayrı yerine koyarak, λ'nın basitleştirilmiş karakteristik polinomu $E_{2,3}$ için şu şekilde belirlenir;

$$\lambda^{165} - 2.468\lambda^{109} + 3.5\lambda^{54} - \lambda - 5.7$$
$$\lambda^{165} - 2.468\lambda^{109} + 3.5\lambda^{54} - \lambda + 11.4$$

Denklem 3.7. Karakteristik polinom

165 set çözümünün minimum faz açısına sahip çözümü $1.0147, 1.0191 + 0.016i$ olduğunda;

$$0.005\pi - min\{|\arg(\lambda)|\} = 0.0157$$

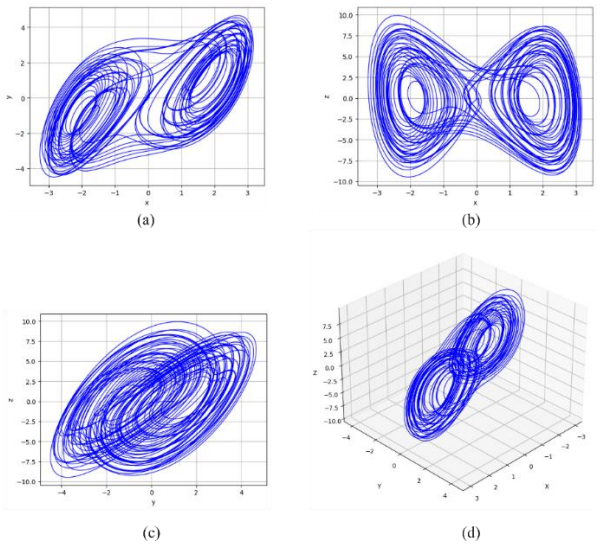
$$0.005\pi - min\{|\arg(\lambda)|\} \approx 0$$

Denklem 3.8. Denklem çözümü

Dolayısıyla, verilen incommensurate derece için, E_1 ve $E_{2,3}$ kararsızlık sergilemektedir (Tavazoei et al., 2008)

3.1.1.2. Faz Portresi

IKA kaotik sisteminin, $q_1 = 0.54, q_2 = 0.55, q_3 = 0.56$ dereceleri olmak üzere, $a = 5.7, b = 3.5$, ve $c = 2.468$ parametresi ve $\{x(0), y(0), z(0)\} = \{0, 1, 0\}$ başlangıç değeri için elde edilen x-y, x-z, y-z ve x-y-z faz portreleri Şekil 3.1'de verilmiştir.

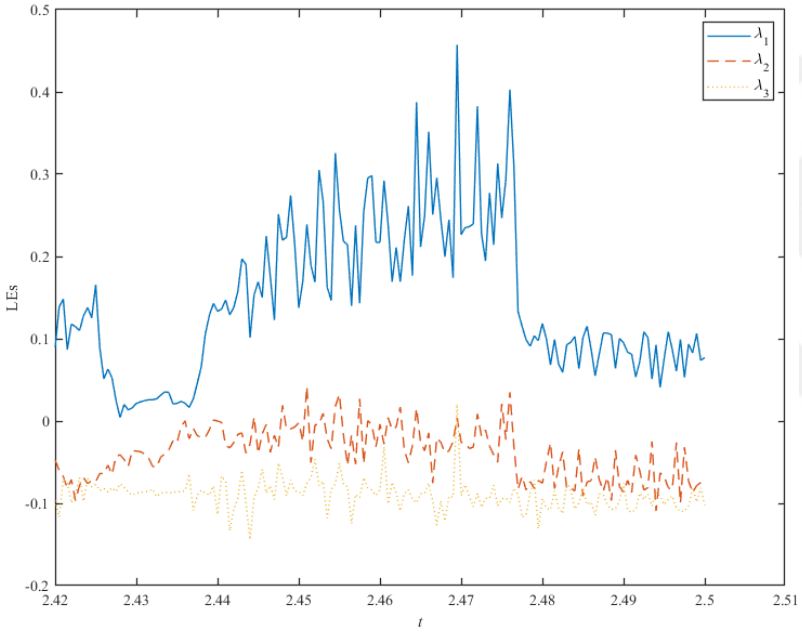


Şekil 3.1. IKA kaotik sisteminin x-y, x-z, y-z ve x-y-z için faz portresi

Şekillerden de görüldüğü gibi, verilen IKA kaotik sistemin zengin dinamik davranışlara sahip olduğu söylenebilir. Faz portelerinin gömülü sistem tabanlı, osiloskop çıktıları Bölüm 3.3'te verilmiştir.

3.1.1.3. Lyapunov Üstelleri

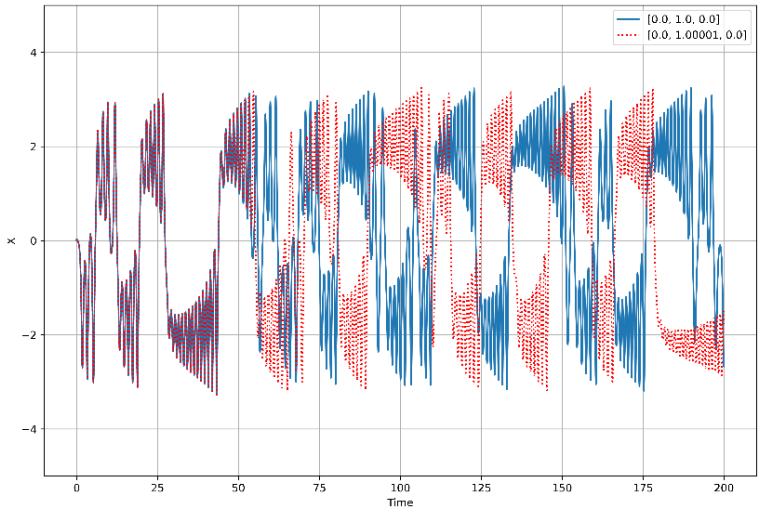
IKA kaotik sisteminin 'c' parametresine göre 2.42-2.51 aralığında Lyapunov Üstel spektrumu Şekil 3.2'de verilmiştir. Lyapunov üstel analizinde, bir sistemin kaotik olması için Lyapunov üstel değerlerinin (+,0,-) olması gerekmektedir. Şekil 3.2'den de görüldüğü üzere sistem belli aralıklarla kaosa girip çıkmaktadır.



Şekil 3.2. IKA kaotik sisteminin Lyapunov üstel grafiği (c=2.42-2.51)

3.1.1.4. Zaman Serilerinde Başlangıç Değerlerine Duyarlılık Analizi

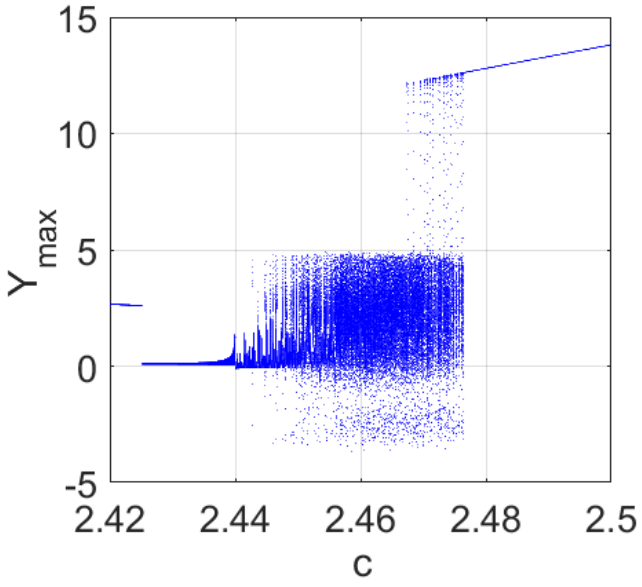
Sistemin başlangıç koşullarında yapılan çok küçük bir değişiklik sonucu ortaya çıkan farklı çıktılar, kaotiklik hakkında önemli bilgiler sağlamaktadır. Şekil 3.3'te verildiği gibi başlangıç şartı $[0.0, 1.0, 0.0]$ alınmış ve mavi eğri elde edilmiştir. Başlangıç şartı $[0.0, 1.00001, 0.0]$ olarak belirlendiğinde ise kırmızı kesikli eğri elde edilmiştir. Şekil 3.3'te yer alan iki eğri incelendiğinde, başlangıç koşullarındaki çok küçük değişikliklerin yeni sistem üzerinde farklı sonuçlar doğurduğu ve sistemin başlangıç şartlarına karşı yüksek hassasiyet gösterdiği gözlemlenebilir.



Şekil 3.3. IKA kaotik sisteminde başlangıç değerlerine duyarlılık analizi

3.1.1.5. Çatallaşma Diyagramı

Bölüm 3.1.1.3'te c parametresine göre Lyapunov üstel spektrumu sunulmuştu. Bu bölümde ise, c parametresine göre çatallaşma diyagramı çizilerek analiz yapılmıştır. Lyapunov üstel grafiği ve çatallaşma diyagramları, aynı aralıklar için benzer sonuçlar vermelidir. Yani, Lyapunov üstelinin kaotik özellik gösterdiği bölgelerde çatallaşma diyagramının da kaotik özellikler sergilemesi beklenir. Şekil 3.4'te, $q_1 = 0.54, q_2 = 0.55, q_3 = 0.56, a = 5.7, b = 3.5$ ve $c \in [2.42, 2.5]$ için y'nin yerel maksimumuna karşılık gelen Çatallaşma diyagramı sunulmuştur. Şekil 3.4, Şekil 3.2'deki Lyapunov üstel grafiği karşılaştırıldığında, her iki grafikte de kaotik özelliklerin aynı bölgelerde ortaya çıktığı gözlemlenebilir.



Şekil 3.4. IKA kaotik sisteminin çatallaşma diyagramı (c ∈ [2.42, 2.5])

3.2. Incommensurate Kesir Dereceli Sprott B Kaotik Sistemi

Julien Sprott, 1994 yılında, A'dan S'ye kadar isimlendirdiği beş ve altı terimli çeşitli kaotik sistemleri tanıtmıştır (Sprott, 1994). Bu sistemler, basit diferansiyel denklemler kullanarak kaotik davranışları modellemekte ve her biri farklı dinamik özellikler sergilemektedir. Bunlar arasında, Sprott B sistemi olarak adlandırılan sistem, beş terimden oluşur ve bunların ikisi nonlineerdir. Sistem, parametrik analizlerin kolaylaştırılması amacıyla iki sabit eklenmiş genel bir formda ifade edilir. Bu formülasyon Denklem 3.9'da verildiği gibi ifade edilebilir.

$$\dot{x} = yz$$

$$\dot{y} = x - \alpha y$$

$$\dot{z} = \beta - \alpha xy$$

Denklem 3.9. Genelleştirilmiş Sprott B kaotik sistemi

Burada, $x, y\ ve\ z$ durum değişkenini, $\alpha\ ve\ \beta$ ise pozitif sabit sistem parametresini temsil etmektedir.

Kesirli dereceli operatörlerin kullanılması, Sprott B sisteminin dinamik zenginliğini artıran analizler yapılmasına olanak tanır. Bu bağlamda, sistem, Denklem 3.10'da sunulduğu gibi kesirli diferansiyel denklemlerle ifade edilebilir.

$$D^{q_1}x = yz$$

$$D^{q_2}y = x - \alpha y$$

$$D^{q_3}z = \beta - \alpha xy$$

Denklem 3.10. Kesirli dereceli Sprott B kaotik sistemi

Burada, D^{q_1}, D^{q_2}, ve D^{q_3} kesirli dereceden operatörleri temsil eder. Bu tez çalışmasında $0 \leq q_i \leq 1\ (i = 1,2,3)$ olacak şekilde her dinamik denklem için farklı kesirli mertebe değerleri seçilmiştir. Seçilen kesirli dereceli değerler ve başlangıç koşulları sonucunda üretilen kaotik sinyaller, karmaşık ve öngörülemez paternler sergiler.

Incommensurate kesir dereceli Sprott B (IKSB) sisteminin sayısal çözümü aşağıdaki gibidir:

$$x(i) = \big(y(i-1).z(i-1)\big).h^{q_1} - \sum_{j=1}^{i-1} c_1^{(q1)}(j)\, x(i-j)$$

$$y(i) = \big(x(i) - \alpha . y(i-1)\big).h^{q_2} - \sum_{j=1}^{i-1} c_2^{(q2)}(j)\, y(i-j)$$

$$z(i) = \big(\beta - \alpha . x(i).y(i)\big).h^{q_3} - \sum_{j=1}^{i-1} c_3^{(q3)}(j)\, z(i-j)$$

Denklem 3.11. IKSB sisteminin sayısal çözümü

T_{sim} simülasyon zamanı olmak üzere, $i = 1,2,3 \ldots N$ ve $N = [T_{sim}/h]$' ı ifade etmektedir. başlangıç koşulu $x(0), y(0)\ ve\ z(0)$'tır. $c_j^{(q_i)}$ ise binominal katsayıyı ifade etmektedir.

3.2.1. IKSB Kaotik Sisteminin Analizi

3.2.1.1. Denge Nokta Analizi

$yz = 0$

$x - \alpha y = 0$

$\beta - \alpha xy = 0$

Denklem 3.12. Denge noktası denklemi

Denklem 3.9'a bakıldığında IKSB sisteminin dengeleri $E_{1,2} = (\pm\sqrt{b}, \mp\frac{\sqrt{b}}{a}, 0)$ olarak hesaplanmaktadır. Denklem 3.10 için Jacobian matrisi aşağıdaki gibi ifade edilebilir;

$$J = \begin{bmatrix} 0 & z & y \\ 1 & -\alpha & 0 \\ -\alpha y & -\alpha x & 0 \end{bmatrix}$$

Denklem 3.13. Jacobian matris

Genel olarak kabul edildiği üzere, Denklem 3.10'daki incommensurate kesirli mertebeden sistemin sıfır çözümü, $\det\big(\Delta(\lambda)\big) = 0$ denkleminin tüm kökleri $|\arg(\lambda)| > \pi/2M$ artını sağladığında, global asimptotik kararlılık elde edilir (Tavazoei et al., 2008). Burada $\lambda(s)$ karakteristik matris olup, $\det(\Delta(s))$ ise Denklem 3.9'un karakteristik polinomu olarak adlandırılır. IKSB sistemi için karakteristik matris aşağıdaki gibi hesaplanır;

$$J_{E_1} = \begin{bmatrix} \lambda^{M_{q1}} & -z & -y \\ -1 & \lambda^{M_{q2}} + \alpha & 0 \\ \alpha y & \alpha x & \lambda^{M_{q3}} \end{bmatrix}$$

Denklem 3.14. Karakteristik matris

Burada M, incommensurate kesirli derecelerin ($q_{1,2,3}$) paydalarının en küçük ortak katıdır. $\alpha = 0.8\,, \beta = 2.2\,, q_1 = 0.9, q_2 = 0.91\ ve\ q_3 = 0.92$ değerlerini alarak denge noktalarını $S_{1,2} = (\pm 1.4832, \pm 1.854, 0)$ olarak Denklem 3.14'te ayrı ayrı yerine koyarak, λ'nın basitleştirilmiş karakteristik polinomu $E_{2,3}$ için şu şekilde belirlenir;

$$\lambda^{273} + 0.8\lambda^{182} + 2.75\lambda^{91} - \lambda + 4.4$$

Denklem 3.15. Karakteristik polinom

273 set çözümünün minimum faz açısına sahip çözümü $1.006 \pm 0.016408i$ olduğunda;

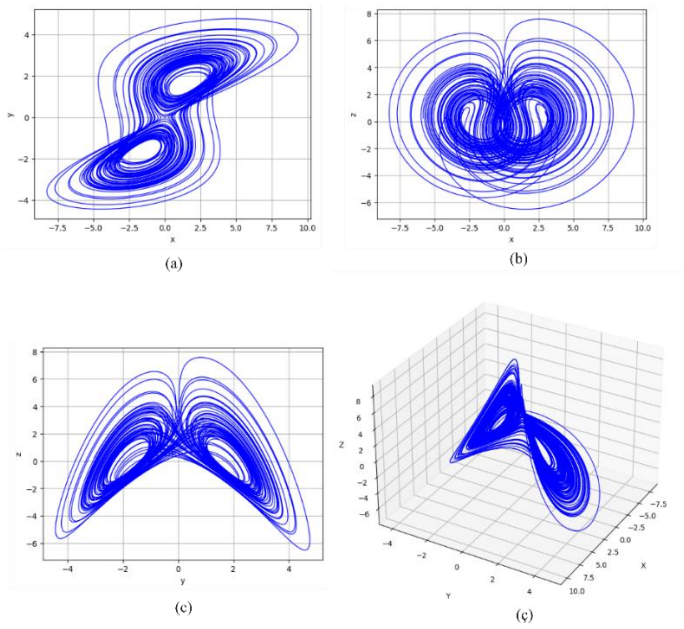
$$0.005\pi - min\{|\arg(\lambda_m)|\} = -0.146$$

Denklem 3.16. Denklem çözümü

Dolayısıyla, verilen incommensurate derece için, $S_{1,2}$ kararlı bir görünüm sergilemektedir (Tavazoei et al., 2008). Bununla birlikte, doğrusal olmayan sistemde kararlı denge noktalarıyla birlikte var olabilecek gizli kaotik çekicilerin bulunabileceği unutulmamalıdır (Ma et al., 2020).

3.2.1.2. Faz Portresi

IKSB kaotik sisteminin, $q_1 = 0.9, q_2 = 0.91, q_3 = 0.92$ kesir dereceleri olmak üzere, $\alpha = 0.8\,, \beta = 2.2$ parametresi ve $\{x(0), y(0), z(0)\} = \{1, 1, 1\}$ başlangıç değeri için elde edilen x-y, x-z, y-z ve x-y-z faz portreleri Şekil 3.5'te verilmiştir.

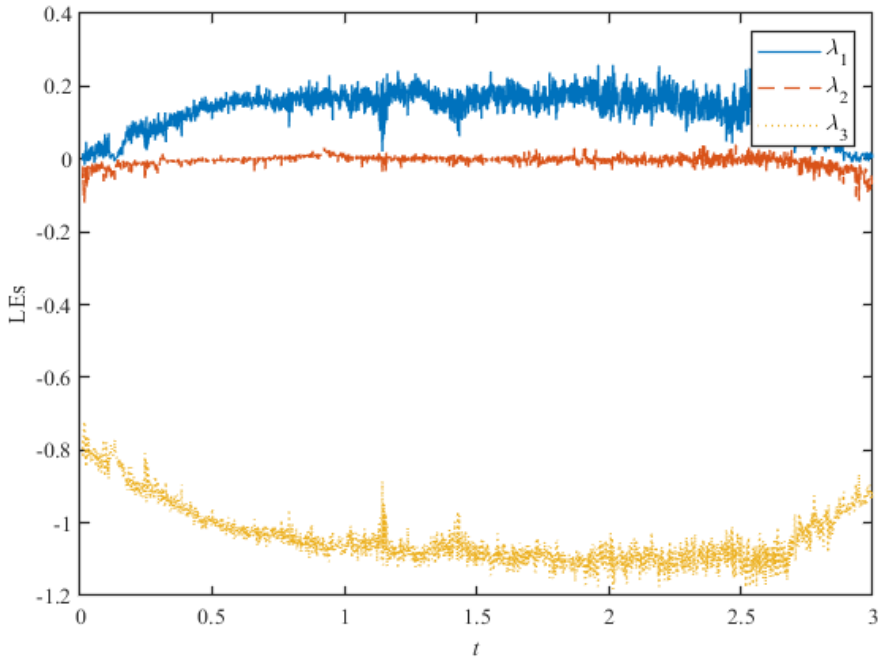


Şekil 3.5. IKSB kaotik sisteminin x-y, x-z, y-z ve x-y-z için faz portresi

Şekillerden anlaşıldığı üzere, sunulan IKSB kaotik sisteminin karmaşık dinamik davranışlar sergilediği görülmektedir. Gömülü sistem tabanlı faz portrelerine ait osiloskop çıktıları Bölüm 3.3'te sunulmuştur.

3.2.1.3. Lyapunov Üstelleri

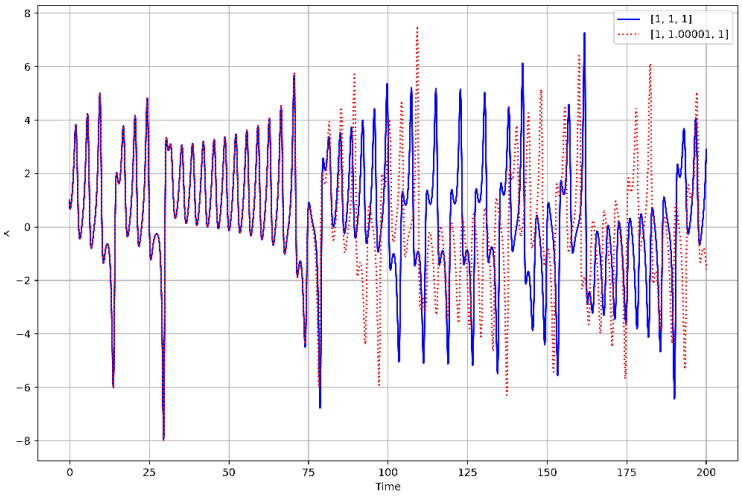
IKSB kaotik sisteminin 'β' parametresine göre 0-3 aralığında Lyapunov Üstel spektrumu Şekil 3.6'da verilmiştir. Lyapunov üstel analizinde, bir sistemin kaotik olması için Lyapunov üstel değerlerinin (+,0,-) olması gerekmektedir. Şekil 3.6'dan da görüldüğü üzere sistem belli aralıklarla kaosa girip çıkmaktadır.



Şekil 3.6. IKSB kaotik sisteminin Lyapunov üstel grafiği (c=0-3)

3.2.1.4. Zaman Serilerinde Başlangıç Değerlerine Duyarlılık Analizi

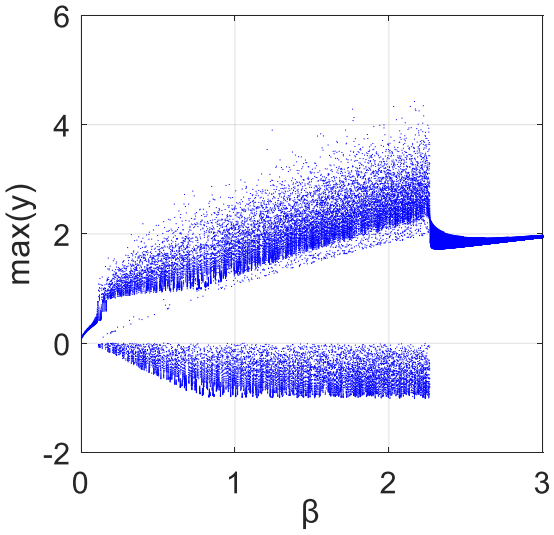
Şekil 3.7'de gösterildiği gibi, başlangıç koşulu [1, 1, 1] olarak alındığında mavi eğri elde edilmiştir. Başlangıç koşulu [1, 1.00001, 1] olarak belirlendiğinde ise kırmızı kesikli eğri elde edilmiştir. Şekil 3.7'deki bu iki eğri incelendiğinde, başlangıç koşullarındaki küçük değişikliklerin sistemin çıktıları üzerinde belirgin farklar yarattığı ve sistemin başlangıç şartlarına karşı yüksek duyarlılık gösterdiği anlaşılabilir.



Şekil 3.7. IKSB kaotik sisteminde başlangıç değerlerine duyarlılık analizi

3.2.1.5. Çatallaşma Diyagramı

Bölüm 3.2.1.3'te, β parametresine göre Lyapunov üstel spektrumu ele alınmıştı. Bu bölümde ise β parametresine bağlı olarak Çatallaşma Diyagramı çizilerek analiz yapılmıştır. Lyapunov üstel grafiği ve çatallaşma diyagramlarının, aynı aralıklar için benzer sonuçlar vermesi beklenir. Özellikle, Lyapunov üstelinin kaotik özellikler sergilediği bölgelerde çatallaşma diyagramının da kaotik davranışlar göstermesi beklenir. Şekil 3.8' de, $q_1 = 0.9, q_2 = 0.91, q_3 = 0.92, \alpha = 0.8$ ve $\beta \in [0,3]$ için y'nin yerel maksimumlarına karşılık gelen ayrıntılı çatallaşma diyagramı sunulmuştur. Şekil 3.8, Şekil 3.6'daki Lyapunov üstel grafikleri karşılaştırıldığında, her iki grafikte de kaotik özelliklerin aynı bölgelerde ortaya çıktığı görülmektedir.



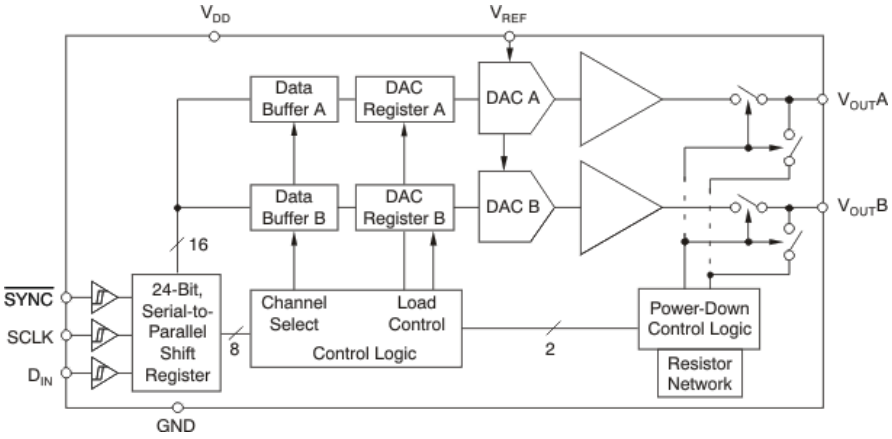
Şekil 3.8. IKSB kaotik sisteminin çatallaşma diyagramı (β ∈ [0, 3])

3.3. Gömülü Sistem Tabanlı Kaotik Sistemlerin Modellenmesi

Kaotik sistemlerin fiziksel olarak somutlaştırılması ve incelenmesi, çeşitli bilimsel ve mühendislik alanlarında önemli pratik uygulamalara olanak tanımaktadır. Bu bağlamda IKA ve IKSB kaotik sistemlerinin fiziksel gerçekleştirilmesi, Nvidia Jetson AGX Orin platformu kullanılarak sağlanmıştır. Ancak, Nvidia Jetson AGX Orin platformunun analog çıkışa sahip olmaması nedeniyle dijital sinyallerin analog sinyallere dönüştürülmesi amacıyla tez kapsamında çevirici kart tasarlanmıştır. Kartın tasarımı Altium Designer programında gerçekleştirilmiştir (Altium Limited, 2021).

Tasarımı yapılan kart, girişten aldığı 24 bitlik veri içerisindeki; ilk 16 bitlik bilgi ve 8 bitlik kontrol mesajlarını kullanarak, çıkışta maksimum referans voltajına kadar gerilim üretir. Bu referans voltajı, çevirici kart üzerinde oluşturulmaktadır. Çıkışta pozitif (+) ve negatif (-) voltajların elde edilebilmesi için DAC entegresinin her iki çıkışına opamp kullanılarak tasarlanan bipolar dönüştürücü devresi eklenmiştir. Opamp devresinin ihtiyaç duyduğu simetrik besleme gerilimi harici olarak alınırken, DAC entegresinin ihtiyaç duyduğu referans voltajı ve besleme gerilimi dahili olarak oluşturulmuştur. DAC entegresinin her iki çıkışı 50 ohm karakteristik empedansa sahip olan SMA konnektörler ile sonlandırılmıştır. Ayrıca tasarlanan çevirici kart, yüksek frekanslı gürültü bileşenlerinden etkilenilmemesi için dekuplaj kapasitörleri ile desteklenmiştir.

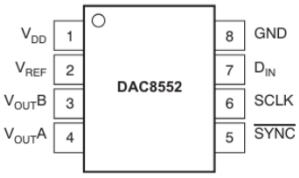
Çıkışta istenilen gerilim değerinin elde edilebilmesi için 16 bit çözünürlüğünde, çok düşük hata aralığında çalışan ve SPI ara yüzüne sahip TI DAC8552 entegresi tercih edilmiştir. Şekil 3.9'da DAC entegresinin blok diyagramı verilmiştir.



Şekil 3.9. DAC8552 içyapısı (Kaynak: DAC8552 Data Sheet, 2020)

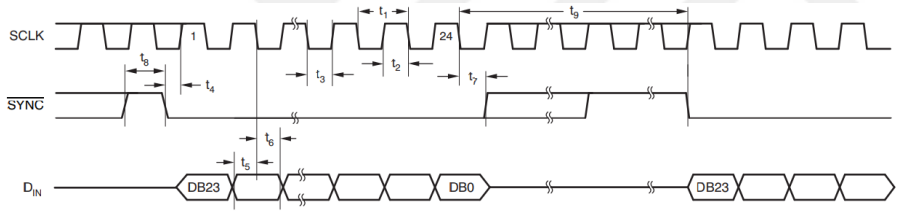
DAC entegresinin maksimum besleme gerilimi 5.5V_{dc} ve SPI arayüzünden alabileceği maksimum veri hızı 30Mhz olarak belirtilmiştir. 16 bit çözünürlüğünde ve iki ayrı kanala sahip olan bu DAC entegresi, her iki kanalın aynı anda kontrol edilebilmesine olanak tanımaktadır. Şekil 3.10'da DAC entegresinin pin konfigürasyonu ve açıklamaları verilmiştir.

Pin No	İsim	Fonksiyonu
1	V_{DD}	Güç Girişi (2.7 v – 5.5 v)
2	V_{REF}	Referans voltaj girişi
3	$V_{OUT}B$	DAC B'nin analog çıkış gerilimi
4	$V_{OUT}A$	DAC A'nin analog çıkış gerilimi
5	$\overline{SYNC}$	Giriş verileri için çerçeve senkronizasyon sinyalidir. SYNC sinyali düşük seviyeye geçtiğinde, giriş kaydedici devresi etkinleşir ve veri, SCLK'nın düşen kenarlarında aktarılır.
6	SLCK	Seri Saat Girişi. Veriler, 5V'da 30MHz'ye kadar hızlarda aktarılabilir.
7	D_{IN}	Seri Veri Girişi. Veriler, SCLK saat girişinin düşen kenarında 24-bitlik giriş kaydediciye kaydedilir.
8	GND	Toprak referans



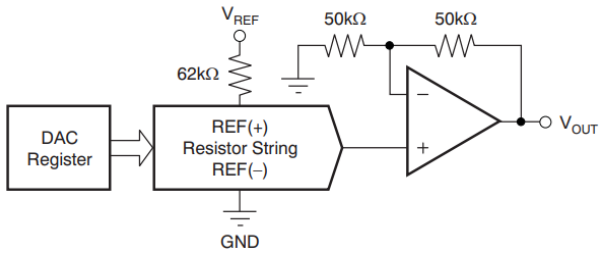
Şekil 3.10. DAC8552 pin tanımlamaları (Kaynak: DAC8552 Data Sheet, 2020)

DAC entegresinin SPI kontrolü için seri yazma işlemine ait görsel Şekil 3.11'de verilmiştir.



Şekil 3.11. Seri yazma operasyonu (Kaynak: DAC8552 Data Sheet, 2020)

Seri saat girişi maksimum 5v 30 MHz olacak şekilde ayarlanır ve ardından SYNC seri verinin alınabilmesi için düşük konuma getirilir. Kontrol ve bilgi verilerini içeren 24 bit veri, seri girişten DAC shift register birimine uygulanır. DAC entegresinde bulunan her kanal bir DAC ve bir buffer opamp devresinden oluşmaktadır. Şekil 3.12'de DAC mimarisinin görseli verilmiştir.



Şekil 3.12. DAC mimarisi (Kaynak: DAC8552 Data Sheet, 2020)

Her bir DAC'ın çıkışı unipolardır ve ideal çıkış voltajı A ve B kanalı için Denklem 3.17'de verilmiştir.

$$V_{OUT}A,B = V_{REF} \times \frac{D}{65536}$$

Denklem 3.17. Referans gerilim tabanlı çıkış voltajı denklemi

Burada D, giriş registerinda bulunan ilk 16 bit verinin desimal formatta karşılığını ve V_{REF} sistem üzerinde bulunan referans voltajını temsil etmektedir.

Giriş register16 bitlik veri ve 8 bitlik kontrol verisi ile toplamda 24 bitten oluşmaktadır. Şekil 3.13'te giriş register formatı verilmiştir.

DB23											**DB12**
0	0	LDB	LDA	X	Buffer Select	PD1	PD0	D15	D14	D13	D12
DB11											**DB0**
D11	D10	D9	D8	D7	D6	D5	D5	D3	D2	D1	D0

Şekil 3.13. Giriş register formatı (Kaynak: DAC8552 Data Sheet, 2020)

Burada;

- D0-D15 çıkışta elde edilmek istenilen voltaj bilgisinin yazıldığı alanı temsil etmektedir.
- PD0-PD1 DAC85552 entegresinde bulunan çalışma modlarının seçilmesini sağlayan alandır.
- Buffer Select hangi kanalın kontrol edileceğinin belirtildiği alandır.
- LDA-LDB verinin ilgili kanala aktarılmasını sağlayan alandır

Yapılan tasarımda DAC8552'nin çalışma modu olarak normal mod (PD0=0, PD1=0) kullanılmıştır.

DAC entegresinin A ve B kanalının eş zamanlı kontrolü için ise Şekil 3.14'te verilen register sırası kullanılmıştır.

- 1st — Write to Data Buffer A:

Reserved	Reserved	LDB	LDA	DC	Buffer Select	PD1	PD0	DB15	—	DB1	DB0
0	0	0	0	X	0	0	0	D15	—	D1	D0

- 2nd — Write to Data Buffer B and Load DAC A and DAC B simultaneously:

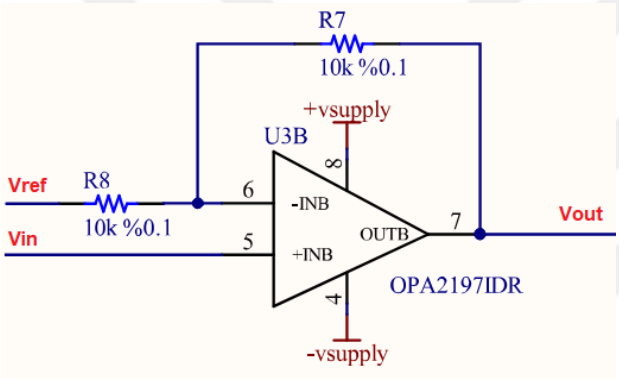
Reserved	Reserved	LDB	LDA	DC	Buffer Select	PD1	PD0	DB15	—	DB1	DB0
0	0	1	1	X	1	0	0	D15	—	D1	D0

Şekil 3.14. DAC8552 A ve B kanalı kontrol register (Kaynak: DAC8552 Data Sheet, 2020)

Bu doğrultuda, ilk olarak buffer select alanı kullanılarak A kanalı seçilir ve ilk 16 bit'lik alana A kanalının çıkışından alınmak istenilen voltaj değeri seri girişten verilir. Bu adımda

verinin çıkışlara aktarılmasını sağlayan LDB ve LDA registerları 0 konumundadır ve çıkışa herhangi bir değer aktarılmaz. İkinci adımda buffer select alanı kullanılarak B kanalı seçilir ve ilk 16 bit'lik alana B kanalının çıkışından alınmak istenilen voltaj değeri seri girişten verilir. Arından bu adımda LDB ve LDA registerları 1 konumuna alınır ve her iki kanal aynı anda yüklenmiş olur.

DAC entegresinin oluşturduğu unipolar çıkışı bipolar çıkışa dönüştürmek için opamp devresi tasarlanmıştır. DAC referans voltajı 5v olacak şekilde belirlenmiştir. DAC maksimum 5v çıkış üretebildiği göz önünde bulundurulduğunda ±5 volt bipolar çıkış alabilmek için Şekil 3.15'te verilen Unipolar-Bipolar dönüştürücü opamp devresi kullanılmıştır.



Şekil 3.15. Unipolar-Bipolar dönüştürücü opamp devresi

Burada opamp DC analizinden eviren giriş (6) Vin olarak kabul edilirse çıkış voltaj fonksiyonu;

$$\frac{V_{in} - V_{ref}}{10k_{R8}} + \frac{V_{in} - V_{out}}{10k_{R7}} = 0$$

Denklem 3.18. Çıkış voltaj fonksiyonu

Elde edilir. Buradan ise,

$$V_{out} = 2V_{in} - V_{ref}$$

Denklem 3.19. Opamp çıkış voltajı

olarak bulunur.

V_{ref} 5v kabul edilirse, DAC çıkışı 5v olduğunda çıkıştan elde edilen voltaj +5v ve DAC çıkışı 0v olduğunda çıkıştan elde edilen voltaj -5v olarak bulunur. Çıkış hatalarını en aza indirmek için Rail to Rail sınıfında yer alan OPA2197 opamp entegresi kullanılmıştır.

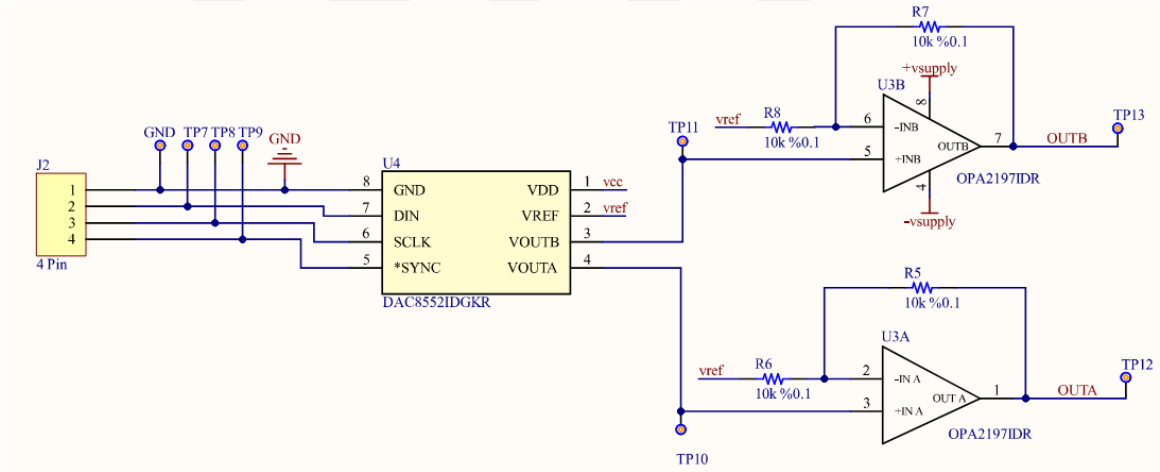
16 bit çözünürlüğe sahip DAC registerına uygulanan desimal bilgi, formüle dâhil edildiğinde her iki kanal için elde edilen çıkış formülü Denklem 3.20'de verilmiştir.

$$V_{OUT}A, B = \left(\frac{10 \times D}{65536}\right) - 5v$$

Denklem 3.20. DAC çıkış voltajı denklemi

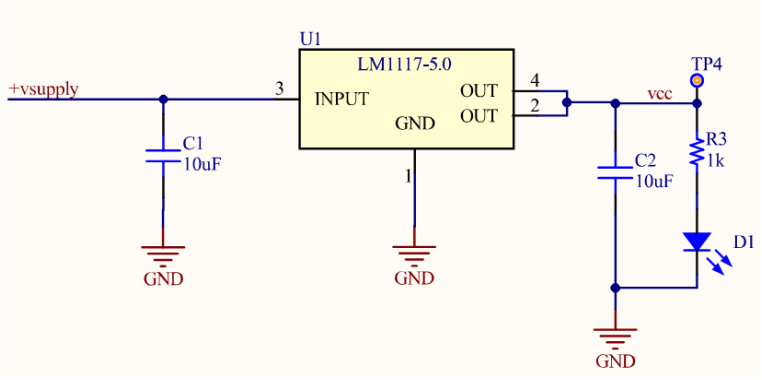
Burada D giriş registerında bulunan ilk 16 bit verinin desimal formatta karşılığını temsil etmektedir.

Tasarlanan bipolar çevirici ve DAC yapısı Şekil 3.16'da verilmiştir.



Şekil 3.16. SPI-Bipolar DAC çevirici

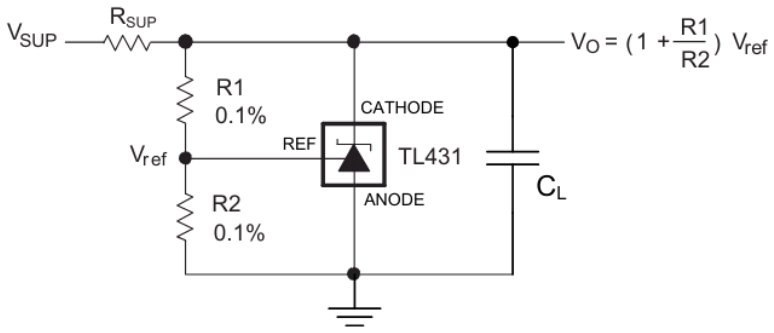
DAC8552 entegresinin ihtiyaç duyduğu 5v besleme voltajının oluşturulması için maliyeti uygun LM1117 sabit lineer voltaj düzenleyici kullanılmıştır. Şekil 3.17'de voltaj düzenleyicinin şeması verilmiştir.



Şekil 3.17. Lineer voltaj düzenleyici

DAC entegresinden daha verimli çıkış alınabilmesi için düşük voltaj sapmalarına sahip TL431 ayarlı referans entegresi V_{ref} voltajını oluşturmak için kullanılmıştır.

Giriş gerilimini 5v referans gerilimine dönüştürmek için TL431 shunt regülatör yapısı kullanılmıştır. Şekil 3.18'de shunt regülatör yapısı verilmiştir.



Şekil 3.18. TL431 Shunt regulatör şeması (Kaynak: TL431 Data Sheet, 2023)

TL431 Referans voltaj düzenleyicisinin çıkış voltaj formülü Denklem 3.21'de verilmiştir.

$$V_0 = \left(1 + \frac{R_1}{R_2}\right) V_{ref}$$

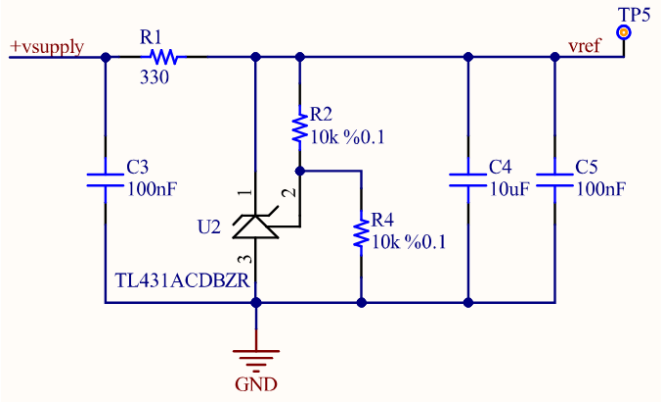
Denklem 3.21. TL431 referans voltaj düzenleyici çıkış denklemi

TL431 referans voltajı 2.5v, R_1 ve R_2 10k olarak alınırsa,

$$5\text{v} = \left(1 + \frac{10\text{k}}{10\text{k}}\right) 2.5\text{v}$$

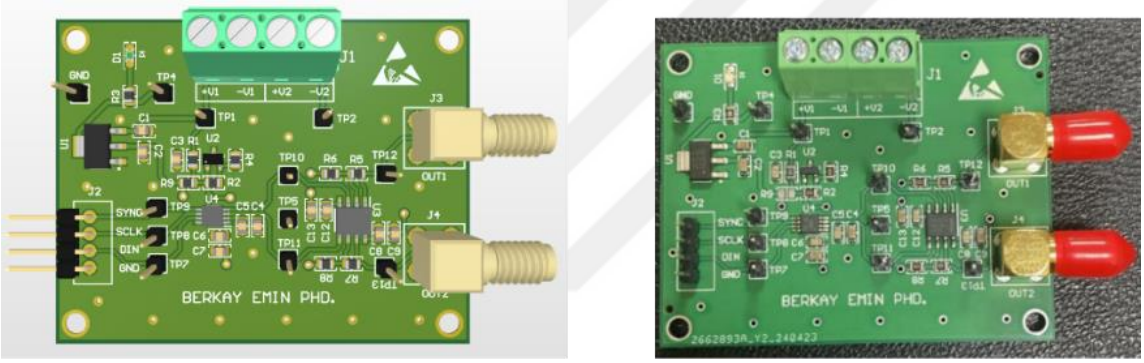
Denklem 3.22. TL431 referans voltajı ile 5v için çıkış denklemi

Buradan ise çıkış voltajı 5v olarak elde edilir. Şekil 3.19'da tasarlanan referans voltajı düzenleyici verilmiştir.



Şekil 3.19. Referans voltaj düzenleyici

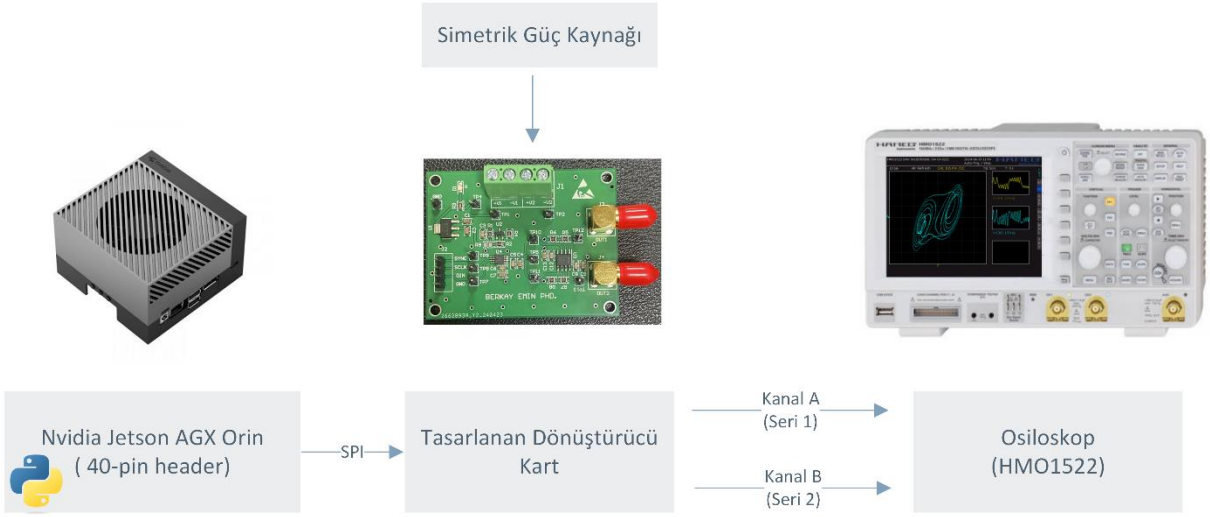
Tasarlanan kartın üç boyutlu görüntüsü ve üretilen kartın görüntüsü Şekil 3.20'de verilmiştir.



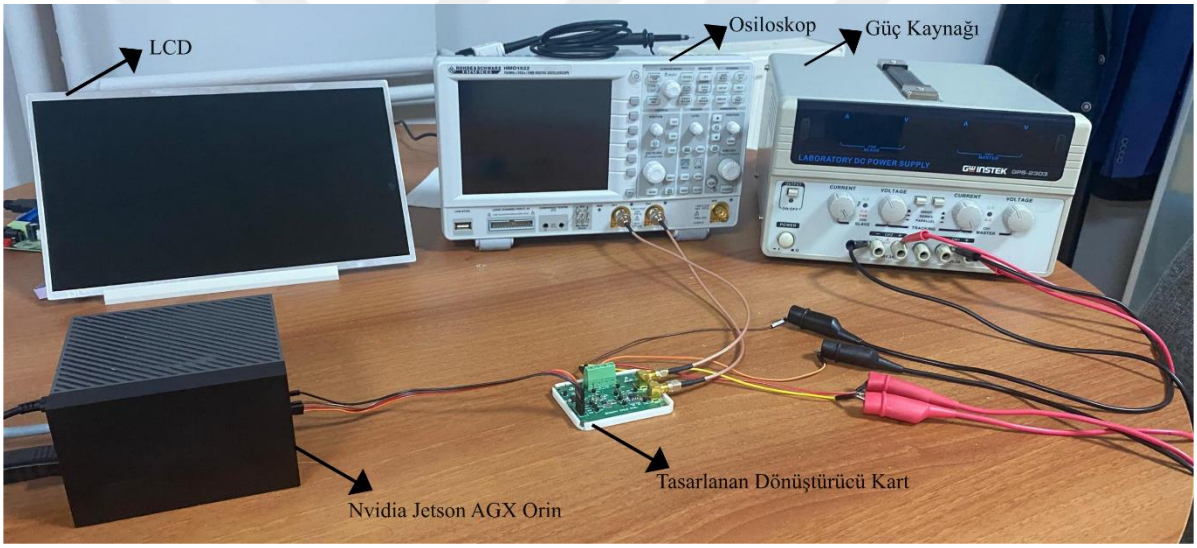
(a) (b)

Şekil 3.20. Tasarlanan kart; (a) Üç Boyutlu Görüntü (b) Üretilen kart

Şekil 3.21'de Nvidia Jetson AGX Orin ile tasarlanan kartın donanım bloğu ilişkisi verilmiştir. Tasarlanan kart, tarafımca Python programlama dili kullanılarak yazılan yazılım aracılığıyla kontrol edilmektedir. Şekil 3.22'de ise test ortamına ait görüntüsü verilmiştir.

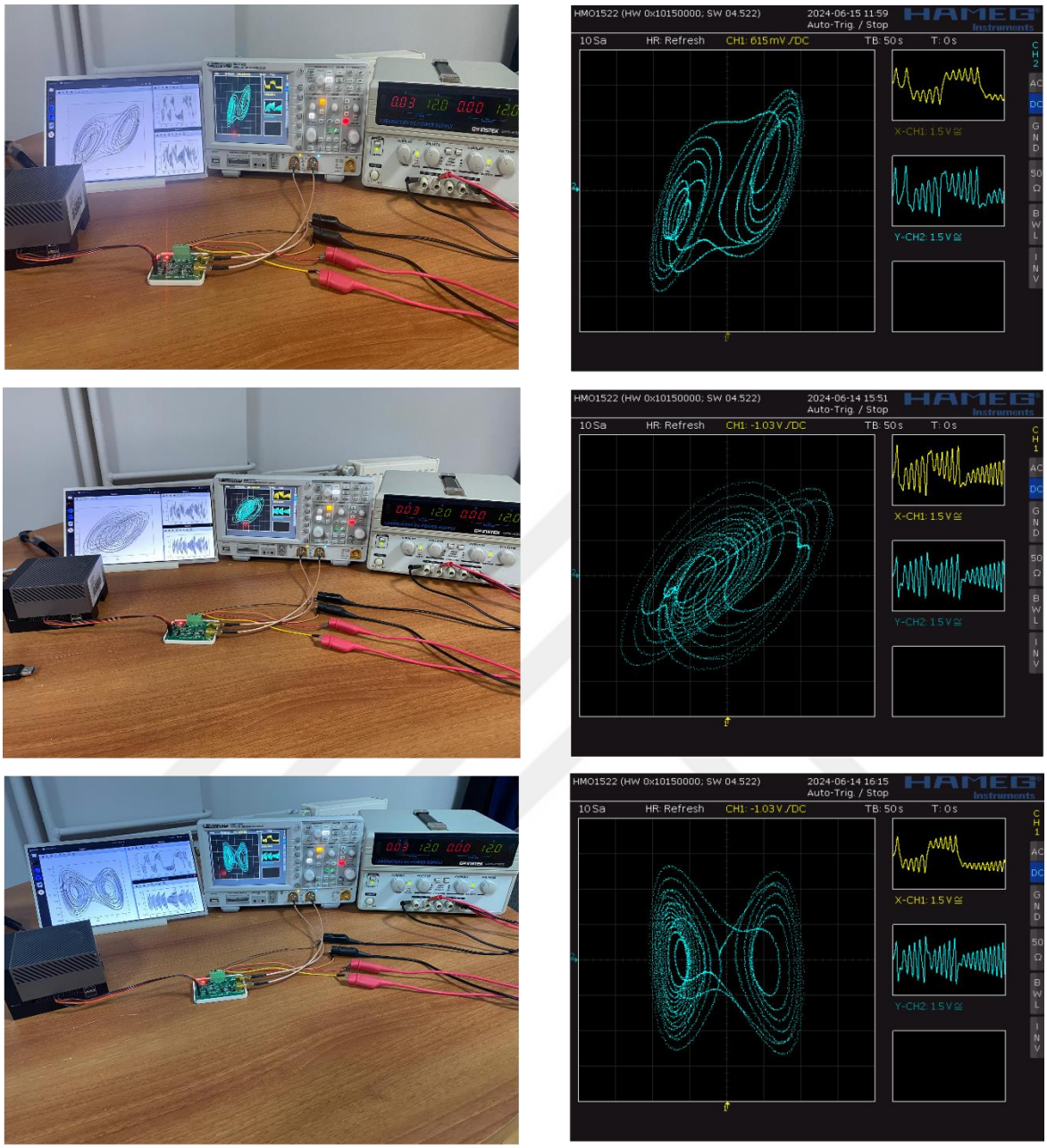


Şekil 3.21. Donanım blok ilişkisi



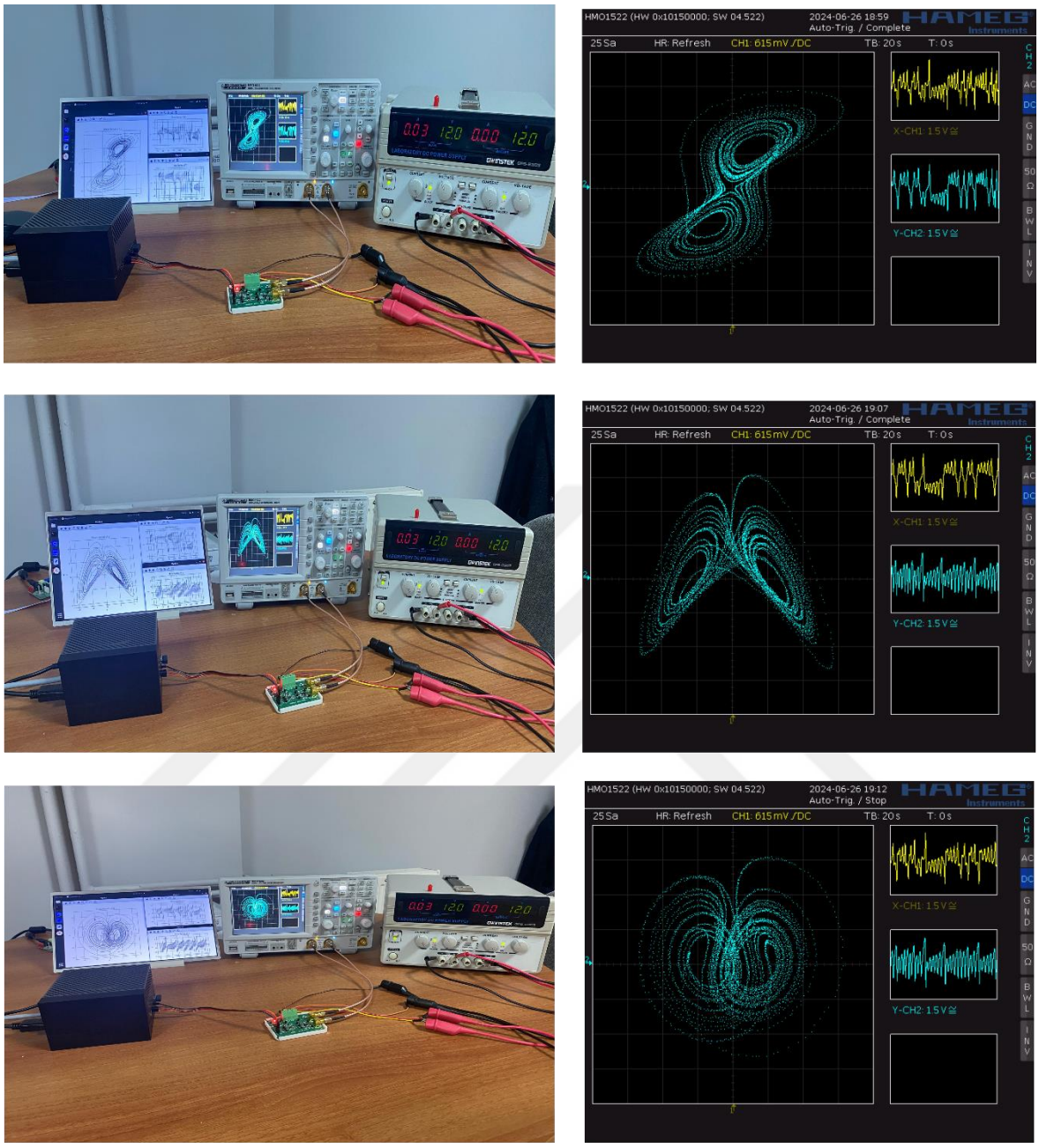
Şekil 3.22. Test ortamı

$a = 5.7\,, b = 3.5, c = 2.468$**,**$q_1 = 0.54, q_2 = 0.55\ ve\ q_3 = 0.56$ ve $\{x(0), y(0), z(0)\} = \{0, 1, 0\}$ için IKA kaotik sisteminin faz portesine ait görüntüler ve $q_1 = 0.9, q_2 = 0.91, q_3 = 0.92, \alpha = 0.8\,, \beta = 2.2\ ve\ \{x(0), y(0), z(0)\} = \{1, 1, 1\}$ için IKSB kaotik sistemine ait faz portesine ait görüntüler sırasıyla Şekil 3.23'te ve Şekil 3.24'te verilmiştir.



(a) (b)

Şekil 3.23. IKA kaotik sistem faz portresi: (a) Modelleme; (b) Osiloskop çıktıları



(a) (b)

Şekil 3.24. IKSB kaotik sistem faz portresi: (a) Modelleme; (b) Osiloskop çıktıları

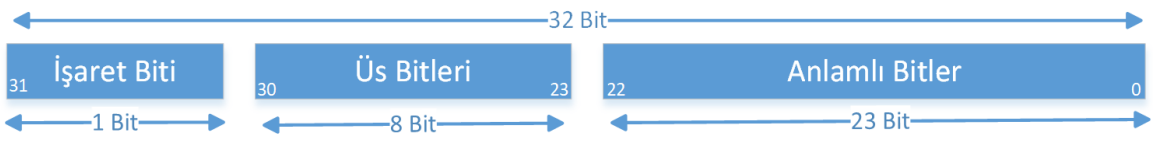
3.4. Incommensurate Kesir Dereceli Kaotik Sistemler ile Gömülü Sistem Tabanlı Rastgele Sayı Üreteç Tasarımı

Kesirli dereceli sistemlerin sayısal çözümleri, Grünwald-Letnikov, Caputo, Riemann-Liouville ve Adams-Bashforth-Moulton gibi nümerik analiz algoritmaları kullanılarak gerçekleştirilmektedir. Tez çalışmasında ele alınan incommensurate kesirli dereceli kaotik sistemlerin sayısal çözümleri, Grünwald-Letnikov nümerik diferansiyel denklem çözüm yöntemleri kullanılarak ayrıklaştırılmış modeli çıkarılmıştır. IKA kaotik sisteminin, y fazı için ayrıklaşma işlemi sonrası elde edilen sayısal değerler 5 adım için Tablo 3.1'de verilmiştir.

Tablo 3.1. IKA sisteminin 'y' fazı ayrıklaşma sonrası elde edilen sayısal değerler

Adım Sayısı	Ayrıklaşma İşlemi Sonrası Elde Edilen Sayısal Değerler
1	1
2	0.55
3	0.42618154
4	0.36218294
5	0.32136701

Grünwald-Letnikov algoritması sonucunda elde edilen sayısal ifadeler, pozitif ve negatif sayılar içermekte olup decimal çıktı vermektedir. Decimal sayıların gerçek ortam uygulamalarında kullanılabilmesi için ikili sayı sistemine dönüştürülmesi gerekmektedir. Yapılan çalışmada ikili sayı sistemine dönüştürmek amacıyla 32-Bit tek duyarlı IEEE-754 kayan noktalı sayı standarttı kullanılmıştır. Kayan Noktalı Aritmetik için IEEE Standardı (IEEE 754), 1985 yılında IEEE (Electrical and Electronics Engineers -Elektrik ve Elektronik Mühendisleri Enstitüsü) tarafından oluşturulan kayan noktalı hesaplama için teknik bir standarttır ("IEEE Standard for Binary Floating-Point Arithmetic," 1985). Şekil 3.25'te genel olarak 32-Bit tek duyarlı IEEE-754 kayan noktalı sayı standarttı verilmiştir.



Şekil 3.25. 32-Bit tek duyarlı IEEE-754 kayan noktalı sayı standarttı

Şekil 3.25'te görüldüğü gibi IEEE-754 kayan noktalı sayı standarttı 32 bitlik bir alan 3 parçadan oluşmaktadır. İşaret biti pozitif sayılar için sıfır, negatif sayılar için 1 değerini almaktadır. Tek duyarlı gösterimde üst için kaydırma değeri $2^{8-1} - 1 = 127$ olarak hesaplanır. Üstel sayıya 127 eklenerek elde edilen sayı ikili olarak kodlanır.

Örnek olarak tek duyarlı gösterimde -6.25 sayısı ifade edilirse,

$6 = (110)_2$,$0.25 = (0.01)_2 \quad -(6.25)_{10} \rightarrow (110{,}01)_2$

Elde edilen sayı normalleştirilmiş formda 1.1001×2^2 olacak şekilde elde edilir.

İşaret Biti: Sayı negatif olduğu için işaret biti 1 değerini alır.

Üs Bitleri: IEEE 754 formatında üs değeri $2 + 127 = 129 \rightarrow 10000001$ olarak hesaplanır.

Anlamlı Bitler: Normalleştirilmiş biçimde 1.1001' deki anlamlı kısmı sadece 1001 olup, 23 bit'e tamamlamak için 0 eklenir: 10010000000000000000000

Sayı son olarak 1 10000001 10010000000000000000000 şeklinde ifade edilir.

Tez kapsamında önerilen rastgele sayı üreteç algoritmasına ait sözde kod Algoritma 1'de verilmiştir. Rastgele sayı üretimi ve istatiksel testlerin tamamı Python dili kullanılarak Nvidia Jetson AGX Orin gömülü kartı ve Jupiter programlama ortamı üzerinde gerçekleştirilmiştir.

Algoritma 1: Rastgele Sayı Üretecine ait Sözde Kod

Input: Kaotik sistemin parametreleri, başlangıç değerleri ve kesir dereceleri q_1, q_2, q_3
Output: Test edilmiş rastgele bitler
1: Başlat
2: Kaotik sisteme ait sistem parametrelerinin, başlangıç koşullarının ve q_1, q_2, q_3 kesir dereceleri girilmesi
3: LSB 's = 16' bit seç;
while *minimum 1 MBit veri* **do**
  a: İlgili kaotik sistemi GL yöntemi ile çöz;
  b: Her bir faz için kaotik işaretleri elde et (float sayı);
  c: Seçilen fazdan elde edilen kaotik işaretleri IEEE-754 standardı kullanarak 32-bit ikili sayı formatına dönüştür;
  d: Elde edilen bitlerden, s biti kadar seç ($sbitsdata = 16$ bit);
  for $i = 0$ **to** *7* **do**
    rastgelebitler(i) = sbitsdata(i) **XOR** sbitsdata($i + 8$);
  end
end
4: Elde edilen $rastgelebitler$ için NIST-800-22, FIPS 140-1 ve ENT testlerini uygula
if *test sonuçları == geçer* **then**
  Rastgeleliği ispatlanmış rastgele bit dizisi;
else
  LSB değiştirmek için 3 adıma geri dön ve işlemleri tekrar et;
end
Çıkış

Algoritma 1'de, sisteme öncelikle kaotik sistemin parametreleri, başlangıç koşulları ve kesir dereceleri q_1, q_2, q_3 girilir. Ardından, "lsb" bit değeri seçilir ve kaotik sistem çözümlenir. Bu çözümden elde edilen ve seçilen faz kullanılarak, IEEE-754 standardına göre 32 bitlik ikili sayılara dönüştürülür. Seçilen LSB bit kadarı yarıya bölünerek elde edilen iki parça, XOR işlemine tabi tutulur. Bu işlem, rastgele bitlerin oluşturulması amacıyla tekrarlanır ve elde edilen her bit, toplamda 1 milyon bit olana kadar biriktirilir. Rastgele sayı üretiminin güvenilirliğini ve kalitesini doğrulamak için 1M bitin sonunda NIST-800-22, FIPS140-1 ve ENT testleri uygulanır. Aksi takdirde, LSB biti değiştirilerek yeni rastgele bit dizileri üretilir ve testler başarılı oluncaya kadar işlemler tekrarlanır.

IKA kaotik sisteminin y fazı için ayrıklaşma işlemi sonrası elde edilen sayısal float değerler, rastgele sayı üretimi için IEEE-754 kayan noktalı sayı standarttı kullanılarak ikili sayı formatına dönüştürülmüştür. Elde edilen sayıların ikili sayı formatına dönüştürülmüş hali Tablo 3.2'de verilmiştir.

Tablo 3.2. IEEE-754 sonrası elde edilen ikili değerler (IKA y fazı)

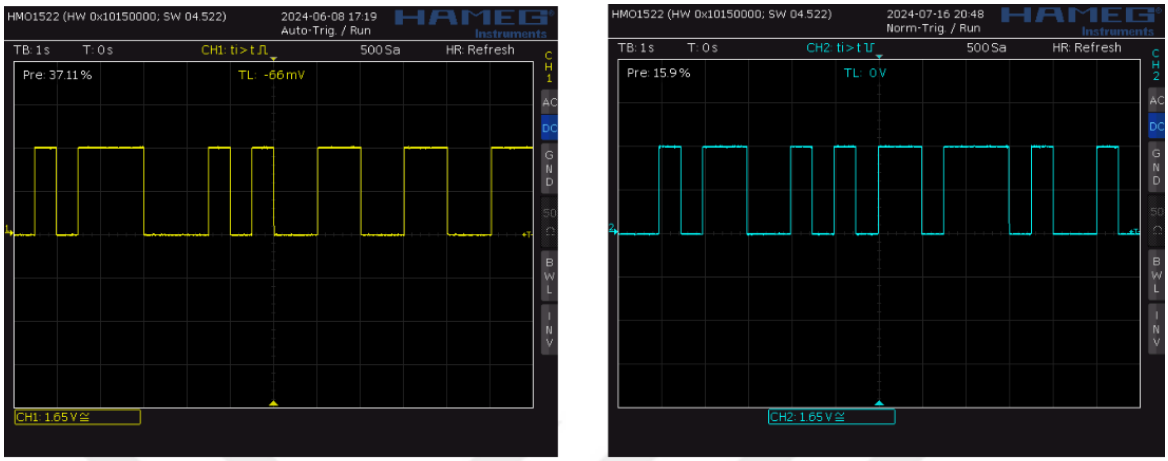
Adım Sayısı	Ayrıklaşma İşlemi Sonrası Elde Edilen Sayısal İfadeler	İkili Sayı Dönüşümü (IEEE-754)																													
		31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
1	1	0	0	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0.55	0	0	1	1	1	1	1	1	0	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	1
3	0.42618154	0	0	1	1	1	1	1	0	1	1	0	1	1	0	1	0	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	1
4	0.36218294	0	0	1	1	1	1	1	0	1	0	1	1	1	0	0	1	0	1	1	1	0	0	0	0	0	0	0	0	1	0	1	1
5	0.32136701	0	0	1	1	1	1	1	0	1	0	1	0	0	1	0	0	1	0	0	0	1	0	1	0	0	0	1	1	1	0	0	0
6	0.29237540	0	0	1	1	1	1	1	0	1	0	0	1	0	1	0	1	1	0	1	1	0	0	1	0	0	0	1	1	1	0	1	1
7	0.27038054	0	0	1	1	1	1	1	0	1	0	0	0	1	0	1	0	0	1	1	0	1	1	1	1	0	1	0	1	0	0	0	1
8	0.25293399	0	0	1	1	1	1	1	0	1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	1
9	0.23864317	0	0	1	1	1	1	1	0	0	1	1	1	0	1	0	0	0	1	0	1	1	1	1	0	1	1	1	0	0	0	0	0
10	0.22664923	0	0	1	1	1	1	1	0	0	1	1	0	1	0	0	0	0	0	0	1	0	1	1	0	1	0	1	1	1	1	0	1
11	0.21638963	0	0	1	1	1	1	1	0	0	1	0	1	1	1	0	1	1	0	0	1	0	1	0	1	0	0	1	1	1	1	1	0
12	0.20747821	0	0	1	1	1	1	1	0	0	1	0	1	0	1	0	0	0	1	1	1	0	1	0	1	0	0	1	0	1	0	1	1
13	0.19963983	0	0	1	1	1	1	1	0	0	1	0	0	1	1	0	0	0	1	1	0	1	1	1	0	0	1	1	0	0	0	1	0
14	0.19267236	0	0	1	1	1	1	1	0	0	1	0	0	0	1	0	1	0	1	0	0	1	0	1	1	1	1	1	0	0	1	1	1
15	0.18642347	0	0	1	1	1	1	1	0	0	0	1	1	1	1	1	0	1	1	1	0	0	1	0	1	1	1	0	0	1	0	1	1

Tablo 3.2 incelendiğinde 15 farklı değeri verilen 32 bitlik sayılara baktığımızda değerler 31. bit değerine yaklaştıkça aynı olmaya başlamaktadır. 0. bitlere doğru ise birbirinden bağımsız değerler elde edilmektedir. Bu doğrultuda RNG tasarımda rastgeleliğini artırmak amacıyla 0 – 16. bit aralığı seçilmiştir.

IKA kaotik sisteminin $'y'$ fazından ve IKSB kaotik sisteminin $'z'$ fazından yararlanılarak sırasıyla 20.000 ve 1.000.000 bit uzunluğunda bit dizileri oluşturulmuştur.

Şekil 3.26 (a)'da IKA kaotik sisteminin 'y' fazından, Şekil 3.26 (b)'de ise IKSB kaotik sisteminin 'z' fazından elde edilen rastgele sayıların gerçek hayatta kullanılabilirliğini

ispatlamak için Nvidia Jetson AGX Orin'in GPIO pini kullanılarak elde edilen osiloskop görüntüleri verilmiştir.



(a) (b)

Şekil 3.26. Rasgele sayıların osiloskop çıktıları; (a) IKA (b) IKSB

3.4.1. Incommensurate Kesir Dereceli Kaotik Sistemler ile Gömülü Sistem Tabanlı Tasarlanan Rastgele Sayı Üreteçlerinin İstatiksel Testleri

Incommensurate kesir dereceli kaotik sistem tabanlı üretilen rastgele sayılar, kriptografik sistemlerde ve güvenlik protokollerinde son derece kritik bir role sahiptir. Rastgele sayılar; şifreleme, anahtar oluşturma, kimlik doğrulama gibi pek çok alanda kullanılmaktadır. Ancak bilgisayar korsanları tarafından güvenlik önlemlerini aşmak, şifrelenmiş verileri çözmek veya sistemlere zarar vermek amacıyla rastgele sayı üreteçlerine saldırılar gerçekleştirilebilir. Bu nedenle, güvenliğin sağlanması ve saldırılardan korunma konusunda rastgelelik özelliklerinin istatistiksel olarak doğrulanması büyük önem taşımaktadır. Tez çalışmamızda üretilen rastgele sayıların rastgelelik özelliklerini değerlendirmek amacıyla Bölüm 2.5.3'te anlatılan NIST 800-22, FIPS 140-1 ve ENT testlerine tabi tutulmuştur. Bu bölümde IKA ve IKSB kaotik sisteminden elde edilen sayı dizilerinin test sonuçları verilmiş olup her iki sistemde ilgili testlerden başarıyla geçmiştir.

3.4.1.1. FIPS 140-1

IKA kaotik sistem tabanlı üretilen rastgele sayıların FIPS 140-1 test sonucu Tablo 3.3' te, IKSB kaotik sistem tabanlı üretilen rastgele sayıların FIPS 140-1 test sonucu ise Tablo 3.4'te verilmiştir. Bölüm 2.5.3.1'de başarı kriteri bahsedilen FIPS 140-1, dört farklı test içermektedir. Tablo 3.3 ve Tablo 3.4'te görüldüğü gibi üretilen sayı dizileri FIPS 140-1

testini başarıyla geçmiştir. Koşu testinde, çeşitli blok uzunluklarına göre farklı sonuçlar elde edilmektedir. Incommensurate kesir dereceli kaotik sistemleriyle üretilen sayı dizileri, tüm blok uzunluklar testlerinden başarıyla geçmiştir.

Tablo 3.3. IKA kaotik sistem tabanlı RSÜ'nün FIPS 140-1 test sonucu

FIPS 140-1 Testleri	Başarı Kriteri	Değerler		Sonuç
Monobit Testi	9654 < x <10346	10022		Başarılı
Poker Testi	1.03 < x < 57.4	11.15520		Başarılı
Uzun Koşu Testi	34 > Koşu	1		Başarılı
		Sürekli 0	Sürekli 1	
Koşu Testi (1)	2267 ≤ x ≤ 2733	2477	2442	Başarılı
Koşu Testi (2)	1079 ≤ x ≤ 1421	1272	1253	Başarılı
Koşu Testi (3)	502 ≤ x ≤ 748	602	684	Başarılı
Koşu Testi (4)	223 ≤ x ≤ 402	310	285	Başarılı
Koşu Testi (5)	90 ≤ x ≤ 223	161	151	Başarılı
Koşu Testi (6)	90 ≤ x ≤ 223	154	161	Başarılı

Tablo 3.4. IKSB kaotik sistem tabanlı RSÜ'nün FIPS 140-1 test sonucu

FIPS 140-1 Testleri	Başarı Kriteri	Değerler		Sonuç
Monobit Testi	9654 < x <10346	9867		Başarılı
Poker Testi	1.03 < x < 57.4	13.5871		Başarılı
Uzun Koşu Testi	34 > Koşu	1		Başarılı
		Sürekli 0	Sürekli 1	
Koşu Testi (1)	2267 ≤ x ≤ 2733	2463	2538	Başarılı
Koşu Testi (2)	1079 ≤ x ≤ 1421	1261	1234	Başarılı
Koşu Testi (3)	502 ≤ x ≤ 748	632	616	Başarılı
Koşu Testi (4)	223 ≤ x ≤ 402	321	330	Başarılı

Tablo 3.4. (devam) IKSB kaotik sistem tabanlı RSÜ'nün FIPS 140-1 test sonucu

Koşu Testi (5)	$90 \leq x \leq 223$	154	144	Başarılı
Koşu Testi (6)	$90 \leq x \leq 223$	172	141	Başarılı

3.4.1.2. NIST 800-22

NIST 800-22 testi, FIPS 140-1 testinden daha kapsamlıdır. Bazı sayı dizileri FIPS 140-1 testini geçtiği halde NIST 800-22 testini geçememektedir. Bu yüzden FIPS140-1 testine ek olarak NIST 800-22 testinin yapılması sağlıklı olacaktır. Bölüm 2.5.3.2'de açıklanan, uluslararası düzeyde en çok kabul gören NIST 800-22 testi 16 farklı test içermekte olup 1.000.000 bit dizisine ihtiyaç duymaktadır. Test sonuçlarının değerlendirilmesinde $P-$değerine bakılmaktadır. P-değeri, anlamlılık düzeyi olan α=0,001'dan büyük veya eşit olmalıdır.

NIST 800-22 test paketinde bulunan Random Excursions Testindeki x değeri $-4 \leq x \leq -1$ ve $4 \leq x \leq 1$ olmak üzere 8 farklı değer almakta ve 8 adet P-değeri üretilmektedir. Hem IKA kaotik sistemi hem de IKSB kaotik sistemi 8 farklı testi başarıyla geçmiştir. Ancak tabloda x= -4 için aldığı değer verilmiştir. Benzer şekilde Random Excursions Variant Testi $-9 \leq x \leq -1$ ve $9 \leq x \leq 1$ olmak üzere 18 adet P-değeri üretmektedir. Her iki sistemde 18 farklı değerin tümü için başarılı sonuçlar elde edilmiştir. Tabloda ise x=-9 için olan değeri verilmiştir.

Tez çalışmanızda, görüntü şifreleme ve steganografi uygulamalarında kullanılmak üzere yaklaşık olarak 4.194.304 bitlik rastgele sayı değerine ihtiyaç duyulmaktadır. Bundan dolayı her bir kaotik denklemden ayrı ayrı 1.000.000 bitlik beş ayrı rastgele bit dizisi oluşturulmuş ve teste tabi tutulmuştur. Toplamda tek bir kaotik denklemden 5.000.000 bitlik bir rastgele bit dizisi elde edilmiştir. IKA kaotik sistem tabanlı üretilen rastgele sayıların NIST 800-22 test sonucu Tablo 3.5'te, IKSB kaotik sistem tabanlı üretilen rastgele sayıların NIST 800-22 test sonucu ise Tablo 3.6'da verilmiştir.

Tablo 3.5. IKA kaotik sistem tabanlı RSÜ'nün NIST 800-22 test sonucu

İstatistiksel Testler	P Değeri					Sonuç
	1. Dizi	2. Dizi	3. Dizi	4. Dizi	5. Dizi	
Frequency (Monobit) Test	0.1603	0.2542	0.7128	0.6847	0.9553	Başarılı

Tablo 3.5. (devam) IKA kaotik sistem tabanlı RSÜ'nün NIST 800-22 test sonucu

Frequency Test within a Block	0.0104	0.5264	0.5056	0.0429	0.5645	Başarılı
Run Test	0.1001	0.7927	0.2954	0.5235	0.3492	Başarılı
Longest Run of Ones in a Block	0.5943	0.4804	0.4274	0.6871	0.1088	Başarılı
Binary Matrix Rank Test	0.6951	0.4918	0.5764	0.5024	0.4587	Başarılı
Discrete Fourier Transform (Spectral) Test	0.6009	0.5882	0.3445	0.3540	0.2401	Başarılı
Non-Overlapping Template Matching Test	0.6569	0.2972	0.7932	0.8578	0.7415	Başarılı
Overlapping Template Matching Test	0.2918	0.5771	0.0919	0.7065	0.5066	Başarılı
Maurer's Universal Statistical test	0.7811	0.4876	0.8025	0.6881	0.6452	Başarılı
Linear Complexity Test	0.7072	0.0119	0.7393	0.9496	0.2038	Başarılı
Serial test 1	0.6286	0.7338	0.2939	0.4093	0.2654	Başarılı
Serial test 2	0.5040	0.8231	0.5397	0.0819	0.4856	Başarılı
Approximate Entropy Test	0.8589	0.6958	0.5914	0.4088	0.1709	Başarılı
Cummulative Sums test	0.2876	0.4187	0.6900	0.8522	0.8986	Başarılı
Random Excursions Test(-4)	0.1944	0.8609	0.3297	0.5463	0.5809	Başarılı
Random Excursions Variant Test(-9)	0.2220	0.2965	0.1081	0.5190	0.1915	Başarılı

Tablo 3.6. IKSB kaotik sistem tabanlı RSÜ'nün NIST 800-22 test sonucu

İstatistiksel Testler	P Değeri					Sonuç
	1. Dizi	2. Dizi	3. Dizi	4. Dizi	5. Dizi	
Frequency (Monobit) Test	0.0969	0.2420	0.6642	0.6326	0.2695	Başarılı
Frequency Test within a Block	0.9241	0.5673	0.8728	0.6427	0.0533	Başarılı
Run Test	0.1312	0.5088	0.0818	0.9459	0.7018	Başarılı
Longest Run of Ones in a Block	0.7139	0.1970	0.0612	0.3508	0.2225	Başarılı
Binary Matrix Rank Test	0.1392	0.9481	0.1060	0.6588	0.6373	Başarılı
Discrete Fourier Transform (Spectral) Test	0.1715	0.2120	0.8043	0.8043	0.5029	Başarılı

Tablo 3.6. (devam) IKSB kaotik sistem tabanlı RSÜ'nün NIST 800-22 test sonucu

Non-Overlapping Template Matching Test	0.7333	0.9676	0.7532	0.6464	0.6560	Başarılı
Overlapping Template Matching Test	0.7184	0.9030	0.0410	0.6493	0.8892	Başarılı
Maurer's Universal Statistical test	0.7036	0.7877	0.6512	0.5245	0.5405	Başarılı
Linear Complexity Test	0.4720	0.5732	0.3183	0.3005	0.9141	Başarılı
Serial test 1	0.0493	0.8765	0.8026	0.8987	0.7559	Başarılı
Serial test 2	0.2881	0.7259	0.9307	0.8942	0.7244	Başarılı
Approximate Entropy Test	0.0724	0.6663	0.3882	0.0517	0.2914	Başarılı
Cummulative Sums test	0.1119	0.4004	0.6754	0.4015	0.2459	Başarılı
Random Excursions Test(-4)	0.2083	0.0807	0.7708	0.4182	0.9856	Başarılı
Random Excursions Variant Test(-9)	0.1500	0.7561	0.2472	0.5852	0.7300	Başarılı

Tablo 3.5 ve Tablo 3.6'da görüldüğü gibi üretilen rastgele bitler NIST 800-22 testinin tümünden başarıyla geçmiştir. Böylece üretilen rastgele bitlerin şifreleme ve steganografi uygulamalarında kullanıma uygun olduğu söylenebilir.

3.4.1.3. ENT

John Walker tarafından, ENT testi, rastgele sayı dizilerini değerlendirmek için geliştirilmiştir. Bölüm 2.5.3.3'te başarı kriterleri açıklanan ENT testi, dizinin rastgelelik özelliklerini belirlemek amacıyla entropi, ki-kare, aritmetik ortalama, Pi için Monte Carlo değeri ve seri korelasyon testlerini uygulamaktadır. IKA kaotik sistem tabanlı üretilen rastgele sayıların ENT test sonucu Tablo 3.7'de, IKSB kaotik sistem tabanlı üretilen rastgele sayıların ENT test sonucu ise Tablo 3.8'de verilmiştir.

Tablo 3.7. IKA kaotik sistem tabanlı RSÜ'nün ENT test sonucu

	Test Değeri	İdeal Değerler
Aritmetik Ortalama	127.6435	127.5
Entropi	7.9984	8
Korelasyon	-0.0013	0
Ki Kare	269.3811 (74.3638%)	10% - 90% arasında

Tablo 3.7. (devam) IKA kaotik sistem tabanlı RSÜ'nün ENT test sonucu

Monte Carlo sayısı	3.1425 (Hata= 0.0002)	Pi Sayısı

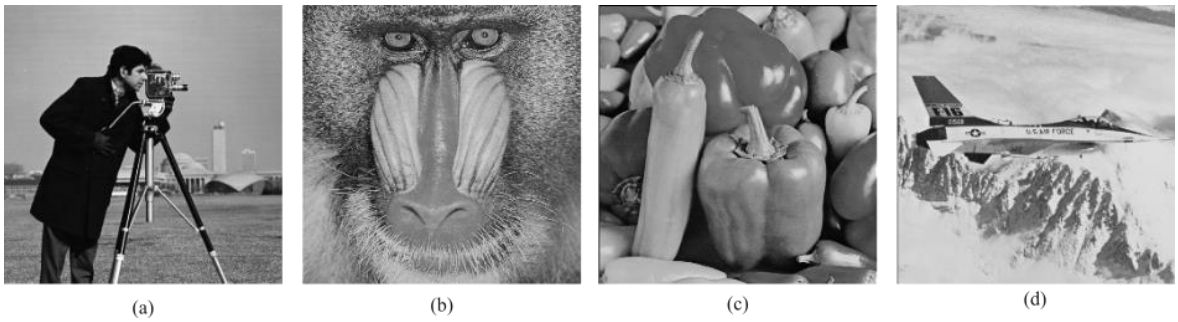
Tablo 3.8. IKSB kaotik sistem tabanlı RSÜ'nün ENT test sonucu

	Test Değeri	İdeal Değerler
Aritmetik Ortalama	127.7703	127.5
Entropi	7.9985	8
Korelasyon	-0.0012	0
Ki Kare	255.1803 (51.4959%)	10% - 90% arasında
Monte Carlo sayısı	3.1439 (Hata = 0.0007)	Pi Sayısı

Tablo 3.7 ve Tablo 3.8 incelendiğinde, elde edilen değerlerin ideal değerlere oldukça yakın olduğu gözlemlenmiştir. Bu durum, üretilen sayı dizilerinin ENT testini başarıyla geçtiğini göstermektedir. Böylece üretilen rastgele bitlerin şifreleme ve steganografi uygulamalarında kullanıma uygun olduğu söylenebilir.

3.5. Incommensurate Kesir Dereceli Sistemler ile Gömülü Sistem Tabanlı Görüntü Şifreleme Uygulaması

Tez çalışmasının bu bölümünde, rastgelelik özellikleri bir önceki bölümde doğrulanmış olan IKA ve IKSB kaotik sistemlerinden üretilen bit dizileri ile 256×256×1 boyutlarında görüntü şifreleme ve analiz süreci gerçekleştirilmiştir. Tez kapsamında kullanılan, cameraman.pgm, 4.2.03.pgm(mandrill.pgm), peppers.pgm ve 4.2.05.pgm (plane.pgm) görüntüler, Şekil 3.27'de sunulmuş olup, bu görüntüler CVG-UGR veri tabanından temin edilmiştir (*CVG-UGR Image database*, 2023).



Şekil 3.27. Tez kapsamında şifreleme amaçlı kullanılan görüntüler

Görüntü şifreleme-şifre çözme ve analizine ait tüm süreçler Python programlama dili kullanılarak Nvidia Jetson AGX Orin gömülü sistem üzerinde ve Jupyter programlama ortamında yürütülmüştür. Tez kapsamında önerilen görüntü şifreleme algoritmasına ait sözde kod Algoritma 2'de verilmiştir.

Algoritma 2: Şifreleme Algoritmasına ait Sözde Kod

Giriş : Test edilmiş rastgele bit dizisi ve görüntü
Çıkış : Şifrelenmiş görüntü
1: Başlat
2: Üretilen rastgele bit dizisini (*RBD*) ve görüntü verisini gir
3: Görüntünün boyutlarını al ($w = 256, h = 256$)
4: Görüntüyü gri tonlamaya dönüştür
5: Görüntüyü $w.h$ boyutuna yeniden boyutlandır
6: $t \leftarrow 0$
for $i = 0$ **to** $w.h$ **do**
  $ORS(i) = \text{bintodec}(RBD(t \rightarrow t + 8))$
  $t = t + 8$
end
7: Ondalık diziyi (*ORS*) küçükten büyüğe sırala ve indeksleri al (*idxN*)
idxN = argsort(*ORS*)
8: for $i = 0$ **to** $w.h$ **do**
  $KGP(i) = GP(idxN(i))$
end
9: for $i = 0$ **to** $w.h$ **do**
  $ŞGP(i) = KGP(i) \oplus ORS(i)$
end
10: Şifrelenmiş görüntüyü $w \times h$ boyutuna yeniden boyutlandır
şifrelenmişgörüntü = *ŞGP*.reshape((*w*, *h*))
Çıkış

Görüntü şifreleme algoritması, test edilmiş rastgele bit dizisi ve bir görüntü kullanarak görüntüyü şifrelemeyi amaçlamaktadır. İşlem, rastgele bit dizisinin *(RBD)* ve görüntü verisinin sisteme girilmesiyle başlar. Görüntünün genişlik *(w)* ve yükseklik *(h)* boyutları alınarak görüntü gri tonlamaya dönüştürülür. Rastgele bit dizisi sekizer sekizer alınarak binary sayılar ondalık sayılara dönüştürülür. Bu işlemde "*bintodec*" fonksiyonu kullanılarak elde edilen ondalık rastgele sayılar *(ORS)* oluşturulur. Ardından, bu ondalık rastgele sayılar *(ORS)* küçükten büyüğe sıralanarak ve indeks numaraları elde edilir *(idxN)*. Bu indeks değerleri kullanılarak karıştırma işlemi gerçekleştirilir. Karıştırılmış görüntü piksellerini (*KGP),* görüntü piksellerini *(GP)* temsil etmektedir. Karıştırma adımı, şifreli metne eklenen "gürültü" gibidir. Bu gürültü, düz metindeki desenlerin şifreli metinde görülmesini engeller ve saldırganların şifreli metni analiz etmelerini zorlaştırmaktadır. Karıştırılmış görüntü pikselleri *(KGP)* ve ondalık rastgele sayılar *(ORS), XOR* işlemine tabi tutularak şifrelenmiş görüntü pikselleri *(ŞGP)* elde edilmektedir. Son olarak, şifrelenmiş görüntü pikselleri *(ŞGP), w×h* boyutuna yeniden boyutlandırılarak şifrelenmiş görüntü elde edilir.

Çözme işlemi ise şifreleme işleminin tersi olarak yapılmaktadır. Görüntü şifre çözme algoritmasına ait sözde kod ise Algoritma 3'te verilmiştir.

Algoritma 3: Şifre Çözme Algoritmasına ait Sözde Kod

Giriş : Test edilmiş rastgele bit dizisi ve şifrelenmiş görüntü
Çıkış : Şifresi çözülmüş görüntü
1: BAŞLAT
2: Rastgele bit dizisini (*RBD*) ve şifrelenmiş görüntü piksellerini (*ŞGP*) al
3: Görüntünün boyutlarını al ($w = 256, h = 256$)
4: Şifrelenmiş görüntüyü $w.h$ boyutuna yeniden boyutlandır
5: $t \leftarrow 0$
for $i = 0$ **to** $w.h$ **do**
  $ORS(i) = \text{bintodec}(RBD(t \rightarrow t + 8))$
  $t = t + 8$
end
6: Ondalık diziyi sırala (*ORS*) ve indeksleri al (*idxN*)
idxN = argsort(*ORS*)
7: for $i = 0$ **to** $w.h$ **do**
  $KGP(i) = ŞGP(i) \oplus ORS(i)$
end
8: for $i = 0$ **to** $w.h$ **do**
  $ÇGP(idxN(i)) = KGP(i)$
end
9: Çözülmüş görüntüyü $w \times h$ boyutuna yeniden boyutlandır
çözülmüşgörüntü = *ÇGP*.reshape((w, h))
ÇIKIŞ

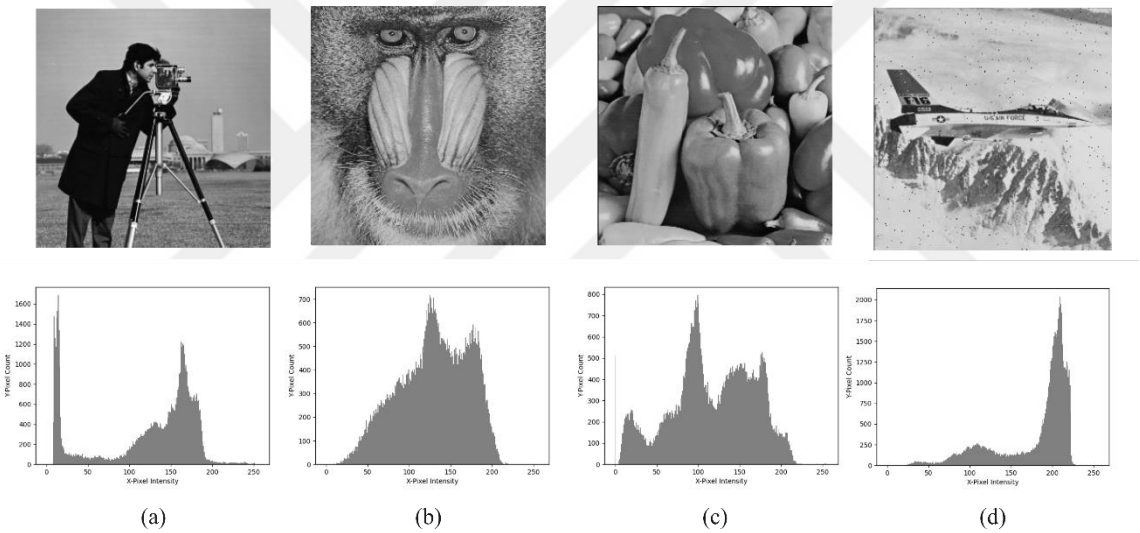
Görüntü şifre çözme algoritması, test edilmiş rastgele bit dizisi ve şifrelenmiş görüntüyü kullanarak orijinal görüntüyü geri kazanmayı amaçlamaktadır. Algoritma, rastgele bit dizisi *(RBD)* ve şifrelenmiş görüntü piksellerini *(ŞGP)* alarak başlar. Görüntünün genişlik *(w)* ve yükseklik *(h)* boyutları alınarak, Şifrelenmiş görüntü *(w.h)* boyutuna yeniden boyutlandırılır ve tek düze hale getirilir. Rastgele bit dizisi sekizer sekizer alınarak binary sayılar ondalık sayılara dönüştürülür. Bu işlemde *"bintodec"* fonksiyonu kullanılarak elde edilen ondalık rastgele sayılar *(ORS)* oluşturulur. Ardından, bu ondalık dizin *(ORS)* küçükten büyüğe sıralanarak indeks numaraları *(idxN)* elde edilir. Şifrelenmiş görüntü pikselleri *(ŞGP)* ve ondalık rastgele sayılar *(ORS) XOR* işlemine tabi tutularak karıştırılmış görüntü pikselleri *(KGP)* elde edilir. Daha sonra, elde edilen indeks değerleri *(idxN)* kullanılarak karıştırma işleminin tersi yapılarak *(ÇGP)* çözülmüş görüntü pikselleri elde edilir. Son olarak, çözümlenmiş görüntü pikselleri *(ÇGP)* $w \times h$ boyutuna yeniden boyutlandırılarak orijinal görüntü elde edilir.

3.5.1. Incommensurate Kesir Dereceli Sistemler ile Gömülü Sistem Tabanlı Görüntü Şifreleme Uygulamasının Analizleri

IKA kaotik sistem ve IKSB kaotik sistem tabanlı, Algoritma 2'de verilen sözde kod kullanılarak ayrı ayrı şifreleme uygulaması Nvidia Jetson AGX Orin gömülü kartı üzerinde gerçekleştirilmiştir. İyi bir şifreleme algoritması tüm kriptanalitik, istatistiksel ve güvenlik saldırılarına karşı dayanıklı olmalıdır. Bu doğrultuda tez çalışmasında gerçekleştirilen analizler ayrıntılı şekilde açıklanmıştır.

3.5.1.1. Histogram Analizi

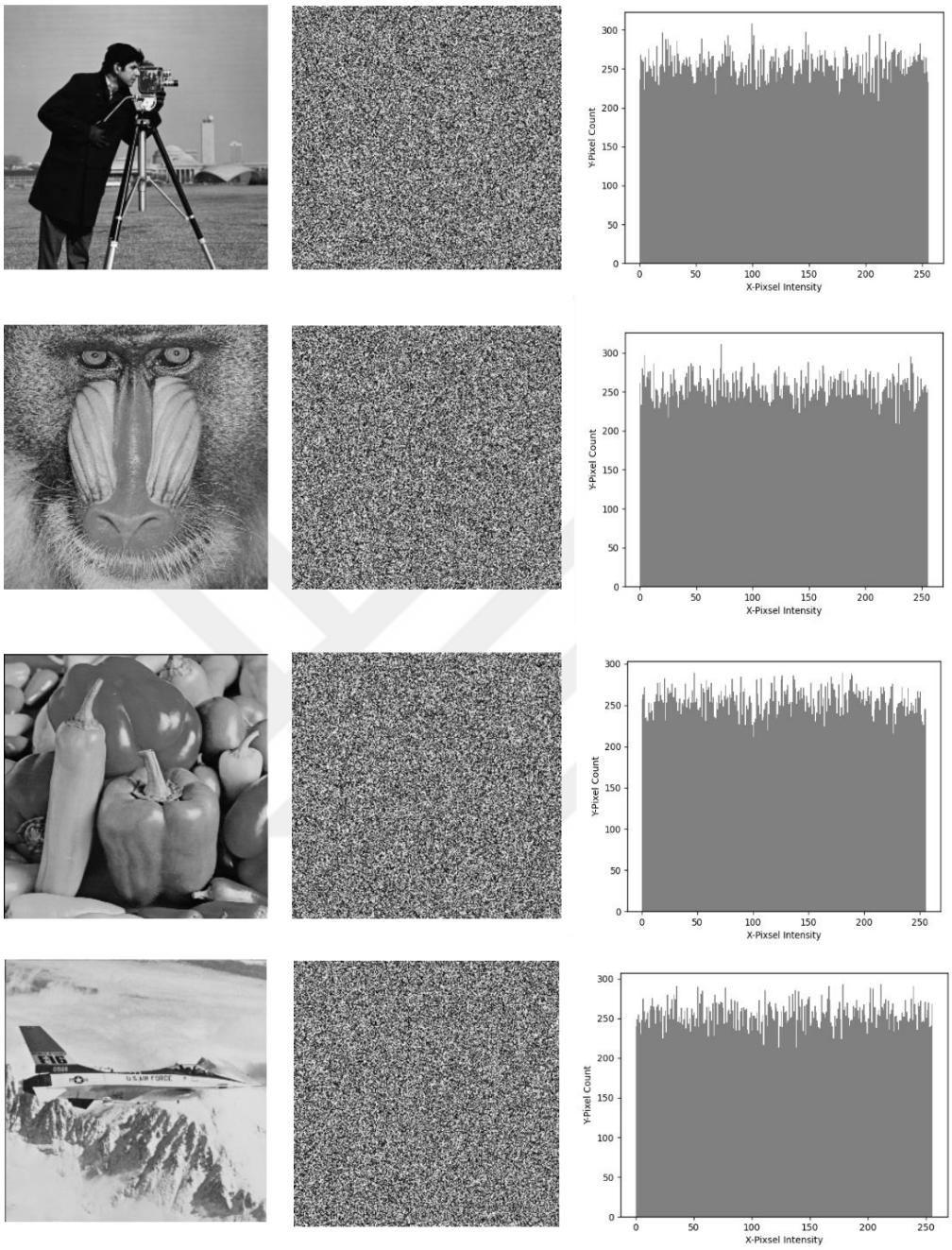
Önerilen görüntü şifreleme işleminde, güvenlik analizleri kapsamında ilk olarak histogram analizi yapılmıştır. Şekil 3.28'de orijinal görüntülerin histogram dağılımı verilmiştir.



Şekil 3.28. Orijinal görüntülerin histogram dağılımı

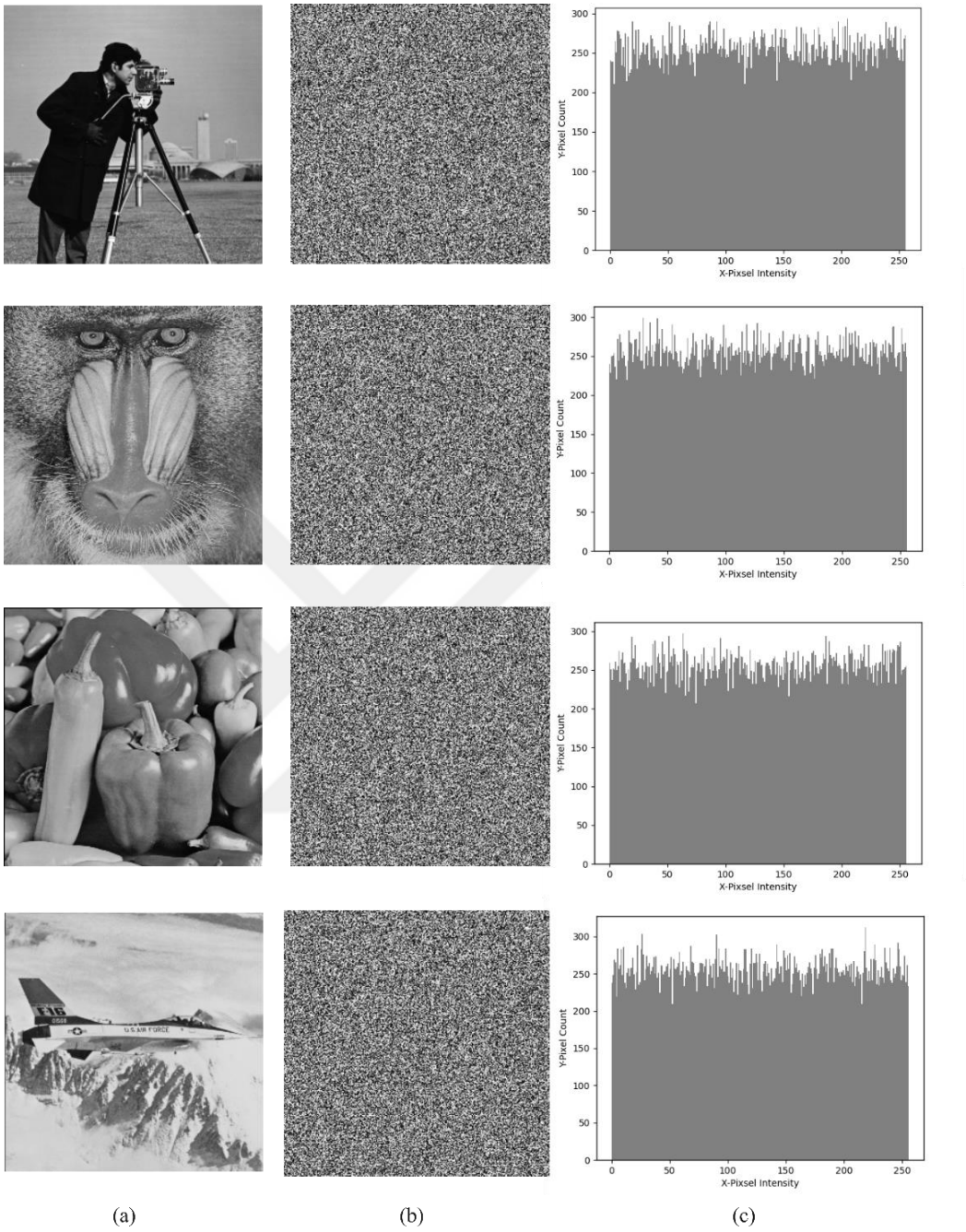
Şekil 3.28 (a) cameraman görüntüsünün, (b) mandrill görüntüsünün, (c) peppers görüntüsünün, (d) ise plane görüntüsünün orijinal histogramını ifade etmektedir. Bu görüntülerin histogram dağılımı incelendiğinde görüntülerin genel tonal yapısı ve piksel yoğunluklarının dağılımının belirli bölgelerde yoğunlaştığı görülmektedir.

Şekil 3.29'un (a) kısmında orijinal görüntüler sunulmakta, (b) kısmında IKA kaotik sistem tabanlı şifrelenmiş görüntüler gösterilmekte ve (c) kısmında ise bu şifrelenmiş görüntülerin histogram dağılımları verilmektedir. Benzer şekilde, Şekil 3.30'un (a) kısmında orijinal görüntüler, (b) kısmında IKSB kaotik sistem tabanlı şifrelenmiş görüntüler, (c) kısmında ise bu şifrelenmiş görüntülerin histogram dağılımları gösterilmektedir.



(a) (b) (c)

Şekil 3.29. IKA kaotik sistem tabanlı şifreli görüntüler ve histogram dağılımı



Şekil 3.30. IKSB kaotik sistem tabanlı şifreli görüntüler ve histogram dağılımı

Şekil 3.29 ve Şekil 3.30 incelendiğinde şifreli görüntülerin histogram dağılımının tek düze bir dağılım sergilediği görülmektedir. Bu durum kripto analizcilerin şifreli verileri çözmesini zorlaştıracaktır. Ayrıca tez çalışmasında, şifreleme işleminin neden olduğu tekdüzeliği doğrulamak amacıyla Denklem 2.30 ve Denklem 2.31'de verilen formüller kullanılarak $variance(var)$ ve $\chi 2$ testleri gerçekleştirilmiştir. Elde edilen sonuçlar Tablo 3.9'da sunulmuştur.

Tablo 3.9. Elde edilen variance ve $\chi 2$ test sonuçları

Görüntü	Orijinal Görüntü Varyans	IKA Kaotik Sistem Tabanlı Şifreli Görüntü Varyans	IKSB Kaotik Sistem Tabanlı Şifreli Görüntü Varyans	Orijinal Görüntü $\chi 2$	IKA Kaotik Sistem Tabanlı Şifreli Görüntü $\chi 2$	IKSB Kaotik Sistem Tabanlı Şifreli Görüntü $\chi 2$
cameraman	110973.3046	285.3203	281.3125	110717.3046	283.2539	280.3125
mandrill	47799.0546	264.2812	256.6796	47543.0546	264.2656	256.4882
peppers	36379.1328	233.7343	254.6406	36123.1328	233.3437	254.6367
plane	182207.9140	233.6875	274.9140	181951.9140	233.125	272.8476

255 serbestlik derecesi ve %5 kritik seviye düzeyinde $\chi 2$ testinin ideal değeri $\chi 2\,(255{,}0{,}05) = 293.2478$ dir. Ayrıca, daha düşük bir varyans değeri, şifrelenmiş görüntülerin daha fazla homojenlik gösterdiği anlamına gelir (X.-Y. Wang et al., 2015). Tablo 3.9'da verilen sonuçlara göre, tüm test görüntülerinden elde edilen $\chi 2$ değeri 293.2478'den küçüktür. Bu durum şifreleme işlemlerinin orijinal görüntülerin piksel yoğunluk dağılımını önemli ölçüde değiştirdiğini ve daha homojen bir dağılım olduğu göstermektedir.

3.5.1.2. Korelasyon Analizi

Bölüm 2.6.1.2'de detaylı olarak anlatılan korelasyon analizi görüntünün pikselleri arasındaki ilişkiyi değerlendirmek amacıyla kullanılmaktadır. Denklem 2.32'de verilen formülle korelasyon katsayıları hesaplanmaktadır. Orijinal ve şifrelenmiş görüntülerin yatay, dikey ve köşegen komşu pikseller arasındaki korelasyon katsayıları Tablo 3.10'da verilmiştir.

Tablo 3.10. Orijinal ve Şifreli görüntülerin yatay, dikey, köşegen korelasyon katsayıları

Görüntü	Yön	Orijinal Görüntü	IKA Kaotik Sistem Tabanlı Şifreli Görüntü	IKSB Kaotik Sistem Tabanlı Şifreli Görüntü
cameraman	Yatay	0.9615	-0.0029	-0.0152
	Dikey	0.9366	0.0108	-7.97×10^{-5}
	Köşegen	0.9150	0.0040	0.0067

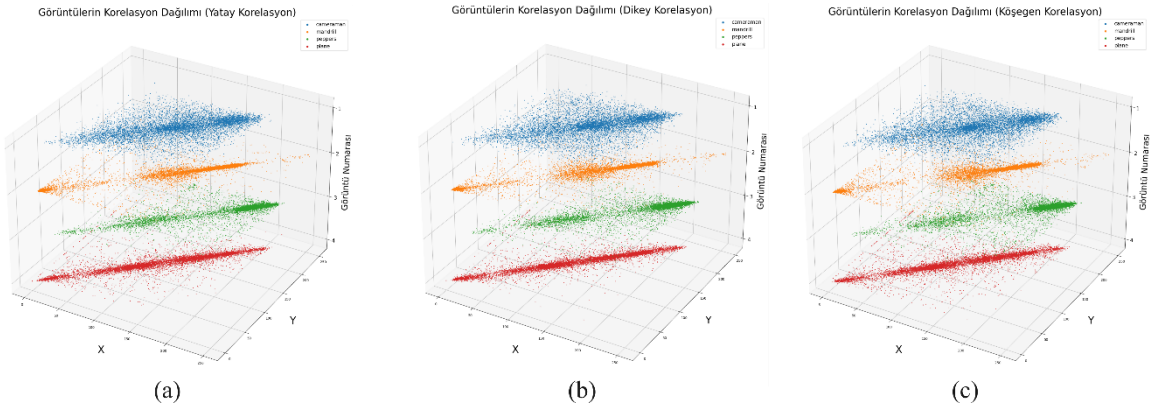
Tablo 3.10. (devam) Orijinal ve Şifreli görüntülerin yatay, dikey, köşegen korelasyon katsayıları

mandrill	Yatay	0.6449	0.0050	-0.0073
	Dikey	0.7304	-0.0026	0.0111
	Köşegen	0.6293	-9.51×10^{-5}	-0.0126
peppers	Yatay	0.9445	-0.0030	0.0165
	Dikey	0.9414	0.0333	-0.0156
	Köşegen	0.8982	-0.0057	0.0024
plane	Yatay	0.9119	0.0147	0.0063
	Dikey	0.9105	0.0081	0.0158
	Köşegen	0.8501	-0.0012	0.0051

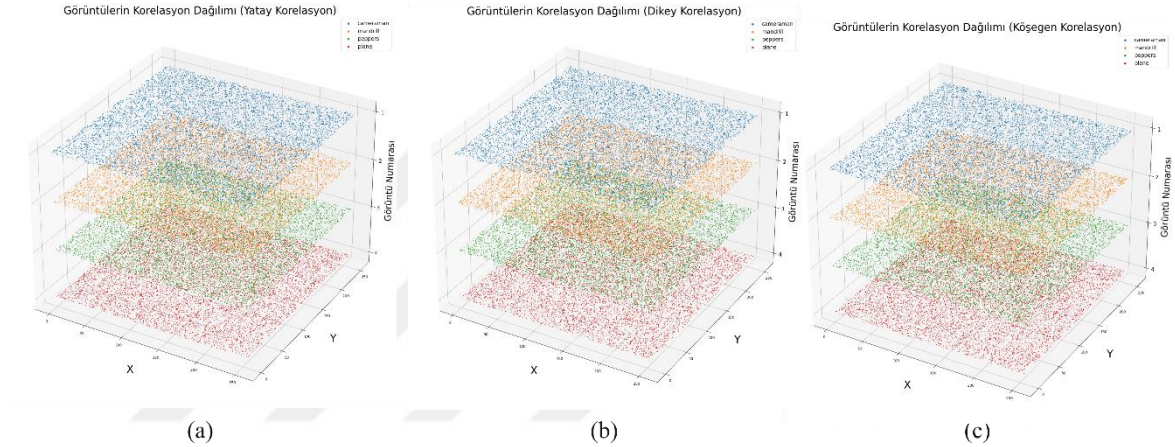
Tablo 3.10'da elde edilen sonuçlar incelendiğinde şifreleme öncesi komşu pikseller arasında yüksek korelasyonun olduğu görülmektedir. Şifreleme işlemi sonrasında ise elde edilen korelasyon değerinin ideal sıfır değerine çok yaklaştığı ve pikseller arasındaki yüksek korelasyonu etkili bir şekilde azaldığı görülmektedir.

Orijinal görüntünün yatay, dikey ve köşegen yönlerde 10000 bitişik pikseller arasındaki 3 boyutlu korelasyon dağılımı Şekil 3.31'de verilmektedir. IKA ve IKSB kaotik sistem tabanlı şifrelenen görüntülere ait yatay, dikey ve köşegen yönlerde 10000 bitişik pikseller arasındaki 3 boyutlu korelasyon dağılımı ise sırasıyla Şekil 3.32 ve Şekil 3.33'te verilmektedir.

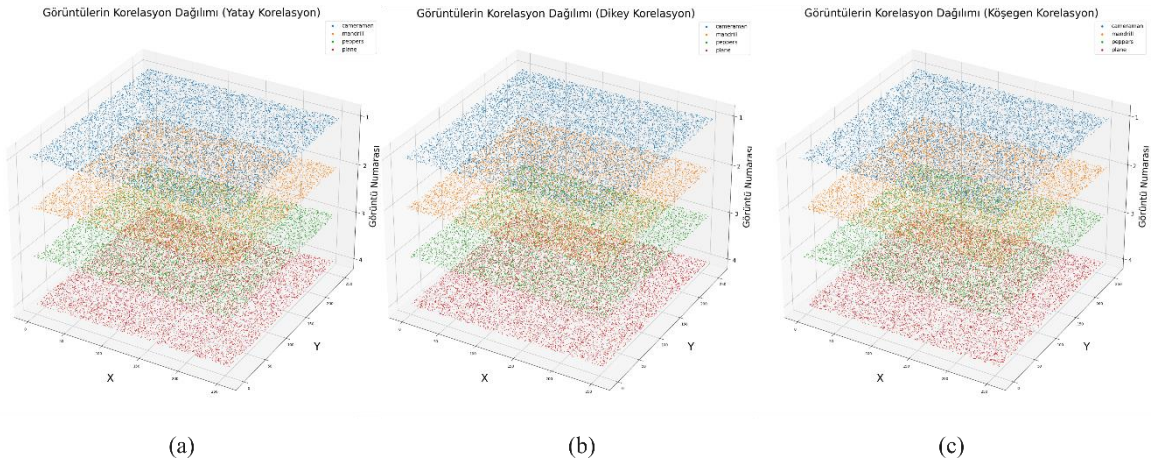
Bu şekillerden de anlaşılabileceği gibi orijinal görüntülerdeki korelasyonun, IKA tabanlı şifreleme ve IKSB tabanlı şifreleme sonrasında azaldığı ve dengeli bir dağılım oluşturduğu gözlemlenmektedir.



Şekil 3.31. Orijinal görüntünün korelasyonu; (a) Yatay (b) Dikey (c) Köşegen



Şekil 3.32. IKA şifreli görüntü korelasyonu: (a) Yatay; (b) Dikey; (c) Köşegen



Şekil 3.33. IKSB şifreli görüntü korelasyonu: (a) Yatay; (b) Dikey; (c) Köşegen

3.5.1.3. Diferansiyel Atak Analizi

Önerilen görüntü şifreleme işleminde, güvenlik analizleri kapsamında yapılan diğer bir analiz ise diferansiyel atak analizidir. Bölüm 2.6.1.3'te ayrıntısı bahsedilen analiz türünde NPCR ve UACI değerleri hesaplanmaktadır. Test görüntülerine ait NPCR ve UACI analiz sonuçları Tablo 3.11'de verilmiştir.

Tablo 3.11. Şifrelenmiş görüntülerin NPCR ve UACI sonuçları

	IKA Kaotik Sistem Tabanlı Şifreli Görüntü		IKSB Kaotik Sistem Tabanlı Şifreli Görüntü	
	NPCR%	UACI%	NPCR%	UACI%
cameraman	99.6078	33.4079	99.6398	33.4012
mandrill	99.6170	33.4818	99.6505	33.4369
peppers	99.6109	33.2283	99.6276	33.5976
plane	99.6047	33.5486	99.6093	33.3188

Literatürde ideal NPCR ve UACI değerleri, sırasıyla >99% ve ≈33% değeri başarı kriteri olarak kabul edilmektedir (M. Khan et al., 2019). Elde edilen analiz sonuçlarına göre NPCR ve UACI değerlerinin başarı kriterine çok yakın olduğu görülmektedir. Bu durum ise önerilen yöntemin diferansiyel saldırılara karşı dayanıklı olduğunu göstermektedir.

3.5.1.4. Bilgi Entropi Analizi

Bilgi entropi analizi, test görüntüsündeki bilgi içeriğinin rastgeleliğini ölçen bir ölçüt olup Denklem 2.36'da verilen formül ile hesaplanmaktadır. Tablo 3.12'de, önerilen şifreleme yöntemi sonucu elde edilen, görüntülerin entropi değeri verilmiştir.

Tablo 3.12. Bilgi Entropi değerleri

Görüntü	Orijinal Görüntü	IKA Kaotik Sistem Tabanlı Şifreli Görüntü	IKSB Kaotik Sistem Tabanlı Şifreli Görüntü
cameraman	7.0097	7.9968	7.9968

Tablo 3.12. (devam) Bilgi Entropi değerleri

mandrill	7.3384	7.9970	7.9971
peppers	7.5251	7.9974	7.9971
plane	6.6743	7.9974	7.9969

Şifrelenmiş görüntülerde ideal entropi değeri 8 olarak kabul edilmektedir (Zhou ve ark., 2015). Sonuçlar incelendiğinde, şifrelenmiş görüntülerin entropi değerleri ideal değere çok yakın olduğunu görülmektedir. Önerilen şifreleme algoritmasıyla şifrelenen görüntülerin yüksek düzeyde rastgelelik sergilediği ispatlanmıştır.

3.5.1.5. MSE-PSNR

Önerilen algoritmanın etkinliğini değerlendirmek amacıyla Denklem 2.37 ve Denklem 2.38'de verilen formüller kullanılarak MSE ve PSNR analizleri gerçekleştirilmiştir. Benzer görüntüler için, PSNR değeri sonsuz, MSE değeri ise sıfırdır. Bu durum iki görüntünün birbirine tamamen eşdeğer olduğunu, yani aralarında hiçbir fark bulunmadığını göstermektedir. Tablo 3.13'te elde edilen PSNR ve MSE değerleri verilmiştir.

Tablo 3.13. PSNR ve MSE değerleri

Görsel	Orijinal- Şifresi Çözülmüş Görsel		Orijinal- Şifreli Görsel			
			IKA Kaotik Sistem Tabanlı		IKSB Kaotik Sistem Tabanlı	
	PSNR	MSE	PSNR	MSE	PSNR	MSE
cameraman	∞	0	8.3491	9.5097×10^3	9.5162	7.2686×10^3
mandrill	∞	0	9.5558	7.2027×10^3	8.3731	9.4572×10^3
peppers	∞	0	9.0306	8.1285×10^3	8.9769	8.2297×10^3
plane	∞	0	8.0625	10.1583×10^3	8.0502	10.1871×10^3

Tablo 3.13'te görüldüğü gibi tüm orijinal ve şifresi çözülmüş görüntüler arasında PSNR değeri sonsuz, MSE değeri de sıfır olarak bulunmuştur. Bu durum şifre çözme işleminin kayıpsız yapıldığını göstermektedir.

28'den büyük bir PSNR değeri için algısal kalitenin sezgisel olarak iyi kabul edilmektedir (Kaur et al., 2020). Bu duruma göre, tüm orijinal ve şifreli görüntü arasındaki PSNR değeri <28'in altında olup bu değer oldukça düşüktür. Bu durum, şifrelenmiş görüntülerin anlaşılmaz olduğunu ve görüntü hakkında hiçbir bilgi sağlamadığını göstermektedir. Ayrıca şifrelenmiş görüntülerin MSE değerleri ise çok yüksektir (10^3 mertebesinde), bu da şifrelenmiş görüntülerin orijinal görüntülerle benzer olmadığını göstermektedir.

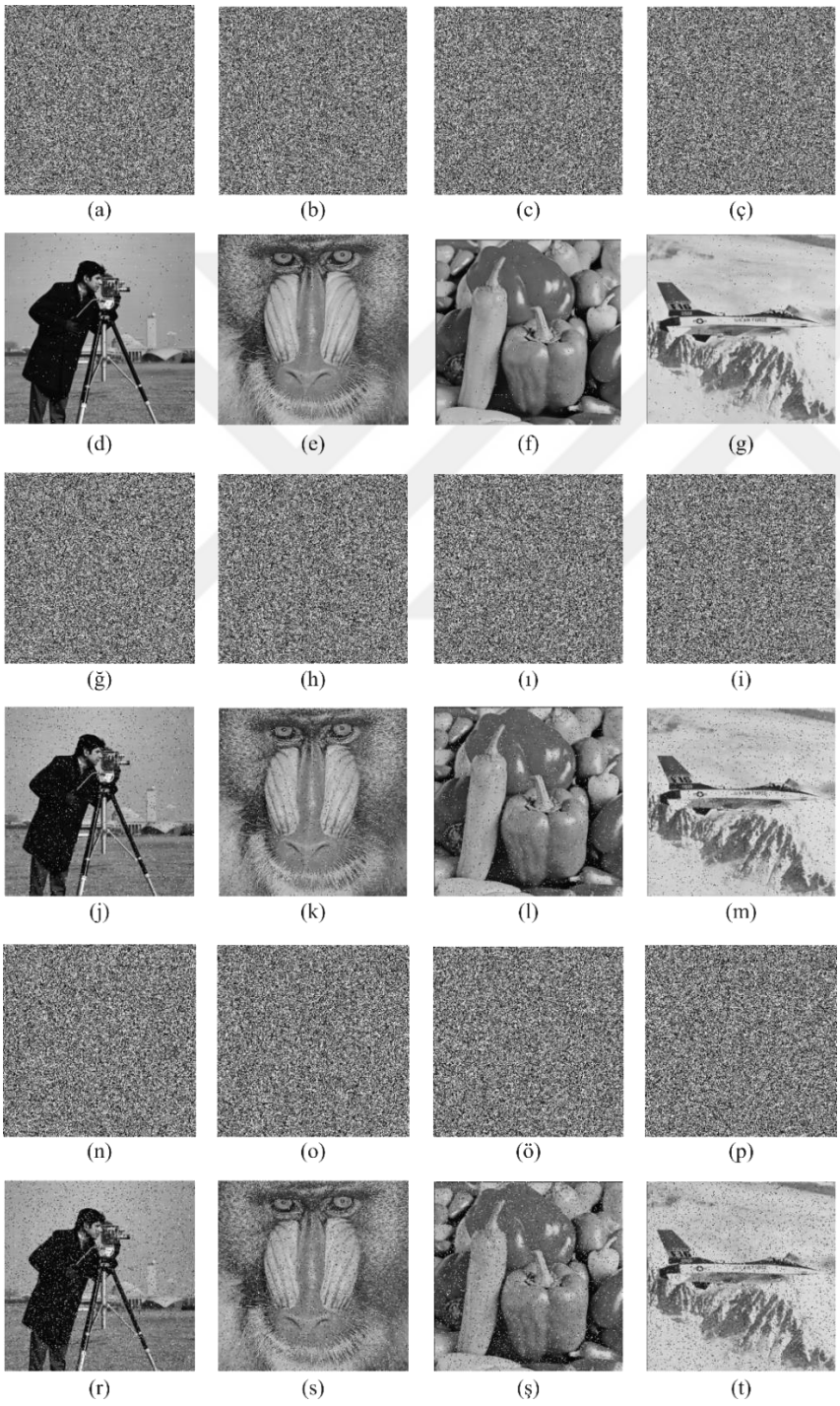
3.5.1.6. Anahtar Uzay Analizi

Anahtar alanının kaba kuvvet saldırılarını etkisiz hale getirmek için en az 2^{100} olması gerektiği önerilmektedir. Tez çalışmasında önerilen IKA kaotik sisteminin anahtar uzayı, $q_1, q_2, q_3, a, b, c, x(0), y(0), z(0)$ değerlerinden oluşmaktadır. IKSB kaotik sisteminin anahtar uzayı ise $q_1, q_2, q_3, \alpha, \beta, x(0), y(0), z(0)$ değerlerinden oluşmaktadır. IEEE kayan nokta standardına göre çift hassasiyetli sayıların hassasiyeti yaklaşık 10^{-15} olduğundan ("IEEE Standard for Binary Floating-Point Arithmetic," 1985) , gizli anahtarların olası değerlerinin toplamı; IKA kaotik sistemi için $(10^{15})^9 \approx 2^{449}$ ve IKSB kaotik sistemi için ise $(10^{15})^8 \approx 2^{399}$ olarak hesaplanmaktadır. Dolayısıyla, önerilen IKA kaotik sistemi tabanlı ve IKSB kaotik sistem tabanlı şifreleme algoritmasının toplam anahtar alanı 2^{100}'den çok daha büyüktür. Bu da önerilen şifreleme algoritmasının şiddetli saldırılara karşı koyabilecek kadar büyük bir anahtar alanına sahip olduğunu göstermektedir.

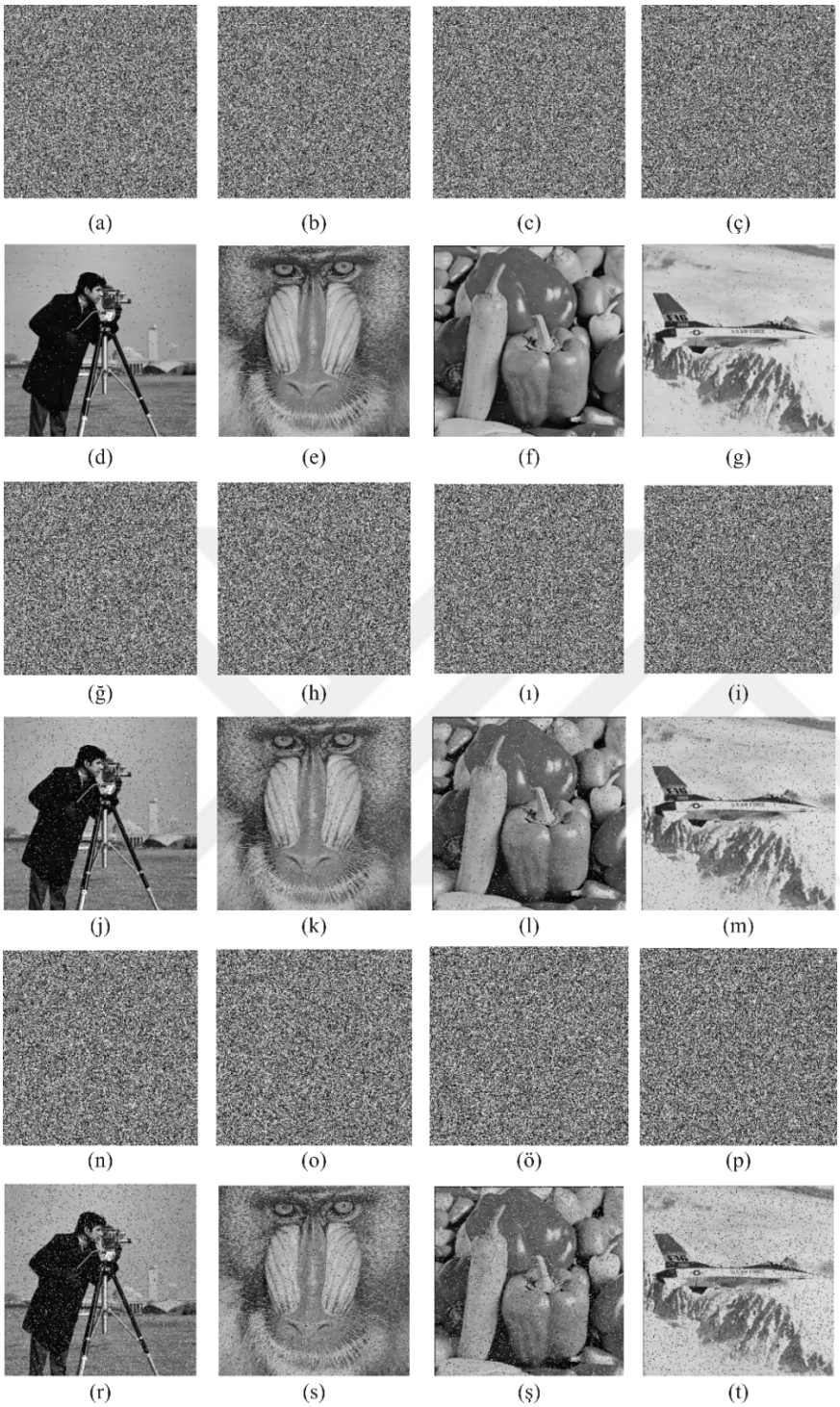
3.5.1.7. Gürültü Analizi

Şifrelenmiş görüntü ağ iletimi ve görüntü depolaması sırasında çeşitli tehditlere maruz kalır. Bir şifreleme algoritması veri kayıplarına karşı direnç gösterebilmelidir. Bu nedenle önerilen şifreleme algoritmasının gürültü saldırısını test etmek için şifrelenmiş görüntülere sırasıyla %1, %5 ve %10 oranında tuz-biber gürültüsü eklenmiş ve sonrasında önerilen şifreleme algoritması kullanılarak şifresi çözülmüştür. Şekil 3.34'te IKA Kaotik Sistem Tabanlı şifreleme yönteminin tuz-biber gürültüsüne maruz kaldıktan sonra elde edilen görüntüleri gösterilmektedir. Şekil 3.35'te ise IKSB Kaotik Sistem Tabanlı şifreleme yönteminin tuz-biber gürültüsüne maruz kaldıktan sonra elde edilen görüntüleri gösterilmektedir. Şekil 3.34 ve Şekil 3.35 serilerinde, (a-ç) %1 gürültü eklenmiş şifreli görüntüler, (d-g) %1 gürültü

eklenmiş şifreli görüntülerin şifresi çözülmüş halleri, (ğ-i) %5 gürültü eklenmiş şifreli görüntüler ve (j-m) %5 gürültü eklenmiş şifreli görüntülerin şifresi çözülmüş halleri gösterilmektedir. Ayrıca, (n-p) %10 gürültü eklenmiş şifreli görüntüler ve (r-t) %10 gürültü eklenmiş şifreli görüntülerin şifresi çözülmüş halleri yer almaktadır. Ayrıca Tablo 3.14'te gürültü saldırısı sonrası elde edilen PSNR değerleri verilmiştir.



Şekil 3.34. IKA sistem tabanlı tuz biber saldırısı ve kurtarılmış görüntüler



Şekil 3.35. IKSB sistem tabanlı tuz biber saldırısı ve kurtarılmış görüntüler

Tablo 3.14. Tuz-Biber gürültüsüne sonrası elde edilen PSNR değerleri

Görüntü	Gürültü Oranı	IKA Kaotik Sistem Tabanlı PSNR	IKSB Kaotik Sistem Tabanlı PSNR
cameraman	1%	28.4143	28.0934
	5%	21.5123	21.3569
	10%	18.3506	18.4210
mandrill	1%	29.6087	29.5441
	5%	22.3012	22.5111
	10%	19.6474	19.5695
peppers	1%	28.6161	28.7671
	5%	22.0676	21.9639
	10%	18.9509	18.9363
plane	1%	28.1813	28.0611
	5%	21.1270	21.0118
	10%	17.9588	17.9641

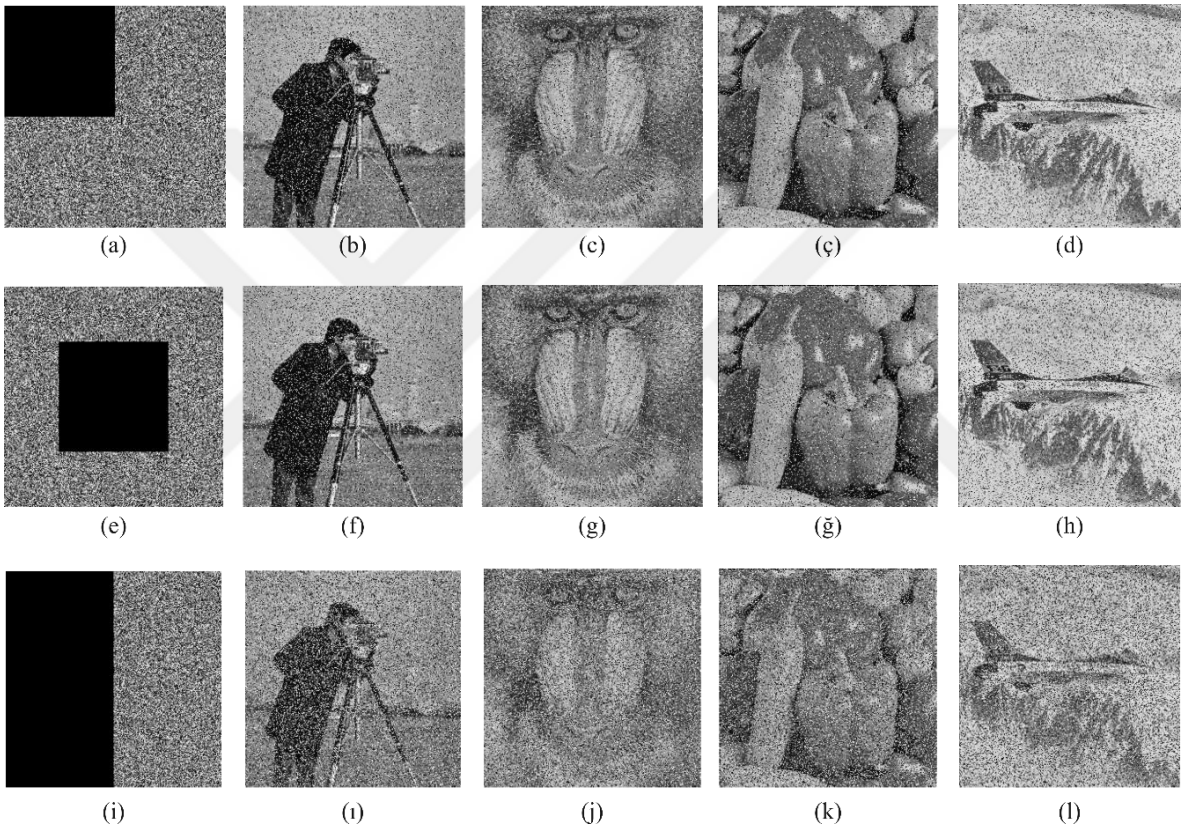
Şekil 3.34 ve Şekil 3.35 incelendiğinde %10 yoğunluğa sahip gürültüden, sonra bile çözümlenen görüntülerin görsel olarak tanımlanabilir olduğunu görülmektedir. Ayrıca IKA Kaotik Sistem Tabanlı Şifreleme Yöntemi, genellikle IKSB Kaotik Sistem Tabanlı Şifreleme yöntemine göre daha yüksek PSNR değerleri gösterdiğinden gürültüye karşı daha iyi performans sergilediği söylenebilir.

3.5.1.8. Veri Kaybı Saldırı Analizi

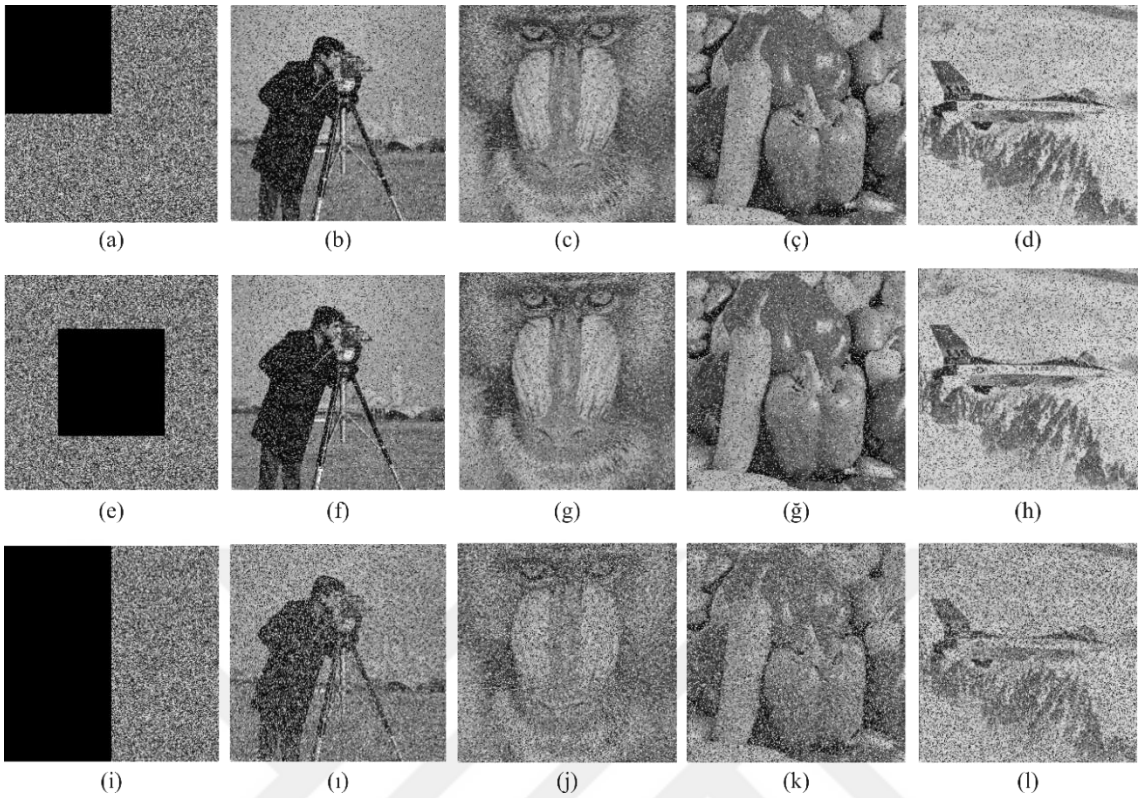
Kötü niyetli kişiler şifreleme işlemini çözebilmek amacıyla görüntü kırpmak suretiyle saldırıda bulunabilirler. Güçlü bir şifreleme algoritması, kötü niyetli kişilerin şifreli veriyi bozabileceği durumlarda bile, bu hasarın çözümlenmiş veri üzerindeki etkisini minimumda tutması gerekmektedir. Tez çalışmamızda veri kaybı saldırı analizini gerçekleştirmek amacıyla şifreli görüntüler ¼(köşe), ¼(orta) ve ½ oranlarında kırpılmıştır ve sonrasında önerilen şifreleme algoritması kullanılarak şifresi çözülmüştür. Şekil 3.36'da IKA kaotik sistem tabanlı elde edilen şifreli görüntüler üzerine uygulanan veri kaybı saldırı analizi

verilmiştir. Şekil 3.37'de ise IKSB Kaotik Sistem Tabanlı elde edilen şifreli görüntüler üzerine uygulanan veri kaybı saldırı analizi verilmiştir.

Şekil 3.36 ve Şekil 3.37 serilerinde (a) ¼ (köşe) veri kaybı ve (b-d) bu veri kaybı sonucu elde edilen görüntüler gösterilmektedir. (e) ¼ (orta) veri kaybı ve (f-h) bu veri kaybı sonucu elde edilen görüntüler sunulmaktadır. Son olarak, (i) ½ veri kaybı ve (ı-l) bu veri kaybı sonucu elde edilen görüntüler yer almaktadır. Ayrıca Tablo 3.15'te veri kaybı saldırı sonrası elde edilen PSNR değerleri verilmiştir.



Şekil 3.36. IKA sistem tabanlı veri kaybı saldırı ve kurtarılmış görüntüler



Şekil 3.37. IKSB sistem tabanlı veri kaybı saldırı ve kurtarılmış görüntüler

Tablo 3.15. Veri Kaybı saldırı sonrası elde edilen PSNR değerleri

Görüntü	Veri Kaybı Oranı	IKA Kaotik Sistem Tabanlı PSNR	IKSB Kaotik Sistem Tabanlı PSNR
cameraman	¼(köşe)	14.4578	14.3580
	¼(orta)	14.4031	14.3567
	½	11.3908	11.3472
mandrill	¼(köşe)	15.6170	15.6275
	¼(orta)	15.5714	15.5538
	½	12.5399	12.5756
peppers	¼(köşe)	15.0012	15.0662
	¼(orta)	15.0126	15.0150
	½	11.9977	12.0328

Tablo 3.15. (devam) Veri Kaybı saldırı sonrası elde edilen PSNR değerleri

plane	¼(köşe)	15.6170	14.0612
	¼(orta)	15.5714	14.0849
	½	12.5399	11.0819

Veri kaybı miktarı artıkça görüntü kalitelerinde düşüşler meydana gelmektedir. Ancak %50 kırpılmada dahi görüntü içeriği rahatlıkla anlaşılabilmektedir. Bu çalışmada önerilen algoritma, gerçek zamanlı iletim kanallarında görüntülerin sağlamlığını garanti etmektedir.

3.5.1.9. Zaman Performansı

Şifreleme süresi, bir şifreleme algoritmasının performansını ve etkinliğini değerlendirmede kritik bir faktördür. Bu ölçüt algoritmaların performansını değerlendirme, kaynak gereksinimlerini tahmin etme ve gerçek zamanlı uygulamalarda kullanılabilirliği belirleme açısından önemli bir metriktir. Görüntü şifreleme ve analizine ait tüm süreçler Python programlama dili kullanılarak 64 GB RAM kapasitesine sahip, 2.2 GHz saat hızında çalışan 12 çekirdekli Arm Cortex-A78AE CPU'ya sahip Nvidia Jetson AGX Orin gömülü sistem üzerinde ve Jupyter programlama ortamında yürütülmüştür. Şifreleme ve şifre çözme uygulamasına ait süreler Tablo 3.16'da saniye cinsinden verilmiştir.

Tablo 3.16. Şifreleme ve Şifre Çözme işlemlerine ait süreler (birim: saniye)

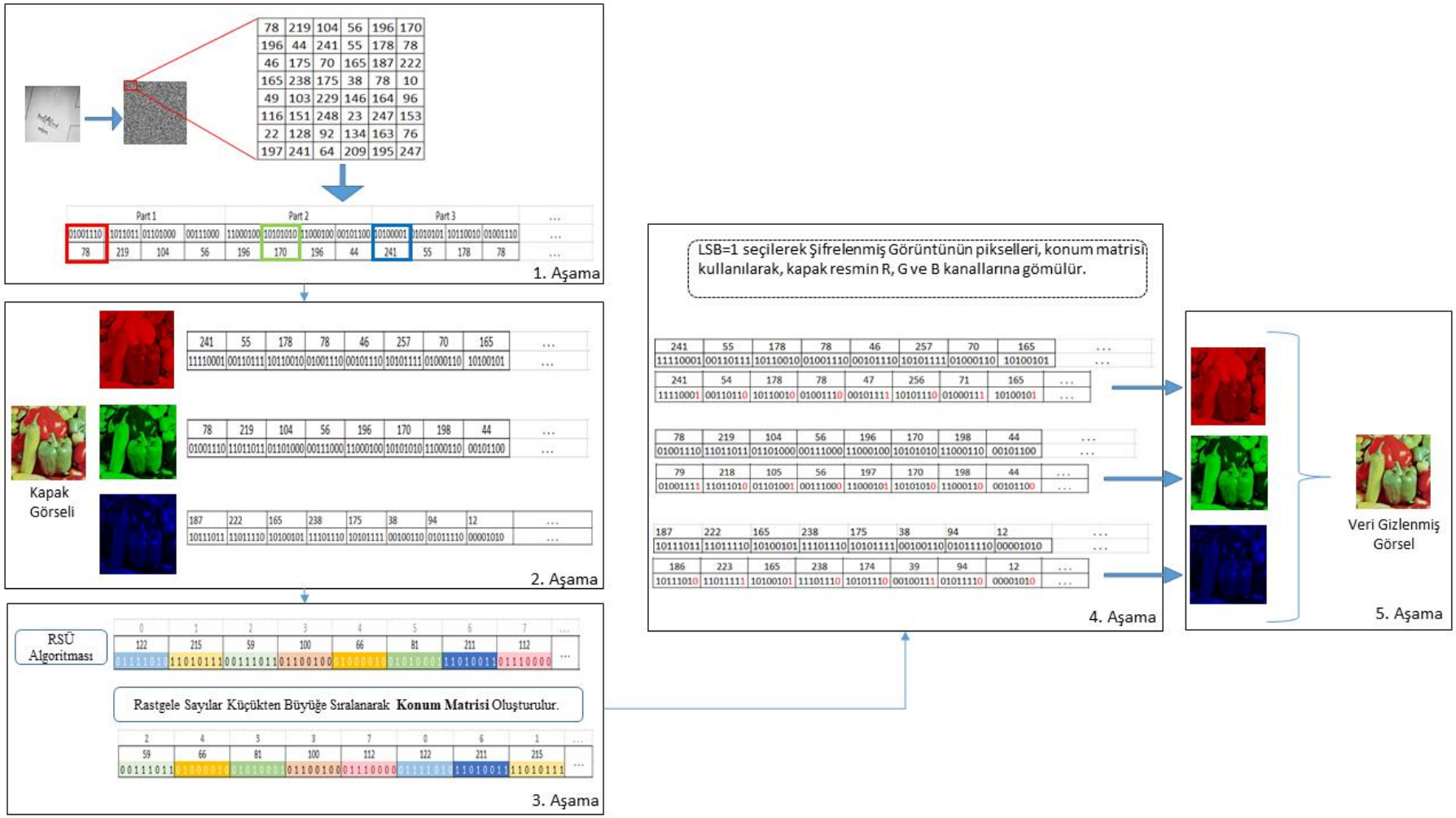
	IKA Kaotik Sistem Tabanlı		IKSB Kaotik Sistem Tabanlı	
	$t_{şifreleme}(s)$	$t_{şifreçözme}(s)$	$t_{şifreleme}(s)$	$t_{şifreçözme}(s)$
cameraman	0.0331	0.0555	0.0328	0.0548
mandrill	0.0333	0.0544	0.0332	0.0563
peppers	0.0331	0.0544	0.0330	0.0552
plane	0.0333	0.0539	0.0335	0.0540

3.6. Incommensurate Kesir Dereceli Sistemler ile Gömülü Sistem Tabanlı Görüntü Stenografi Uygulaması

Tezin bu bölümünde, IKA kaotik sistemi ve IKSB kaotik sistemi kullanılarak Nvidia Jetson AGX Orin gömülü kartı üzerinde, iki seviyeli görüntü steganografi uygulaması gerçekleştirilmiştir. Önerilen steganografi algoritmasına ait akış diyagramı Şekil 3.39'da verilmiştir.

Görüntü steganografi uygulaması için kapak görüntüsü olarak 512×512×3 pepper dosyası seçilmiştir. Gizlenecek görüntü olarak ise önceki bölümde, IKA kaotik sistem tabanlı (Şekil 3.38-b) ve IKSB (Şekil 3.38-c) kaotik sistem tabanlı şifrelenen 256×256×1 plane görüntüsü kullanılmıştır. Gizlenecek veri, 256×256×1 boyutlarında bir görüntü olduğu için, bilgi hacmi 524.288 bit (512 Kbit) olarak hesaplanmaktadır. Bu nedenle, gizlenecek verinin boyutunun oldukça büyük olduğu açıktır. Kapak ve gizlenecek görüntüye ait görseller Şekil 3.38'de verilmiştir.

Şekil 3.38. Tez kapsamında Görüntü Steganografisinde kullanılan görüntüler



Şekil 3.39. Önerilen Steganografi yöntemine ait akış diyagramı

Önerilen yöntem her bir adımında gerçekleşen işlemler aşağıda verilmiştir.

1.Aşamada gizlenecek görsel (plane), Algoritma 2'de verilen görüntü şifreleme algoritmasının sözde kodu kullanılarak gömülü sistemde şifrelenir. Şifrelenmiş görüntünün pikselleri tek boyutlu matris haline dönüştürülür. R-G-B kanallarında gizlenmek üzere üç parçaya ayrılır.

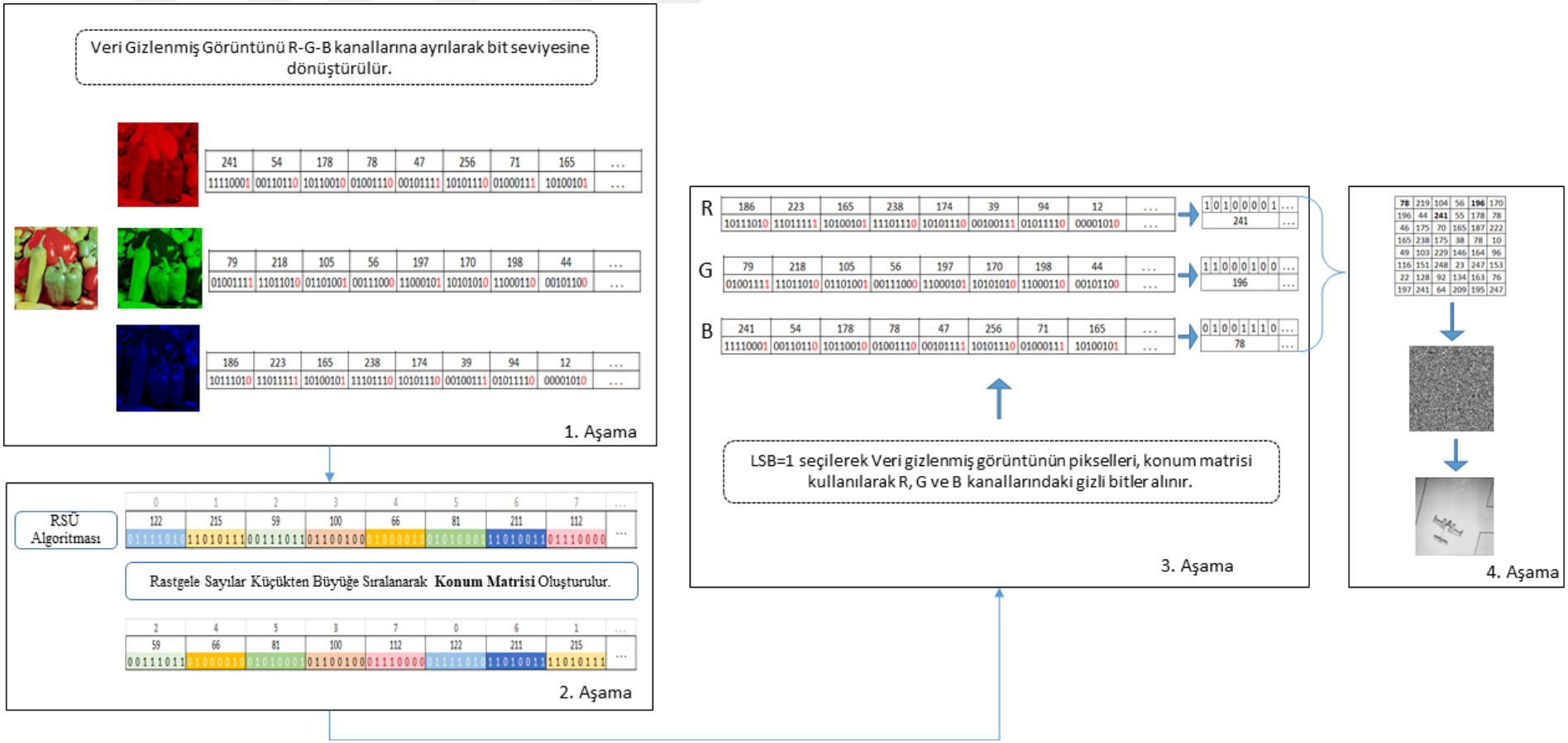
2.Aşamada kapak görseli (peppers) R-G-B kanallarına ayrılır ve her bir kanalın pikselleri tek boyutlu matris haline dönüştürülür.

3.Aşamada rastgele sayı üretecine ait Algoritma 1 kullanılarak rastgele sayı üretilir. Üretilen rastgele sayılar sekizer bit ayrılarak decimal sayılara dönüştürülür. Bu işlem, kapak görselin boyutu kadar devam eder. Elde edilen rastgele sayılar küçükten büyüğe sıralayarak konum matrisi elde edilir.

4.Aşamada, şifrelenmiş görüntü piksellerinin her parçası konum matrisi kullanılarak kapak görüntüsünün her bir R, G, B kanalına ayrı ayrı gömülür. Bu işlemde, kapak görüntüsünün her bir kanalındaki piksellerin $LSB = 1$ olacak şekilde şifrelenmiş görüntü pikselleri ile yer değiştirilir.

5.Aşamada kapak görüntüsünün her bir R, G, B kanalı birleştirilerek yeniden boyutlandırılır ve stego görüntü elde edilir.

Gizli görüntünün tekrardan elde edilme süreci ise steganografi işleminin tersten çalıştırılmasıyla elde edilmektedir. Gizli görüntünün elde edilmesini sağlayan akış diyagramı ise Şekil 3.40'ta verilmiştir.



Şekil 3.40. Gizli görüntünün elde edilmesini sağlayan yöntemin akış diyagramı

Gizli görüntünün elde edilmesini sağlayan yöntemin her bir aşamasında gerçekleşen işlemler aşağıda verilmiştir.

1.Aşamada stego görüntü, R-G-B kanallarına ayrılarak bit seviyesine dönüştürülür. Bu aşamada kapak görseli olan "peppers" resmi R-G-B kanallarına ayrılır ve her bir kanalın pikselleri tek boyutlu matris haline getirilir.

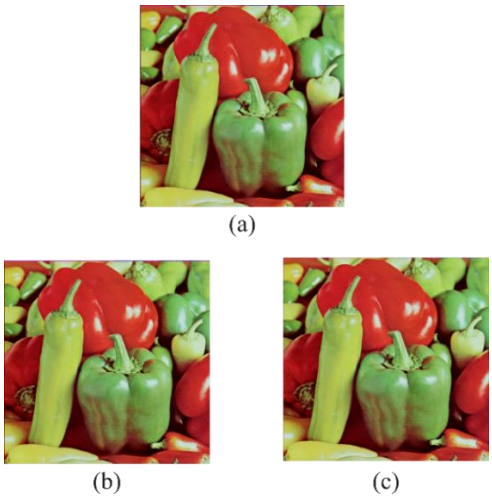
2.Aşamada, rastgele sayı üretecine ait Algoritma 1 kullanılarak rastgele sayılar üretilir. Bu rastgele sayılar, sekizer bitlik parçalara ayrılarak ondalık (decimal) sayılara dönüştürülür. Bu işlem, kapak görselinin boyutu kadar devam eder. Elde edilen rastgele sayılar küçükten büyüğe sıralanarak bir konum matrisi oluşturulur.

3.Aşamada, gizli görüntünün pikselleri, konum matrisi kullanılarak kapak görüntüsünün R, G, B kanallarından LSB=1 seçilerek gizli görüntünün her parçasının pikselleri elde edilir.

4.Aşamada ise elde edilen gizli görüntünün parçaları birleştirilir ve yeniden boyutlandırılır. Böylece, stego görüntüden geri elde edilen gizlenmiş görüntü oluşur. Gizlenmiş görüntü Algoritma 3 ile çözülerek orijinal görüntü elde edilir.

Steganografi uygulaması, iki farklı kaotik sistem tabanlı yöntem kullanılarak gerçekleştirilmiştir. IKA kaotik sistemine dayalı olarak şifrelenen orijinal görüntü ve IKA kaotik sistem tabanlı rastgele sayı üreteci kullanılarak uygulanmıştır. Benzer şekilde IKSB kaotik sistemine dayalı şifreleme kullanılarak elde edilen orijinal görüntü ve IKSB kaotik sistem tabanlı rastgele sayı üreteci kullanılarak gerçekleştirilmiştir.

Şekil 3.41'de önerilen görüntü steganografi uygulaması sonucu elde edilen stego görüntüler verilmiştir.



Şekil 3.41. Orijinal ve Stego görüntüler

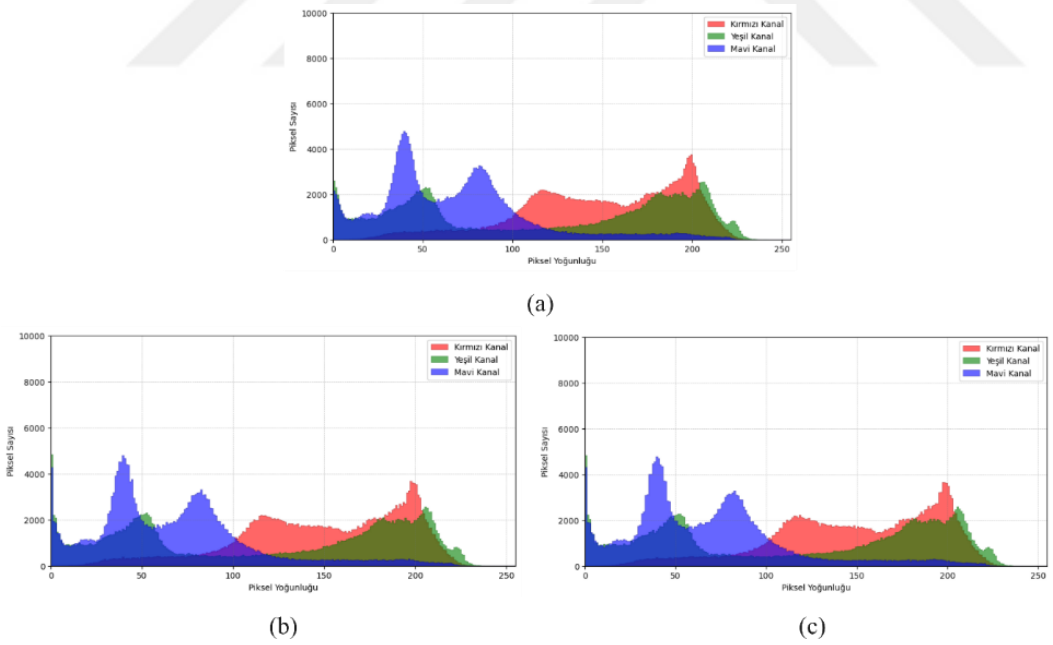
Şekil 3.41 dikkatlice incelendiğinde 3.41(a)'da bulunan orijinal görüntü ile 3.41(b)'de bulunan IKA kaotik sistem tabanlı steganografi işlemi sonrası elde edilen stego görüntü ve 3.41(c)'de bulunan IKSB kaotik sistem tabanlı steganografi işlemi sonrası elde edilen elde edilen stego görüntü arasında gözle görülebilir bir fark bulunmamaktadır. Bu durum güvenliği maksimize ederken aynı zamanda şüphe uyandırmamayı sağlamaktadır.

3.6.1. Gömülü Sistemde Kesir Dereceli Arneodo Kaotik Sistem Tabanlı Görüntü Stenografi Uygulamasının Analizleri

İyi bir steganografi yöntemi, gizli bilgiyi başarılı bir şekilde saklarken aynı zamanda bu bilginin tespit edilmesini zorlaştıran özelliklere sahip olmalıdır. Bu bölümde ise önerilen steganografi yönteminin güvenlik analizleri ele alınmıştır.

3.6.1.1. Histogram Analizi

Bir görüntüdeki piksellerin dağılımını göstermek için histogram analizi gerçekleştirilir. Tez çalışmasında orijinal ve stego görüntüde elde edilen histogram dağılımı Şekil 3.42'de verilmiştir.

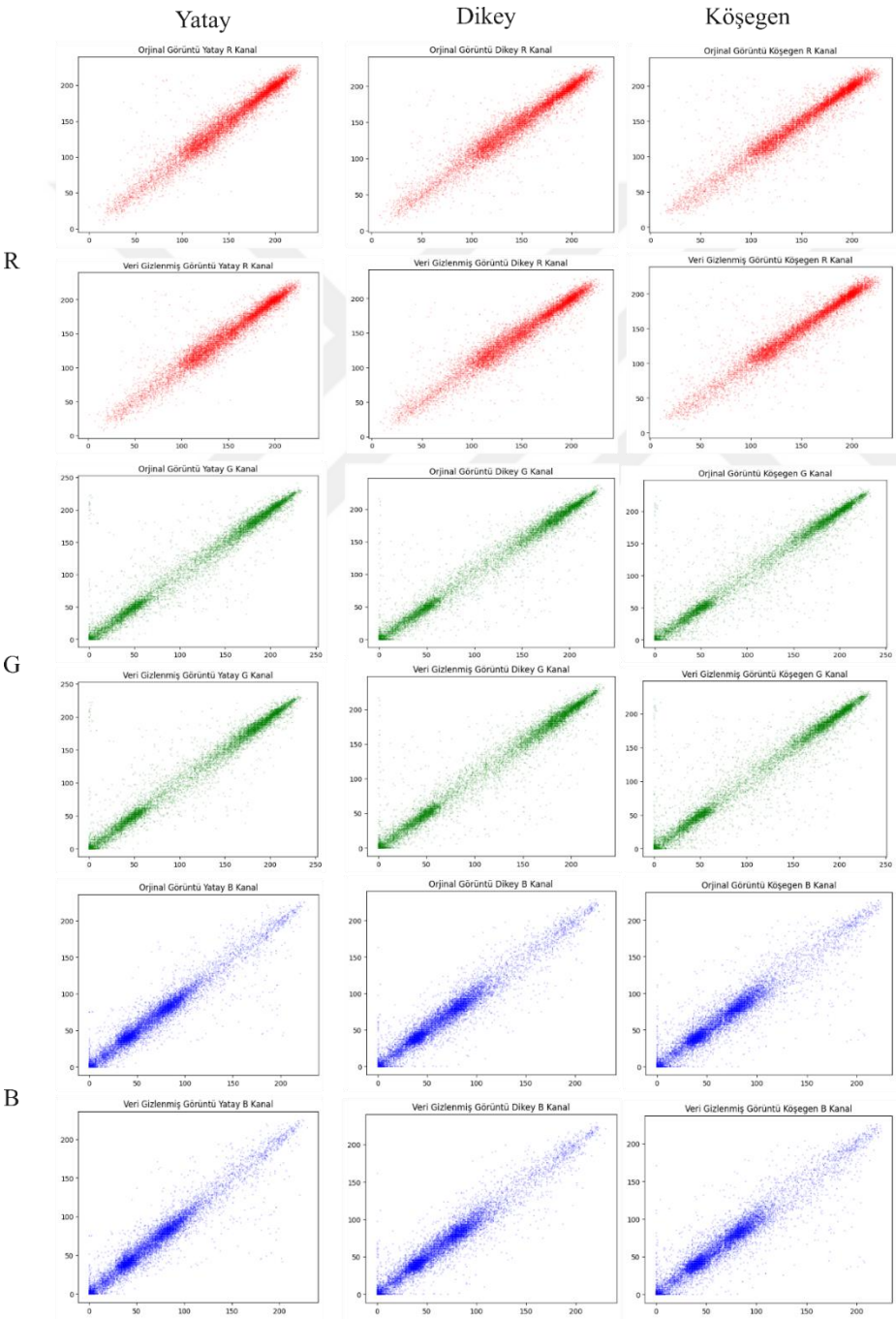


Şekil 3.42. Orijinal ve Stego görüntülerin histogramı

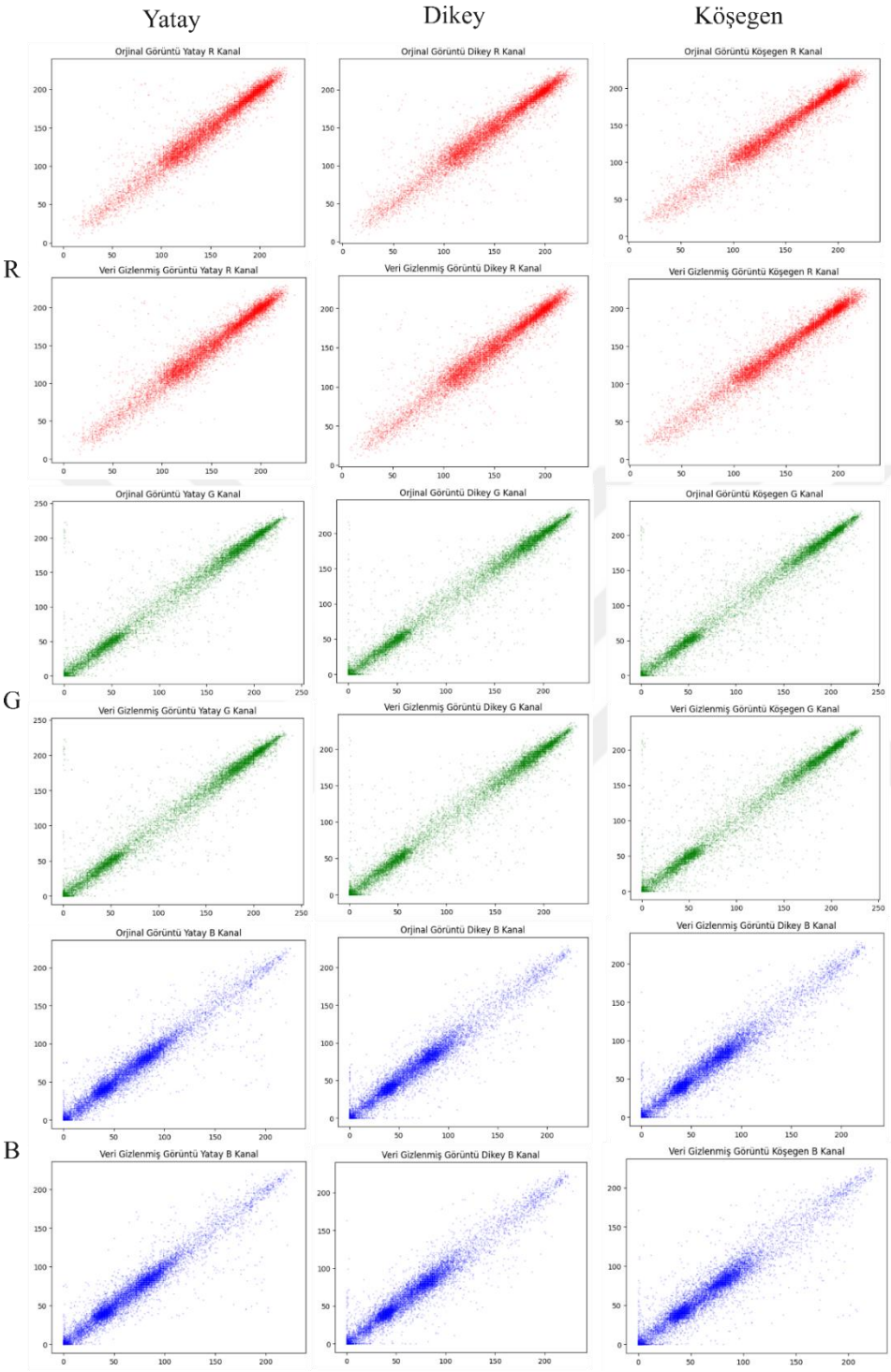
Şekil 3.42 incelendiğinde, (a) Orijinal Kapak Görüntüsünün Histogramı ile (b) IKA kaotik sistem tabanlı elde edilen stego görüntünün histogramı ve (c) IKSB kaotik sistem tabanlı elde edilen stego görüntünün histogramının benzer olduğu görülmektedir. Bu sonuç ile önerilen yöntemin başarılı olduğu söylenebilir.

3.6.1.2. Korelasyon Analizi

Korelasyon analizi iki görüntü arasındaki ilişkiyi belirlemek amacıyla kullanılmaktadır. Şekil 3.43'te, orijinal görüntü ile IKA kaotik sistem tabanlı elde edilen stego görüntü arasındaki korelasyon haritası sunulmuştur. Şekil 3.44'te ise, orijinal görüntü ile IKSB kaotik sistem kullanılarak elde edilen tabanlı elde edilen stego görüntü arasındaki korelasyon haritası gösterilmektedir.



Şekil 3.43. Orijinal ve IKA sistem tabanlı stego görüntü korelasyonu



Şekil 3.44. Orijinal ve IKSB sistem tabanlı stego görüntü korelasyonu

Denklem 2.39'da verilen formüle göre hesaplanan korelasyon değeri Tablo 3.17'de verilmiştir.

Tablo 3.17. Steganografi uygulaması sonrası elde edilen korelasyon katsayıları

	Orijinal Görüntü			IKA Kaotik Sistem Tabanlı Stego Görüntü			IKSB Kaotik Sistem Tabanlı Stego Görüntü		
	Yatay	Dikey	Köşegen	Yatay	Dikey	Köşegen	Yatay	Dikey	Köşegen
R	0.9673	0.9641	0.9550	0.9670	0.9639	0.9549	0.9671	0.9640	0.9548
G	0.9833	0.9815	0.9690	0.9833	0.9815	0.9690	0.9833	0.9814	0.9690
B	0.9647	0.9621	0.9447	0.9644	0.9619	0.9446	0.9646	0.9619	0.9446

Tablo 3.17 incelendiğinde orijinal ve stego görüntü arasında oldukça yakın korelasyon değerleri elde edilmiştir. Bu durum, veri gizleme yönteminin yüksek düzeyde etkinliğini ve gizlenmiş verilerle elde edilen görüntülerin görsel olarak önemli bir zarar görmemiş olduğunu göstermektedir.

3.6.1.3. Bilgi Entropi Analizi

Bilgi entropi analizi, düzensizlik ve rastgeleliği ölçer. Bir görüntüye veri gizlendiğinde, eğer bu görüntünün entropi değeri orijinal görüntünün entropi değeri ile benzerse bu durum pikseller arasındaki düzensizliğin korunduğunu gösterir. Denklem 2.40'ta verilen formüle göre hesaplanan Entropi sonuçları Tablo 3.18'de verilmiştir.

Tablo 3.18. Steganografi uygulaması sonrası elde edilen entropi analiz sonuçları

	Orijinal Görüntü	IKA Kaotik Sistem Tabanlı Stego Görüntü	IKSB Kaotik Sistem Tabanlı Stego Görüntü
R	7.3463	7.3468	7.3469
G	7.5699	7.5808	7.5808
B	7.1440	7.1547	7.1549

Tablo 3.18 incelendiğinde her iki sistemde de gizli veri yerleştirilmiş görüntülerin entropi değerleri orijinal görüntünün entropi değerlerine çok yakın olduğu görülmektedir. Bu durum, veri gizleme yönteminin başarılı olduğunu göstermektedir.

3.6.1.4. Homojenlik, Kontrast ve Enerji Analizi

Denklem 2.41, 2.42 ve 2.43'te verilen formüllere göre hesaplanan Homojenlik, Kontrast ve Enerji testlerinin sonuçları Tablo 3.19'da verilmiştir.

Tablo 3.19. Steganografi sonrası homojenlik, kontrast ve enerji değerleri

	Orijinal Görüntü			IKA Kaotik Sistem Tabanlı Stego Görüntü			IKSB Kaotik Sistem Tabanlı Stego Görüntü		
	R	G	B	R	G	B	R	G	B
Homojenlik	0.8900	0.9000	0.8951	0.8900	0.9000	0.8951	0.8900	0.9000	0.8951
Kontrast	0.2646	0.2953	0.2418	0.2646	0.2953	0.2418	0.2646	0.2953	0.2418
Enerji	0.1349	0.1212	0.1707	0.1349	0.1212	0.1707	0.1349	0.1212	0.1707

Tablo 3.19'a göre, iki farklı kaotik sistem tabanlı steganografi uygulamalarının her iki yöntemi içinde orijinal görüntünün homojenlik, kontrast ve enerji değerlerini değiştirmeden korumuştur. Homojenlik değerleri, görüntünün düzgünlük ve uniform yapıda olduğunu gösterirken bu değerlerin değişmemesi steganografi işlemlerinin görsel bütünlüğü bozmadığını işaret etmektedir. Kontrast değerleri, pikseller arasındaki parlaklık farkını ifade eder ve bu metriklerin sabit kalması, görüntünün detay ve derinlik algısının korunduğunu göstermektedir. Enerji değerleri ise, görüntünün piksel değerlerinin karelerinin toplamı ile ilişkilendirilir ve bu değerlerin sabitliği, görüntü içeriğinin gücünün ve canlılığının korunmuş olduğunu belirtmektedir. Sonuç olarak; bu steganografi uygulamaları, veri gizleme işleminin başarılı bir şekilde gerçekleştirildiğini ve orijinal görüntü özelliklerinin etkilenmeden korunduğunu göstermektedir.

3.6.1.5. MSE ve PSNR Analizi

Ortalama karesel hata (MSE, Mean Squared Error), orijinal görüntü piksel değerleri ile stego görüntü piksel değerlerinin karşılaştırılmasında kullanılmaktadır. MSE Denklem 2.44'te verilen formüle göre hesaplanmaktadır. Orijinal görüntü ile stego görüntü arasındaki MSE değeri minimum seviyede olmalıdır. Tepe sinyal gürültü oranı (PSNR, Peak Signal to Noise Ratio) testi ise orijinal ve stego görüntüler arasındaki bozulmayı değerlendirmek için kullanılan bir ölçüttür. PSNR ise Denklem 2.45'te verilen formüle göre hesaplanmaktadır. PSNR değerinin 30 dB'den yüksek olduğunda orijinal ve stego görüntülerin görsel olarak ayırt edilemez olduğu kabul edilmektedir (Y.-X. Liu et al., 2019). Tablo 3.20'de her iki kaotik sistem tabanlı steganografi uygulaması için orijinal görüntü ve verinin gizlenmiş görüntüleri arasındaki MSE ve PSNR değeri verilmiştir.

Tablo 3.20. Steganografi sonrası elde edilen MSE ve PSNR değeri

	IKA Kaotik Sistem Tabanlı Stego Görüntü			IKSB Kaotik Sistem Tabanlı Stego Görüntü		
	R	G	B	R	G	B
MSE	0.3332	0.3341	0.3343	0.3340	0.3340	0.3332
PSNR	52.9026	52.8909	52.8885	52.8927	52.8925	52.9029

Her iki yöntem için de R, G, B renk kanallarındaki MSE değerleri oldukça düşük olup 0.3332 ile 0.3343 arasında değişmektedir. Bu durum orijinal ve stego görüntüler arasındaki farkın minimal olduğunu göstermektedir. Aynı şekilde, PSNR değerleri her iki yöntem için de 52.88 dB ile 52.90 dB arasında olup bu değerler 30 dB'nin oldukça üzerindedir. Bu durum, orijinal ve stego görüntülerin görsel olarak ayırt edilemez olduğunu ifade etmektedir.

3.6.1.6. Görüntü Kalite Analizi

UIQI (Universal Image Quality Index), görüntü kalitesini değerlendirmek için kullanılan bir metriktir. UIQI değeri Denklem 2.46'da verilen formüle göre hesaplanmaktadır. UIQI değerin -1'e yakın olması karşılaştırılan iki görüntünün tamamen farklı olduğunu, 1 olması ise iki görüntünün tamamen aynı olduğunu ifade eder (Z. Wang et al., 2002).

Görüntü kalite analizlerinden bir diğeri ise görüntü doğruluğu (Image Fidelity-IF) analizidir. Orijinal görüntü ile stego görüntü arasındaki benzerliği belirlemek amacıyla kullanılmaktadır. Görüntü doğruluğu analizi Denklem 2.52'de verilen formüle göre hesaplanmaktadır. Elde edilen analiz değerin 1'e yakın olması, orijinal görüntü ile stego görüntünün o kadar benzer olduğunu ifade etmektedir.

Tez çalışmasında elde edilen UIQI ve IF analiz sonuçları Tablo 3.21'de verilmiştir.

Tablo 3.21. Steganografi sonrası elde edilen UIQI ve IF değeri

	IKA Kaotik Sistem Tabanlı Stego Görüntü			IKSB Kaotik Sistem Tabanlı Stego Görüntü		
	R	G	B	R	G	B
UIQI	0.99991	0.99997	0.99991	0.99991	0.99997	0.99991
IF	0.99998	0.99998	0.99994	0.99998	0.99998	0.99994

3.6.1.7. Zaman Performansı

Steganografi işlemlerinin süresi, bir steganografi algoritmasının performansını ve etkinliğini değerlendirmek için kritik bir faktördür. Bu ölçüt, algoritmaların performansını değerlendirmenin yanı sıra kaynak gereksinimlerini tahmin etme ve gerçek zamanlı uygulamalarda kullanılabilirliklerini belirleme açısından da önemlidir. Görüntü steganografi ve analiz süreçleri, Python programlama dili kullanılarak, 64 GB RAM'a sahip, 2.2 GHz saat hızında çalışan 12 çekirdekli Arm Cortex-A78AE CPU içeren Nvidia Jetson AGX Orin gömülü sistem üzerinde Jupyter programlama ortamında yürütülmüştür. Steganografi ve stego çözme işlemlerine ait süreler, Tablo 3.22'de saniye cinsinden sunulmuştur.

Tablo 3.22. Steganografi işlemlerine ait süreler (birim: saniye)

	Steganografi Süresi	Stego Çözme Süresi
IKA Kaotik Sistem Tabanlı Steganorafi	103.9584	106.0944
IKSB Kaotik Sistem Tabanlı Steganorafi	107.1162	105.7656

4. BULGULAR

Tez çalışmasının başlangıç bölümünde, Arneodo ve Sprott B kaotik sistemleri incommensurate kesir dereceli olarak tanımlanmıştır. Bu tanım, söz konusu sistemlerin daha karmaşık ve çeşitli dinamik özellikler sergilemesine imkân tanımaktadır, bu da daha geniş bir davranış spektrumu modellemesine olanak sağlamaktadır. Özellikle, bu sistemlerden elde edilen kaotik dizilerin yüksek düzeyde rastgelelik ve öngörülemezlik göstermesi, şifreleme ve steganografi uygulamaları için ideal koşullar sunmaktadır. Nvidia Jetson AGX Orin gömülü kart üzerinde yürütülen simülasyonlar, tasarlanan elektronik kartın gerçek dünya uygulamalarında başarıyla işlev gördüğünü doğrulamıştır. Bu bağlamda, tez kapsamında geliştirilen sistemlerin teorik avantajları, mühendislik uygulamalarıyla güçlendirilmiştir.

IKA ve IKSB kaotik sistem tabanlı gerçekleştirilen rastgele sayı üreteci, görüntü şifreleme ve steganografi uygulamaları, Nvidia Jetson AGX Orin gömülü kartı üzerinde gerçekleştirilmiştir. Bu bağlamda IKA ve IKSB Kaotik Sistemi Grünwald-Letnikov nümerik analiz yöntemleriyle ayrıklaştırılarak float tipi ifadeler, IEEE 754 standardı ile ikili formata dönüştürülmüştür. Önerilen RSÜ algoritması kullanılarak rastgele bit dizileri üretilmiştir. Üretilen bit dizileri NIST 800-22, FIPS 140-1 ve ENT testlerine tabi tutulmuştur. FIPS 140-1' deki tüm testleri (Tablo 3.3 ve Tablo 3.4), NIST 800-22' deki tüm testleri (Tablo 3.5 ve Tablo 3.6) ve ENT testlerinin tamamını (Tablo 3.7 ve Tablo 3.8) başarıyla geçerek şifreleme ve steganografi de kullanılabileceği gösterilmiştir. Ayrıca Nvidia Jetson AGX Orin gömülü kartının GPIO pinleri kullanılarak rastgele sayıların gerçek hayatta kullanılabilirliğini osiloskop ekranında gösterilmiştir.

Tez kapsamında IKA ve IKSB kaotik sistem tabanlı özgün bir şifreleme algoritması önerilerek 256×256×1 boyutlarında görüntü şifreleme uygulaması Nvidia Jetson AGX Orin gömülü kartı üzerinde gerçekleştirilmiştir. Şifreleme işlemlerinde daha az işlem yükü nedeniyle karmaşık olmayan mantıksal operatörler kullanılmıştır. Şifreleme işleminin güvenirliliğini ispatlamak amacıyla histogram analizi, korelasyon analizi, diferansiyel atak analizi, bilgi entropi analizi, MSE-PSNR analizi, anahtar uzay analizi, gürültü analizleri, veri kaybı saldırı analizi ve zaman performans analizi yapılmıştır.

Şifrelenmiş görsellerin histogram analizinde tek düze bir dağılım beklenmektedir. Şekil 3.29 (c) ve Şekil 3.30 (c) görüldüğü üzere tek düze bir dağılım vardır ve analiz sonuçları oldukça

iyidir. Ayrıca gerçekleştirilen $variance(var)$ ve $\chi 2$ testleri ile dağılım tek düze olduğunu ve Tablo 4.1'de verilen literatürdeki çalışmalarla uyumlu olduğu görülmüştür.

Tablo 4.1. *var* ve *χ2* karşılaştırma sonucu

	Görüntü	$\boldsymbol{var}$	$\chi 2$
IKA Kaotik Sistem Tabanlı Görüntü Şifreleme	cameraman	285.3203	283.2539
	mandrill	264.2812	264.2656
	peppers	233.7343	233.3437
	plane	233.6875	233.125
IKSB Kaotik Sistem Tabanlı Görüntü Şifreleme	cameraman	281.3125	280.3125
	mandrill	256.6796	256.4882
	peppers	254.6406	254.6367
	plane	274.9140	272.8476
(Bavand Savadkouhi et al., 2023)	cameraman	265.1016	265.1
(Shihua Zhou, 2021)	peppers	248.359	254.5391
(Shahna, 2023)	peppers	249.84	255.45

Tablo 3.10 incelendiğinde ise IKA ve IKSB kaotik sistem tabanlı şifreli görüntülerde sıfıra yakın korelasyon değerinin elde edildiği görülmektedir. Şekil 3.31-3.33 incelendiğinde ise şifreli görüntülerin korelasyon dağılımlarının, orijinal korelasyondan tamamen farklı olduğu doğrusal bir ilişkiden ziyade çok iyi bir homojen dağılım sergilediği görülmektedir. Ayrıca Tablo 4.2'de ise elde edilen korelasyon değerleri diğer sistemlerle karşılaştırdığımızda, genellikle daha iyi veya benzer sonuçlar verdikleri görülmektedir.

Tablo 4.2. Korelasyon katsayıları ve karşılaştırmalar

	Görüntü	Yatay	Dikey	Köşegen
IKA Kaotik Sistem Tabanlı Görüntü Şifreleme	cameraman	-0.0029	0.0108	0.0040
	mandrill	0.0050	-0.0026	-9.51×10^{-5}
	peppers	-0.0030	0.0333	-0.0057
	plane	0.0147	0.0081	-0.0012

Tablo 4.2. (devam) Korelasyon katsayıları ve karşılaştırmalar

IKSB Kaotik Sistem Tabanlı Görüntü Şifreleme	cameraman	-0.0152	-7.97×10^{-5}	0.0067
	mandrill	-0.0073	0.0111	-0.0126
	peppers	0.0165	-0.0156	0.0024
	plane	0.0063	0.0158	0.0051
(Bavand Savadkouhi et al., 2023)	cameraman	-0.0024	0.0029	-0.0040
(N. Wang et al., 2024)	mandrill	0.0097	0.0156	0.0050
(Shihua Zhou, 2021)	peppers	0.0078	0.0058	0.0164
(Hosny et al., 2021)	plane	0.0229	0.0103	0.0100

Şifreleme algoritmasının, diferansiyel saldırılara karşı ne kadar dirençli olduğunu değerlendirmek amacıyla diferansiyel atak analizi kullanılmaktadır. Tablo 3.11'de çalışmada elde edilen NPCR ve UACI değerleri verilmiş olup elde edilen analiz sonuçlarına göre NPCR ve UACI değerlerinin başarı kriterine çok yakın olduğu görülmektedir. Ayrıca Tablo 4.3'te, elde NPCR ve UACI literatürdeki bazı çalışmalar ile karşılaştırıldığında rekabetçi ve güvenilir şifreleme işlemi sağlandığı kanıtlanmaktadır.

Tablo 4.3. NPCR-UACI değerleri ve karşılaştırmalar

	Görüntü	NPCR %	UACI %
IKA Kaotik Sistem Tabanlı Görüntü Şifreleme	cameraman	99.6078	33.4079
	mandrill	99.6170	33.4818
	peppers	99.6109	33.2283
	plane	99.6047	33.5486
IKSB Kaotik Sistem Tabanlı Görüntü Şifreleme	cameraman	99.6398	33.4012
	mandrill	99.6505	33.4369
	peppers	99.6276	33.5976
	plane	99.6093	33.3188
(Bavand Savadkouhi et al., 2023)	cameraman	99.6216	33.4327
(N. Wang et al., 2024)	mandrill	99.6347	33.4710

Tablo 4.3. (devam) NPCR-UACI değerleri ve karşılaştırmalar

Zhou (Shihua Zhou, 2021)	peppers	99.63%	33.53%
(Tang et al., 2024)	plane	99.6017	33.5053

Tablo 3.12'de ise çalışmada elde edilen bilgi entropi değerleri verilmiştir. Sonuçlar incelendiğinde, şifrelenmiş görüntülerin entropi değerlerinin ideal değere çok yakın olduğunu görülmektedir. Tablo 4.4'te elde edilen değerler literatürdeki bazı çalışmalardan daha yakın bir şekilde ideal değer olan sekiz bite ulaşmıştır.

Tablo 4.4 Bilgi Entropi değeri ve karşılaştırmalar

	Görüntü	Bilgi Entropi
IKA Kaotik Sistem Tabanlı Görüntü Şifreleme	cameraman	7.9968
	mandrill	7.9970
	peppers	7.9974
	plane	7.9974
IKSB Kaotik Sistem Tabanlı Görüntü Şifreleme	cameraman	7.9968
	mandrill	7.9971
	peppers	7.9971
	plane	7.9969
(Bavand Savadkouhi et al., 2023)	cameraman	7.9971
(N. Wang et al., 2024)	mandrill	7.9971
(Shihua Zhou, 2021)	peppers	7.9974
(Tang et al., 2024)	plane	7.9972

Anahtar uzay alanı, şifreleme algoritmasının kaba kuvvet saldırılarına karşı güvenli olup olmadığını belirleyen anahtar boyutu aralığını ifade etmektedir. Tez çalışmasında IKA kaotik sistemi için $(10^{15})^9 \approx 2^{449}$ ve IKSB kaotik sistemi için ise $(10^{15})^8 \approx 2^{399}$ olarak hesaplanmıştır. Tablo 4.5'te literatürdeki bazı çalışmaların elde etmiş oldukları anahtar boyutları verilmiştir.

Tablo 4.5. Anahtar Uzay Alanı ve karşılaştırmalar

	Anahtar Uzay Alanı
IKA Kaotik Sistem Tabanlı Görüntü Şifreleme	2^{449}
IKSB Kaotik Sistem Tabanlı Görüntü Şifreleme	2^{399}
(Meng et al., 2023)	2^{239}
(Alharbi et al., 2023)	2^{240}
(T. Li et al., 2024)	2^{249}

Tablo 4.5'te de görüldüğü gibi hem IKA kaotik sistem tabanlı hem de IKSB kaotik sistem tabanlı şifreleme algoritmasının geniş ve kaba kuvvet saldırılarına karşı güvenli bir anahtar uzunluğuna sahip olduğu görülmektedir.

Genellikle, görüntüler bilgi içermektedir ancak iletim sürecinde görüntü çeşitli gürültülerle bozulabilir. Bu bozulmalar, görüntüdeki orijinal bilgilerin kaybına neden olabilir. İdeal bir şifreleme algoritması, gürültü saldırılarına karşı etkili bir performans sağlamalıdır. Çalışmada algoritmanın tuz–biber gürültüsü üzerine etkisi incelenmiş; farklı tuz-biber gürültü oranları, saldırı şiddetini temsil etmektedir. Şekil 3.34 ve Şekil 3.35 incelendiğinde, %10 yoğunluğa sahip gürültüden sonra bile çözümlenen görüntülerin görsel olarak tanımlanabilir olduğunu görülmektedir. Tablo 3.14'te ise tuz-biber gürültüsü sonrası elde edilen PSNR değerleri verilmiştir. Bu tabloya göre, IKA kaotik sistem tabanlı şifreleme algoritmasının, IKSB kaotik sistem tabanlı şifreleme algoritmasına göre genellikle daha yüksek PSNR değerleri sunduğunu göstermektedir.

Şifrelenmiş görüntülerin bazı pikselleri, iletim sırasında ele geçirilebilir veya yanlışlıkla kaybolabilir. Bu durumda iyi bir şifreleme algoritması veri kaybına uğramış bir şifreli görüntüyü en az bozulma ile geri kazanması gerekmektedir. Şekil 3.36 ve Şekil 3.37'de de görüldüğü gibi %50 kayba uğrasa bile görüntüler halen tanınır haldedir. Tablo 3.15'te ise veri kaybı saldırı sonrası elde edilen PSNR değerleri verilmiştir. Bu tabloya göre veri kaybı oranı arttıkça her iki kaotik sistem tabanlı şifreleme işlemleri sonucu PSNR değerlerinde genel bir düşüş yaşandığı görülmektedir. Özellikle, IKA algoritması veri kaybı oranı düşük olduğunda (¼ köşe ve ¼ orta) daha yüksek PSNR değerleri sunarak üstün görüntü kalitesi sağlarken IKSB algoritması benzer veya daha düşük PSNR değerleri göstermektedir. Bu

sonuçlar, IKA kaotik sistem tabanlı şifreleme algoritmasının veri kaybı durumunda daha iyi görüntü kalitesi koruma kapasitesine sahip olduğunu ortaya koymaktadır.

Şifreleme ve şifre çözme süreleri hem güvenlik hem de performans açısından önemli bir faktördür. Algoritmaların ve sistemlerin, güvenlik ihtiyaçlarını karşılayacak ve aynı zamanda verimli ve hızlı performans sağlayacak şekilde tasarlanması gerekmektedir. Bu çalışmada Nvidia Jetson AGX Orin gömülü sistem üzerinde gerçekleştirilen şifreleme ve şifre çözme sürelerine ait sonuçlar Tablo 3.16'da verilmiş olup, IKA kaotik sistem tabanlı şifreleme işleminin küçük bir avantaj sağlayarak hafif bir hız farkı sunmaktadır. Bu bulgular, her iki algoritmanın da benzer performans seviyelerinde olduğunu ve uygulama gereksinimlerine göre tercih edilebileceğini göstermektedir.

Tezin son bölümünde ise IKA ve IKSB kaotik sistem tabanlı özgün iki aşamalı bir steganografi yöntemi önerilmiştir. Bu yöntemde öncelikle gizlenecek veri tez kapsamında önerilen şifreleme algoritmasıyla şifrelenip daha sonra kapak görsele gömülmüştür. Bu durum, çift katmanlı güvenlik sağlamakta olup saldırganların veriyi çözme veya tespit etme işlemlerini zorlaştırmaktadır. Steganografi uygulamasının güvenilirliğini ispatlamak amacıyla histogram, korelasyon, bilgi entropisi, homojenlik, kontrast, enerji, MSE ve PSNR analizi ile görüntü kalitesi ve zaman performansı analizleri gerçekleştirilmiştir.

Stego görüntü ile orijinal görüntünün histogram grafiklerinin aynı veya çok benzer olması beklenmektedir. Şekil 3.42'de R, G, B kanallarına ait histogramlarının çok benzer olduğu görülmektedir. Bu durum stego görüntünün fark edilmesini zorlaştırmakta ve gizli verinin varlığını daha iyi saklamaktadır. Böylece önerilen steganografi yönteminin başarılı olduğu görülmektedir.

Aynı şekilde stego görüntü ile orijinal görüntünün korelasyon değerlerinin birbirine yakın veya çok benzer olması beklenmektedir. Şekil 3.43 ve Şekil 3.44 verilen korelasyon dağılım grafiklerinde ve Tablo 3.17'de görüldüğü üzere R, G, B kanalar için yatay, dikey ve köşegen doğrultulardaki korelasyon değerleri orijinal görüntüye çok yakın olduğu görülmektedir. Her iki steganografi yönteminin de orijinal görüntü ile stego görüntü arasında yüksek bir benzerlik sağladığını ve gizli verinin varlığını başarıyla sakladığını açıktır. Tablo 4.6'da steganografi işlemi sonrası korelasyon değerleri ve literatür ile karşılaştırması sunulmuştur. IKA ve IKSB, kaotik sistem temelli steganografi uygulamalarında orijinal ve stego görüntüler arasındaki minimal farklılıklar ile diğer sistemlere kıyasla üstün bir performans

sergilemektedir. Minimal farklılıklar, söz konusu sistemlerin yüksek seviyede gizlilik ve görünmezlik sağladığını göstermekte olup, orijinal görüntünün kalitesini neredeyse bozmadan steganografik bilgiyi etkili bir şekilde gizleyebilme yeteneklerini ortaya koymaktadır. Bu bulgular, IKA ve IKSB sistemlerinin steganografi uygulamalarında güvenilir ve etkili çözümler sunduğunu kanıtlamaktadır.

Tablo 4.6. Korelasyon değerleri ve karşılaştırmalar

		Orijinal Görüntü			Stego Görüntü		
		Yatay	Dikey	Köşegen	Yatay	Dikey	Köşegen
IKA Kaotik Sistem Tabanlı Steganografi	R	0.9673	0.9641	0.9550	0.9670	0.9639	0.9549
	G	0.9833	0.9815	0.9690	0.9833	0.9815	0.9690
	B	0.9647	0.9621	0.9447	0.9644	0.9619	0.9446
IKSB Kaotik Sistem Tabanlı Steganografi	R	0.9673	0.9641	0.9550	0.9671	0.9640	0.9548
	G	0.9833	0.9815	0.9690	0.9833	0.9814	0.9690
	B	0.9647	0.9621	0.9447	0.9646	0.9619	0.9446
(Sharafi et al., 2021)	R	0.9230	0.8659	0.8543	0.9227	0.8658	0.8541
	G	0.8654	0.7650	0.7347	0.8647	0.7639	0.7336
	B	0.9073	0.8808	0.8398	0.9068	0.8805	0.8393
(Satria et al., 2021)	R	0.98179	0.98319	0.97159	0.9817	0.9831	0.9715
	G	0.99057	0.99090	0.98291	0.9905	0.9908	0.9828
	B	0.98328	0.98328	0.97025	0.9832	0.9832	0.9702
(Yousefian Darani et al., 2024)	R	0.9726	0.9568	0.9343	0.9741	0.9580	0.9358
	G	0.9577	0.9677	0.9325	0.9596	0.9696	0.9349
	B	0.9639	0.9353	0.9145	0.9691	0.9400	0.9204
(Tokatlıoğlu, 2024)	R	0.9646	0.9680	0.9369	0.9681	0.9810	0.9574
	G	0.9698	0.9750	0.9466	0.9624	0.9786	0.9482
	B	0.9570	0.9636	0.9263	0.9374	0.9657	0.9206

Tablo 3.18'de ise elde edilen bilgi entropi değerleri verilmiştir. Steganografi uygulaması sonrasında elde edilen değerlerin, orijinal görüntü ile kıyaslandığında çok yakın olduğunu

göstermektedir. Ayrıca Tablo 4.7'de steganografi işlemi sonrası bilgi entropi değerleri ve literatür ile karşılaştırması sunulmuştur. Bu sonuçlar IKA ve IKSB sistemlerinin, orijinal ve stego görüntüler arasındaki entropi farklarının minimal olduğunu göstermektedir. IKA ve IKSB sistemlerinde R, G, B kanallarda gözlemlenen entropi farkları oldukça küçüktür ve bu da steganografik bilgiyi etkili bir şekilde gizlediklerini göstermektedir.

Tablo 4.7. Bilgi Entropi değerleri ve karşılaştırmalar

	Orijinal Görüntü			Stego Görüntü		
	R	G	B	R	G	B
IKA Kaotik Sistem Tabanlı Steganografi	7.3463	7.5699	7.1440	7.3468	7.5808	7.1547
IKSB Kaotik Sistem Tabanlı Steganografi	7.3463	7.5699	7.1440	7.3469	7.5808	7.1549
(Martínez-González et al., 2016)	7.6798	7.3730	7.6976	7.6799	7.3746	7.6979
(Sharif et al., 2017)	7.7880	7.5484	7.7927	7.7881	7.5484	7.7927
(Pak et al., 2020)	7.7435	7.4685	5.8341	7.6507	7.4891	6.1616

Tablo 3.19, steganografi uygulaması sonrasında elde edilen homojenlik, kontrast ve enerji değerleri sunulmuş olup, R, G, B renk kanallarında hem IKA hem de IKSB kaotik sistem tabanlı steganografi yöntemleri kullanılarak elde edilen stego görüntüler, orijinal görüntü ile tam olarak aynı homojenlik, kontrast ve enerji değerlerine sahiptir. Ayrıca Tablo 4.8'de, steganografi işlemi sonrası homejen, kontrast ve enerji değerleri ve literatür ile karşılaştırması sunulmuştur. Bu sonuçlar, steganografi yöntemlerinin görüntünün görsel ve yapısal özelliklerini değiştirmeden veriyi başarıyla gizleyebildiğini göstermektedir.

Tablo 4.8. Homejen, kontrast ve enerji değerleri ve karşılaştırmalar

		Orijinal Görüntü			Stego Görüntü		
		R	G	B	R	G	B
IKA Kaotik Sistem Tabanlı Steganografi	homojenlik	0.8900	0.9000	0.8951	0.8900	0.9000	0.8951
	kontrast	0.2646	0.2953	0.2418	0.2646	0.2953	0.2418
	enerji	0.1349	0.1212	0.1707	0.1349	0.1212	0.1707

Tablo 4.8. (devam) Homejen, kontrast ve enerji değerleri ve karşılaştırmalar

IKSB Kaotik Sistem Tabanlı Steganografi	homojenlik	0.8900	0.9000	0.8951	0.8900	0.9000	0.8951
	kontrast	0.2646	0.2953	0.2418	0.2646	0.2953	0.2418
	enerji	0.1349	0.1212	0.1707	0.1349	0.1212	0.1707
(S. M. Hameed et al., 2021)	homojenlik	0.8388	0.8079	0.8062	0.8388	0.8076	0.8054
	kontrast	0.3946	0.4913	0.4976	0.3946	0.4952	0.5119
	enerji	0.0893	0.0913	0.0768	0.0893	0.0912	0.0766
(Sharif et al., 2017)	homojenlik	0.6970	0.6769	0.6774	0.6970	0.6769	0.6774
	kontrast	0.7425	0.7847	0.7546	0.7425	0.7847	0.7546
	enerji	0.0456	0.0463	0.0463	0.0456	0.0463	0.0463
(Pak et al., 2020)	homojenlik	0.9044	0.9071	0.9247	0.9044	0.9071	0.9247
	kontrast	0.2939	0.3238	0.2792	0.2939	0.3238	0.2792
	enerji	0.1111	0.1513	0.4457	0.1111	0.1513	0.4457

Tablo 3.20, IKA ve IKSB kaotik sistem tabanlı steganografi yöntemleri kullanılarak elde edilen stego görüntülerin R, G, B renk kanalları için MSE ve PSNR değerlerini göstermektedir. MSE değerleri, orijinal görüntü ile stego görüntü arasındaki piksel bazındaki ortalama kare farkıdır; bu değerlerin düşük olması, iki görüntü arasında minimal fark olduğunu göstermektedir. PSNR değerleri ise görüntü kalitesinin bozulma miktarını değerlendirmede kullanılır, yüksek PSNR değerleri, yüksek görüntü kalitesini işaret eder. Her iki yöntem için MSE değerleri son derece düşük (0.3332 ile 0.3343 arası), bu da steganografi işlemi sonucunda orijinal görüntüye çok az değişiklik yapıldığını göstermektedir. PSNR değerleri ise oldukça yüksek (yaklaşık 52.89 ile 52.90 arası), bu da stego görüntülerin yüksek kalitede olduğunu ve orijinal görüntüden gürültü veya bozulma eklendiğinde bile görsel kalitenin korunduğunu belirtmektedir. Ayrıca Tablo 4.9'da steganografi işlemi sonrası PSNR ve MSE değerleri literatür ile karşılaştırılmalı olarak sunulmuştur. IKA ve IKSB kaotik sistem temelli steganografi uygulamaları, diğer tüm çalışmalara kıyasla en yüksek PSNR ve en düşük MSE değerleri ile en iyi performansı göstermektedir. Bu sonuçlar, önerilen steganografi yönteminin de etkin bir şekilde gizlilik sağladığını ve görsel kaliteyi yüksek düzeyde tuttuğunu göstermektedir.

Tablo 4.9. PSNR ve MSE değerleri ve karşılaştırmalar

	PSNR	MSE
IKA Kaotik Sistem Tabanlı Stego Görüntü	52.894	0.3338
IKSB Kaotik Sistem Tabanlı Stego Görüntü	52.8960	0.3337
(Sharif et al., 2017)	38.7540	8.6632
(Pak et al., 2020)	37.1197	12.6212
(Jing-yu et al., 2023)	35.70	17.502
(Alabaichi et al., 2020)	45.8661	1.6845

Tablo 3.21' de ise IKA ve IKSB kaotik sistem tabanlı steganografi yöntemleri kullanılarak elde edilen stego görüntülerin R, G, B renk kanalları için UIQI (Universal Image Quality Index) ve IF (Image Fidelity) değerlerini sunmaktadır. Her iki yöntem için UIQI değerleri son derece yüksek (0.99991 ile 0.99997 arası), bu da steganografi uygulamasının orijinal görüntünün yapısal özelliklerini neredeyse tamamen koruduğunu göstermektedir. Aynı şekilde, IF değerleri de çok yüksek (0.99994 ile 0.99998 arası), bu da stego görüntülerin orijinal görüntüye çok yüksek bir doğruluk oluşturulduğunu belirtmektedir. Ayrıca Tablo 4.10'da steganografi işlemi sonrası PSNR ve MSE değerleri literatür ile karşılaştırılmalı olarak sunulmuştur. IKA ve IKSB kaotik sistem temelli steganografi uygulamalarında elde edilen, UIQI ve IF değerlerinin neredeyse 1'e çok yakın olması nedeniyle literatürdeki diğer çalışmalara göre daha yüksek performansı göstermektedir. Bu sonuçlar, steganografi yönteminin de görsel kaliteyi etkilemeden veriyi başarılı bir şekilde gizlediğini ve orijinal görüntü ile stego görüntü arasında yüksek derecede benzerlik sağladığını göstermektedir.

Tablo 4.10. UIQI ve IF değerleri ve karşılaştırmalar

	UIQI	IF
IKA Kaotik Sistem Tabanlı Stego Görüntü	0.99993	0.99997
IKSB Kaotik Sistem Tabanlı Stego Görüntü	0.99993	0.99997
(Sharif et al., 2017)	0.99967	0.99940
(Pak et al., 2020)	0.998406	0.999227
(J. Sun et al., 2023)	0.9999	-
(Alabaichi et al., 2020)	0.9998	0.9999

Bu çalışmada Nvidia Jetson AGX Orin gömülü sistem üzerinde gerçekleştirilen steganografi ve stego çözme sürelerine ait sonuçlar Tablo 3.22'de verilmiştir. Elde edilen sonuçlar, her iki yöntemin de steganografi ve çözme işlemlerini benzer ve kabul edilebilir zaman dilimlerinde tamamlayabildiğini göstermektedir. IKA metodunun steganografi süreci biraz daha çabuk tamamlanırken, IKSB metodunun çözme süreci biraz daha kısa sürmüştür. İlerleyen çalışmalarda hibrit bir yaklaşım geliştirilerek zaman performansının optimizasyonu üzerine çalışmalar gerçekleştirilebilir.

5. SONUÇ VE ÖNERİLER

Bu tez çalışmasında, Arneodo ve Sprott B kaotik sistemleri, incommensurate kesir dereceli olarak ifade edilmiştir. Bu kapsamda, kaotik sistemlerin çeşitli analizleri gerçekleştirilmiştir. Incommensurate kesir dereceli sistemler, Nvidia Jetson AGX Orin üzerinde modellenerek simülasyonlar yapılmış ve tasarlanan elektronik kart aracılığıyla devre uygulamaları gerçekleştirilmiştir.

Nvidia Jetson AGX Orin gömülü kart tabanlı olarak, IKA ve IKSB kaotik sistemlerinin rastgele sayı üretimi, görüntü şifreleme ve görüntü steganografisi alanlarındaki uygulanabilirliği araştırılmıştır. Bu çerçevede geliştirilen özgün rastgele sayı üreteci (RSÜ), uluslararası en yüksek standartlar olan NIST 800-22, FIPS 140-1 ve ENT testlerinden başarıyla geçmiştir. Ayrıca, incommensurate kesir dereceli kaotik sistemler tabanlı şifreleme ve steganografi algoritmaları geliştirilmiş ve bu algoritmalar gömülü kart üzerinde başarıyla uygulanmıştır.

Tez kapsamında ilk olarak IKA ve IKSB Kaotik Sistemlerinin denge noktası analizi, faz portresi analizi, Lyapunov üstel analizi, zaman serisi analizi ve çatallaşma diyagramı gibi detaylı analizleri gerçekleştirilmiştir. IKA Kaotik Sistemi için kesir dereceleri $q_1 = 0.54, q_2 = 0.55, q_3 = 0.56$ olarak, IKSB Kaotik Sistemi için ise $q_1 = 0.9, q_2 = 0.91, q_3 = 0.92$ olarak belirlenmiştir. Bu analizler sonucunda, incommensurate kesir dereceli sistemlerin tam dereceli sistemlere kıyasla daha fazla parametre seçeneği sunarak daha karmaşık ve zengin dinamik davranışlar sergilediği tespit edilmiştir. Ayrıca, kaotik sistemlerin zaman serilerini ve faz portrelerini fiziksel olarak somutlaştırmak amacıyla bir kart tasarımı yapılmıştır.

Incommensurate Kesir Dereceli kaotik sistemler, kaos tabanlı rastgele sayı üreteci (RSÜ) tasarımı için kullanılmıştır. Grünwald-Letnikov nümerik analiz yöntemiyle çözümlenerek elde edilen float tipi ifadeler, ikili sayı formatına dönüştürülerek Nvidia Jetson AGX Orin gömülü sistem tabanlı RSÜ tasarımı gerçekleştirilmiştir. Önerilen RSÜ algoritması, NIST 800-22, FIPS 140-1 ve ENT testlerinin hepsinden başarıyla geçmiştir. Test sonuçlarına göre, üretilen bit dizisinin şifreleme ve steganografi çalışmalarında kullanımının uygun olduğu görülmüştür.

Incommensurate Kesir Dereceli kaotik sistem tabanlı özgün bir şifreleme algoritması geliştirilmiş ve görsel verilerin şifreleme işlemi gerçekleştirilmiştir. Şifreleme işleminde

işlem yükünü azaltmak amacıyla mantıksal operatörler kullanılmıştır. Bu sayede gömülü sistem tabanlı efektif bir şifreleme uygulaması gerçekleştirilmiştir. IKA ve IKSB kaotik sistem tabanlı şifreleme işleminin yüksek güvenilirlikte olduğunu kanıtlamak için çeşitli güvenlik analizleri gerçekleştirilmiştir.

Son aşamada, incommensurate Kesir Dereceli kaotik sistem tabanlı özgün bir steganografi algoritması geliştirilmiştir. Steganografi algoritması, Nvidia Jetson AGX Orin gömülü sistem kartı üzerinde yürütülmüştür. Önerilen steganografi uygulaması iki seviyeli güvenlik adımları içermektedir. İlk olarak gizlenecek veri tez kapsamında önerilen özgün bir şifreleme algoritması ile şifrelenmiş, ikinci aşamada ise LSB yöntemi kullanılarak şifreli görüntü RGB resmin kanallarına gömülmüştür. Bu yöntemin başarılı bir şekilde bilgi gizleme süreçlerinde kullanılabileceğini göstermek amacıyla çeşitli güvenlik analizleri gerçekleştirilmiştir.

Elde edilen sonuçlar, gömülü sistem üzerinde güvenilir, hızlı ve incommensurate kesir dereceli kaotik sistem tabanlı şifreleme ve steganografi uygulamalarının gerçekleştirilebileceğini göstermektedir.

Gelecekteki çalışmalar, bu tezde incelenen incommensurate kesir dereceli kaotik sistemlerin rastgele sayı üretimi ve şifreleme uygulamalarının ötesinde, haberleşme, görüntü işleme, kontrol ve fizik gibi çeşitli alanlarda kullanım potansiyelini araştırabilir. Ayrıca, tasarlanan RSÜ kullanılarak farklı veya hibrit şifreleme yöntemleri geliştirilebilir ve gerçek zamanlı görüntülerin güvenli bir şekilde şifrelenmesi işlemlerinde kullanılabilir. Steganografi uygulamasında farklı teknikler kullanılarak performans kıyaslamaları yapılabilir. Özgün olarak geliştirilen incommensurate kesir dereceli kaos tabanlı şifreleme ve steganografi yönteminin savunma sanayi, haberleşme, tıp ve kişisel veri gizliliği gibi çeşitli sektörlerde bilgi güvenliği teknolojisine önemli katkılar sağlaması öngörülmektedir.

Bu çalışma, incommensurate kesir dereceli kaotik sistemlerin gömülü sistemlerdeki potansiyelini ortaya koymuş ve gelecekteki araştırmalar için sağlam bir temel oluşturmuştur.

6. KAYNAKLAR

Ahmad, J., Khan, M. A., Hwang, S. O., & Khan, J. S. (2017). A compression sensing and noise-tolerant image encryption scheme based on chaotic maps and orthogonal matrices. *Neural Computing and Applications*, *28*, 953–967.

Akçay, L., Çil, E., Vardar, A., Yaman, İ., Yeniçeri, R., & Yalçın, M. E. (2017). Implementation of a chaotic time-delay RNG based secure communication system on FPGA. *2017 10th International Conference on Electrical and Electronics Engineering (ELECO)*, 1277–1280.

Akgül, A. (2015). *Yeni Kaotik Sistemler İle Rasgele Sayı Üreteci Tasarımı Ve Çoklu-Ortam Verilerinin Yüksek Güvenlikli Şifrelenmesi* (Yayın No. 387525) [Doktora tezi, Sakarya Üniversitesi]. Ulusal Tez Merkezi

Akgul, A., Moroz, I., Pehlivan, I., & Vaidyanathan, S. (2016). A new four-scroll chaotic attractor and its engineering applications. *Optik*, *127*(13), 5491–5499. doi: 10.1016/j.ijleo.2016.02.066

Al-Shabi, M. A. (2019). A Survey on Symmetric and Asymmetric Cryptography Algorithms in information Security. *International Journal of Scientific and Research Publications (IJSRP)*, *9*(3), p8779. doi: 10.29322/ijsrp.9.03.2019.p8779

Alabaichi, A., Khodher, M., & Salih, A. (2020). Image steganography using least significant bit and secret map techniques. *International Journal of Electrical and Computer Engineering (IJECE)*, *10*, 935. doi: 10.11591/ijece.v10i1.pp935-946

Alharbi, S., Elsonbaty, A., Elsadany, A. A., & Kamal, F. (2023). Nonlinear Dynamics in the Coupled Fractional-Order Memristor Chaotic System and Its Application in Image Encryption. *Mathematical Problems in Engineering*, *2023*(1), 8994299. doi: https://doi.org/10.1155/2023/8994299

Altaay, A. A. J., Sahib, S. B., & Zamani, M. (2012). An Introduction to Image Steganography Techniques. *2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, 122–126. doi: 10.1109/ACSAT.2012.25

Altium Limited. (2021). *Altium Designer*. Retrieved from https://www.altium.com/altium-

designer

Arneodo, A., Coullet, P. H., Spiegel, E. A., & Tresser, C. (1985). Asymptotic chaos. *Physica D: Nonlinear Phenomena*, *14*(3), 327–347. doi: https://doi.org/10.1016/0167-2789(85)90093-4

Arneodo, A., Pierre, C., & Tresser, C. (1981). Possible new strange attractors with spiral structure. *Communications in Mathematical Physics, 79*. doi: 10.1007/BF01209312

Arslan, C. (2019). *Tamsayılı Ve Kesirli Dereceden Farklı Kaotik Sistemler İle Rasgele Sayı Üreteçleri Ve Arayüz Tasarımı* (Yayın No. 553149) [Yüksek lisans tezi, Sakarya Uygulamalı Bilimler Üniversitesi]. Ulusal Tez Merkezi

Artuğer, F., & Özkaynak, F. (2024). A new chaotic system and its practical applications in substitution box and random number generator. *Multimedia Tools and Applications*. doi: 10.1007/s11042-024-19053-7

Awadh, W. A., Alasady, A. S., & Hamoud, A. K. (2022). Hybrid information security system via combination of compression, cryptography, and image steganography. *International Journal of Electrical and Computer Engineering*, *12*(6), 6574.

Bader, A., Mohammed, K., Jasem, F., & Sagheer, A. (2024). *Image Steganography Technique based on Lorenz Chaotic System and Bloom Filter*. doi: 10.12785/ijcds/160161

Bassham, L., Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Leigh, S., Levenson, M., Vangel, M., Heckert, N., & Banks, D. (2010). *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD. Retrieved from https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762

Bavand Savadkouhi, M., Haj Seyyed Javadi, H., & Akbari Tootkaboni, M. (2023). Application of S-Boxes based on the chaotic Hindmarsh-Rose system for image encryption. *Journal of Mathematical Modeling*, *11*(2), 277–300. doi: 10.22124/jmm.2023.23199.2068

Bolotin, Y., Tur, A., & Yanovsky, V. (2017). *Chaos: Concepts, control and constructive use*. Springer Cham. https://doi.org/10.1007/978-3-319-42496-5

Borah, M., Singh, P. P., & Roy, B. K. (2016). Improved Chaotic Dynamics of a Fractional-Order System, its Chaos-Suppressed Synchronisation and Circuit Implementation.

Circuits, Systems, and Signal Processing, *35*(6), 1871–1907. doi: 10.1007/s00034-016-0276-9

Broemeling, L. D. (2011). An account of early statistical inference in Arab cryptology. *American Statistician*, *65*(4), 255–257. doi: 10.1198/tas.2011.10191

Butcher, J. C. (1997). Numerical methods for differential equations and applications. *Arabian Journal for Science and Engineering*, 10, 113-121.

Cafagna, D. (2007). Fractional calculus: A mathematical tool from the past for present engineers [Past and present]. *IEEE Industrial Electronics Magazine*, *1*(2), 35–40. doi: 10.1109/MIE.2007.901479

Calgan, H. (2024). Incommensurate fractional-order analysis of a chaotic system based on interaction between dark matter and dark energy with engineering applications. *Physica A: Statistical Mechanics and Its Applications*, *635*, 129490. doi: https://doi.org/10.1016/j.physa.2023.129490

Carter, B., & Magoc, T. (2007). Classical Ciphers and Cryptanalysis. *Space*, *1000*, 1–10.

Chan, C.-K., & Cheng, L. M. (2004). Hiding data in images by simple LSB substitution. *Pattern Recognition*, *37*(3), 469–474. doi: https://doi.org/10.1016/j.patcog.2003.08.007

Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. *Signal Processing*, *90*(3), 727–752. doi: 10.1016/j.sigpro.2009.08.010

Chua, L., Komuro, M., & Matsumoto, T. (1986). The double scroll family. *IEEE Transactions on Circuits and Systems*, *33*(11), 1072–1118. doi: 10.1109/TCS.1986.1085869

Cui, X., Zhang, H., Fang, X., Wang, Y., Wang, D., Fan, F., & Shu, L. (2023). A Secret Key Classification Framework of Symmetric Encryption Algorithm Based on Deep Transfer Learning. *Applied Sciences*, *13*(21), 12025. doi: 10.3390/app132112025

CVG-UGR Image database. (2023). Retrieved from https://ccia.ugr.es/cvg/dbimagenes/g256.php

da Silva, D. M., da Costa Farias, R., Cunha, A., Casagrande, L. S., & Peres, R. A. (2024). History and Legacy of Alan Turing for Computer Science. *International Journal of*

Scientific Research and Management (IJSRM), 12(02), 1047–1056.

Dahat, A. V, & Chavan, P. V. (2016). Secret Sharing Based Visual Cryptography Scheme Using CMY Color Space. *Procedia Computer Science*, *78*, 563–570. doi: https://doi.org/10.1016/j.procs.2016.02.103

Dash, S., Mondal, J., & Swain, D. (2023). A survey on symmetric text encryption techniques. *AIP Conference Proceedings*, *2981*(1), 20020. doi: 10.1063/5.0182894

Delfs, H., & Knebl, H. (2002). *Introduction to Cryptography: Principles and Applications*. doi: 10.1007/978-3-662-47974-2

Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography Engineering - Design Principles and Practical Applications*. Retrieved from https://api.semanticscholar.org/CorpusID:33098209

Fujisaki, E., & Okamoto, T. (2013). Secure Integration of Asymmetric and Symmetric Encryption Schemes. *Journal of Cryptology*, *26*(1), 80–101. doi: 10.1007/s00145-011-9114-1

Gautam, D., Agrawal, C., Sharma, P., Mehta, M., & Saini, P. (2018). An Enhanced Cipher Technique Using Vigenere and Modified Caesar Cipher. *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, 1–9. doi: 10.1109/ICOEI.2018.8553910

Gokyildirim, A., Akgul, A., Calgan, H., & Demirtas, M. (2024). Parametric fractional-order analysis of Arneodo chaotic system and microcontroller-based secure communication implementation. *AEU - International Journal of Electronics and Communications*, *175*, 155080. doi: 10.1016/j.aeue.2023.155080

Gokyildirim, A., Çiçek, S., Calgan, H., & Akgul, A. (2024). Fractional-order Sprott K chaotic system and its application to biometric iris image encryption. *Computers in Biology and Medicine*, *179*, 108864. doi: https://doi.org/10.1016/j.compbiomed.2024.108864

Google. (2024). *Google Colaboratory*. Retrieved from https://colab.research.google.com/

Gupta, M., Singh, V. P., Gupta, K. K., & Shukla, P. K. (2023). An efficient image encryption technique based on two-level security for internet of things. *Multimedia Tools and Applications*, *82*(4), 5091–5111. doi: 10.1007/s11042-022-12169-8

Hameed, A. (2015). Hiding of Speech based on Chaotic Steganography and Cryptography Techniques. *International Journal of Engineering Research*, *4*, 165–172. doi: 10.17950/ijer/v4s4/401

Hameed, S. M., Ali, Z. H., AL-Khafaji, G. K., & Ahmed, S. (2021). Chaos-based Color Image Steganography Method Using 3 D Cat Map. *Iraqi Journal of Science*, *62*(9), 3220–3227. doi: 10.24996/ijs.2021.62.9.34

Hasanbayli, M., & Tavas, V. (2021). A New Random Number Generator Desıgn Based On Tausworthe Equatıon with Verilog. *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi*, *20*(39), 112–126. Retrieved from https://dergipark.org.tr/en/pub/ticaretfbd/issue/63129/936440

Hénon, M. (1976). A two-dimensional mapping with a strange attractor. *Communications in Mathematical Physics*, *50*(1), 69–77. doi: 10.1007/BF01608556

Hernandez-Castro, J., & Barrero, D. F. (2017). Evolutionary generation and degeneration of randomness to assess the indepedence of the Ent test battery. *2017 IEEE Congress on Evolutionary Computation (CEC)*, 1420–1427. doi: 10.1109/CEC.2017.7969470

Hosny, K. M., Kamal, S. T., Darwish, M. M., & Papakostas, G. A. (2021). New Image Encryption Algorithm Using Hyperchaotic System and Fibonacci Q-Matrix. *Electronics*, *10*(9). doi: 10.3390/electronics10091066

IEEE Standard for Binary Floating-Point Arithmetic. (1985). In ANSI/IEEE Std 754-1985 (pp. 1–20). doi: 10.1109/IEEESTD.1985.82928

Janakiraman, S., Thenmozhi, K., Rayappan, J. B. B., & Amirtharajan, R. (2018). Lightweight chaotic image encryption algorithm for real-time embedded system: Implementation and analysis on 32-bit microcontroller. *Microprocessors and Microsystems*, *56*, 1–12. doi: https://doi.org/10.1016/j.micpro.2017.10.013

Jia, H. Y., Chen, Z. Q., & Qi, G. Y. (2014). Chaotic Characteristics Analysis and Circuit Implementation for a Fractional-Order System. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *61*(3), 845–853. doi: 10.1109/TCSI.2013.2283999

Jing-yu, S., Hong, C., Gang, W., Zi-bo, G., & Zhang, H. (2023). FPGA image encryption-steganography using a novel chaotic system with line equilibria. *Digital Signal Processing*, *134*, 103889. doi: https://doi.org/10.1016/j.dsp.2022.103889

Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. *Computer*, *31*(2), 26–34. doi: 10.1109/MC.1998.4655281

Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *Neurocomputing*, *335*, 299–326. doi: https://doi.org/10.1016/j.neucom.2018.06.075

Karcı, A. (2015). Kesir Dereceli Türevin Yeni Yaklaşımının Özellikleri. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, *30*(3). doi: 10.17341/gummfd.76509

Kaur, G., Agarwal, R., & Patidar, V. (2020). Chaos based multiple order optical transform for 2D image encryption. *Engineering Science and Technology, an International Journal*, *23*(5), 998–1014. doi: https://doi.org/10.1016/j.jestch.2020.02.007

Kawaguchi, E., & Eason, R. O. (1999). Principles and applications of BPCS steganography. *Proc.SPIE*, *3528*, 464–473. doi: 10.1117/12.337436

Khan, J., Ahmad, J., & Hwang, S. O. (2015). An efficient image encryption scheme based on: Henon map, skew tent map and S-Box. *2015 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO)*, 1–6.

Khan, M., & Masood, F. (2019). A novel chaotic image encryption technique based on multiple discrete dynamical maps. *Multimedia Tools and Applications*, *78*(18), 26203–26222. doi: 10.1007/s11042-019-07818-4

Kharrazi, M., Sencar, T., & Memon, N. (2004). *Image steganography: Concepts and practice*. *22*.

Kiran, H. E., Akgul, A., Yildiz, O., & Deniz, E. (2023). Lightweight encryption mechanism with discrete-time chaotic maps for Internet of Robotic Things. *Integration*, *93*, 102047. doi: https://doi.org/10.1016/j.vlsi.2023.06.001

Kocher, P. C. (1995). C*ryptanalysis of Diffie-Hellman, RSA, DSS, and other systems using timing attacks.* In *Extended abstract*. Citeseer

Korkmaz, M. (2013). *Kesirli Dereceden PI D Denetleyicilerin, Tasarımı, Uygulaması Ve Karşılaştırılması* (Yayın No. 335347) [Yüksek lisans tezi, Selçuk Üniversitesi]. Ulusal Tez Merkezi

Krawczyk, H., Bellare, M., & Canetti, R. (1997). *RFC2104: HMAC: Keyed-hashing for*

message authentication. RFC Editor.

L'Ecuyer, P. (1994). Uniform random number generation. *Annals of Operations Research*, *53*(1), 77–120. doi: 10.1007/BF02136827

Li, B., Liao, X., & Jiang, Y. (2019). A novel image encryption scheme based on improved random number generator and its implementation. *Nonlinear Dynamics*, *95*(3), 1781–1805. doi: 10.1007/s11071-018-4659-2

Li, P., Qian, J., & Xu, T. (2024). New chaotic systems and application in DNA colored image encryption. *Multimedia Tools and Applications*, *83*(17), 50023–50045. doi: 10.1007/s11042-023-17605-x

Li, T., Fan, W., Wu, J., & Zhang, D. (2024). Image encryption based on a fractional-order hyperchaotic system and fast row-column-level joint permutation and diffusion. *Nonlinear Dynamics*, *112*(12), 10555–10581. doi: 10.1007/s11071-024-09597-6

Liu, H., & Wang, X. (2010). Color image encryption based on one-time keys and robust chaotic maps. *Computers & Mathematics with Applications*, *59*(10), 3320–3327. doi: https://doi.org/10.1016/j.camwa.2010.03.017

Liu, P., Zhang, Y., Mohammed, K. J., Lopes, A. M., & Saberi-Nik, H. (2023). The global dynamics of a new fractional-order chaotic system. *Chaos, Solitons & Fractals*, *175*, 114006. doi: https://doi.org/10.1016/j.chaos.2023.114006

Liu, Y.-X., Yang, C.-N., Sun, Q.-D., Wu, S.-Y., Lin, S.-S., & Chou, Y.-S. (2019). Enhanced embedding capacity for the SMSD-based data-hiding method. *Signal Processing: Image Communication*, *78*, 216–222. doi: https://doi.org/10.1016/j.image.2019.07.013

Liu, Z., Xia, T., & Wang, T. (2023). Dynamic analysis of fractional-order six-order discrete chaotic mapping and its application in information security. *Optik*, *272*, 170356. doi: https://doi.org/10.1016/j.ijleo.2022.170356

Lorenz, E. N. (1963). Deterministic Nonperiodic Flow. *Journal of the Atmospheric Sciences*. doi: 10.1175/1520-0469(1963)020<0130:dnf>2.0.co;2

Uzun, M. (2023). *Sayısal Renkli Görüntüler İçin Uzamsal Düzlem Yöntemleri Kullanan Yeni Bir Hibrit Steganografi Algoritması* (Yayın No. 823516) [Yüksek lisans tezi, Kocaeli Üniversitesi]. Ulusal Tez Merkezi

Ma, C., Mou, J., Liu, J., Yang, F., Yan, H., & Zhao, X. (2020). Coexistence of multiple attractors for an incommensurate fractional-order chaotic system. *The European Physical Journal Plus*, *135*, 1–21.

Mandal, P. C., Mukherjee, I., Paul, G., & Chatterji, B. N. (2022). Digital image steganography: A literature survey. *Inf. Sci.*, *609*(C), 1451–1488. doi: 10.1016/j.ins.2022.07.120

Martínez-González, R. F., Díaz-Méndez, J. A., Palacios-Luengas, L., López-Hernández, J., & Vázquez-Medina, R. (2016). A steganographic method using Bernoulli's chaotic maps. *Computers & Electrical Engineering*, *54*, 435–449. doi: https://doi.org/10.1016/j.compeleceng.2015.12.005

Megherbi, O., Hamiche, H., & Bettayeb, M. (2024). Implementation of a wireless text data transmission based on the impulsive control of fractional-order chaotic systems. *Computers and Electrical Engineering*, *116*, 109224. doi: https://doi.org/10.1016/j.compeleceng.2024.109224

Meng, F., & Gu, Z. (2023). A Color Image-Encryption Algorithm Using Extended DNA Coding and Zig-Zag Transform Based on a Fractional-Order Laser System. *Fractal and Fractional*, *7*(11). doi: 10.3390/fractalfract7110795

Morkel, T., Eloff, J. H. P., & Olivier, M. S. (2005). A*n overview of image steganography*. In Information Security for South Africa. https://api.semanticscholar.org/CorpusID:11829365

Munoz-Pacheco, J. M., Zambrano-Serrano, E., Volos, C., Jafari, S., Kengne, J., & Rajagopal, K. (2018). A New Fractional-Order Chaotic System with Different Families of Hidden and Self-Excited Attractors. *Entropy*, *20*(8). doi: 10.3390/e20080564

NIST. (1994). *Security Requirements for Cryptographic Modules (FIPS 140-1)*. Retrieved from https://csrc.nist.gov/files/pubs/fips/140-1/upd1/final/docs/fips1401.pdf

Yavuz, N. (2006). *Kaotik Ortamlarda Güvenli Veri Transferi* (Yayın No. 182987) [Yüksek lisans tezi, Karadeniz Teknik Üniversitesi]. Ulusal Tez Merkezi.

NVIDIA. (2024). *NVIDIA Jetson AGX Orin Module*. Retrieved from https://www.nvidia.com/en-us/autonomous-machines/embedded-systems/jetson-orin/

Ozkaynak, F. (2020). A Novel Random Number Generator Based on Fractional Order Chaotic

Chua System. *Elektronika Ir Elektrotechnika*, *26*(1), 52–57. doi: 10.5755/j01.eie.26.1.25310

Pak, C., Kim, J., An, K., Kim, C., Kim, K., & Pak, C. (2020). A novel color image LSB steganography using improved 1D chaotic map. *Multimedia Tools and Applications*, *79*(1), 1409–1425. doi: 10.1007/s11042-019-08103-0

Parida, P., Pradhan, C., Gao, X.-Z., Roy, D. S., & Barik, R. K. (2021). Image encryption and authentication with elliptic curve cryptography and multidimensional chaotic maps. *IEEE Access*, *9*, 76191–76204.

Pehlivan, I. (2007). *Yeni Kaotik Sistemler: Elektronik Devre Gerçeklemeleri, Senkronizasyon Ve Güvenli Haberleşme Uygulamaları* (Yayın No. 212246) [Doktora tezi, Sakarya Üniversitesi]. Ulusal Tez Merkezi.

Petitcolas, F., Anderson, R., & Kuhn, M. (1999). Information Hiding - A Survey. *Proceedings of the IEEE, 87*, 1062–1078. doi: 10.1109/5.771065

Petráš, I. (2011). *Fractional-Order Nonlinear Systems: Modeling, Analysis and Simulation*. Springer Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-18101-6

Petráš, I. (2022). The fractional-order Lorenz-type systems: A review. *Fractional Calculus and Applied Analysis*, *25*(2), 362–377. doi: 10.1007/s13540-022-00016-4

Por, L. Y., Yang, J., Ku, C. S., & Khan, A. A. (2023). Special Issue on Cryptography and Information Security. *Applied Sciences (Switzerland)*, *13*(10), 10–11. doi: 10.3390/app13106042

Provos, N., & Honeyman, P. (2003). Hide and seek: an introduction to steganography. *IEEE Security & Privacy*, *1*(3), 32–44. doi: 10.1109/MSECP.2003.1203220

Ross, B. (1974). *Fractional calculus and its applications: Proceedings of the international conference held at the University of New Haven, June 1974* (Vol. 457). Springer

Rössler, O. E. (1976). An equation for continuous chaos. *Physics Letters A*. doi: 10.1016/0375-9601(76)90101-8

Sandri, M. (1996). Numerical calculation of Lyapunov exponents. *Math. J.*, *6*.

Santos, A., & Júnior, R. V. (2021). Improving Caesar cipher for greater security. *Kriativ Tech*, https://doi.org/10.31112/kriativ-tech-2021-10-49

Satria, Y., Suryadi, M. T., & Cahyadi, D. J. (2021). Digital text and digital image encryption and steganography method based on SIYu map and least significant bit. *Journal of Physics: Conference Series*, *1821*(1), 12035. doi: 10.1088/1742-6596/1821/1/012035

Sayed, W. S., Roshdy, M., Said, L. A., & Radwan, A. G. (2020). Chaotic Dynamics and FPGA Implementation of a Fractional-Order Chaotic System With Time Delay. *IEEE Open Journal of Circuits and Systems*, *1*, 255–262. doi: 10.1109/OJCAS.2020.3031976

Schindler, W. (2009). *Random number generators for cryptographic applications* (Ç. K. Koç, Ed.). Springer. https://doi.org/10.1007/978-0-387-71817-0_2

Sene, N. (2022). Theory and applications of new fractional-order chaotic system under Caputo operator. *An International Journal of Optimization and Control: Theories & Applications (IJOCTA)*, *12*(1), 20–38. doi: 10.11121/ijocta.2022.1108

Shahna, K. U. (2023). Novel chaos based cryptosystem using four-dimensional hyper chaotic map with efficient permutation and substitution techniques. *Chaos, Solitons & Fractals*, *170*, 113383. doi: https://doi.org/10.1016/j.chaos.2023.113383

Sharafi, J., Khedmati, Y., & Shabani, M. M. (2021). Image steganography based on a new hybrid chaos map and discrete transforms. *Optik*, *226*, 165492. doi: https://doi.org/10.1016/j.ijleo.2020.165492

Sharif, A., Mollaeefar, M., & Nazari, M. (2017). A novel method for digital image steganography based on a new three-dimensional chaotic map. *Multimedia Tools and Applications*, *76*(6), 7849–7867. doi: 10.1007/s11042-016-3398-y

Simmons, G. J. (1983). *Contemporary Cryptography*. (Vol. 2). doi: 10.5860/choice.43-2161

Sprott, J. C. (1994). Some simple chaotic flows. *Phys. Rev. E*, *50*(2), R647--R650. doi: 10.1103/PhysRevE.50.R647

Sun, F., & Liu, S. (2009). Cryptographic pseudo-random sequence from the spatial chaotic map. *Chaos, Solitons and Fractals*, *41*(5), 2216–2219. doi: 10.1016/j.chaos.2008.08.032

Sun, J., Cai, H., Gao, Z., Wang, C., & Zhang, H. (2023). A novel non-equilibrium hyperchaotic system and application on color image steganography with FPGA implementation. *Nonlinear Dynamics*, *111*(4), 3851–3868. doi: 10.1007/s11071-022-07993-4

Tang, C., Chen, J., & Wang, J. (2024). Image Encryption Algorithm Based on 2D-Linear-Infinite-Collapse Chaotic Map and Improved Hilbert Curve. *International Journal of Bifurcation and Chaos*, *34*(06), 2450067. doi: 10.1142/S0218127424500676

Tavazoei, M. S., & Haeri, M. (2008). Chaotic attractors in incommensurate fractional order systems. *Physica D: Nonlinear Phenomena*, *237*(20), 2628–2637.

The MathWorks Inc. (2021). *MATLAB version: 9.11.0 (R2021)*. Natick, Massachusetts, United States: The MathWorks Inc. Retrieved from https://www.mathworks.com

Thenmozhi, S., & Chandrasekaran, M. (2013). A novel technique for image steganography using nonlinear chaotic map. *2013 7Th International Conference on Intelligent Systems and Control (ISCO)*, 307–311.

Thiyagarajan, J., Murugan, B., & Gounden, N. G. A. (2019). A chaotic image encryption scheme with complex diffusion matrix for plain image sensitivity. *Serbian Journal of Electrical Engineering*, *16*(2), 247–265.

TL431 Data Sheet (Issue May). (2023). Retrieved from www.ti.com

Tokatlıoğlu, S. (2024). *Kaotik Haritalar Ve Steganografi Yöntemleri Kullanılarak Önem Derecesi Yüksek Verilerin Görüntü İçerisine Gizlenmesi* (Yayın No. 856383) [Yüksek lisans tezi, T.C. Maltepe Üniversitesi]. Ulusal Tez Merkezi

VenkatramanS, Abraham, A., & Paprzycki, M. (2004). Significance of steganography on data security. *International Conference on Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004.*, *2*, 347-351 Vol.2. doi: 10.1109/ITCC.2004.1286660

Vogels, M., Zoeckler, R., Stasiw, D. M., & Cerny, L. C. (1975). P. F. Verhulst's "notice sur la loi que la populations suit dans son accroissement" from correspondence mathematique et physique. Ghent, vol. X, 1838. *Journal of Biological Physics*, *3*(4), 183–192. doi: 10.1007/BF02309004

Verhulst, P. F. (1838). *Notice sur la loi que la population suit dans son accroissement*. Correspondence Mathematique et Physique (Ghent), 10, 113-121.

Walker, J. (2008). *ENT-a pseudorandom number sequence test program*. Retrieved from www.fourmilab.ch/random/

Wang, N., Cui, M., Yu, X., Shan, Y., & Xu, Q. (2024). Generation of no-equilibrium multi-fold chaotic attractor for image processing and security. *Applied Mathematical Modelling*, *133*, 271–285. doi: https://doi.org/10.1016/j.apm.2024.05.022

Wang, X.-Y., Gu, S.-X., & Zhang, Y.-Q. (2015). Novel image encryption algorithm based on cycle shift and chaotic system. *Optics and Lasers in Engineering*, *68*, 126–134. doi: https://doi.org/10.1016/j.optlaseng.2014.12.025

Wang, Z., & Bovik, A. C. (2002). A universal image quality index. *IEEE Signal Processing Letters*, *9*(3), 81–84. doi: 10.1109/97.995823

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*. Cengage Learning.

William, S. (2017). C*ryptography and network security: Principles and practice*. Pearson Education India.

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. doi: https://doi.org/10.1016/0167-2789(85)90011-9

Xu, C., Liu, Z., Pang, Y., Saifullah, S., & Khan, J. (2023). Torus and fixed point attractors of a new hyperchaotic 4D system. *Journal of Computational Science*, *67*, 101974. doi: https://doi.org/10.1016/j.jocs.2023.101974

Xu, S., Wang, X., & Ye, X. (2022). A new fractional-order chaos system of Hopfield neural network and its application in image encryption. *Chaos, Solitons & Fractals*, *157*, 111889. doi: https://doi.org/10.1016/j.chaos.2022.111889

Yang, F., Mou, J., Ma, C., & Cao, Y. (2020). Dynamic analysis of an improper fractional-order laser chaotic system and its image encryption application. *Optics and Lasers in Engineering*, *129*, 106031. doi: 10.1016/j.optlaseng.2020.106031

Yardım, F., & Afacan, E. (2013). Lorenz-Tabanlı Diferansiyel Kaos Kaydırmalı Anahtarlama (Dcsk) Modeli Kullanılarak Kaotik Bir Haberleşme Sisteminin Simülasyonu. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, *25*(1).

Yassein, M. B., Aljawarneh, S., Qawasmeh, E., Mardini, W., & Khamayseh, Y. (2017). Comprehensive study of symmetric key and asymmetric key encryption algorithms.

2017 International Conference on Engineering and Technology (ICET), 1–7. doi: 10.1109/ICEngTechnol.2017.8308215

Ye, G. (2010). Image scrambling encryption algorithm of pixel bit based on chaos map. *Pattern Recognition Letters*, *31*(5), 347–354. doi: https://doi.org/10.1016/j.patrec.2009.11.008

Yousefian Darani, A., Khedmati Yengejeh, Y., Navarro, G., Pakmanesh, H., & Sharafi, J. (2024). Optimal location using genetic algorithms for chaotic image steganography technique based on discrete framelet transform. *Digital Signal Processing*, *144*, 104228. doi: https://doi.org/10.1016/j.dsp.2023.104228

Yu, Y., Li, H.-X., Wang, S., & Yu, J. (2009). Dynamic analysis of a fractional-order Lorenz chaotic system. *Chaos, Solitons & Fractals*, *42*(2), 1181–1189. doi: https://doi.org/10.1016/j.chaos.2009.03.016

Zajac, B. P. (1994). Applied cryptography: Protocols, algorithms, and source code in C. *Computers \& Security*, *13*, 217–218. Retrieved from https://api.semanticscholar.org/CorpusID:57917681

Zhang, Y.-Q., Hao, J.-L., & Wang, X.-Y. (2020). An Efficient Image Encryption Scheme Based on S-Boxes and Fractional-Order Differential Logistic Map. *IEEE Access*, *8*, 54175–54188. doi: 10.1109/ACCESS.2020.2979827

Zhang, Y., Xiao, D., Shu, Y., & Li, J. (2013). A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations. *Signal Processing: Image Communication*, *28*, 292–300. doi: 10.1016/j.image.2012.12.009

Zhao, M., Yuan, Z., Li, L., & Chen, X.-B. (2024). A novel efficient S-box design algorithm based on a new chaotic map and permutation. *Multimedia Tools and Applications*, *83*(24), 64899–64918. doi: 10.1007/s11042-023-17720-9

Zhou, G., Zhang, D., Liu, Y., Yuan, Y., & Liu, Q. (2015). A novel image encryption algorithm based on chaos and Line map. *Neurocomputing*, *169*, 150–157. doi: 10.1016/j.neucom.2014.11.095

Zhou, Shihua. (2021). A real-time one-time pad DNA-chaos image encryption algorithm based on multiple keys. *Optics & Laser Technology*, *143*, 107359. doi: https://doi.org/10.1016/j.optlastec.2021.107359

Zhou, Shuang, Qiu, Y., Wang, X., & Zhang, Y. (2023). Novel image cryptosystem based on new 2D hyperchaotic map and dynamical chaotic S-box. *Nonlinear Dynamics*, *111*(10), 9571–9589. doi: 10.1007/s11071-023-08312-1

Zhu, S., Deng, X., Zhang, W., & Zhu, C. (2023). Secure image encryption scheme based on a new robust chaotic map and strong S-box. *Mathematics and Computers in Simulation*, *207*, 322–346. doi: 10.1016/j.matcom.2022.12.025

Dış Kapak Sırt

Dış Kapak_Arka

T.C.
YOZGAT BOZOK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

Tez Ön Kapak, Sırt ve Arka Kapak görünümü

T.C.
YOZGAT BOZOK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
..... ANABİLİM DALI

TEZ BAŞLIĞI
(Büyük harflerle ve ortalanmış olarak tez adı bu bölüme yazılacaktır)

ADINIZI SOYADINIZ

YÜKSEK LİSANS/DOKTORA TEZİ

Danışman: Unvanı Adı SOYADI
İkinci Danışman (varsa): Unvanı Adı SOYADI

ARALIK – 2022
YOZGAT

Ahmet BOZOK

YÜKSEK LİSANS TEZİ

YOZGAT 2022

T.C.
YOZGAT BOZOK ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ