T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KAOS TABANLI HİBRİT SİMETRİK VE ASİMETRİK ŞİFRELEME ALGORİTMALARI TASARIMI VE UYGULAMASI

DOKTORA TEZİ

Ünal ÇAVUŞOĞLU

Enstitü Anabilim Dalı	**:**	**BİLGİSAYAR VE BİLİŞİM MÜHENDİSLİĞİ**
Tez Danışmanı	**:**	**Doç. Dr. Ahmet ZENGİN**

Aralık 2016

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KAOS TABANLI HİBRİT SİMETRİK VE ASİMETRİK ŞİFRELEME ALGORİTMALARI TASARIMI VE UYGULAMASI

DOKTORA TEZİ

Ünal ÇAVUŞOĞLU

Enstitü Anabilim Dalı : BİLGİSAYAR VE BİLİŞİM MÜHENDİSLİĞİ

Bu tez 23/12/2016 tarihinde aşağıdaki jüri tarafından Oybirliği/~~Oyçokluğu~~ ile kabul edilmiştir.

Doç. Dr. Ahmet ZENGİN Jüri Başkanı	Doç. Dr. İhsan PEHLİVAN Üye	Doç. Dr. Ayhan İSTANBULLU Üye
Doç. Dr. Resul KARA Üye	Yrd. Doç. Dr. Murat İSKEFİYELİ Üye	

BEYAN

Tez içindeki tüm verilerin akademik kurallar çerçevesinde tarafımdan elde edildiğini, görsel ve yazılı tüm bilgi ve sonuçların akademik ve etik kurallara uygun şekilde sunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, tezde yer alan verilerin bu üniversite veya başka bir üniversitede herhangi bir tez çalışmasında kullanılmadığını beyan ederim.

Ünal ÇAVUŞOĞLU
23 /12 /2016

TEŞEKKÜR

Öncelikle bizi yaratan ve sayısız nimetlerle nimetlendiren, bu güzel dünyaya gönderen ve bizler için çok daha güzel alemler ihzar edecek olan Zat'a sonsuz teşekkürler ediyorum.

Bu tez çalışmasında danışmanlığımı yaparken bilgi ve birikimlerinden yararlandığım değerli hocam Doç. Dr. Ahmet ZENGİN'e, desteğini hiçbir zaman esirgemeyen Doç. Dr. İhsan PEHLİVAN'a, tez jürimde bulunan ve fikirleriyle katkıda bulunan Yrd. Doç. Dr. Murat İSKEFİYELİ'ye, tez çalışmasında desteklerini esirgemeyen Yrd. Doç. Dr. Sezgin KAÇAR'a tez çalışmasının gerçekleştirilmesi için destek sağlayan ve emeği geçen herkese teşekkür ederim.

Ayrıca maddi ve manevi desteklerini her zaman hissettiğim eşime ve çocuklarıma, üzerimde çok emekleri olan anneme ve ahiret alemine göç etmiş babama çok teşekkürler ediyorum. Şehadet şerbetini içen tüm şehitlerimize de Allah'tan rahmetler diliyorum.

Bu çalışma Sakarya Üniversitesi Bilimsel Araştırma Projeleri kapsamında desteklenmiştir (Proje Numarası: 2016-12-10-007).

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

3DES	: Triple Data Encryption Standard
AES	: Advanced Encryption Standard
BIC	: Bit Independence Criteria
CRSA	: Chaos based Rivest Shamir Adleman
CS-AES	: Chaos based Simplified Advanced Encryption Standard
CBC	: Cipher Block Chaining
CFB	: Cipher Feedback
CTR	: Counter Mode
cov	: Kovaryans
DES	: Data Encryption Standard
DP	: Differantial approximation probability
ECC	: Elliptic Curve Cryptography
ECB	: Electronic Codebook
FFT	: Discrete Fourier Transform
GCD	: Greatest Common Denominator
GF	: Galois Field
IEEE	: The Institute of Electrical and Electronical Engineers
IEEE-754	: IEEE Kayan noktalı sayı formatı
J	: Kaotik Sistemlere ait Jacobian Matrisi
Kb	: Kilo Bayt
k1	: RK4 algoritmasında ilk hesaplanan değişken
k2	: RK4 algoritmasında ikinci hesaplanan değişken
k3	: RK4 algoritmasında üçüncü hesaplanan değişken
k4	: RK4 algoritmasında dördüncü hesaplanan değişken
LSB	: Least Significant Bit

Matlab	: Matrix laboratory
NCS	: Yeni Kaotik Sistem-1
Nr	: Döngü Sayısı
NPCR	: Number of Pixels Change Rate
NIST	: National Institute of Standards and Technology
OFB	: Output Feedback
PRNG	: Pseudo Random Number Generator
p-değeri	: NIST-800-22 testlerinde hesaplanan rasgelelik değeri
QoS	: Quality of Service
RK4	: Dördüncü dereceden Runge-Kutta algoritması
RK5	: Beşinci dereceden Runge-Kutta algoritması
RC4	: Rivest Cipher 4
RC5	: Rivest Cipher 5
RC6	: Rivest Cipher 6
RSA	: Ronald, Shamir, Adleman
RSÜ	: Rasgele Sayı Üreteci
S-Box	: Substitution-Box
S-AES	: Simplified Advanced Encryption Standard
SRTP	: Secure Real Time Protocol
SAC	: Strict Avalanche Criteria
SPN	: Substitution-Permutation Networks
sn.	: Saniye
TCP	: Transmission Control Protocol
TRNG	: True Random Number Generator
UACI	: Unified Average Changing Intensity
XOR	: eXclusive OR
λ	: Kaotik Sisteme ait Özdeğerler
Δh	: Örnekleme adım aralığı

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar kelimeler: Kaos, Kaos Tabanlı Şifreleme, Simetrik-Asimetrik Şifreleme Algoritmaları, RSA, AES, Rasgele Sayı Üreteci, S-Box

Bilişim alanında yaşanan hızlı gelişmeler ile birlikte, veri güvenliğinin sağlanması günümüzün en önemli konularından birisi olmuştur. Veri güvenliğinin sağlanması için daha yüksek güvenlik seviyesine sahip aynı zamanda etkin şifreleme sistemlerinin geliştirilmesine çalışılmaktadır. Modern şifreleme algoritmaları özellikle büyük boyutlu veriler ve gerçek zamanlı uygulamalarda ağır işlem yüklerinden dolayı performans kaybına sebep olmaktadır. Kaotik sistemlerin şifreleme tasarımında kullanılması, kaos ve kriptoloji bilimleri arasındaki ilişkinin ortaya konması sonucu ortaya çıkmıştır. Kaotik sistemler sahip olduğu özelliklerden dolayı, kriptolojik uygulamaların temel gereksinimleri olan karıştırma ve yayılma özelliklerini sağlamaktadırlar. Bu tez çalışmasının amacı, kaotik sistemlerin zengin dinamik özellikleri ile modern şifreleme algoritmalarının güçlü yönlerini bir araya getirerek, yüksek güvenlikli ve efektif kaos tabanlı hibrit şifreleme algoritmaları tasarımları gerçekleştirmektir. Tez çalışmasında aşağıdaki temel adımlar gerçekleştirilmiştir:

i. Şifreleme çalışmalarında kullanılmak üzere; literatürdeki kaotik sistemlere alternatif olarak, iki yeni kaotik sistem (NCS ve skala edilmiş Zhongtang) tasarlanmış ve analizleri yapılmıştır. Yapılan analizler ile yeni sistemlerin zengin dinamik özelliklere ve rasgeleliğe sahip olduğu gösterilmiştir.
ii. Yeni geliştirilen kaotik sistemler ile geliştirilecek şifreleme algoritmalarında rasgele sayıların üretimi için iki yeni RSÜ tasarımı yapılmıştır. Yeni RSÜ'lerden elde edilen bit dizilerinin yeterli rasgeleliğe sahip oldukları, NIST 800-22 testleri ile ortaya konmuştur.
iii. Blok şifreleme algoritmalarının en önemli bileşenlerinden olan S-Box üretimi için, yeni geliştirilen RSÜ'nün kullanıldığı yeni kaos tabanlı S-Box üretim algoritması geliştirilmiştir. Önerilen S-Box'lar üzerinde performans testleri gerçekleştirilmiştir. S-Box performans test sonuçları literatürdeki kaos tabanlı diğer çalışmalar ile karşılaştırılarak, önerilen S-Box'ların saldırılara karşı daha güçlü ve dayanıklı olduğu gösterilmiştir.
iv. RSÜ ve S-Box algoritmalarının tasarımından sonra; RSÜ-1 ile kaos tabanlı asitmetrik şifreleme algoritması CRSA, RSÜ-2 ve S-Box üretim algoritmaları ile kaos tabanlı simetrik hibrit şifreleme algoritması CS-AES geliştirilmiştir.
v. Yeni şifreleme algoritmaları ile resim şifreleme uygulamaları yapılmış ve şifreleme çalışmaları üzerinde güvenlik ve performans analizleri gerçekleştirilmiştir. Geliştirilen hibrit şifreleme algoritmalarının resim şifreleme uygulamalarına ait güvenlik ve performans analiz sonuçları, modern şifreleme algoritmalarının sonuçları ile karşılaştırılarak, saldırılara karşı daha güçlü ve dayanıklı, daha kısa sürede şifreleme gerçekleştiren ve efektif bellek kullanımına sahip oldukları gösterilmiştir.

DESIGN AND IMPLEMENTATION OF CHAOS BASED HYBRID SYMETRIC AND ASYMETRIC ENCRYPTION ALGORITHMS

SUMMARY

Keywords: Chaos, Chaos Based Encryption, Symmetric-Asymmetric Encryption Algorithms, RSA, AES, Random Number Generator, S-Box

With the rapid development in the field of information, data security has become one of the most important issues of today. To ensure data security, the studies are continued to develop encryption systems with higher security levels and performance. Modern encryption algorithms cause performance loss due to heavy processing loads especially in real-time applications and for large-size data. Chaotic systems provide the confusion and diffusion properties that are main requirements of cryptography, due to their inherent properties. The aim of this thesis is to design high-security and effective chaos-based hybrid encryption algorithms by combining the powerful features of chaotic systems with the powerful aspects of modern encryption algorithms. The following basic steps have been performed in the thesis study:

i. For use in encryption operations; As an alternative to the chaotic systems in the literature, two new chaotic systems are designed and analyzed. It has been shown that the new systems have rich dynamic features and randomness.
ii. Two new RNGs are designed for generation of random number in the new chaos based encryption algorithms. Sufficient randomness of the bit sequences obtained from the new RNGs is proven with NIST 800-22 tests.
iii. For S-Box generation, a new chaos-based S-Box generation algorithm has been developed using the new RNG. Performance tests have been carried out on the proposed S-Boxes to prove strong cryptographic features. Comparing the S-Box performance test results with other chaos-based studies in the literature has shown that the proposed S-Boxes are stronger and more resistant to attacks.
iv. After the design of RNG's and S-Box algorithms; a chaos-based asymmetric encryption algorithm (CRSA) using RNG-1 and the chaos-based symmetric hybrid encryption algorithm (CS-AES) using RNG-2 and S-Box generation algorithms have been developed.
v. The image encryption have been realized with the new encryption algorithms; security and performance analyzes have been carried out. The test results of the image encryption applications of the developed algorithms have been shown that they are stronger and more robust against attacks, perform encryption in a shorter time and have efficient memory usage compared with the results of modern encryption algorithms.

BÖLÜM 1. GİRİŞ

Dünyayı ve kâinatı incelediğimizde, aslında herşeyin birbiri ile irtibatlı ve müthiş bir nizam, intizam ve düzen içinde hareket ettiğini farkedebiliriz. En karmaşık ve birbirinden ayrık görünen şeylerin içinde bile bu intizamı ve düzeni görmek mümkündür. İşte kaos dediğimiz kavram, görünüşte düzensiz ve karmakarışık olarak görünen şeyler içindeki düzeni ortaya koyan bir bilim dalıdır. Kaos kuramına göre herşey birbiri ile bağlı ve bir düzen içinde hareket etmektedir [1]. Kaos kuramı ile ilgili birçok farklı bilim dalında çalışmalar gerçekleştirilmiştir. Bu alanlardan birisi de kaos tabanlı sistemlerin bilgisayar bilimlerinde ve özellikle şifreleme uygulamalarında kullanılmasıdır. Günümüzde özellikle internetin yaygınlaşması, bilgisayar ağlarındaki veri transferinin artması ve iletişim teknolojilerindeki gelişmeler ile birlikte veri güvenliğinin sağlanması en önemli konulardan birisi olmuştur [2]. İnternet herkese açık bir ortam olduğu için, veri güvenliği hayati bir konudur. Veri güvenliğinin sağlanması adına, hem bireysel hemde kurumsal anlamda çalışmalar gerçekleştirilmektedir. Veri güvenliği ihlalinde, bireylerin şahsi bilgileri veya kurumlara, ülkelere ait çok kritik bilgiler deşifre edilmektedir. Veri güvenliğini sağlamak adına yapılan çalışmalar gün geçtikçe artmakta ve giderek daha da önem kazanan bir konu olmaktadır [3]. Geliştirilen şifreleme sistemlerinin daha yüksek güvenlik seviyelerine sahip olması için çalışmalar devam etmektedir. Gerçek zamanlı uygulamalar ve büyük boyutlu veriler üzerindeki işlemlerde, güvenlik seviyesinin yanı sıra performans ve kaynak tüketim değerleri algoritmaların değerlendirilmesinde önemli bir hale gelmiştir. Modern şifreleme algoritmaları, büyük boyutlu verilerin şifrelenmesinde ve gerçek zamanlı veri şifrelemede, işlem yüklerinden dolayı dezavantajlar oluşturmaktadır.

Yapılan çalışmalarda, kaotik sistemler ile kriptoloji biliminin yakın ilişki gösterdiği tespit edilmiştir [4,5]. Kaotik sistemler, rasgelelik, ergodiklik, kontrol ve başlangıç parametrelerine hassas bağımlı olmaları sayesinde, kriptolojinin temel gereksinimleri

olan karıştırma ve yayılma özelliklerini karşılamaktadır. Ergodiklik, kaotik sistemlerin takip ettiği yörüngenin, uzun süreli durumlar için başlangıç şartlarına ve sistem parametrelerine olan bağlılığını ifade etmektedir. Kaotik sistemler bir düzen içinde görünmesine rağmen oldukça rassal çıktılar üretmektedir [6]. Kaos ve kriptoloji arasındaki bu ilişkinin kullanılması ile birçok çalışma gerçekleştirilmiştir. Bu çalışmalar literatür özetlerinde verilecektir.

Bu tez çalışmasında kaotik sistemlerin zengin rassallık özellikleri ve modern şifreleme algoritmaları kullanılarak, yüksek güvenlik seviyesine sahip ve performanslı hibrit şifreleme algoritmalarının geliştirilmesi hedeflenmiştir. Kaos tabanlı hibrit şifreleme algoritmalarının tasarımında, modern şifreleme algoritmaları ile birlikte dinamik özellikleri yüksek yeni kaotik sistemler, bu kaotik sistemlerin kullanıldığı RSÜ ve yeni S-Box üretim algoritmaları kullanılmıştır.

1.1. Tezin Amacı ve Katkıları

Bu tez çalışmasında, literatürdeki modern ve kaos tabanlı şifreleme algoritmalarından daha güvenli ve performanslı yeni kaos tabanlı hibrit şifreleme algoritmalarının tasarımı amaçlanmaktadır. Bu amaca ulaşabilmek için aşağıdaki işlemler gerçekleştirilmiştir.

- RSÜ tasarımında kullanılmak üzere, dinamik yapısı karmaşık ve rasgeleliği daha yüksek yeni kaotik sistem tasarımlarının gerçekleştirilmesi,
- Yeni tasarlanan kaotik sistemleri kullanan ve ürettiği rasgele sayı dizileri tüm NIST testlerinden geçen özgün RSÜ tasarımlarının gerçekleştirilmesi,
- Yeni tasarlanan RSÜ'nün kullanıldığı kaotik S-Box üretim algoritmasının tasarlanması ve literatürdeki kaos tabanlı çalışmalardan daha iyi performans sonuçlarına sahip S-Box'ların üretimi,
- Yeni tasarlanan RSÜ'nün ve S-Box üretim algoritmalarının kullanıldığı yüksek hızlı ve güvenlikli simetrik (CS-AES) ve asimetrik (CRSA) hibrit şifreleme algoritmalarının tasarımı ve

- Geliştirilen şifreleme algoritmaları ile resim şifreleme uygulamalarının gerçekleştirilmesi, şifreleme işlemlerine ait performans ve güvenlik testlerinin yapılması.

Çalışmada yeni geliştirilecek olan dinamik özellikleri yüksek kaotik sistem tasarımları, RSÜ algoritmaları ve S-Box üretim algoritması literatüre kazandırılarak başka çalışmalarda da kullanılabilecektir. Ayrıca geliştirilen yapıların kullanıldığı yeni kaos tabanlı hibrit şifreleme algoritmaları da yeni şifreleme sistemleri olarak sunulmuştur. Literatürdeki ve gerçek ortam uygulamaları incelendiğinde, sadece kaos tabanlı veya modern şifreleme yöntemlerinin kullanıldığı çalışmalar bulunduğu görülmüştür. Sadece kaotik sistemlerin kullanıldığı şifreleme çalışmalarındaki güvenlik zafiyetleri literatürdeki çalışmalarda ortaya konmuştur. Yüksek güvenlikli ve efektif şifreleme işlemi için, kaotik sistemlerin ve modern şifreleme algoritmalarının güçlü yönlerini bir araya getiren, kaos tabanlı hibrit şifreleme yöntemlerinin kullanılması ile daha güvenlikli ve performanslı bir şifreleme sağlanmış olacaktır.

1.2. Literatürde Yapılan Çalışmaların Özetleri

Kaotik sistemler, güvenli haberleşmenin sağlanması için, farklı kriptolojik tasarımlarda yaygın olarak kullanılmaktadır. Bu bölümde, tezde çalışma konuları olan kaos tabanlı şifreleme algoritmaları, kaos tabanlı rasgele sayı üreteçleri, S-Box üretim algoritmaları ve hibrit şifreleme algoritmalarına ait literatür verilecektir. Literatürde kaos tabanlı şifrelemenin kullanıldığı bir çok çalışma vardır.

Bakhache ve arkadaşları [7] yapmış oldukları çalışmada yeni bir kaotik şifreleme algoritması önermişlerdir. Çalışmada önerilen kaotik şifreleme algoritması özellikle Zigbee ağlarında kullanım üzerine tasarlanmıştır. Wang ve arkadaşları [8] yeni bir kaos tabanlı şifreleme algoritması önermişlerdir. Çalışmada şifrelemenin iki ana gereksinimi olan karıştırma ve yayılma özelliklerini sağlayan iki ayrı adımın birleştirilerek tek adımda tüm resim piksellerinin taranarak işlem görmesini sağlayacak bir mimari sunulmuştur. Liu ve arkadaşları [9] çalışmalarında kablosuz algılayıcı ağlarda kullanılmak üzere yeni bir kaotik şifreleme algoritması

tasarlamışlardır. Chen ve arkadaşları [10] kablosuz algılayıcı ağlarda güvenli iletişimin sağlanması için kaos tabanlı yeni bir blok şifreleme algoritması önermişlerdir. Kablosuz algılayıcı ağlar üzerinde çalışan düğümlerin enerji tüketimi ve bellek kullanımı gibi kısıtlarından dolayı daha az enerji tüketen ve daha az bellek gereksinimi olan bir mimari oluşturulmaya çalışılmıştır. Mohammed ve arkadaşları [11] RTP (Real Time Protocol) üzerinde gerçekleşen gerçek zamanlı veri aktarımının güvenliğinin artırılması için kaos tabanlı sistemleri kullanarak SRTP (Secure Real Time Protocol) protokolü üzerinde QoS ve güvenliği artıran bir algoritma tasarlamışlardır. Kocarev ve Jakimoski [12] makalelerinde kaos tabanlı algoritma tasarım üzerinde durmuşlardır. Çalışmada kaos ve kriptolojinin yakın ilişkisi hakkında bilgi verilmiş, kriptoloji çalışmalarında kaos tabanlı sistemlerin taşımış olduğu özelliklerden dolayı şifreleme gereksinimlerini karşıladıkları anlatılmıştır. Tong ve arkadaşları [13] kablosuz algılayıcı ağların düşük enerji ve bellek gereksinimi ve sınırlı hesaplama kapasitesi gibi kısıtlarından dolayı, bu sistemlerde kullanılan şifreleme algoritmalarının uygun olmadığını ifade etmiş ve bu gereksinimleri karşılayacak kaos tabanlı yeni bir şifreleme algoritması önermişlerdir.

Tong ve arkadaşları [14] kablosuz algılayıcı ağlar için, kübik ve lojistik kaotik haritalarını kullanan bileşik bir kaos tabanlı şifreleme algoritması tasarlamışlardır. Tasarımda kaotik haritaların birlikte kullanılmasının yanında, fiestel ağ mimarisi kullanılmıştır. Çavuşoğlu ve arkadaşları [15] TCP data paketleri üzerinde kaos tabanlı şifreleme gerçekleştiren, yeni bir model önermişlerdir. Hassan ve arkadaşları [16] çalışmalarında, hızlı ve güvenli bir şifreleme gerçekleştirecek olan kaos tabanlı bir şifreleme algoritması tasarlamışlardır. Mansour ve arkadaşları [17] günümüzde kullanılan şifreleme algoritmalarının karmaşık algoritmik yapılarından dolayı, sınırlı kaynaklara sahip kablosuz algılayıcı ağ düğümleri için kullanışlı olmadığını, bu sistemlerde çalışacak daha az enerji tüketen ve daha kısa sürede işlemlerin gerçekleşebileceği kaos tabanlı bir simetrik şifreleme algoritması tasarlamışlardır. Assad ve arkadaşları [18] çalışmasında kaos tabanlı blok şifreleme algoritmaları ile ilgili genel bir değerlendirme yapmışlardır. AES, 3DES, DES gibi klasik şifreleme algoritmalarından daha esnek, modüler ve kolay uygulanabilir olduğunu ve kaotik üreteçlerin kaos tabanlı şifreleme algoritmalarının en önemli kısmı olduğunu ifade

etmişlerdir. Chen ve arkadaşları [19] makalelerinde, resim şifreleme için 3 boyutlu bir kaotik haritanın kullanıldığı asimetrik bir şifreleme algoritması geliştirmişlerdir. Tasarlanan 3 boyutlu kaotik tabanlı resim şifreleme algoritması, iki boyutlu ve klasik yöntemler ile karşılaştırıldığında daha iyi dağılma özelliğini sağladığından dolayı gerçek zamanlı uygulamalarda kullanılabileceği ifade edilmiştir. Zhang ve Shiliang [20] çalışmalarında, lojistik kaotik haritasını kullanan kaos tabanlı bir resim şifreleme algoritması geliştirmişlerdir. Hraoui ve arkadaşları [21] çalışmalarında resim şifrelemede kullanılmak üzere lojistik kaotik haritasını kullanan kaos tabanlı bir şifreleme algoritması tasarlamış ve AES algoritması ile karşılaştırmalı performans ve güvenlik analizlerini gerçekleştirmişlerdir. Burada kısaca açıklamaları yapılan çalışmaların dışında, literatürde kaotik sistemlerin kullanıldığı birçok şifreleme çalışması bulunmaktadır [22–32].

Kaotik sistemlerin kullanıldığı RSÜ tasarımları da literatürde oldukça yaygındır. Khan ve Jiashu [33] makalelerinde, farklı kaotik sistemler kullanılarak tasarlanan akış şifreleme algoritmaları ve bu algoritmalara ait rasgelelik testlerini yapmışlardır. Özkaynak [34] çalışmasında, lojistik ve skew tent kaotik haritalarını ve Grostl özet fonksiyonunun kullanıldığı hibrit bir rasgele sayı üreteci tasarımı gerçekleştirmiştir. Avaroğlu ve arkadaşları [35] kriptolojik sistemlerde kullanılmak üzere, donanımsal rasgele sayı üreteci içeren hibrit bir şifreleme mimarisi önermişlerdir. Hu ve arkadaşları [36] makalelerinde Chen kaotik sistemini kullanan ve test sonuçlarına göre rasgele karakteristik taşıyan ve ataklara karşı koyabilecek bir rasgele sayı üreteci tasarımı gerçekleştirmişlerdir. Angulo ve arkadaşları [37] yeni bir kaotik osilatör tabanlı rasgele sayı üreteci tasarımı gerçekleştirmişlerdir. Avaroğlu ve arkadaşları [38] çok boyutlu kaotik sarmallı atraktör kullanarak, rasgele sayı üreteci tasarlamışlardır. Zhu ve arkadaşları [39] iris resmi ve kaotik fonksiyonlardan yararlanarak, yeni bir rasgele sayı üreteci tasarımı önermişlerdir. Son yıllarda gerçek ve sözde RSÜ'ler ile ilgili literatürde birçok çalışma bulunmaktadır [40–50]. Kaos tabanlı RSÜ'ler ile birçok ortamda daha güvenli bir şekilde şifreleme işlemleri gerçekleştirilmiştir.

Kaotik sistemlerin kullanıldığı bir başka alan S-Box (Substitution Box - Yer Değiştirme Kutuları) üretimidir. S-Box yapıları blok şifreleme algoritmalarında

doğrusal olmayan karıştırıcı yapılardır. Şifreleme algoritmasında kullanılacak S-Box'un saldırılara karşı dayanıklı, diferansiyel ve lineer kriptanalize dirençli, güçlü kriptolojik özelliklere sahip olması, güçlü bir şifreleme için gereklidir. Tang ve arkadaşları [51] çalışmalarında, lojistik kaotik haritasını kullanan kaos tabanlı bir S-Box üretim algoritması önermişlerdir. Peng ve arkadaşları [52] blok şifreleme algoritmalarında kaotik tabanlı dinamik S-Box yapılarının oluşturulması için yeni bir yaklaşım sunmuşlardır. Özkaynak ve Özer [53] çalışmalarında şifreleme algoritmalarında S-Box yapılarını güçlendirmek için Lorenz kaotik sisteminin kullanıldığı bir yapı önermişlerdir. Zaibi ve arkadaşları [54] çalışmalarında, S-Box'ların kaos tabanlı dinamik yapıda tasarlanması için bir çalışma gerçekleştirmişlerdir. Zaibi ve arkadaşları [55] çalışmalarında kablosuz algılayıcı ağlarda güvenliği artırmak için, şifreleme algoritmalarında kullanılan S-Box yapılarını kaotik tabanlı olarak tasarlamışlardır. Liu ve arkadaşları [56] Chen kaotik haritası ile üretilen S-Box'ın kullanıldığı bir resim şifreleme algoritması önermişlerdir. Özkaynak ve Yavuz [57] çalışmalarında, zaman gecikmeli kaotik sistemler ile kaotik S-Box algoritması tasarımı gerçekleştirmişlerdir. Çalışmada 3 farklı sistem (Ikeda, Sine, Lojistik) kullanılmıştır. Asim ve Jeoti [58] çalışmasında, parçalı ve lojistik kaotik haritalar ile üretilen S-Box'un kullanıldığı, hibrit bir resim şifreleme algoritması tasarımı gerçekleştirmişlerdir. Zaibi ve arkadaşları [59] çalışmalarında bir ve üç boyutlu parçalı iki kaotik sistem ile dinamik S-Box tasarlamışlardır. Önerilen S-Box tasarımlarının Zigbee protokolünde, AES CCM algoritmaları gibi yapılarda güvenli bir şekilde kullanılabileceği ifade edilmiştir. Yukarıda açıklanan çalışmaların haricinde literatürde kaos tabanlı S-Box çalışmaları bulunmaktadır [60–68].

Kaotik sistemler basit iterasyonlar ile rassallığı yüksek bit dizileri üretebilmekte, işlem yükünü ve şifreleme süresini ciddi oranda düşürebilmektedir. Fakat sadece kaotik sistemler ile gerçekleştirilen şifreleme çalışmalarının, kullanılan kaotik sistemlerin iyi analiz edilmemesi, çözümleme işleminde meydana gelen hatalar ve anahtar uzayının doğru tespit edilememesi gibi güvenlik noktasında dezavantajlar taşıdığı ortaya konulmuştur [69–78]. Bu sebeple, sadece kaotik sistemlerin kullanıldığı şifreleme çalışmaları ile birlikte, modern şifreleme algoritmaları ile kaotik sistemlerin birlikte kullanıldığı hibrit şifreleme algoritmaları önerilmiştir. Silva ve arkadaşları [79]

eLoBa(enhanced Lorenz Based) adını verdikleri, Lorenz kaotik haritasını kullanan gelişmiş bir veri akış şifreleme algoritması geliştirmişlerdir. Ginting ve Dillak [80] makalelerinde, dijital resimlerin şifrelenmesi için RC4 şifreleme algoritması ve lojistik kaotik haritasının kullanıldığı karma bir şifreleme algoritması tasarlamışlardır. Test sonuçlarına göre, RC4 akış şifreleme metodu ve lojistik kaotik haritası ile oluşturulan hibrit şifreleme metodunun renkli resimler için alternatif bir şifreleme metodu olduğu görülmüştür. Alireza ve Mirghadri [81] çalışmalarında, Baker's kaotik haritası ve S-AES blok şifreleme algoritmasının kullanıldığı bir resim şifreleme algoritması tasarlamışlardır. Atteya ve Madian [82] çalışmalarında, henon kaotik haritası ve AES algoritması benzeri satır ve sütün karıştırma tekniklerinin kullanıldığı hibrit bir şifreleme algoritmasının, FPGA üzerinde donanımsal gerçekleşmesini yapmışlardır. Huijian ve arkadaşları [83] çalışmalarında, AES ve lojistik kaotik haritasının kullanıldığı bir resim şifreleme algoritması geliştirmişlerdir. Önerilen yöntem yapılan şifreleme çalışmalarında, oto-korelasyon ve yayılma etkileri ölçülerek, sistemin iyi bir şifreleme sağladığı tespit edilmiştir. Nicole ve Backhache [84] yaptıkları çalışmada, biyomedikal uygulamalarda kullanılmak üzere kaotik sistemler kullanılarak güçlendirilmiş bir S-AES algoritması önermişlerdir. Chen ve arkadaşları [85] AES algoritmasında, anahtar dağıtım işlemini gerçekleştirecek, kaotik tabanlı bir sistem önermişlerdir. Çalışmada çift boyutlu lojistik harita kullanılmıştır. Pradhan ve Ajay [86] çalışmalarında AES algoritmasının güvenli bir algoritma olduğu, algoritmada en kritik iki işlemin S-Box oluşturulması ve anahtar dağıtımı olduğu ifade edilmiştir. Çalışmada AES algoritmasının anahtar dağıtımın işleminin, kaotik tabanlı bir yapı tarafından gerçeklemesini sağlayacak bir mimari önerilmiştir. Muhaya çalışmasında [87] uydu görüntülerinin şifrelenmesi için kaotik sistem ve AES algoritmasını kullanan yeni bir algoritma geliştirmiştir. Meghdad ve arkadaşları [88] simetrik blok şifreleme kullanarak, yeni bir kaos tabanlı medikal resim şifreleme algoritması geliştirmişlerdir. Kun ve arkadaşları [89], Zeghid ve arkadaşları [90], Acharya [91] çalışmalarında kaos tabanlı hibrit AES şifreleme algoritması önermişlerdir.

Literatürdeki çalışmalar değerlendirildiğinde, kaotik sistemlerin şifreleme uygulamalarında yaygın olarak kullanıldığı görülmektedir. Kaotik sistemler, şifreleme çalışmalarında anahtar oluşturmada, rasgele sayı üretiminde, protokol tasarımlarında

ve farklı amaçlar için resim şifreleme çalışmalarında yaygın olarak kullanılmıştır. Kaos tabanlı S-Box tasarımlarında ve modern şifreleme algoritmaları ile birlikte hibrit şifreleme algoritmaları tasarımlarında da kullanıldığı görülmektedir. Ayrıca tasarlanan şifreleme algoritmaları üzerinde kriptoanaliz çalışmaları da yapılmıştır. Kaos tabanlı şifreleme üzerine yapılan çalışmalar gün geçtikçe artmakta ve yeni çalışmalar literatüre katılmaktadır.

1.3. Tez Organizasyonu

Bu tez çalışması altı bölümden oluşmaktadır. Giriş bölümünün ardından, ikinci bölümde kriptoloji ile ilgili temel kavramlar özetlenmiş, kaos ve kriptoloji arasındaki bağlantı açıklanmış, rasgele sayı üreteçleri ile ilgili temel bilgiler verilmiş ve NIST testleri kısaca açıklanmıştır. Bölümün devamında blok şifreleme algoritmalarının temel yapılarından olan S-Box hakkında bilgi verilmiş ve S-Box'ların performans testleri kısaca anlatılmıştır. Bölümün sonunda ise AES ve RSA şifreleme algoritması hakkında bilgi verilmiştir.

Üçüncü bölümde, ilk olarak kaotik sistemlerin analiz yöntemleri açıklanmıştır. Ardından yeni tasarlanan NCS kaotik sistemi tanıtılmış ve sistemin analizleri yapılmıştır. Sonrasında RSÜ tasarımlarında kullanılacak olan yeni skala edilmiş Zhongtang kaotik sisteminin skala işlemleri açıklanarak sistem tanıtılmış ve analizleri gerçekleştirilmiştir.

Dördüncü bölümde, geliştirilecek şifreleme algoritmalarında kullanılacak olan rasgele sayıların üretimi için 2 adet RSÜ tasarımı gerçekleştirilmiştir. RSÜ'lerin üretmiş olduğu rasgele sayılara NIST rasgelelik testleri uygulanmıştır. Yeni kaos tabanlı simetrik hibrit şifreleme algoritmasında kullanılmak üzere, kaos tabanlı S-Box üretim algoritması geliştirilmiştir. Geliştirilen S-Box üretim algoritmasının üretmiş olduğu 2 adet S-Box üzerinde performans testleri gerçekleştirilmiş, literatürdeki çalışmalar ile karşılaştırılmıştır. Dördüncü bölümde son olarak, CRSA ve CS-AES adı verilen iki adet simetrik ve asimetrik tabanlı hibrit şifreleme algoritma tasarımları yapılmıştır. Geliştirilen kaos tabanlı hibrit algoritmalar detaylı olarak açıklanmıştır.

Beşinci bölümde, geliştirilen hibrit şifreleme algoritmaları ile resim şifreleme uygulamaları yapılmış, şifreleme uygulamalarının güvenlik ve performanslarını test etmek için kullanılacak olan analizler hakkında bilgi verilmiş ve analizler gerçekleştirilmiştir.

Altıncı ve son bölümde ise, yapılan çalışmalar değerlendirilmiş ve gelecekte yapılabilecek çalışmalar ile ilgili öneriler sunulmuştur.

BÖLÜM 2. TEMEL KAVRAMLAR

2.1. Kriptoloji

Kriptoloji, kriptografi ve kriptoanaliz olmak üzere iki alt bilim dalından oluşan ve genel olarak bilgi güvenliğinin sağlanması üzerine çalışan bilim dalıdır [92]. Kriptografide bilgi güvenliğinin sağlanması için veriler üzerinde şifreleme işlemlerini gerçekleştiren algoritma, protokol gibi yapıların tasarlanması ve uygulanmasına, kriptoanalizde ise şifrelenmiş olan karmaşık veriler üzerinden orijinal veriyi elde etmek için çalışmalar gerçekleştirilmektedir. Kriptoanaliz kısaca şifre çözme bilimi olarakta tanımlanmaktadır [93–95]. Kriptolojide sistemler gönderici ve alıcı tarafı olarak iki yönlü işlem gerçekleştirecek şekilde tasarlanmaktadır. Gönderici tarafında şifreleme, alıcı tarafta ise orijinal metnin elde edilmesi için şifre çözme işlemi gerçekleşmektedir. Kriptolojide şifrelenecek olan veriler, bir anahtar kullanılarak şifreleme işlemine tabi tutulmakta ve şifreli metin elde edilmektedir. Şifrelemenin çözülmesi için ise, alıcı tarafta şifreyi çözecek olan anahtarın kullanılması gerekmektedir. Kriptoloji bilimi, sistem tasarımlarında genellikle matematik bilimini ve alt dallarını kullanmaktadır.

Gönderici ve alıcı arasındaki iletim özellikle günümüzde, herkese açık internet ortamı kullanılarak gerçekleşmektedir. İletim ortamında güvenliğin sağlanması için protokol ve algoritma tasarımları gerçekleştirilmektedir. Bu tasarımlar gönderici tarafında verinin nasıl şifreleneceğini, alıcı tarafında ise nasıl çözüleceğini tanımlayan kurallar ve tekniklerden oluşmaktadır. İletişim kanalında kullanılacak olan, kritik öneme sahip kriptoloji sistemlerinin belli güvenlik gerekesinimlerini taşıması gerekmektedir. Bu gereksimler; veri bütünlüğü (data integrity), kimlik doğrulama (authentication), gizlilik (confidentiality) ve reddedilemezlik (non-repudiation) ilkeleridir [96, 97]. Bu ilkeleri kısaca açıklayacak olursak;

- Veri Bütünlüğü: İletişim kanalında bulunan verinin, üçüncü kişiler tarafından değiştirilmemesini garanti etmektir. İletim kanalında bulunan veri üzerinde üçüncü kişiler tarafından, ekleme, silme veya değiştirme gibi operasyonlar veri üzerinde gerçekleştirilebilir. Veri bütünlüğü bu gibi işlemlerin gerçekleşmediğini garanti etmektedir. Gönderilen verinin üzerinde, alıcı tarafa herhangi bir değişiklik yapılmadan ulaştığını teyit etmek için özetleme ve benzeri teknikler kullanılmaktadır.
- Kimlik Doğrulama: İletişim kanalının iki ucunda bulunan gönderici ve alıcının birbirlerinin kimlik bilgilerini teyit etmesi gerekmektedir. Alıcı tarafına ulaşan verinin, gerçekten veriyi gönderen kişi tarafından gönderildiğini ispatlayan bir gereksinimdir.
- Gizlilik: Gönderici ve alıcı arasında işlem gören verinin üçüncü kişiler tarafından okunmasının engellenmesini sağlayan bir gereksinimdir. Bu gereksinim, iletişim cihazlarının fiziki olarak korunması ve geliştirilen güvenlik protokolleri, algoritma tasarımları vb. yapılar kullanılarak sağlanmaktadır.
- Reddedilemezlik: Gönderici tarafından iletişim kanalına gönderilen verinin, kendisi tarafından gönderildiğini inkâr etmesini engelleyen bir gereksinimdir. Gönderilen verinin ilgili kişi tarafıdan işlem gördüğünü ve gönderildiğini ispatlamada kullanılmaktadır.

2.1.1. Kerckhoffs ilkesi

Kriptolojik sistem tasarımlarında, dikkat edilmesi gereken ilkelerden birisi de Auguste Kerckhoffs tarafından ortaya atılan Kerckhoffs ilkesidir [98]. Bu ilkeye göre tasarlanan kriptolojik yapıların güvenliği sadece ve sadece anahtar gizliliğine bağlı olmalıdır. Şifreleme sistemini çözmeye çalışan kişi, anahtar haricinde sistem hakkında tüm detayları bilse bile şifreyi çözememelidir. Tasarlanacak olan güvenli sistemlerin bu ilkeye uyması gerekmektedir.

Cloude Shannon [99] yayınlamış olduğu makalesinde güçlü bir şifreleme sistemi tasarımının, karıştırma ve yayılma özelliklerini sağlaması gerektiğini ifade etmektedir. Bir şifreleme sisteminin, karıştırma özelliğine sahip olması için, her bir şifreleme

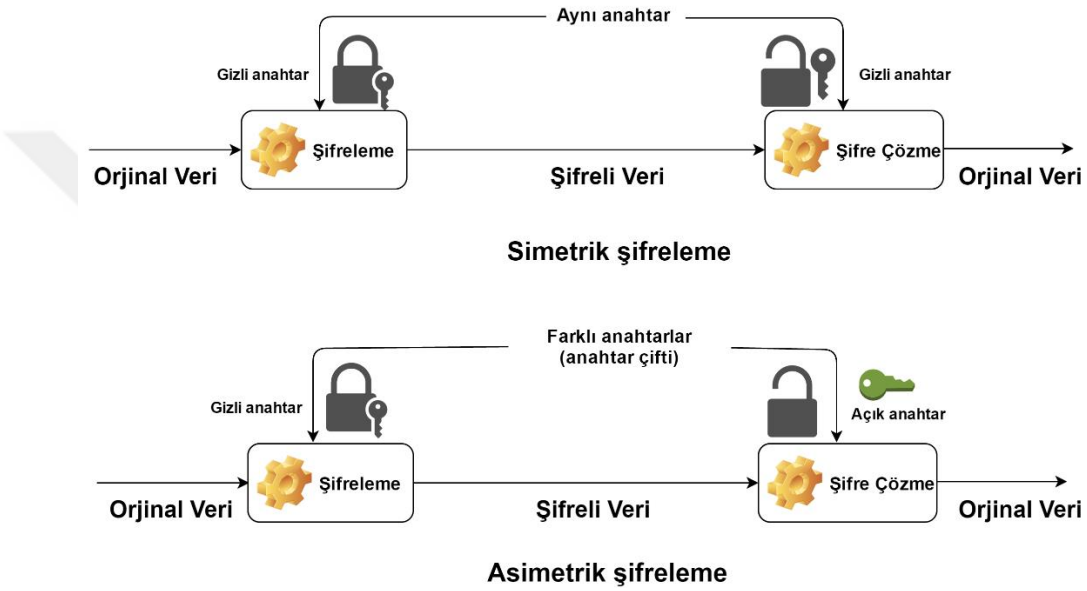
anahtarı ile şifreli metin arasındaki ilişkinin, istatistiki metotlar kullanılarak tespit edilememesi gerekmektedir. Karıştırma özelliğinin sağlanması için daha çok yerine koyma tekniklerini içeren yapılar kullanılmaktadır. Bu özelliğin sağlanması için şifreleme anahtarı, şifreli metinin her bir biti üzerinde bir etki oluşturmalıdır. Yayılma özelliği ise, orijinal metin üzerinde bir karakter üzerinde gerçekleştirilecek olan değişimin şifreli metinde birden çok karakter üzerinde değişime sebep olmasını ifade etmektedir. Yayılma özelliğinde amaç, incelenecek olan şifreli ve düz metin çiftleri üzerinde yapılacak olan incelemelerde anahtarın tespit edilmesini sağlayacak istatistiki bağların gizlenmesidir. Güvenli bir kripto sistem tasarımı için, karıştırma ve yayılma özelliğini birlikte sağlayan yapıların geliştirilmesi zorunludur.

2.1.2. Simetrik ve asimetrik şifreleme

Güvenli bir kripto sistemin tasarımı için geliştirilen şifreleme algoritmaları, simetrik ve asimetrik olarak sınıflandırılabilir. Şekil 2.1.'de simetrik ve asimetrik şifreleme blok diyagramları görülmektedir. Simetrik şifreleme algoritmaları, şifreleme ve çözme işlemlerinde aynı anahtarın kullanıldığı ve anahtarın alıcı tarafına güvenli bir kanal üzerinden aktarıldığı sistemlerdir. Gönderici tarafında şifreleme anahtarı kullanılarak şifrelenmiş olan veri iletim kanalı üzerinden alıcı tarafa gönderilmekte ve güvenli bir kanal üzerinden iletilen şifreleme anahtarı ile çözülerek orijinal veri elde edilmektedir [2], [100]. Simetrik şifrelemede şifreleme ve çözme işlemleri için tek anahtar kulllanıldığı için, anahtarı bilen veya ele geçiren kişi tüm iletişimi çözebilmektedir. Simetrik şifreleme algoritmaları değerlendirildiğinde, asimetrik yapılara göre hızlıdır fakat anahtar dağıtım problemleri ve bazı güvenlik gereksinimlerini karşılamama gibi dezavantajları bulunmaktadır. Ayrıca güvenliğin sağlanması için, kullanılan anahtarların yeterli uzunlukta olması gerekmektedir.

Simetrik şifreleme algoritmaları da blok ve akış şifreleme algoritmaları olarak iki kısma ayrılmaktadır. Blok şifreleme algoritmaları, orijinal metindeki sabit boyuta sahip veri bloklarını şifreleme işlemine tabi tutarak aynı boyuttaki şifreli veriyi elde etmektedirler. Şifre çözme işlemi ise, yine aynı anahtar kullanılarak, tersi işlem uygulanıp aynı boyuttaki orijinal verinin elde edilmesi işlemidir. Literatürde tanımlı simetrik blok şifreleme algoritmalarına örnek olarak Data Encryption Standart (DES)

[101], Triple DES (3DES) [102], Advanced Encryption Standart (AES) [103] verilebilir. Blok şifreleme algoritmalarında, Feistel ve SPN(Substitution-Permutation Networks) mimarilerinin kullanıldığı yapılar tercih edilmektedir [104]. Her iki mimaride çoklu döngüler içinde üretilen yeni anahtarlar kullanılarak şifreleme ve çözme işlemleri gerçekleştirilir. DES algoritması Feistel mimarisini AES algoritması ise SPN mimarisini kullanmaktadır. SPN mimarisinde veri bloğunun tamamı işlem görürken, Feistel mimarisinde ise veri bloğunun yarısı üzerinde işlem yapılmaktadır.



Şekil 2.1. Simetrik ve Asimetrik şifreleme blok diyagramı

Akış şifreleme algoritmaları, simetrik şifreleme algoritmalarının diğer bir tasarım biçimidir. Rivest Cipher 4 (RC4) ve Rivest Cipher 5 (RC5) [105] yaygın olarak bilinen akış şifreleme algoritmalarıdır. Akış şifreleme algoritmalarında, blok şifrelemedeki veri bloklarının yerine, verinin bitleri üzerinde üretilen değişken boyuttaki anahtar ile şifreleme işlemi gerçekleştirilmektedir. Akış şifrelemede üretilecek olan anahtarın boyutu veya özelliği şifrelenecek olan veriye göre farklılık göstermektedir. Orijinal metindeki verinin boyutuna eşit şifreleme anahtarı RSÜ tarafından üretilerek, bit bazında XOR işlemi ile veri şifrelenmektedir. Blok şifreleme işlemleri ile karşılaştırıldığında daha hızlı bir şifreleme gerçekleştirilmektedir.

Asimetrik şifreleme güvenli iletişim için kullanılan bir diğer şifreleme algoritması türüdür. Simetrik şifreleme algoritmalarından farklı olarak bu algoritmalarda, tek bir

anahtar yerine şifreleme ve çözme işlemlerinde kullanılmak üzere, iki farklı anahtar mevcuttur. Simetrik şifrelemedeki en büyük sorun, tüm güvenliğin anahtara bağlı olması ve bu anahtarın taraflar arasında paylaşım sorunudur. Asimetrik şifrelemede anahtar paylaşımına ihtiyaç duyulmaması sebebiyle güvenlik artmaktadır. Daha büyük boyuta sahip bir anahtarın kullanımı, güvenlik seviyesini artıracaktır. Fakat işlem yükünü artıracağı için daha fazla kaynak kullanımına sebep olacak ve şifreleme-çözme süresini uzatacaktır. Asimetrik şifrelemede, herkesin bildiği genel ve kişiye özel olan gizli anahtar olmak üzere iki adet anahtar kullanılmaktadır. İletişim genel anahtar ile yapılırken, gizli anahtarın hiçbir şekilde gönderimi söz konusu değildir. Gönderici kendisine gönderilen genel anahtar ile orijinal veriyi şifreleyip, alıcıya göndermektedir [2], [100]. Alıcı tarafına ulaşan şifreli veri ise sadece ve sadece alıcı tarafında bulunan özel anahtar ile çözülebilmektedir. Rivest, Shamir ve Adleman (RSA) [106], Eliptik Eğri algoritması (Elliptic Curve Cryptography-ECC) [107], ve Diffie Helman [93] yaygın olarak kullanılan asimetrik şifreleme algoritmalarıdır. Asimetrik şifrelemede, genel ve gizli anahtar arasında matematiksel bir bağlantı bulunmaktadır. Şifreyi kırmanın zorluğu, herkese açık olan genel anahtarı kullanarak özel anahtarın elde edilmesinin imkânsızlığıdır. Asimetrik şifreleme algoritmasının güçlü yanı, özel anahtarın paylaşılmak zorunda olmaması ve simetrik şifrelemedeki anahtar paylaşım sorununu ortadan kaldırmasıdır. Asimetrik şifreleme algoritmaları sayısal imzalama uygulamalarında, gönderilen verinin doğru kişiden gelip gelmediğini test etmek için yaygın olarak kullanılmaktadır.

2.1.3. Kriptoanaliz

Kriptografi biliminin, bir diğer alt dalı kriptoanalizdir. Kriptoanaliz bilimi, şifreleme sistemlerini kırarak, iletilen şifreli veriyi elde etmeye çalışmaktadır. Şifreleme sistemlerinin güvenli bir yapıya sahip olduğunun ispatlanması için, güvenlik analizleri yapılmaktadır. Güvenlik analizlerinde klasik kriptoanaliz yöntemleri veya uygulama atakları kullanılabilmektedir. Klasik kriptoanaliz eldeki verileri ve matematiksel yöntemleri kullanarak, şifreli veri veya anahtar üzerinden orijinal veriye ulaşmaya çalışmaktadır. Bu çalışma sırasında elinde bulunan verinin türüne göre saldırı çeşidi farklılık göstermektedir. Matematiksel yöntemler kullanılarak gerçekleştirilen

kriptoanaliz yöntemleri [108,109], eldeki verinin türüne göre şu şekilde sınıflandırılmaktadır.

- Sadece şifreli metin saldırısı (Ciphertext only attack): Saldırıyı gerçekleştirecek kişinin sadece şifreli veriye sahip olduğu türdür. Elinde bulunan şifreli veriyi kullanarak, şifreleme anahtarını ve açık metni elde etmeye çalışmaktadır.
- Bilinen açık metin saldırısı (Known plaintext attack): Bu saldırı türünde, kriptanalist şifreli veriye, şifreli ve orijinal veri bloklarına sahiptir.
- Seçilmiş açık metin saldırısı (Chosen plaintext attack): Bilinen açık metin saldırısından farklı olarak, üzerinde işlem yapılacak veri çiftleri kriptanalist tarafından belirlenmiştir.
- Seçilmiş şifreli metin saldırısı (Chosen ciphertext attack): Seçilmiş açık metin saldırısından farklı olarak, kriptoanaliz bazı şifreli verileri seçebilmekte, istediği orijinal ve şifreli veri çiftine şifre çözme işlemi uygulayabilmektedir.

Kaba kuvvet saldırılarında, şifreleme işleminde kullanılmış olan anahtar, sistemin anahtar uzayında bulunan tüm anahtarların denenmesi ile tespit edilmeye çalışılmaktadır. Kaba kuvvet saldırılarına karşı anahtar uzayı geniş olan sistemlerin tasarlanması bu saldırıların önlenmesinde büyük öneme sahiptir.

Ayrıca kriptolojik sistemler üzerinde, donanımsal cihazların çalışma özellikleri analiz edilerek, sistem hakkında bilgi edinilmesi suretiyle gerçekleştirilen ataklar da mevcuttur. Bu ataklara yan kanal saldırısı denilmektedir [110]. Şifreleme sisteminin çalıştığı donanımsal yapıların çekmiş olduğu akım, işlemi gerçekleştirme süresi, yaymış olduğu elektromanyetik dalga ve güç analizleri gibi veriler toplanarak, analiz edilmekte ve sistem kırılmaya çalışılmaktadır.

2.2. Kaos ve Kriptoloji

Kaos kuramı, 1963 yılında Edward Lorenz [111] tarafından ortaya atılmış ve daha sonrasında üzerinde gerçekleştirilen bilimsel çalışmalar ve önerilen yeni sistemler

[112–116] ile hızlı bir gelişim göstermiştir. Bilimsel çalışmaların artması ile kaotik sistemler kendilerine haberleşme ve elektronik sistem tasarımları, biyomedikal ve robotik uygulamaları, fizik ve kimya gibi temel alanlar, şifreleme gibi birçok farklı konuda uygulama alanı bulmuştur [117–124].

Kaotik sistemlerin sahip olduğu temel özellikler aşağıdaki şekilde sıralanabilir.

- Bir sonraki durumun, bir önceki duruma bağlı olduğu periyodik olmayan davranışlara sahip olması.
- Sisteme ait başlangıç şartlarına ve sistem parametrelerine aşırı hassas bağımlı olması.
- Belli sınırlar içerisinde değişen, farklı genlik ve frekans değerlerinde karmaşık davranışlar sergilemesi.
- Sınırsız çoklukta birbirinden farklı periyodik yörüngeler takip etmesi.

Kaotik sistemler, sürekli zamanlı ve ayrık zamanlı kaotik sistemler olmak üzere 2 kısımda incelenmektedir. Sürekli zamanlı kaotik sistemler en az üç adet bağımsız dinamik değişkene sahip olmalı ve sistemi oluşturan denklemler bir tane doğrusal olmayan terim içermelidir. Sürekli zamanlı kaotik sistemler genel olarak adi diferansiyel denklem takımları kullanılarak oluşturulmaktadır. Ayrık zamanlı sistemler ise tek bir denklem kullanılarakta oluşturulabilmektedir. Fakat iki ve üç denklemden oluşan ayrık zamanlı kaotik sistemlerde bulunmaktadır. Bir sistemin kaotik olup olmadığının test edilmesi için birçok farklı analiz bulunmaktadır. Bu analizler Bölüm 3'te detaylı olarak, yeni önerilen sistemler ile birlikte incelenecektir.

Kaotik sistemlerin yıkarıda bahsedilen özelliklerinden dolayı kriptoloji bilimi ile arasında yakın bir ilişki bulunmaktadır [4,5]. Kaos tabanlı kriptoloji doğrusal olmayan sistemlerin karmaşık dinamiklerine dayanmaktadır. Kaotik sistemler, başlangıç şartlarına ve kontrol parametrelerine hassas bağımlı olması, ergodiklik, rasgele davranışlar ve uzun periyotlu sabit olmayan yörüngelere sahip olma gibi özellikler taşımaktadır [125,126]. Shanon mükemmel gizlilik prensipleri [99] olarak bilinen ve kriptolojik sistemlerin sahip olması gereken karıştırma ve yayılma özellikleri kaotik sistemlerin başlangıç şartlarına ve kontrol parametrelerine hassas bağımlı olması ve

ergodiklik özellikleri ile sağlanabilmektedir [127]. Karıştırma özelliği, açık metin ile şifreli metin arasında herhangi bir istatistiki analiz ile çözülebilecek bir benzerlik ve bağlantı olmaması gerektiğini ifade etmektedir. Yayılma özelliğinde ise şifreli metin ile anahtar arasındaki bağlantının olabildiğince karmaşık olması gerekmektedir. Kaotik sistemlerin başlangıç ve kontrol parametreleri üzerinde yapılacak olan ufak değişimler sistemin üretmiş olduğu değerler üzerinde büyük değişimler meydana getirmekte ve yayılma özelliğini sağlamaktadır. Kaotik sistemlerin sahip olduğu ergodiklik özelliği, kaotik sistemin takip ettiği yörüngenin uzun bir zaman dilimindeki davranışının başlangıç şartlarına ve kontrol parametrelerine hassas bağımlı olduğunu ortaya koymaktadır [127]. Çünkü kaotik sistemlerde takip edilen yörüngenin t+1 zamanında almış olduğu değer tamamıyla t anındaki değer ile bağımlıdır. Kriptolojik tasarımlarda bir diğer değerlendirme kriteri algoritma karmaşıklığı kavramıdır. Kaos tabanlı tasarımlarda ise, bu karmaşıklık yapısal karmaşıklık olarak ifade edilmektedir. Şifrelemede kullanılan kaotik sistemin taşımış olduğu zengin dinamik özellikler, modern kriptolojideki algoritma karmaşıklığının benzeri bir kriter olarak sunulmaktadır. Özetle, kaotik sistemlerin sahip olduğu özelliklerden dolayı, kaotik sistemlerin şifreleme uygulamalarında kullanılabileceği sonucuna varılmıştır. Kaos tabanlı şifreleme algoritmaları, blok şifreleme, akış şifreleme ve özet şifreleme algoritmaları gibi farklı tasarımlarda kullanılmaktadır.

2.3. Rasgele Sayı Üreteçleri (RSÜ) ve NIST Testleri

Rassallık en genel tanımda, kesin olarak belli olmamak demektir. RSÜ, rasgele değerlerin üretilmesi için, kriptolojide yaygın olarak kullanılan yapılardan birisidir. Kriptolojik uygulamalarda kullanılan RSÜ'lerin ürettiği sayıların rasgeleliği, şifreleme uygulamalarının güvenliğini doğrudan etkilediklerinden kritik öneme sahiptirler. RSÜ'nün üretmiş olduğu rasgele değerlerin, istatistiki olarak bağımsız, eşit dağılıma sahip ve tahmin edilemez özellikler taşıması gerekmektedir. Rasgele sayılar, benzetim, sayısal analiz, programlama, istatistik uygulamalarında ve yaygın olarak şifrelemede kullanılmaktadır [128]. Şifrelemede, anahtar üretimi ve dağıtımında, başlangıç verktörünün oluşturulmasında, kimlik doğrulamada ve asal sayı üretimi gibi işlemler için kullanılmaktadır[129]. RSÜ'ler şifrelemede genel olarak rassal bit

dizilerinin üretiminde kullanılmaktadır. RSÜ'lerin üretmiş olduğu rasgele bit dizileri, birçok kriptolojik uygulamanın temelini teşkil etmektedir.

RSÜ'ler gerçek (GRSÜ-True Random Generator) ve sözde (SRSÜ- Pseudo Random Generator) olarak sınıflandırılabilir. Gerçek RSÜ rassal sayı üretiminde donanımsal, sözde RSÜ'ler ise yazılımsal bir kaynağı kullanmaktadır. SRSÜ genel olarak, çekirdek-tohum adı verilen başlangıç değerleri ile deterministik bir yapı kullanarak bu değerlerin genişletilmesi ve yeni değerler üretilmesi vasıtasıyla rasgele bit dizilerini oluşturmaktadır. GRSÜ'ler gürültü kaynağının güçlendirilmesi, çift osilatör kullanımı ve kaotik sistemlerin kullanımı gibi farklı şekilde yöntemler kullanılarak tasarlanabilmektedir. GRSÜ'lerin rasgele bit dizisinin bir kısmına sahip olunduğunda diğer kısımlarının tespit edilememesi, periyodik bir yapıda olmamaları ve dizilerin kendi içinde bağlantılarının bulunmaması en önemli avantajlarıdır. Fakat kullanım maliyetinin yüksekliği ve uzun sayı dizilerinin üretiminde verimsizlik gibi dezavantajları da bulunmaktadır. SRSÜ'ler ise matematiksel algoritmaları kullanarak yazılımsal tabanlı üretim gerçekleştirdiklerinden maliyetleri düşük, üretimleri kolaydır. Fakat güvenlik noktasında ilk değerlerin iyi seçilmesi ve gizli tutulması, üretilen değerler arasında istatistiki bir bağlantının bulunmaması, uzun periyotlarda üretim gibi dikkat edilmesi gereken noktalar da bulunmaktadır. Aksi takdirde bu durumlar SRSÜ'lerin güvenlik testlerini geçmelerini engellemektedir.

Şifrelemede kullanılacak olan RSÜ tasarımlarında, kaotik tabanlı sistemler taşımış olduğu başlangıç şartlarına ve kontrol parametrelerine hassas bağımlılık gibi özelliklerinden dolayı yaygın olarak kullanılmaktadır. Yüksek rassallığa sahip bit dizileri ile daha güçlü bir şifreleme gerçekleştirilebilmektedir. Kaotik sistemin üretmiş olduğu değerleri rasgele bit dizisi oluşturulmasında kullanmak için sistemin çözümlenmesi ve algoritmik işlemlere tabi tutulması gerekmektedir.

RSÜ'nün üretmiş olduğu rasgele bit dizilerinin, kriptolojik uygulamalarda kullanılabilmesi için, rasgelelik testlerine tabi tutulması ve bu testlerin hepsinden geçmesi gerekmektedir. Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından geliştirilen ve standart olarak kabul edilen NIST-800-22 rasgelelik testleri, yaygın olarak

kullanılan ve uluslarası kabul görmüş en önemli testlerden birisidir. Üretilen bit dizisinin NIST testlerinin tamamından geçmesi, bit dizisinin şifreleme işlemlerinde kullanılacak bir rastsallığa sahip olduğunu göstermektedir. Üretilen rasgele bit dizileri, NIST-800-22 testinde karmaşık ve detaylı testlere tabi tutulmaktadır. Bu testler, üretilen rasgele bit dizilerinin, rassallık ölçüsünün tespiti için gerçekleştirilen istatistiki testlerdir. NIST-800-22 testinde, çıkan sonuçlar değiştirilebilen p-değerine göre değerlendirilmektedir. Eğer koşul olarak p-değeri 0.001 kabul edilmişse, bir testin başarılı olabilmesi için p-değeri, 0.001<p-değeri<0.01 aralığında olması gerekmektedir. NIST-800-22 testinde bulunan ve bit dizilerinin rasgeleliğini tanımlayan 15 farklı istatistiksel test bulunmaktadır [130]. 15 farklı teste göre sayı dizilerinin rasgelelik başarımı güvenlilir olarak ölçülebilmektedir. Bu testlerin kısaca açıklamaları aşağıda yapılmıştır [130].

1. Frekans testi: Rasgele bit dizisinin içindeki 0 ve 1 değerlerinin sayısını tespit eden testtir. Bu değerlerin birbirine yakın olması gerekmektedir. Bu test sonucu diğer tüm testleri etkilemekte ve dizinin rassalığı hakkında önemli bilgi vermektedir.
2. Blok frekans testi: Testi gerçekleştirilen dizinin m uzunlukta farklı boyutlardaki alt dizinleri içindeki 0 ve 1 dağılımı incelenmektedir.
3. Akış testi: Rasgele bit dizisindeki 0 ve 1 bloklarının uzunlukları analiz edilmektedir.
4. Bir blok içerisinde en uzun birler akış testi: Rasgele bit dizisindeki en uzun 0 ve 1 bloklarının uzunlukları test edilmektedir.
5. İkili matris derece testi: Rasgele bit dizisinden ayrıştırılan alt matrislerin, orijinal dizi ve sabit uzunluktaki alt blokları arasındaki ilişkinin doğrusallığı test edilmektedir.
6. Ayrık Fourier dönüşüm testi: Rasgele bit dizisinin Fourier dönüşümü elde edilerek, elde edilen sonuçların genlik değerlerindeki periyodiklik sınaması gerçekleştirilmektedir.
7. Örtüşmeyen şablon eşleştirme testi: Rasgele bit dizisinin içinde, test başında belirlenmiş olan bir bit dizisinin varlığı test edilmektedir.

8. Örtüşen şablon eşleştirme testi: Bu testtede örtüşmeyen şablon testinde olduğu gibi belirlenen m boyutlu bir dizinin bulunup bulunmadığı test edilir. Fakat aranılan bloğun bulunması veya bulunamaması durumunda rasgele bit dizisi üzerinde bit kaydırma işlemi ile arama işlemine devam edilmektedir.
9. Maurer'in "evrensel istatistik" testi: Yüksek rassallık taşımayan bir bit dizisi çok yüksek oranlarda sıkıştırılabilmekte tezinden hareketle veri kaybı olmaksızın test edilen dizinin sıkıştırabilirliği test edilmektedir.
10. Doğrusal karmaşıklık testi: Rasgele bit dizisinin yeterli karmaşıklığa sahip olup olmadığını test eder. Bunun için dizi LFSR (Linear-feedback shift register) dizisi olarak düşünülmekte ve yeterli uzunluğa sahip olup olmadığı belirlenmektedir.
11. Seri testi: Bu test rasgele bit dizisi içindeki tekrar eden m bitlik 2^m adet bloğun tekrar adetinin dağılımını analiz etmektedir.
12. Yaklaşık entropi testi: Rasgele bir dizisi içinde yer alan (m) ve (m+1) bitlik katarların entropi değerlerini analiz etmektedir.
13. Birikimli toplamlar testi: Bu testte, bit dizisi üzerinde ardışık uzunlukta bloklar oluşturularak, bu bloklar üzerinde 1 ve 0 değerlerinin frekansı belirlendikten sonra, bloklar arası dengesizlik değerleri karşılaştırılmaktadır.
14. Rasgele gezinimler testi: Bu testte, birikimli toplamlar testinde olduğu gibi bloklara ayırma ve 0-1 dengesi belirlendikten sonra, blokların dengesizlik dağılımı yerine denge dağılımı incelenmektedir.
15. Rasgele gezinimler değişken testi: Rasgele gezinimler değişken testinde 13 ve 14 numaralı testte olduğu gibi, bloklara ayırma ve 1-0 dengesi tespitinden sonra, ortalama değer üzerinden sapma miktarı belirlenmektedir.

2.4. Yer Değiştirme Kutuları (Substitution Box–S-Box) ve Performans Kriterleri

Şifreleme algoritmalarında, güçlü bir şifreleme için karıştırma ve yayılma özelliklerinin sağlanması gerekmektedir. Karıştırma ve yayılma kriterlerinin yerine getirilmesi için algoritmalarda S-Box'lar yani yer değiştirme kutuları, dönüşüm işlemleri ve şifreleme anahtarının her döngüde değiştirildiği anahtar genişletme işlemleri uygulanmaktadır. S-Box'lar simetrik şifreleme algoritmalarında, karıştırma

özelliğinin sağlanması için kullanılan en temel yapılardır. Şifreleme algoritmalarına gerçekleştirilen saldırılara karşı dirençli bir yapı oluşturulması için, güçlü kriptolojik özelliklere sahip S-Box kutularının kullanılması gereklidir [131]. AES, DES gibi blok şifreleme yöntemlerinde yer değiştime işlemleri için S-Box kutuları kullanılmaktadır. S-Box üzerindeki işlem sonucunda m bitlik giriş farklı bir m bitlik çıkış olarak değiştirilmektedir. S-Box tasarımlarında kullanılan birçok farklı yaklaşım bulunmaktadır. Sonlu cisimlerde ters alma ve üssel fonksiyon kullanımı bu teknikler içinde en yaygın olarak tercih edilen yöntemlerdir. AES algoritmasında S-Box üretimi GF (2^8) sonlu cisimler ve modülo terslenebilirlik kullanılarak gerçekleştirilmektedir. Bu yöntemde gönderici tarafında şifreleme işlemi için sonlu cisimler yöntemi kullanılarak oluşturulan bir S-Box, alıcı tarafında ise çözme işlemi için ters alma işlemleri kullanılarak farklı bir S-Box oluşturulmaktadır. Gönderici tarafında değiştirilen değer, alıcı tarafında oluşturulan ters S-Box üzerinden tekrar elde edilmektedir. AES algoritmasının anlatıldığı Bölüm 2.5'te bayt değişim işleminde kullanılan S-Box ve ters S-Box'lar gösterilmiştir.

2.4.1. S-Box performans testleri

Şifreleme uygulamalarının güçlü ve saldırılara karşı dayanıklı olmasında çok kritik öneme sahip S-Box yapılarının belli kriterleri sağlaması ve performans testlerinden geçmesi beklenmektedir. S-Box'lar üzerinde gerçekleştirilen birçok performans testi mevcuttur. Doğrusal olmama (nonlinearity), katı çığ kriteri (strict avalanche criteria-SAC), çıkış bitlerinin bağımsızlık kriteri (outputs bit independence criteria-BIC) , giriş ve çıkış bitleri arasındaki XOR dağılımı analizi (Differantial approximation probablity-DP) en önemli testler olarak sayılabilir [132].

2.4.1.1. Doğrusal olmama kriteri

S-Box'ların kriptolojik olarak gücünü test etmek için uygulanan testlerden en önemlilerinden birisi doğrusal olmama kriteridir. Doğrusal olmayan özellikler taşıması şifrelemeyi güçlü ve saldırılara karşı dayanıklı kılmaktadır. Bir S-Box'un doğrusal olmama değeri hesaplanırken Walsh spectrum analizi kullanılmaktadır. g(x)

fonksiyonunun doğrusal olmaması Walsh spectrum analizi ile ifade edilmektedir. Bu hesaplamaya ilişkin formüller Denklem 2.1'de verilmektedir [132].

$$
\begin{aligned}
&N(g) = 2^{n-1}(1-2^{-n}\max(\omega \in GF(2^n))\left|S_g(\omega)\right|) \\
&S_g(\omega) = \sum_{\omega \in GF(2^n)} -1^{g(x)\oplus x*\omega} \\
&\omega \in GF(2^n) \Rightarrow x*\omega = x_1*\omega_1 \oplus .....\oplus x_n*\omega_n
\end{aligned}
\tag{2.1}
$$

2.4.1.2. Katı çığ kriteri

Katı çığ kriteri (SAC) giriş bitlerindeki değişime bağlı olarak, çıkış bitlerinin değişme olasılığını hesaplayan Webster ve Tavares[132] tarafından geliştirilen bir performans kriteridir. Bu metot, giriş bitlerinin tek bir tanesi değiştiğinde, çıkış bitlerinin her birinin yarısının değişme olasılığını hesaplamaktadır. Hesaplanan değer 0,5 ise bu en ideal durumdur. Hesaplanan değer 0,5' e ne kadar yakın olursa, değer o kadar optimumdur ve S-Box SAC kriterini sağlıyor demektir.

2.4.1.3. Bit bağımsızlık kriteri

S-Box'ların performans değerlendirilmesinde kullanılan bir diğer yöntem, Webster ve Tavares [132] tarafından geliştirilmiş olan çıkış bitlerinin bağımsızlığı yöntemidir. Bu yöntem ile, açık metnin bir bitinin tersiyle üretilen vektörlerin kümesinin tüm çığ değişken çiftlerinden bağımsız olma durumu test edilmektedir. Çığ değişken çiftleri arasındaki bağlantıyı ölçerken, korelasyon değerinin hesaplanması gerekmektedir [64]. $F_i = f_i \oplus f_k (j \neq k, 1 \leq j,k \leq n)$ Boolean fonksiyonun iki çıkış biti olan f_i ve f_k BIC kriterini sağlıyorsa, doğrusal olmama ve SAC kriterini de sağlamaktadırlar.

2.4.1.4. Giriş ve çıkış bitleri yaklaşık fark ihtimali analizi

Giriş ve çıkış bitleri arasındaki fark dağılımı analizinde, S-Box'un giriş ve çıkış bitleri arasındaki XOR dağılımı tespit edilmektedir. Bu metot Biham ve Shamir tarafından

geliştirilen bir diferansiyel kriptanaliz metodudur [131]. Her bir çıkış XOR değeri, giriş değerleri için eşit olasılığa sahip olmalıdır. Giriş ve çıkış bitleri arasındaki XOR dağılım olasılığının birbirine yakın olması S-Box'un diferansiyel atak saldırılarına dirençli olduğunu göstermektedir. Hesaplanan DP değerinin düşük olması S-Box'un saldırılara daha dirençli olduğunu göstermektedir. Bir sistemin giriş çıkış XOR dağılım dengesi Denklem 2.2'deki gibi hesaplanmaktadır.

$$DP_g = \max_{\Delta x \neq 0, \Delta y} (\#\{x \in X, g_{(x)} \oplus g(x \oplus \Delta x) = \Delta y\} / 2^n) \quad (2.2)$$

2^n → tüm olası giriş değerleri (x) Δx → giriş farkı değeri Δy → çıkış farkı değeri

2.5. Simetrik ve Asimetrik Şifreleme Algoritmaları

2.5.1. RSA şifreleme algoritması

RSA algoritması [106] 1977 yılında R.Rivest, A.Shamir ve L.Adleman tarafından geliştirilmiştir. RSA algoritması açık anahtarlı şifreleme ve digital imza uygulamalarında yaygın olarak kullanılmaktadır. Aralarında asal iki büyük asal sayının seçimi, bu sayılardan elde edilen yüksek mod değerinin kullanılması ve çarpanlara ayırma işlemleri temeline dayanmaktadır. RSA algoritmasının sözde kodu aşağıda görülmektedir.

Anahtar üretimi

1: p ve q değerlerini üret (aralarında asal sayılar)
2: n ve φ(n) değerini hesapla → n= p*q , φ(n)=(p-1)*(q-1)
3: e değerini seç, 1<e<φ(n) → gcd(e,φ(n))=1, gcd(en büyük ortak bölen)
4: d değerini hesapla, 1<d<φ(n) → e*d ≡ 1 (mod φ(n))

açık anahtar → n,e gizli anahtar → n,d özel değer → p,q,φ(n)

C → şifreli veri, M → orjinal veri

Şifreleme süreci

$C = M^e \pmod n$

Şifre çözme süreci

$M = C^d \pmod n$

RSA algoritmasında ilk olarak aralarında asal rasgele p ve q değerleri üretilmektedir. Daha sonra, p ve q' nun çarpımından n değeri, (p-1)*(q-1) çarpmından ise φ (n) değeri elde edilmektedir. Ardından e değeri algoritmada görüldüğü şekilde hesaplanmaktadır. Hesaplanan n ve e değerleri mesajı şifreleyecek kişiye iletilmektedir. Şifreleme sürecinde ise gönderilecek olan mesaj algoritmadaki gibi şifrelenerek şifreli metin elde edilir ve bu şekilde alıcıya ulaştırılır. Alıcı taraf kendisine ulaştırılan n ve e değerlerini kullanarak, d değerini hesaplar ve algoritmada görüldüğü gibi çözme işlemini gerçekleştirerek orijinal metni elde eder. RSA algoritmasında güvenliği artırmak için, p ve q asal sayı değerlerinin seçiminde özel algoritmalar kullanılarak anahtar oluşumu sağlanabilir. Bu algoritmanın güvenlik seviyesini artırmaktadır. Genel kullanımda güvenliğin sağlanması için en az 1024 bit uzunluğunda (n sayısı) anahtar kullanımı tavsiye edilmektedir. Daha yüksek güvenliğe ihtiyaç duyulan noktalarda 2048 veya 4096 bit anahtarlar tercih edilmektedir. Fakat RSA kripto sisteminde özellikle yüksek bit uzunluğundaki anahtar kullanımlarında, çok büyük asal sayılar ile mod işlemleri gerçekleştirildiği için hem şifrelemede hemde çözme işleminde hız problemi ortaya çıkmaktadır. Bu yavaşlamayı engellemek ve süreyi kısaltmak için şifreleme ve çözme işlemlerinde, mod ve üs alma işlemlerini hızlandıracak algoritmalar geliştirilmiştir.

RSA Algoritması örnek şifreleme ve çözme:

Anahtarların üretimi:

- İki asal sayı seçilir.
  p=73, q=83
- n değeri hesaplanır
  n=73*83=6059
- φ(n) değeri hesaplanır.
  φ(n) = (p-1)*(q-1)=72*82= 5904
- φ(n) ile aralarında asal olan e değeri seçilir. Seçilecek e değeri 1< e < φ(n) şartını sağlamalıdır.
  e=19
- 1 < d < φ (n) ve e, d ≡ 1 mod (φ (n)) olacak şekilde d sayısı hesaplanır.
  d = 1243

Bu hesaplamalara göre alıcı tarafında:

Genel anahtarı e=19, n=6059

Gizli anahtarı d=1243, n=6059 olmaktadır.

Şifreleme işlemi:

- Alıcı açık anahtarı olan e ve n değerlerini göndericiye iletim kanalından iletmektedir.
- Gönderici göndermek istediği M değerini (M=145)

  $C = 145^{19} \pmod{6059}$ ile hesaplamaktadır. Bu işleme göre C değeri 1751 olarak bulunur.
- Gönderici bulmuş olduğu bu değeri yani şifreli veriyi iletim kanalından alıcıya iletir.

Şifre çözme işlemi:

- Alıcı kendisine ulaşan C değerini aşağıdaki şekilde çözerek iletilmek istenen orijinal veriyi elde etmiş olur.

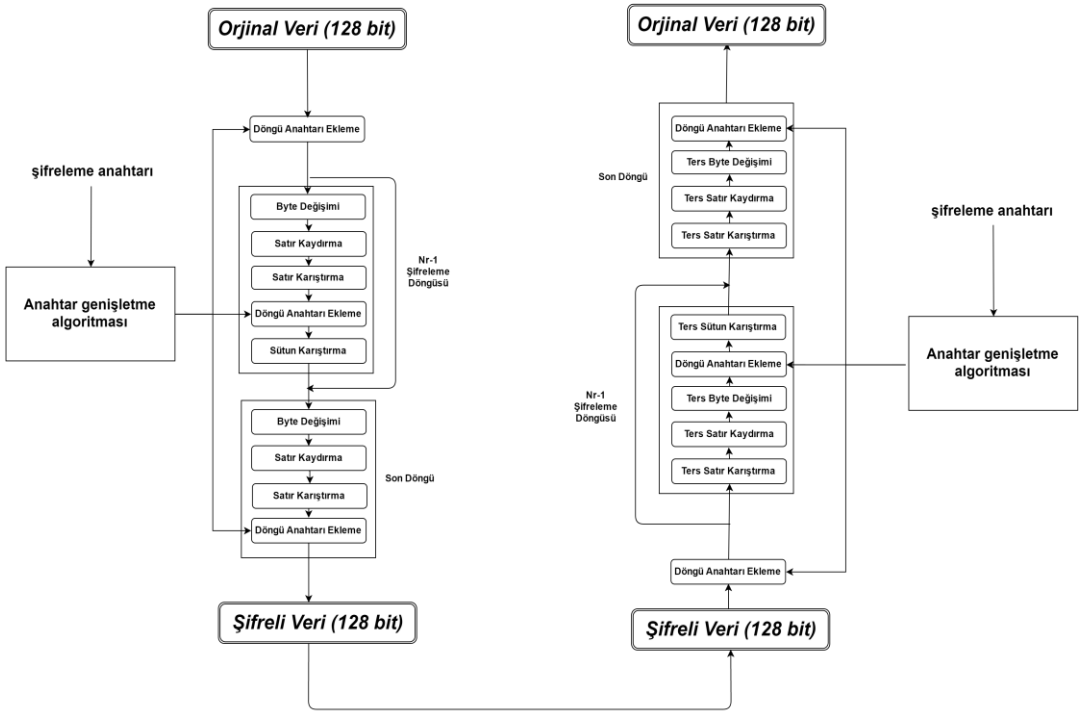
  $M = 1751^{1243} \pmod{6059}$ Bu işlem sonucunda M değeri 145 olarak bulunmaktadır.

2.5.2. AES şifreleme algoritması

AES algoritması [103] J.Daemen ve V. Rijmen tarafından geliştirilen ve NIST tarafından 2000 yılında standart olarak kabul edilen bir simetrik blok şifreleme algoritmasıdır. AES algoritması tasarım olarak SPN (substitution permutation network) yapısında tasarlanmıştır [104]. AES şifreleme işleminde ECB(Electronic Code Book), CBC (Cipher Block Chaining), CFB (Cipher Feed Back), OFB (Output Feed Back), CTR (Counter Mode) gibi farklı çalışma modları bulunmaktadır. Farklı modlar sayesinde veri akışı veya veri bloklarının sıralamasında uygulama alanına göre şifreleme tekniği değişmektedir. Bu modların birbirine göre avantaj ve dezavantajları bulunmaktadır. AES blok şifreleme işlemleri 128 bit şifreleme için durum adı verilen 16 bayt 4x4 durum matrisi üzerinde gerçekleşmektedir. AES şifreleme algoritması anahtar uzunluğu esnek bir yapıya sahiptir. 128 bit, 192bit ve 256 bit uzunluğuna sahip anahtarlar ile şifreleme gerçekleştirilebilmektedir. AES-128 10, AES-192 12 ve AES-

256 14 döngüde şifreleme işlemlerini gerçekleştirmektedir. AES algoritmasının anahtar uzunluğu algoritmayı kaba kuvvet ve diğer saldırılara karşı daha dayanıklı hale getirmektedir. S-AES algoritması [133], daha az işlem gücü ve kaynak kullanımı maksadıyla AES algoritmasının basitleştirilmiş versiyonudur.

AES algoritması tekrar eden döngüsel bir yapıdan oluşmaktadır. Bu döngüler içerisinde bayt değişimi, satır kaydırma, sütun karıştırma ve döngü anahtarının eklenmesi olmak üzere 4 adım bulunmaktadır. Son döngüde sütunları karıştırma işlemi gerçekleştirilmez. Diğer tüm döngülerde bu 4 adım sırasıyla gerçekleştirilmektedir. AES algoritması için döngü sayısı 10, S-AES algoritması için ise 2'dir. Şifre çözme sürecinde ise, şifreleme işleminde gerçekleştirilen işlemlerin tersi gerçekleştirilerek, orijinal veri elde edilmektedir. Şifreleme işlemine başlamadan önce 16 bayt uzunluğundaki şifrelenecek olan veri durum matrisi diye ifade edilen 4x4 lük bir matris şekline getirilmektedir. Algoritmada her döngüde kullanılmak üzere oluşturulacak anahtarlar, anahtar genişletme algoritması kullanılarak üretilmektedir. Şekil 2.2.'de görüldüğü gibi AES şifreleme algoritmasında 4 temel adım vardır. Bu adımların şifreleme ve çözme işlemlerinin detayları aşağıda açıklanmıştır.



Şekil 2.2. AES algoritması şifreleme ve çözme blok diyagramı

Bayt değişimi - Ters bayt değişimi: Bayt yer değişimi adımı şifrelemede doğrusal olmayan işlemlerden birisidir. Çok iyi doğrusal olmama özelliğine sahip olduğu bilinen GF (2^8) [130] ters alma ve affine dönüşüm işlemleri temel alınarak oluşturulan S-Box kullanılarak, şifreleme işlemine giren her bayt S-Box üzerindeki satır ve sütunda kendine karşılık gelen değer ile değiştirilmektedir. Alıcı tarafında ise terslenebilme özelliği sayesinde ters S-Box oluşturulmakta ve şifreli değerlerin orijinali bu şekilde elde edilmektedir. S-Box sonlu elemanlar teorisinde (Galois Field) GF(2^8) de, 8 bitlik değerler $P(x)= x^8+x^4+x^3+x+1$ indirgenemez polinom tabanlı sonlu cisim kullanılarak, tersi alınıp doğrusal bir dönüşüm işleminden sonra elde edilmektedir.

Tablo 2.1. AES algoritmasında kullanılan S-Box Kutusu [100]

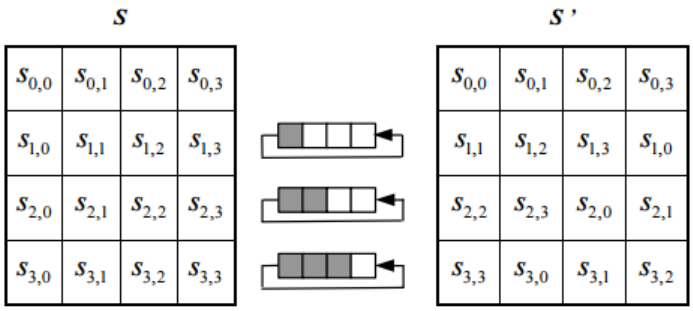
		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Tablo 2.1.'de şifreleme sırasında bayt değişim adımında kullanılmak üzere oluşturulmuş S-Box, Tablo 2.2.'de ise çözme işlemi için oluşturulan ters S-Box kutuları görülmektedir. Tablo üzerindeki değerler 16'lık sayı formatındadır. Örnek olarak, şifreleme işleminde Tablo 2.1.'deki S-Box kullanılarak, '9a' değeri bu adımda satır değeri olarak '9' sütun değeri olarak 'a' değerine karşılık gelen değer ile yer değiştirilmektedir. Dolayısıyla '9a' değeri 'b8' olarak değiştirilmektedir. Çözme işleminde ise Tablo 2.2.'deki S-Box kullanılarak ters S-Box tablosu üzerinde değişim işlemi gerçekleştirilmektedir. 'b8' değerinin Tablo 2.2.'de karşılığına bakacak olursak, 'b' değerinin bulunduğu satır ile '8' değerinin bulunduğu sütunun kesişiminde bulunan değerin, şifrelenen orijinal değer olan '9a' olduğu görülmektedir.

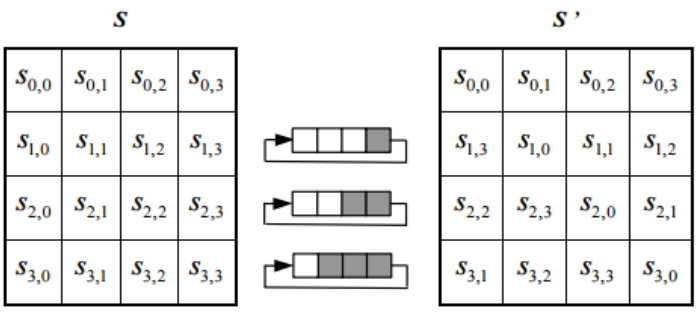
Tablo 2.2. AES algoritmasında kullanılan ters S-Box Kutusu [100]

		y														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
	6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

- Satır kaydırma – Ters satır kaydırma: Satır kaydırma işlemi basit bir döndürme işlemidir. Bu işlemde 4x4' lük bir matris için ilk satır ötelenmez ve diğer satırlar sırası ile 1, 2 ve 3 defa şifreleme işleminde sola, çözme işleminde sağa ötelenerek bu adım gerçekleştirilmektedir. Şekil 2.3.'de durum matrisi üzerinde satır kaydırma operasyonu, Şekil 2.4.'de şifre çözme işleminde kullanılan ters satır kaydırma operasyonu işlemi görülmektedir.



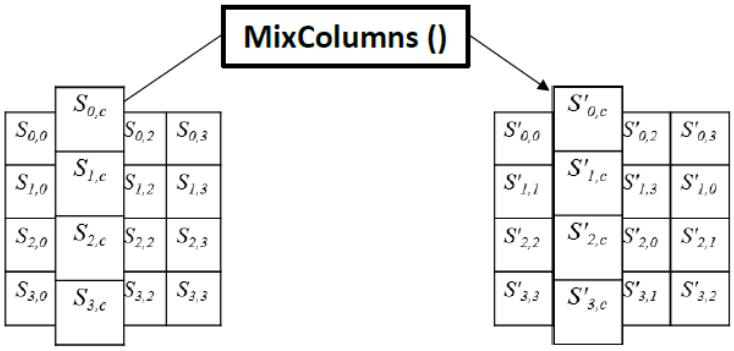
Şekil 2.3. Satır kaydırma operasyonu [100]



Şekil 2.4. Ters Satır kaydırma operasyonu [100]

- Sütun karıştırma–Ters sütun karıştırma: Sütun karıştırma işleminde, durum matrisindeki her bir sütun yani 4 bayt, GF (2^8) de oluşturulan ve çarpmaya göre terslenebilir bir matris ile çarpılarak 4 bayt'lık yeni değer elde edilir. Her bir sütun için aynı işlem gerçekleştirilir. Son döngüde sütun karıştırma adımı uygulanmamaktadır. Bu işlem satır kaydırma operayonu ile birlikte şifreleme algoritmasındaki yayılma özelliğini sağlamaktadır. İşlemde her bir sütun için, A(x) polinomu ile modülo (x^4+1)'de çarpma işlemi uygulanır. Çarpma işleminde kullanılan A(x) polinomu A(x)= $\{03\}x^3+\{01\}x^2+\{01\}x+\{02\}$ şeklindedir. Sütun karıştırma işlemine ait kullanılan fonksiyonun matris üzerinde gerçekleştirdiği işlem aşağıda verilmiştir. Şekil 2.5.'de ise matris üzerinde işlem öncesi ve sonrası durumları gösterilmiştir.

$$\begin{bmatrix} S'_0 \\ S'_1 \\ S'_2 \\ S'_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{bmatrix}$$



Şekil 2.5. Sütun karıştırma operasyonu [100]

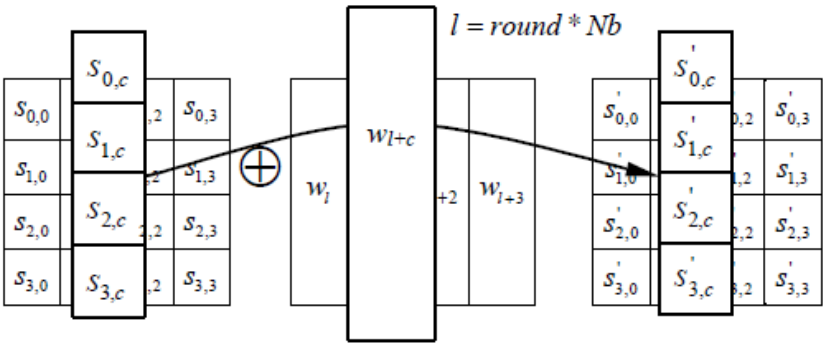
Ters sütun karıştırma işleminde ise, durum matrisinde yer alan sütunlar sabit bir polinom ile çarpma işlemine tabi tutulmaktadır. Şifre çözme işleminde kullanılacak olan sabit polinom GF (2^8)'de şifreleme işleminde kullanılan sabit polinomun çarpmaya göre tersi alınarak hesaplanmakta ve bu polinom kullanılmaktadır. AES algoritmasında kullanılan A ve A^{-1} matrisi Şekil 2.6.'da gösterilmiştir.

$$A \qquad\qquad A^{-1}$$

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \leftrightarrow \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}$$

Şekil 2.6. Sütun karıştırma işleminde kullanılan A ve A^{-1} matrisi

- Anahtar ekleme: Döngü anahtarı ekleme işlemi, şifreleme ve çözme işlemi için birbirinin aynıdır. Döngüye girilmeden şifrelemede kullanılacak anahtar ile durum matrisinin yani şifrelenecek olan veri bloğunun sütun bazında XOR işlemi yapılmaktadır. Daha sonraki her döngüde kullanılmak üzere alt döngü anahtarları döngü anahtarları oluşturma algoritması ile elde edilmektedir. Elde edilen alt döngü anahtarı ile her döngüde durum matrisi ile XOR işlemi gerçekleştirilmektedir. Şekil 2.7.'de durum matrisi ile oluşturulan döngü anahtarının sütun bazında XOR'lanması ve şifreli matrisin elde edilmesi görülmektedir.

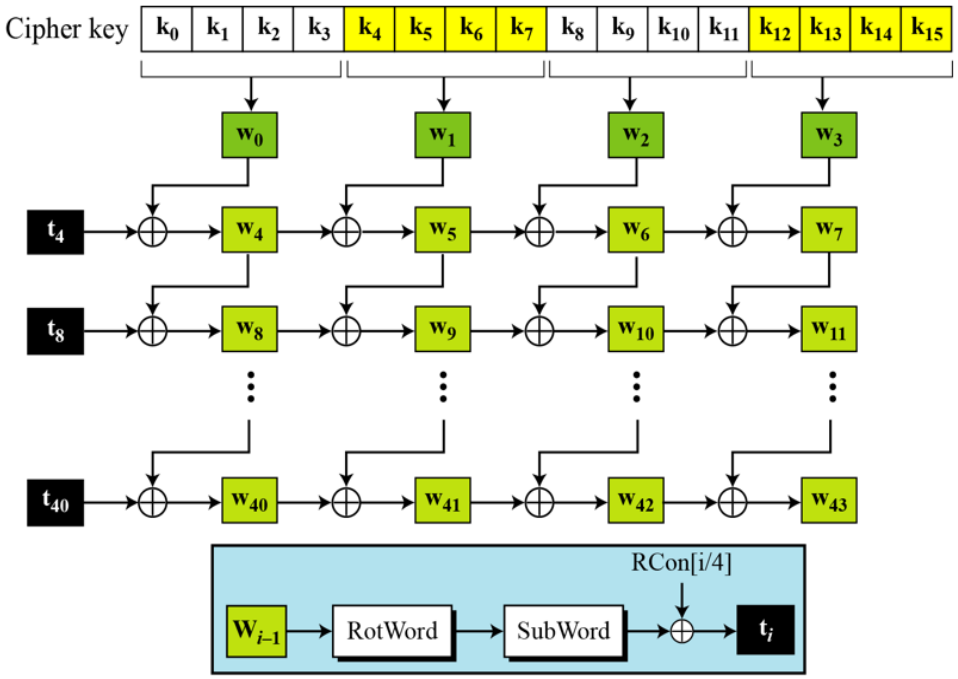


Şekil 2.7. Anahtar ekleme operasyonunda, döngü anahtarı ile durum matrisinin XOR işlemi [100]

- Döngü anahtarlarının oluşturulması

  AES algoritmasında en önemli bileşenlerden birisi döngü anahtarlarının oluşturulması işlemidir. AES algoritmasında kullanılacak olan anahtar uzunluğuna göre (128 bit için 10, 192 bit için 12, 256 bit için 14) döngü sayısı değişim göstermektedir. Algoritmada her döngünün anahtarı şifrelemede kullanılacak olan anahtar (128-192-256) üzerinden anahtar genişletme

fonksiyonu kullanılarak üretilmektedir. Şekil 2.8.'de anahtar genişletme algoritmasına ait blok diyagram görülmektedir. Döngü sayısı Nr olarak kabul edilirse, algoritma tarafından (Nr+1) adet döngü anahtarı şifreleme anahtarından elde edilmektedir. Şifrelemeye verilen ilk anahtar döngüler başlamadan önce, oluşturulan diğer anahtarlar her döngünün içinde kullanılmaktadır. Algoritmada Word (32 bit) kavramı kullanılmakta, döngü sayısına göre algoritma tarafından 4x(Nr+1) adet Word oluşturulmaktadır. 128 bitlik şifreleme için anahtar genişletme algoritması 44, 192 bitlik şifreleme için 52, 256 bitlik şifreleme için 60 adet Word oluşturmaktadır.



Şekil 2.8. AES algoritmasında anahtar genişletme fonksiyonu [131]

Algoritmada temel işlemler olarak rotword ve subword işlemi bulunmaktadır. Rotword işlemi, satır kaydırma işlemine benzemektedir. Bu işlemde bir Word üzerinde bir bayt sola öteleme işlemi yapılmaktadır. Subword işlemi ise bayt değiştirme işlemine benzemektedir. S-Box kullanılarak her bir Word üzerinde bayt değişim işlemi yapılmaktadır. Ayrıca anahtar genişletme işlemi sırasında,

döngü sabiti olarak RCon matrisi denilen bir matris kullanılmaktadır. RCon matrisinin hesaplanmasında GF(2^8) sonlu cisimler teoremi kullanılmaktadır

BÖLÜM 3. YENİ KAOTİK SİSTEMLERİN TASARIMI VE ANALİZLERİ

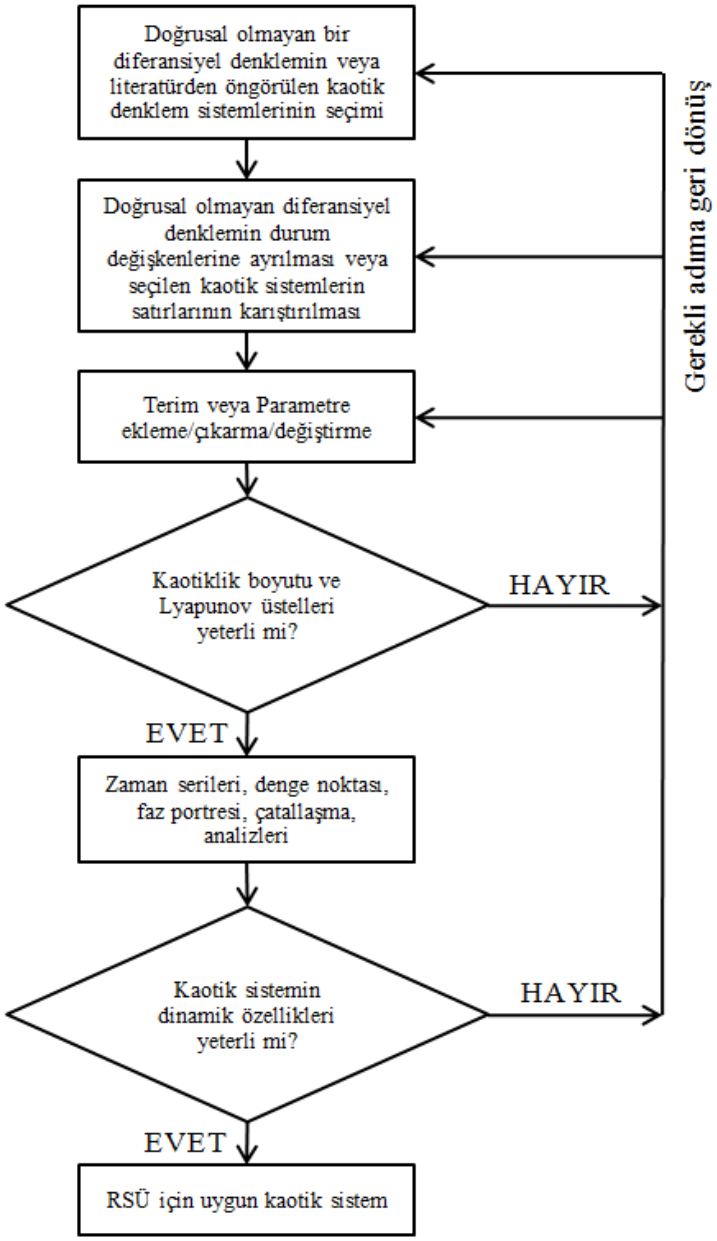
Bu bölümde geliştirilecek olan şifreleme algoritmalarında kullanılmak üzere, daha rassal ve zengin dinamik özelliklere sahip yeni kaotik sistem tasarımları gerçekleştirilmiştir. Dinamik özellikleri yüksek ve daha zengin dinamik özelliklere sahip sistemlerin şifreleme algoritmalarında kullanımı şifrelemenin kalitesini doğrudan etkilemektedir. Yeni kaotik sistem tasarımı için yapılan işlemler Şekil 3.1.' deki blok diyagramda detaylı olarak gösterilmiştir. Yeni kaotik sistem tasarımında, doğrusal olmayan diferansiyel denklemlerin veya denklem sistemlerinin seçiminin ardından, sistemin durum değişkenlerine ayrılması, sisteme parametre veya terim ekleme, çıkarma işlemleri gerçekleştirilmiştir. Bu işlemlerin ardından faz portresi ve zaman serileri analizi, lyapunov üstelleri testleri, çatallaşma diyagramı, denge noktaları gibi analizler ile dinamik özelliklerinin yeterli olup olmadığı test edilmiştir. Yeterli bulunması durumunda, kaotik sistemlerin RSÜ tasarımında kullanımı mümkün olacaktır. Yeni kaotik sistem tasarımlarından önce, bir sistemin kaotik olup olmadığını ve kaotik özellikler göstermesi durumunda dinamik özelliklerinin belirlenmesi için kullanılan analiz yöntemleri hakkında bilgi verilmiştir.

3.1. Kaotik Sistem Analiz Yöntemleri

Kaotik sistemlerin analizi için geliştirilen birçok metot bulunmaktadır. Faz portreleri analizi, zaman serileri analizi, denge noktaları analizi, lyapunov üstelleri analizi, çatallaşma analizi bu yöntemlerden bazılarıdır[114]. Bu yöntemlerden bir kaçı analiz edilerek sistemin kaotik özelliğe sahip olup olmadığı tespit edilebilir. Sistem hakkında daha detaylı bir bilgi için diğer analizlerin de yapılmasına ihtiyaç vardır. Kaotik sistem analiz yöntemlerinin açıklanmasında, literatürde yaygın olarak kullanılan Denklem 3.1'de görülen Lorenz kaotik sistemi kullanılacaktır. Denklem takımı toplamda yedi

terimden oluşmaktadır. Başlangıç şartları x_0=0, y_0= -0.1, z_0=9 ve sistem parametreleri a=10, r=28 ve b=8/3 olarak belirlenmiştir.

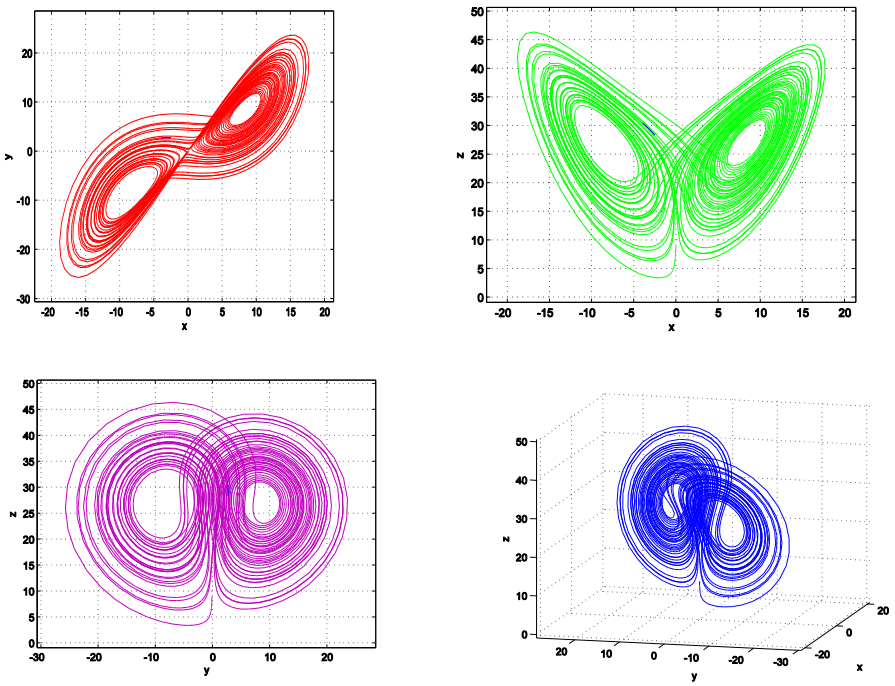
$$x' = a(y - x)$$
$$y' = -xz + rx - y \quad (3.1)$$
$$z' = xy - bz$$



Şekil 3.1. Kaotik sistem tasarım blok diyagramı

3.1.1. Faz portreleri analizi

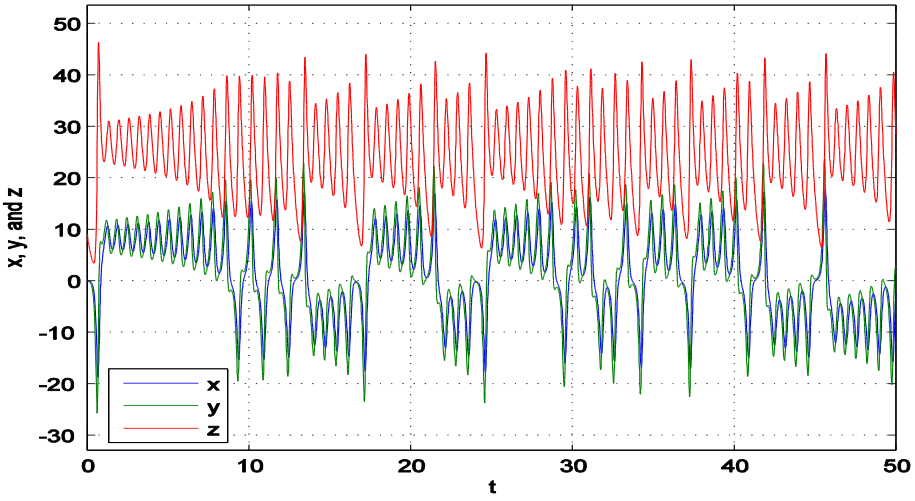
Faz uzayı, sistemin durum değişkenleri ve türevlerinin oluşturduğu uzaydır. Faz portreleri analizinde bir sistemin takip ettiği yörünge görüntülenebilir. Dinamik sistemlerin analizinde sistem hakkında bilgi sahibi olmak için sistemin takip ettiği yörüngenin bilinmesi çok önemlidir. Sistemin zaman sonsuza doğru giderken almış olduğu değerlerin kümesi sistemin haritası veya faz portresi olarak tanımlanmaktadır. Kararlı periyodik bir sistemin faz portresi kapalı bir geometrik şekil oluşturur. Kaotik sistemlerde yörüngeler aynı nokta üzerinden tekrar geçmezler. Bu durum periyodik sistem olmamalarına sebep olmaktadır. Dolayısıyla bir sisteme ait faz portresi sistemin kaotik olup olmadığı ve dinamik özellikleri hakkında önemli bilgiler vermektedir. Üç boyutlu bir sistem için x-y, x-z, y-z ve x-y-z olarak dört farklı şekilde bir sistemin kaotik çekicileri yani faz portrelerine bakılabilir. Şekil 3.2.'de Lorenz sistemine ait xy, xz, yz ve xyz fazlarına ait portreler görülmektedir. Lorenz sistemine ait faz portreleri incelendiğinde, sistemin takip ettiği yörünge ve değer aralıkları net olarak görülebilmektedir.



Şekil 3.2. Lorenz sistemi faz portreleri

3.1.2. Zaman serileri analizi

Zaman serileri analizi sistemin durum değişkenlerinin zaman içinde almış oldukları değerleri tespit etmek için kullanılan bir yöntemdir. Bu yöntemde sisteme ait değişkenlerin nasıl bir değişim izlediği tespit edilebilmektedir. Eğer sistem düzensiz, sabit ve periyodik olmayan davranışlar gösteriyor ise, sistem kaotik bir sistemdir. Fakat bu analiz sistemin kaotik olup olmadığını tespit etmek için yeterli değildir. Çünkü bu analiz yönteminde sistemin üretmiş olduğu belli bir aralıktaki değerler gözlemlenebilmektedir. Bunun için başka analizlerin uygulanmasına ihtiyaç vardır. Zaman serileri analizi ayrıca sistemin başlangıç değerlerine olan hassas bağımlılığını da tespit etmek için kullanılan bir yöntemdir. Başlangıç şartlarındaki ufak bir değişimin sistemin üretmiş olduğu çıktıların tamamen değiştiğini gösterebilmektedir. Şekil 3.3.'de Lorenz sistemine ait 50 iterasyon sonucu elde edilen x, y ve z faz çıktılarına ait zaman serisi analizi grafiği görülmektedir.



Şekil 3.3. Lorenz sistemine ait zaman serileri analizi (x, y, z)

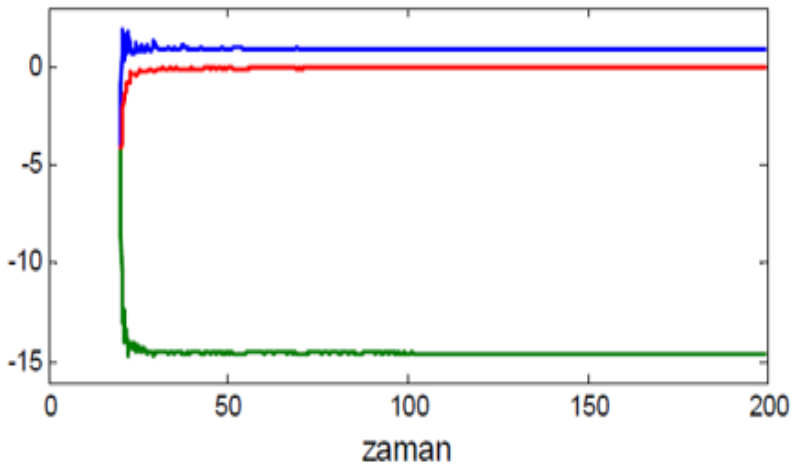
3.1.3. Denge noktaları analizi

Denge noktaları analizi, dinamik sistemlerin davranışları hakkında bilgi veren bir diğer analiz yöntemidir. Bulunan denge noktaları gerçek sayılar kümesine dahil ise sistem denge noktalarına sahiptir. Sistem, bulunan denge noktaları etrafında bir yörüngede kalıyor ise sistem kararlıdır. Aksi durumda sistemin kararsız bir yapıda olduğu

anlaşılmaktadır. Sistem denge noktalarının bulunması için sistemde bulunan her bir denklem 0' a eşitlenir ve çözüm gerçekleştirilir. Daha sonra bulunan denge noktaları sistemin Jacobian matrisi üzerinde yerine yazılarak $|J-\lambda I|=0$ karakteristik denge çözümü gerçekleştirilip sistemin öz değerleri tespit edilir. Sistemin öz değerlerinden en az bir tanesinin gerçek kısmının pozitif olması sistemin kaotik bir davranış gösterdiğine işaret etmektedir [134].

3.1.4. Lyapunov üstelleri analizi

Lyapunov üstelleri analizi, dinamik sistemlerin davranışlarını analiz etmek için kullanılan en önemli yöntemlerden birisidir. Bu analiz sonucunda sistemin kaotik özelliklere sahip olup olmadığı tespit edilebilmektedir. Bu analiz başlangıç şartlarındaki değişimlere sistemin tepkisini tespit etmektedir. N boyutlu bir sistem için n adet λ değeri hesaplanmaktadır. Eğer bulunan λ değeri pozitif ise başlangıç şartları arasındaki fark gittikçe artmakta, eğer negatif ise bu değer birbirine yakınlaşmaktadır. Bunun sonucu olarak λ değeri negatif olduğunda sistem yakın başlangıç şartları için aynı değerleri üretebilir. Bulunan λ değerlerinden en az birinin pozitif olması durumunda ise sistemin kaotik davranış gösterdiği sonucuna varılabilmektedir. Kaotik bir sistemden beklenen davranış başlangıç şartlarındaki en ufak bir değişiklikte birbirinden tamamen bağımsız çıktılar üretmesidir. Lyapunov üstelleri diyagramında sistemin (+, 0, -) olarak üç farklı değer aldığı bölgelerde sistem kaotik özellik göstermekte, diğer kısımlarda kaostan çıkmaktadır [135].

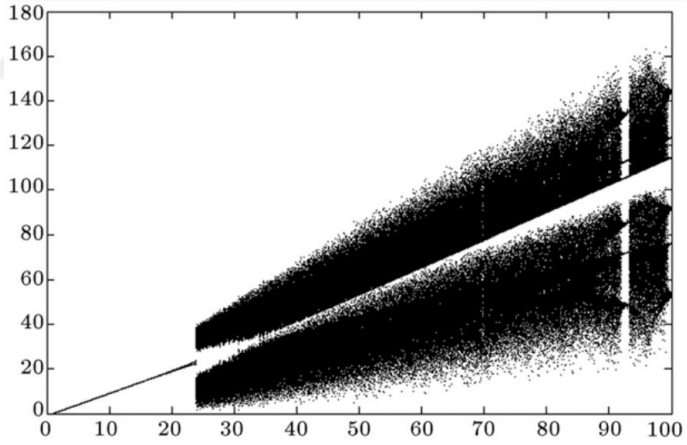


Şekil 3.4. Lorenz sistemine ait lyapunov üstelleri grafiği

Lorenz sistemine ait Lyapunov üstelleri grafiği Şekil 3.4.'de görülmektedir. Lorenz sisteminin λ değerleri (λ_1=0.901, λ_2=0 , λ_3= -14.56) incelendiğinde bir değerinin pozitif, birinin 0 ve birinin de negatif olduğu, yani istenen kaotik davranış özelliklerini taşıdığı görülmektedir.

3.1.5. Çatallaşma analizi

Sistemin herhangi bir parametresindeki değişimin sistem üzerinde nasıl bir değişikliğe yol açtığını görmek için en iyi yöntemlerden birisi çatallaşma analizidir. Bu analiz sonucunda ilgili parametrenin değişimine bağlı olarak sistemin kaosa girdiği ve çıktığı değer aralıklarını tespit etmek mümkündür. Parametreler üzerinde ufak değişimler ile sistemin davranışı tespit edilebilmektedir [134]. Şekil 3.5.'te Lorenz sisteminin r parametresinin 0-100 değerleri arasında çizdirilen çatallaşma diyagramı görülmektedir. Diyagram incelendiğinde sistemin r parametresi için 25 ile 100 değerleri arasında kaosa girip çıktığı görülmektedir.

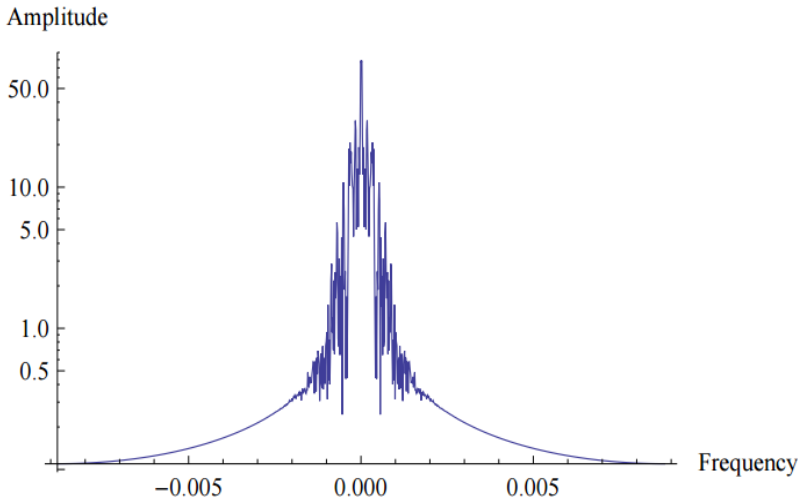


Şekil 3.5. Lorenz sistemi çatallaşma diyagramı (r parametresi [0-100] aralığında)[134]

3.1.6. Frekans spektrum analizi

Frekans spektrum analizi, kaotik sistemin davranışının tespitinde önemli bir kriterdir. Bu analizde test edilen parametre değerinde sistemin hangi frekansta hangi genlikte değerler ürettiği tespit edilebilmektedir. Kaotik sistemlerin özellikle şifreleme uygulamalarında daha rasgele değerler üretmesi istenmektedir. Geniş bant aralığında çıktı üreten sistemler şifreleme ve rasgele sayı üretiminde kullanım için daha

elverişlidir [136]. Şekil 3.6.'da Lorenz sisteminin r=14,5463 parametre değeri için çizdirilen frekans spekturm grafiği görülmektedir.



Şekil 3.6. Lorenz sisteminin frekans spektrum analizi (r=14,5463) [136]

3.2. Yeni NCS Kaotik Sistemi Tasarımı ve Analizleri

Çalışmada geliştirilecek olan şifreleme algoritmalarında kullanılmak üzere, zengin dinamik özelliklere sahip iki adet yeni kaotik sistem geliştirilmiştir. Bu sistemlerden birincisi yeni NCS kaotik sistemidir. Yeni kaotik sistemin tasarımı için, bir araya getirilen denklem takımları üzerinde terim ekleme-çıkarma ve parametreler üzerinde değişiklikler gerçekleştirilmiştir. Geliştirilen yeni kaotik sisteme (NCS) ait denklem takımları aşağıda verilmiştir. (Denklem 3.2)

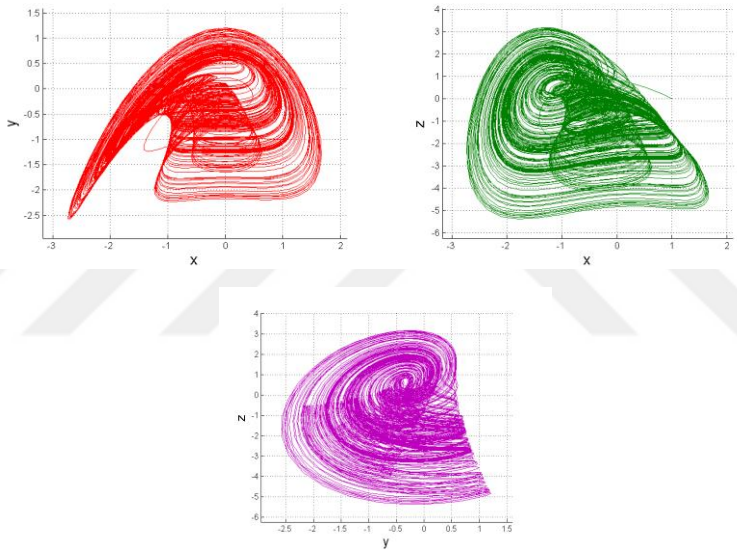
$$\begin{aligned} x' &= cy - x - bz \\ y' &= axz - xy - bx \\ z' &= dxy + b \end{aligned} \tag{3.2}$$

Denklemde kullanılan sistem parametreleri a=1, b=1, c=2, d= -3 ve başlangıç koşulları x_0 =1, y_0 = -1, z_0 = 0.01 şeklinde olduğunda system kaotik davranış sergilemektedir. Sistem parametreleri yerine yazıldığında Denklem 3.3'te verilen denklem takımı elde edilmektedir.

$$
\begin{aligned}
x' &= 2y - x - z \\
y' &= xz - xy - x \\
z' &= -3xy + 1
\end{aligned}
\tag{3.3}
$$

3.2.1. Faz portreleri analizi

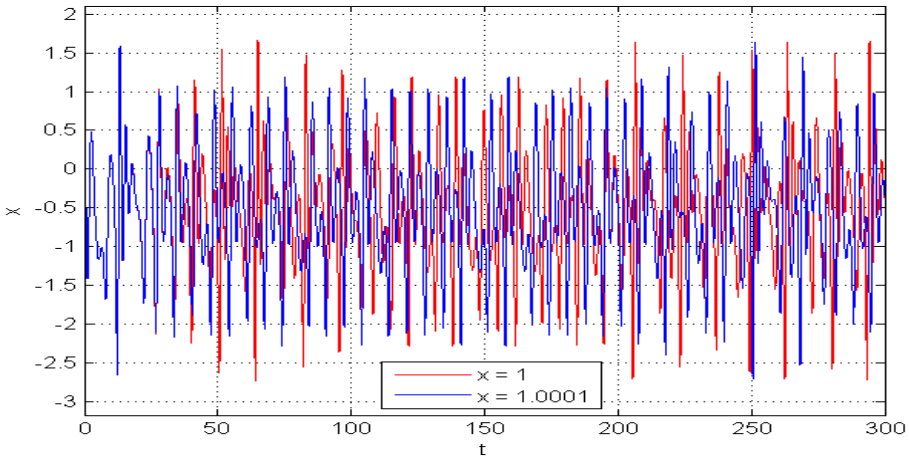
Yeni NCS sistemine ait x-y, x-z ve y-z fazlarına ait faz portreleri çıktıları, Matlab odesolve.m isimli program dosyası kullanılarak çizdirilmiştir. Şekil 3.7.'de sistemin faz portreleri çıktıları görülmektedir. Faz portreleri incelendiğinde sistemin zengin dinamik davranışlara sahip olduğu görülmektedir.



Şekil 3.7. NCS kaotik sistemi faz portreleri çıktıları

3.2.2. Zaman serileri analizi

Sistemin başlangıç şart değerlerindeki çok küçük bir değişiklik sonucu farklı çıktılar vermesi kaotiklik hakkında önemli ipuçları vermektedir. Şekil 3.8.'de görüldüğü üzere, yeni NCS kaotik sisteminin 'x' başlangıç şartı "1" olarak alınmış ve sonucu kırmızı olan çıktı elde edilmiştir. Daha sonra x 1/10000 değiştirilerek, yani "1.0001" yapılarak mavi çıktı elde edilmiştir. İki çıktı Şekil 3.8.'de beraber incelendiğinde çok küçük değişimlerin yeni sistem üzerinde farklı sonuçlar verdiği, yani başlangıç şartlarına çok hassas olduğu görülebilmektedir.



Şekil 3.8. NCS kaotik sistemi zaman serileri analizi

3.2.3. Denge noktaları analizi

Sistemin kararlı bir yapıda olduğunun tespit edilmesi için denge noktaları analizi gerçekleştirilmektedir. Yeni NCS kaotik sisteminin denge noktalarının bulunması için, sistemin denklem takımındaki tüm denklemler sıfıra eşitlenerek çözülmektedir. (Denklem 3.4)

$$\begin{aligned} 0 &= 2y - x - z \\ 0 &= xz - xy - x \\ 0 &= -3xy + 1 \end{aligned} \tag{3.4}$$

Bu denklem sistemi çözüldüğünde denge noktaları:

$E_1 = (0.263763, 1.263763, 2.263763)$
$E_2 = (-1.263763, -0.263763, 0.736238)$ olarak bulunur.

Denge noktaları analizinde sistemin iki adet gerçek denge noktasına sahip olduğu görülmektedir. Denge noktalarının kararlı bir yapıya sahip olup olmadığını test etmek için sistemin özdeğerlerinin tespit edilmesi gerekmektedir. Sistemin özdeğerleri hesaplanırken öncelikle, sistemin Jacobian matrisi hesaplanmalıdır. Sistemin Jacobian matrisi aşağıda görüldüğü gibidir.

$$J = \begin{bmatrix} -1 & 2 & -1 \\ z-y-1 & -x & x \\ -3y & -3x & 0 \end{bmatrix}$$

E_1 denge noktasına ait özdeğerlerin bulunması için, denge noktası değerleri, Jacobian matrisinde yerlerine yazıldığında birinci denge noktasına ait matris ($J(E_1)$) elde edilmektedir. Bu denklem üzerinden $|\lambda I - J(E_1)| = 0$ çözümü gerçekleştirilir.

$$J(E_1) = \begin{bmatrix} -1 & 2 & -1 \\ 0 & -0.2637 & 0.2637 \\ -3.789 & -0.7911 & 0 \end{bmatrix}$$

Sistemin ilk denge noktası için özdeğerleri bulunur.

$$\lambda_1 = 2.6739 \quad \lambda_2 = 0.9178 \quad \lambda_3 = 0.4924$$

Aynı şekilde ikinci denge noktası içinde, denge noktaları Jacobian matrisinde yazılırsa, aşağıdaki matris edilmektedir.

$$J(E_2) = \begin{bmatrix} -1 & 2 & -1 \\ -0.0001 & -1.2637 & 1.2637 \\ 0.7911 & 3.7911 & 0 \end{bmatrix}$$

Bu denklem üzerinden $|\lambda I - J(E_2)| = 0$ çözümü gerçekleştirilir. Sistemin ikinci denge noktası için de özdeğerleri bulunur.

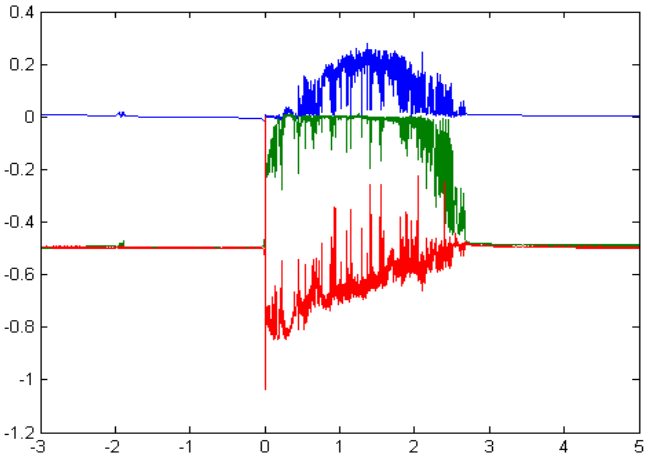
$$\lambda_1 = 1.6224 \quad \lambda_2 = -1.4889 \quad \lambda_3 = -2.3973$$

Sistemin denge noktalarına ait özdeğerlerinden en az birinin pozitif olması durumunda, sistemin kaotik olduğu sonucuna varılmaktadır. Yapılan analizde iki denge noktasına ait öz değerler incelendiğinde, iki denge noktasının özdeğerlerinden

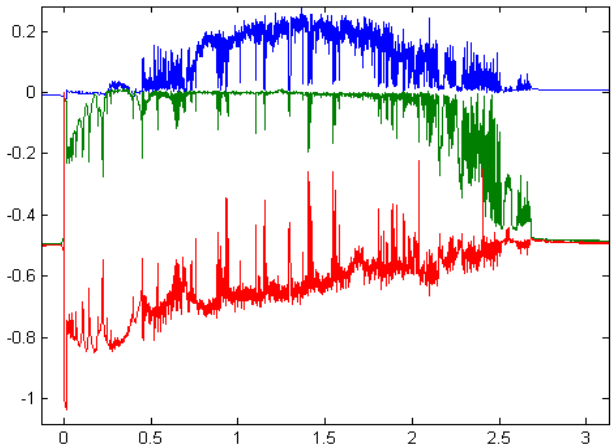
en az birinin pozitif değerlere sahip olduğu görülmektedir. Bunun sonucu olarak, sistemin kaotik özellikler taşıdığı sonucuna varılmıştır.

3.2.4. Lyapunov üstelleri analizi

Yeni NCS kaotik sisteminin 'b' parametresi -3 ile +5 aralığında değiştirilerek elde edilen Lyapunov üstelleri spektrumuna ait grafik Şekil 3.9.'da görülmektedir. Sistem belirli aralıklarda pozitif Lyapunov üsteline sahip olarak kaotik davranışa sahip olmaktadır. 3 boyutlu kaotik bir sistem için Lyapunov üstelleri (-, 0, +) olmalıdır. Diğer durumlarda sistem kaostan çıkmaktadır.



Şekil 3.9. NCS kaotik sisteminin Lyapunov üstelleri spektrumu grafiği(b parametresi [-3,5] aralığında

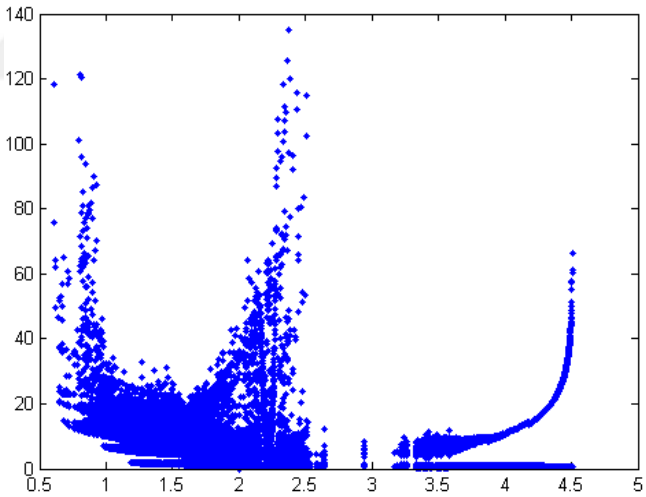


Şekil 3.10. NCS kaotik sisteminin Lyapunov üstelleri spektrumu grafiği(b parametresi [0,3] aralığında

Şekil 3.10. incelendiğinde -3 ile 0 arası (-, 0, +) durumu sağlanmadığından dolayı kaotiklik yoktur. 0 ile 3 arasında ise istenen şart sağlandığından dolayı, sistem b parametresinin bu aralıktaki değerleri için kaotik özellikler taşımaktadır. Sistemin b parametresinin 3 ile 5 arasında değerleri için, Şekil 3.9.'dan görüldüğü üzere sistem kaostan çıkmaktadır. Şekil 3.10.'da ise sistemin kaotiklik durumu b parametresini 0-3 aralığı için tekrar çizdirilmiştir. Daha detaylı olarak bu aralıkta kaotiklik şartlarını sağladığı görülmektedir.

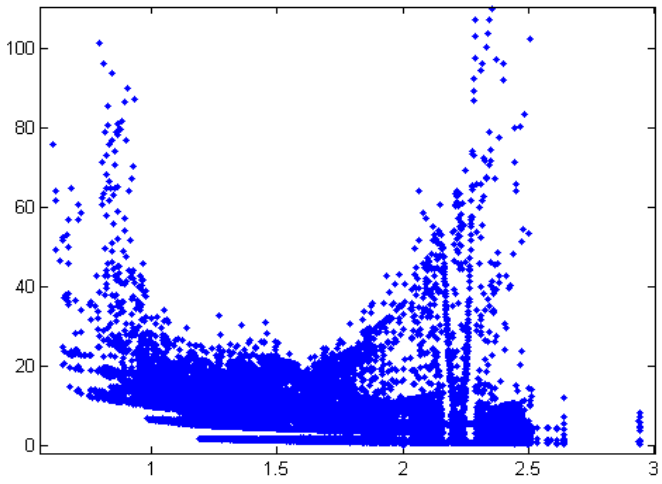
3.2.5. Çatallaşma diyagramı analizi

Yeni NCS kaotik sisteminin, Lyapunov üstellerinde incelendiği gibi, b parametresine göre çatallaşma diyagramı analizi yapılmıştır. Lyapunov üstelleri ve çatallaşma diyagramı analizinde aynı parametre değerleri kullanıldığında, analiz sonucunda kaosa girdiği bölgelerin örtüşmesi gerekmektedir. Lyapunov üstelleri analizinde bir nokta için ne kadar çok değer üretilirse, o aralıkta kaotiklik oranının arttığını söyleyebiliriz.



Şekil 3.11. NCS kaotik sistemi b parametresi için çatallaşma Diyagramı (b= 0-5)

Şekil 3.11.'de b parametresi için 0-5 aralığında çatallaşma diyagramı çizdirilmiştir. Şekil 3.12.'de ise daha detaylı bir gösterim için, b parametresinin 0-3 aralığında çizdirilen çatallaşma diyagramı görülmektedir. Yeni NCS kaotik sisteminin b parametresi için çatallaşma diyagramı ve Lyapunov üstelleri analizleri birlikte incelendiğinde 0-2,7 aralığında kaotik davranış gösterdiği tespit edilmiştir.



Şekil 3.12. NCS kaotik sistemi b parametresi için çatallaşma Diyagramı (b= 0-3)

3.3. Yeni Skala Edilmiş Zhongtang Kaotik Sistemi ve Analizleri

Bu bölümde, Zhongtang kaotik sistemi [136] skala edilerek, sistemin dinamik özelliklerinin zenginleştirilmesi sağlanmış, rasgele sayı üretecine daha uygun karmaşık bir yapı elde edilmiştir. İlk olarak sistemin skala işlemleri gerçekleştirilmiş, zaman serileri ve faz portresi analizleri yapılmış, denge noktaları, özdeğerleri belirlenmiş ve son olarak çatallaşma ve Lyapunov üstelleri incelenmiştir. Zhongtang kaotik sistemi orijinal denklemi aşağıda verilmiştir. (Denklem 3.5)

$$\begin{aligned} x' &= 40y - 40x \\ y' &= 22,5x + 22,5y - xz^2 \\ z' &= -20x - 15z + x^2 z \end{aligned} \tag{3.5}$$

Skala işlemleri için u=x, v=y/2, w=z/2 olarak alınmıştır.

x=u, y=2v, z=2w ve x'=u', y'=2v', z'=2w' elde edilir.

Buna göre ilk denklem:

x' = 40y-40x → u'=40(2v)-40u ve

u'=80v-40u

İkinci denklem:

$y'=22.5x+22.5y-xz^2 \rightarrow 2v'=10u+10(2v)-u(2w)^2$
$v' =5u+10v-2uw^2$

Üçüncü denklem:

$z' = -20x-15z+x^2z \rightarrow 2w'=-20u-15(2*w)+u^2(2w)$
$w' =-10*u-15*w+ w*u^2$
olarak bulunur.

Denklem 2, 3, 4 birleştirilirse,

$$\begin{aligned} u' &= 80v - 40u \\ v' &= 5u + 10v - 2uw^2 \\ w' &= -10u - 15w + wu^2 \end{aligned} \tag{3.6}$$

Denklem 3.6'daki durum değişkenlerinin orijinal harfleri olan x, y, z kullanılırsa, algoritma tasarımında kullanılacak olan, skala edilmiş Zhongtang kaotik sistemi (Denklem 3.7) elde edilir.

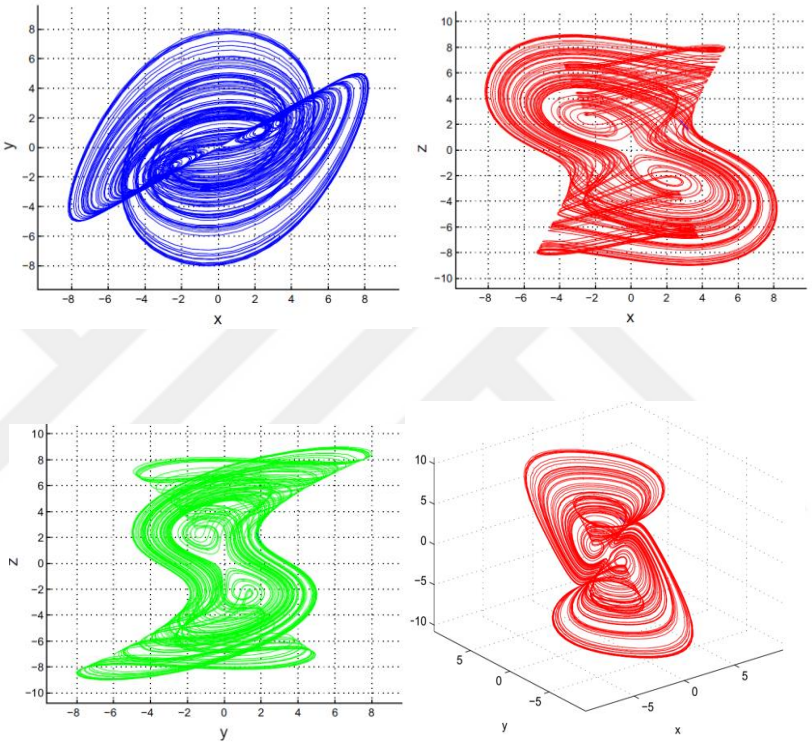
$$\begin{aligned} x' &= 80y - 40x \\ y' &= 5x + 10y - 2xz^2 \\ z' &= -10x - 15z + zx^2 \end{aligned} \tag{3.7}$$

3.3.1. Faz portreleri analizi

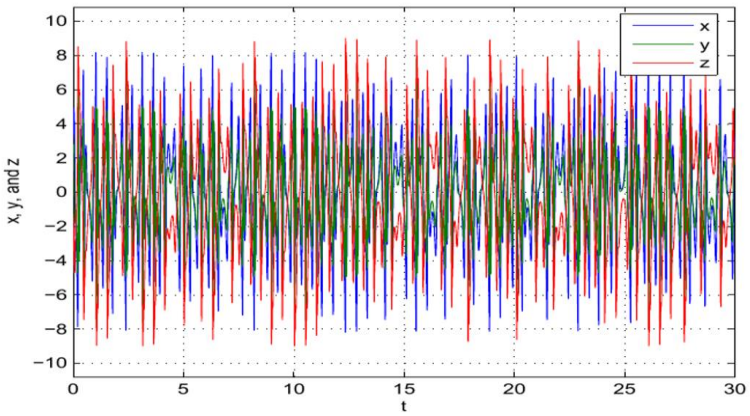
Yeni skala edilmiş Zhongtang kaotik sistem ait x-y, x-z, y-z ve x-y-z fazlarına ait faz portre çıktıları, Matlab odesolve.m isimli program dosyası kullanılarak çizdirilmiştir. Şekil 3.13.'de sistemin faz portreleri çıktıları görülmektedir. Sistemin faz portrelerinde, belli sınırlar içinde, karmaşık yörüngeler takip ettikleri ve zengin dinamik davranışlar taşıdığı görülmektedir.

3.3.2. Zaman serileri analizi

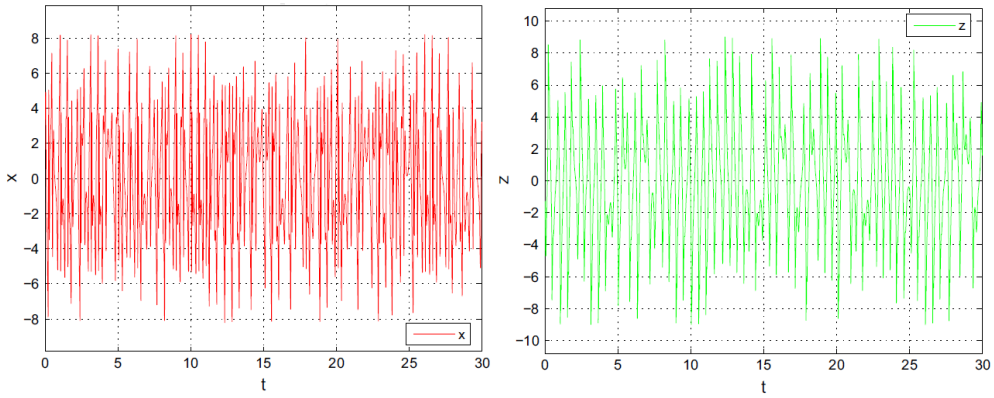
Skala edilmiş yeni Zhongtang kaotik sistemine ait x, z ve x-y-z fazlarının zaman serilerine ait grafikler Şekil 3.14. ve Şekil 3.15.'te görülmektedir. Zaman serileri analizindeki grafikler incelendiğinde, test edilen zaman dilimi boyunca her üç faz içinde oldukça rasgele değerler aldığı, karmaşık ve zengin dinamiklere sahip olduğu görülmektedir.



Şekil 3.13. Yeni skala edilmiş Zhongtang sisteminin faz portresi çıktıları(x-y, y-z, x-z, x-y-z)



Şekil 3.14. Yeni skala edilmiş Zhongtang kaotik sisteminin x-y-z fazlarına ait zaman serileri analizi sonucu



Şekil 3.15. Yeni skala edilmiş Zhongtang sisteminin x ve z fazlarına ait zaman serisi analizi sonuçları

3.3.3. Denge noktaları analizi

Yeni skala edilmiş Zhongtang kaotik sisteminin denge noktlarını ve özdeğerlerini bulmak için, denklem takımındaki tüm denklemler 0'a eşitlenerek Denklem 3.8 elde edilir. Bu denklem çözülerek sistemin denge noktaları bulunmaktadır. Yeni kaotik sistemin 5 adet denge noktasına sahip olduğu tespit edilmiştir. Bu denge noktaları Tablo 3.1.' de verilmiştir. Denge noktaları incelendiğinde hem gerçek, hem de karmaşık sayılardan oluşan denge noktalarına sahip olduğu görülmektedir.

$$\begin{aligned} 0 &= 80y - 40x \\ 0 &= 5x + 10y - 2xz^2 \\ 0 &= -10x - 15z + zx^2 \end{aligned} \tag{3.8}$$

Denge noktalarının bulunmasından sonra, sistemin özdeğerlerini tespit etmek için, sistemin Jacobian matrisi hesaplanmıştır. Bulunan denge noktaları bu matris üzerinde yazılıp çözümleme yapılarak, her bir denge noktasına ait 3 adet özdeğer bulunmuştur. Sistemin her bir denge noktasına ait özdeğerler Tablo 3.1.'de verilmiştir. Sistemin denge noktalarına ait özdeğerlerinden en az birinin pozitif olması durumunda, sistemin kaotik özellik taşıdığı sonucuna varılmaktadır. Tablo 3.1.'deki denge noktalarına ait öz değerler incelendiğinde, her bir denge noktasına ait özdeğerlerden en az birinin gerçek kısmının pozitif olduğu görülmektedir. Dolayısıyla sistemin kaotik özellik taşıdığı sonucuna varılmıştır.

Tablo 3.1. Denge noktaları ve özdeğerler

Denge Noktaları	Özdeğerler
S_1=(0,0,0)	λ_1= -15, λ_2=17.0156, λ_3=-47.0156
S_2=(4.5890,2.2945,7.5738)	λ_1= 17.7033+99.9205i, λ_2= 17.7033-99.9205i, λ_3=-59.3476
S_3=(3.1580,1.5790,-6.2830)	λ_1= 8.6148+80.5800i, λ_2= 8.6148-80.5800i, λ_3=-52.2566
S_4=(-3.8735+0.7216i, -1.9367+0.3608i, -0.6454-6.9882i)	λ_1= 100.64-12.30i, λ_2=-72.05-15.04i, λ_3= -59.11+21.75i
S_5=(-3.8735-0.7216i, -1.9367-0.3608i, -0.6454+ 6.9882i)	λ_1= 100.64+12.30i, λ_2=-72.05+15.04i, λ_3= -59.11-21.75i

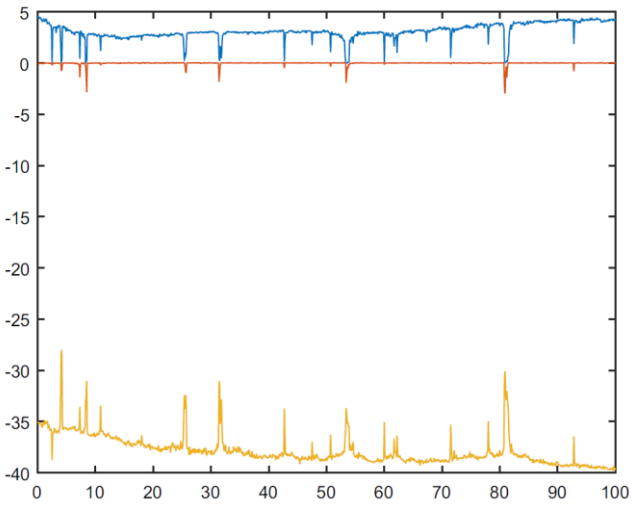
3.3.4. Lyapunov üstelleri analizi

Lyapunov üstelleri analizinde, sistemdeki herhangi bir parametrenin değişimine göre sistemin davranışı test edildiği için, yeni skala edilmiş Zhongtang kaotik sistemi Denklem 3.9'daki şekilde harflendirilmiştir. Denklemdeki parametrelerin değerleri ve başlangıç şartları şu şekildedir : (a = 80, b = 40, c = 5, d = 10, e = 2, f = 10, g = 15) (x_0=1, y_0=0, z_0=1)

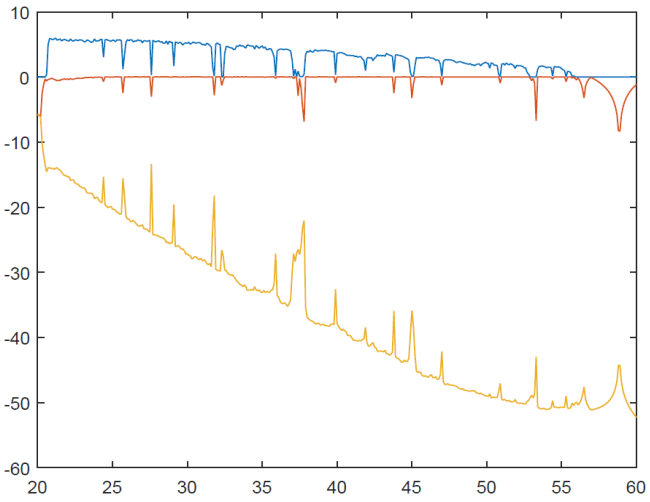
$$\begin{aligned} x' &= ay - bx \\ y' &= cx + dy - exz^2 \\ z' &= -fx - gz + x^2 z \end{aligned} \tag{3.9}$$

Denklem 3.9'daki "a" parametresi, [0 - 100] değer aralığında değiştirilerek elde edilen, sisteme ait Lyapunov üstelleri spektrumu grafiği Şekil 3.16.'da görülmektedir. Lyapunov üstelleri değerlerine ait işaretlerin (-,0,+) olduğu noktalarda sistem kaotik davranışa sahiptir. Sistemin, "a" parametresinin [0 - 100] değer aralığında, çok yüksek

bir oranda kaotik özelliğe sahip olduğu ve çok nadiren kaostan çıktığı Şekil 3.16.'da görülmektedir. Sistem 'a' parametresi [0-100] aralığında değiştirilirken diğer parametreler sabit bırakılmıştır. Denklem 3.9'daki "b" parametresi, [20 - 60] değer aralığında değiştirilerek elde edilen, Lyapunov üstelleri spektrumu grafiği Şekil 3.17.'de görülmektedir. Lyapunov üstelleri değerlerine ait işaretlerin b parametresinin [20-60] aralığında (-,0,+) olduğu noktalarda sistem kaotik davranışa sahiptir. Sistemin 'a' parametresinde de olduğu gibi, "b" parametresinin [20 - 60] değer aralığında, çok yüksek bir oranda kaotik özelliğe sahip olduğu ve çok nadiren kaostan çıktığı Şekil 3.17.'de görülmektedir. Sistem 'b' parametresi [20-60] aralığında değiştirilirken, diğer parametreler üzerinde herhangi bir değişiklik yapılmamıştır.



Şekil 3.16. Yeni skala edilmiş Zhongtang kaotik sistemi Lyapunov üstelleri spekturumu grafiği (a - [0-100])

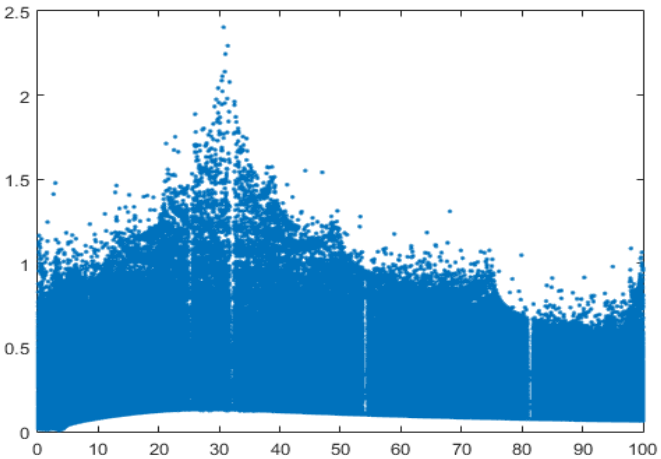


Şekil 3.17. Yeni skala edilmiş Zhongtang kaotik sistemi lyapunov üstelleri spektrumu grafiği (b- [20-60])

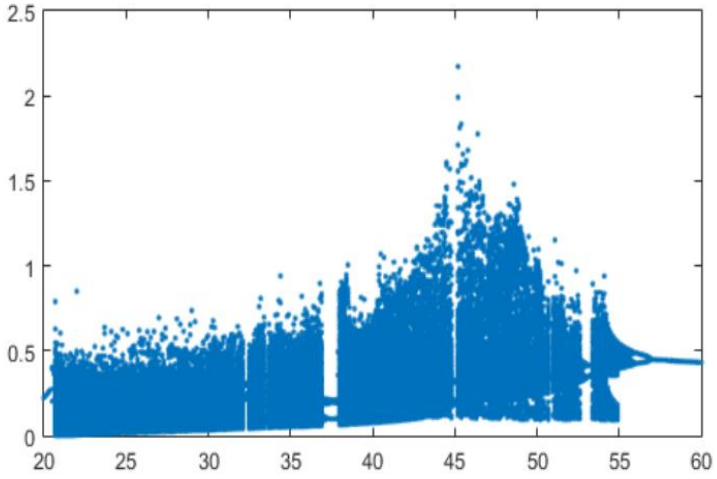
3.3.5. Çatallaşma diyagramı analizi

Yeni kaotik sistemin çatallaşma diyagramı analizi, Lyapunov üstelleri analizinde olduğu gibi Denklem 3.9'daki a ve b parametrelerinin aynı değerleri kullanılarak çizdirilmiştir. Denklem 3.9'daki "a" parametresi, [0-100] değer aralığında değiştirilerek elde edilen, sisteme ait çatallaşma diyagramı Şekil 3.18.'de görülmektedir. Şekil 3.18. incelendiğinde, sistemin Lyapunov üstelleri spektrumundaki aynı parametre değerlerinde, kaosta olduğu ve kaostan çıktığı görülmektedir. Çatallaşma diyagramı ve Lyapunov üstelleri spekturumu grafikleri çizdirilirken diğer parametre değerleri b=40, c=5, d=10, e=2, f=10, g=15 olarak alınmıştır.

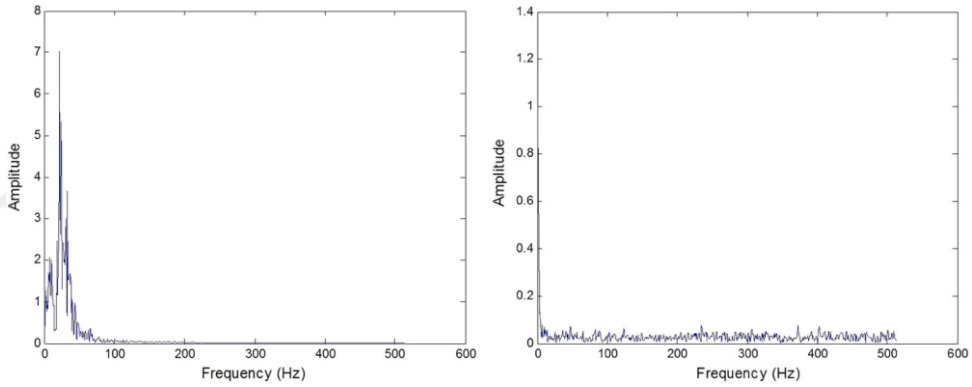
Denklem 3.9'daki "b" parametresi, [20 - 60] değer aralığında değiştirilerek elde edilen, sisteme ait çatallaşma diyagramı Şekil 3.19.'da görülmektedir. Şekil 3.19. incelendiğinde, sistemin Lyapunov üstelleri spektrumundaki aynı parametre değerlerinde, a parametresinde olduğu gibi, kaosta olduğu ve kaostan çıktığı görülmektedir. Çatallaşma diyagramı ve Lyapunov üstelleri spektrumu grafiklerinin 'a' ve 'b' parametreleri için çizdirilen grafiklerinin birebir örtüştüğü, ve sistemin çok zengin ve rasgele dinamik özellikler taşıdığı belirlenmiştir. Çatallaşma diyagramı ve Lyapunov üstelleri spekturumu grafikleri çizdirilirken diğer parametre değerleri a=80, c=5, d=10, e=2, f=10, g=15 olarak alınmıştır.



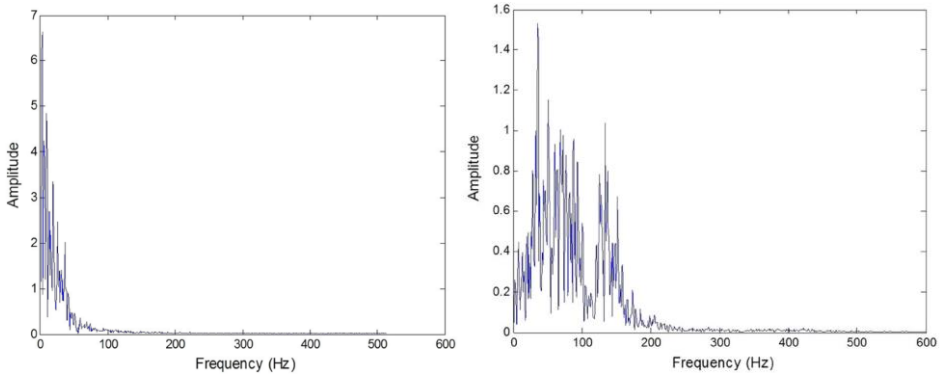
Şekil 3.18. Yeni skala edilmiş Zhongtang kaotik sistemi çatallaşma diyagramı grafiği (a- [0-100])



Şekil 3.19. Yeni skala edilmiş Zhongtang kaotik sistemi çatallaşma diyagramı grafiği (b- [20-60])



(a) Chen (b) Lojistik



(c) Lorenz (d) Yeni skala edilmiş Zhongtang

Şekil 3.20. Kaotik sistemlerin frekans spektrumu analizi sonuçları

3.3.6. Frekans spectrum analizi

Yeni skala edilmiş Zhongtang kaotik sisteminin, şifreleme sistemlerinde uygunluğunun gösterilmesi için frekans spektrum analizi gerçekleştirilmiştir. Şekil 3.20'de literatürde yaygın olarak kullanılan kaotik sistemler Chen [137], Lojistik [138] ve Lorenz [139] ile yeni skala edilmiş Zhongtang sisteminin frekans spektrumu grafikleri görülmektedir. Şekil 3.20. incelendiğinde, yeni kaotik sistemin diğer karşılaştırılan kaotik sistemlerden daha yüksek bant genişliğine sahip olduğu görülmektedir. Bu sebeple yeni sistemin, şifreleme ve rasgele sayı üreteci uygulamalarında kullanım için uygun olduğu sonucuna varılmıştır. Literatürde var olan sistemleri kullanmak yerine bu tez çalışmasında yeni kaotik sistemler geliştirilerek, daha zengin dinamik özelliklere sahip sistemler tasarlanmıştır.

BÖLÜM 4. YENİ KAOS TABANLI RSÜ, S-BOX VE ŞİFRELEME ALGORİTMASI TASARIMLARI

4.1. Yeni Kaos Tabanlı RSÜ Algoritmaları Tasarımı ve NIST Testleri

Bu bölümde, tasarlanan yeni kaotik sistemler kullanılarak, şifreleme algoritmalarında kullanılmak üzere iki adet RSÜ tasarımı gerçekleştirilmiştir. Kaos tabanlı yeni RSÜ tasarımlarında, literatürdekilerden farklı olarak kayan noktalı sayıların hassas basamakları kullanılarak rasgeleliği yüksek bit dizileri üretilmiştir. RSÜ tarafından üretilen rassal bit dizilerine NIST rasgelelik testleri uygulanarak üretilen bit dizilerinin rassallıkları değerlendirilmiştir. Rasgele sayı üretiminde kullanılacak olan RSÜ algoritmalarının basit operasyonlar ile güçlü rassallığa sahip bit dizileri üretmesi istenilmektedir. Kaotik sistemlerin üretmiş olduğu değerlerin, RSÜ tasarımında kullanımı için öncelikle nümerik analiz algoritmalarıyla diferansiyel denklem takımlarının çözümlenmesi gerekmektedir. Euler, Heun, Runge Kutta 4 (RK4) ve Runge Kutta 5 (RK5) bu algoritmalardan bazılarıdır [140]. Kaotik sistemler başlangıç şartlarına çok hassas bağımlı olduklarından dolayı, bu çalışmada kaotik sistem çözümlemesi için, çok hassas çözümler yapamayan Euler ve yüksek frekanslı sistemlerde kullanımı uygun olmayan Heun algoritmalarının yerine hassas değerler üzerinde hata oranı düşük çözümleme yapan RK4 algoritması kullanılmıştır. Kaotik sistem RK4 algoritması kullanılarak çözümlenmiş ve kayan noktalı sayıların üretimi gerçekleştirilmiştir. RK4 algoritmasının matematiksel ifadesi Denklem 4.1'de verilmiştir.

RK4 algoritmasında $y_{\lambda}+1$ değerinin hesaplanması için; k_1, k_2, k_3 ve k_4 değerlerinin bulunması gerekmektedir. Algoritmanın ilk başlangıcındaki k_1 değeri algoritmada belirlenen örnekleme adımı olan Δh örnekleme adımı değeri sonucundaki eğim değeridir. k_2, k_3 ve k_4 değerleri de sırasıyla Δh örnekleme adımının orta değeri ve k_1, k_2, k_3 değerleri kullanılarak hesaplanan eğim değerleridir.

$$
\begin{aligned}
k_1 &= f(y_\lambda) \\
k_2 &= f(y_\lambda + \frac{\Delta h}{2} k_1) \\
k_3 &= f(y_\lambda + \frac{\Delta h}{2} k_2) \\
k_4 &= f(y_\lambda + \Delta h k_3) \\
y_{\lambda+1} &= y_\lambda + \frac{1}{6}(k_1 + 2k_2 + 2k_3 + k_4)\Delta h
\end{aligned}
\qquad (4.1)
$$

Algoritmanın son adımında ise, y_λ değeri kullanılarak $y_{\lambda+1}$ değeri hesaplanmakta ve sistem sayısal bir değer üretmektedir. Sistem bu şekilde çözümlenerek istenilen kadar sayısal değer üretimi gerçekleştirilmektedir [141]. RK4 algoritmasının üretmiş olduğu sayılar IEEE 754 standardına göre tek duyarlı (32 bit) veya çift duyarlı (64 bit) olarak elde edilmektedir. 32 bitli gösterim için yüksek anlamlı kısım (MSB) 1 bit işaret biti, 8 bit üs bitleri ve 23 bit anlamlı kısımdır. 64 bitlik format için ise yüksek anlamlı kısım (MSB) 1 bit işaret biti, 11 bit üs bitleri ve 52 bit anlamlı kısımdır.

4.1.1. Yeni RSÜ-1 tasarım algoritması

RSÜ-1 tasarım algoritması, geliştirilen yeni kaotik sistemlerin, RK4 algoriması ile çözümlenmesi sonucu elde edilen kayan noktalı sayıların ikilik sayı sistemine dönüştürülerek, bu dizilerden bit seçimi suretiyle rasgele bit dizilerini oluşturmaktadır. Şekil 4.1.'de algoritmaya ait blok diyagram ve ardından RSÜ-1 algoritmasının sözde kodu verilmiştir. Algoritma adımları aşağıda açıklanmıştır.

Adım 1: Kaotik sistemin başlangıç şartları ve sistem parametrelerinin girilmesi.

Adım 2: Daha rasgele sonuçlar elde etmek için, kaotik sistemin zaman serilerine en uygun Δh örnekleme aralığı tespit edilmesi.

Adım 3: Kaotik sistemin RK4 sayısal analiz metodu ile çözülerek, zaman serilerinin elde edilmesi.

Adım 4: Zaman serilerinden belirlenen örnekleme aralığı ile kayan noktalı sayıların elde edilmesi.

Adım 5: Elde edilen kayan noktalı sayıların 32 bitlik sayı dizilerine dönüşümü.

Adım 6: Her bir örnekleme adımından elde edilen kayan noktalı sayıların dönüşümünde elde edilen 32 bitlik dizilerden, rastgeleliğin artırılması için daha hassas olan düşük anlamlı kısımdan (LSB) bitler çekilerek şifrelemede kullanılacak olan bit dizisi oluşturulması.

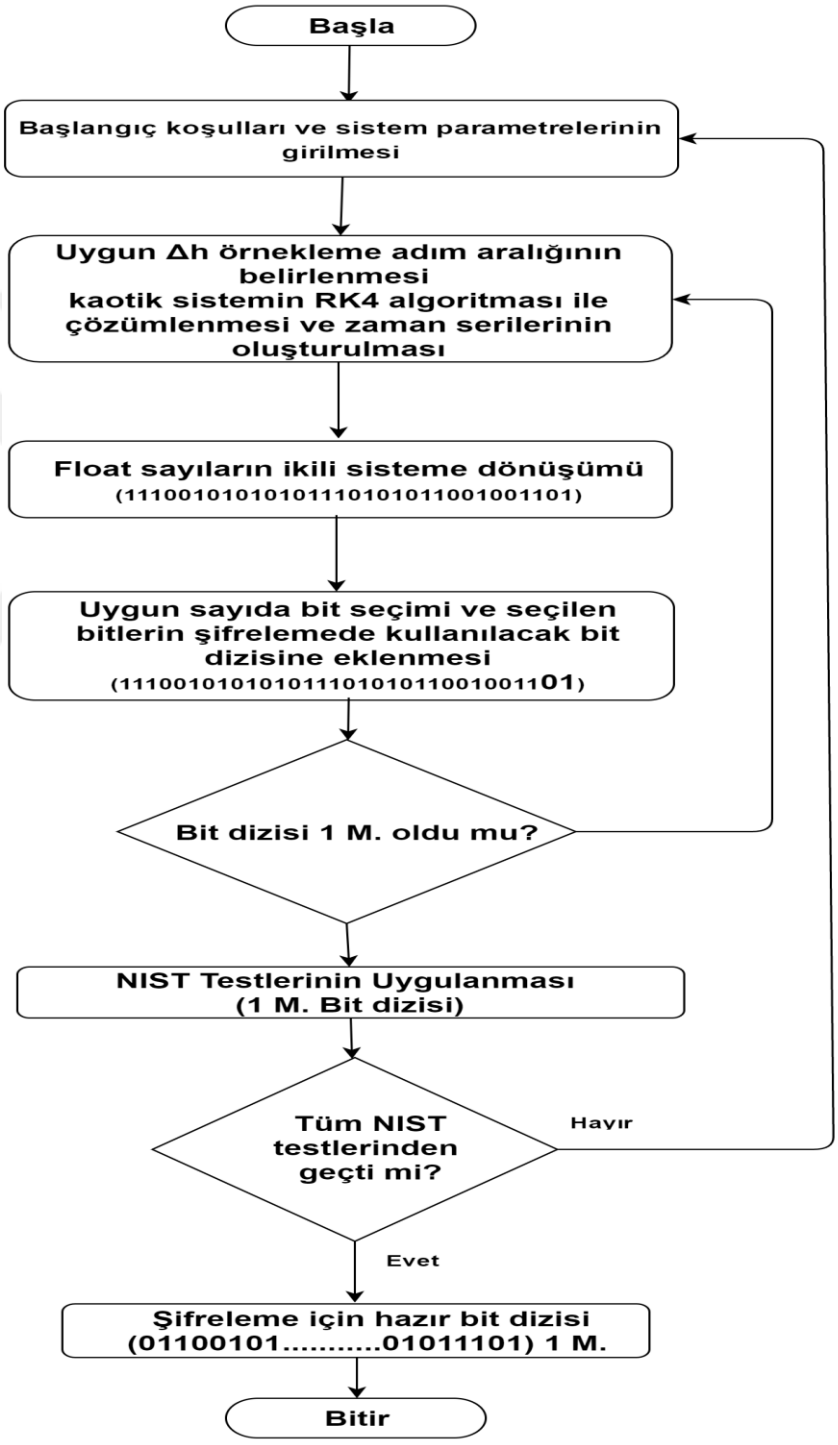
Adım 7: Her bir adımda seçilen bitlerin rasgele bit dizisine eklenmesi.

Adım 8: Bu işlemler rasgele bit dizisinin boyutu 1 milyon bite ulaşıncaya kadar devam etmektedir.

Adım 9: RSÜ tasarımının son adımında, elde edilen bit dizilerinin rasgeleliğinin test edilmesi için uluslararası en üst düzey standart olan NIST testleri uygulanır. Elde edilen 1 M rasgele bit dizisinin NIST testlerinden kalması durumunda Şekil 4.1.'de görüldüğü üzere önceki adımlara dönüş yapılarak, seçilen bitler veya örnekleme adımı değiştirilerek bit dizisinin tekrar üretilmesi gerekmektedir. Testlerin tamamından geçmiş olan bit dizilerini üreten sistem şifreleme algoritmasında rasgele bit üretimi için kullanılabilmektedir.

Adım 6'da birbirini takip eden bitlerin seçilmesi durumunda oluşturulan bit dizisi rasgelelik testlerini geçememektedir. Bu yüzden oluşturulan 32 bitlik diziler üzerinden uygun sıradaki bitler çekilerek ve gerek duyulması halinde doğrusal olmayan işlemlere tabi tutularak şifrelemede kullanılacak bit dizileri oluşturulur. Bu çalışmada her 32 bitlik sayı dizisinden sırası ile 1 artırılarak daha fazla bit alınarak test edilmiş ve en rasgele bit dizilerinin 2 bit alındığında elde edildiği görülmüştür. NIST testlerinde farklı sayıda bit seçimi ile gerçekleştirilen testlere ait sonuçlar verilmiştir. Rasgele bit üretme işlemi bu algoritmada her faz için ayrı gerçekleştirilerek, algoritmanın bir kez çalışması ile 3 ayrı faza ait rasgele bit dizileri elde edilebilmektedir. Fakat elde edilen

3 farklı rasgele bit dizisi, NIST test sonuçlarına göre farklı rassal özellikler gösterdiğinden, test sonuçlarına göre bu dizilerin şifreleme işlemlerinde kullanımı için tercih yapılması gerekmektedir. 3 faza ait çıktılardan bazı fazlara ait rasgele bit dizileri testlerin tümünden geçerken bazıları testlerin tamamını geçememektedir.



Şekil 4.1.RSÜ-1 Algoritması blok diyagramı

```
Başla
Sistem parametreleri ve başlangıç koşullarının kaotik sisteme girilmesi
Uygun Δh değerinin belirlenmesi
while (Until 1 M. Bit) do
    Kaotik sistemin RK4 algoritması kullanılarak çözümlenmesi ve zaman serilerinin elde edilmesi
    Kayan noktalı sayıların ikili sisteme çevrilmesi(32 bit)
    32 bit sayı dizisinden uygun bitlerin seçilmesi (LSB- 2 bit)
end while
Sayı dizisine NIST testlerinin uygulanması (1 M. bit)
if (test sonucu == geçti) then
    şifreleme için hazır bit dizisi
else {test sonucu == kaldı}
    önceki adımlara dönülerek yeni bit dizilerinin oluşturulması (adım 3)
end if
Bitir
```

4.1.2. Yeni RSÜ-2 tasarım algoritması

RSÜ-2 tasarım algoritmasında, RSÜ-1 tasarım algoritmasından farklı olarak üretilen kayan noktalı değerlerin ikili sayı sistemine dönüştürülmesinin yerine, üretilen kayan noktalı sayıların basamak değerleri üzerinde mod işlemi yapılarak, rasgele bit dizilerinin üretimi sağlanmıştır. Geliştirilen yeni RSÜ-2 algoritmasına ait adımlar şu şekildedir.

Adım 1: Kaotik sistemin başlangıç koşulları ve sistem parametrelerinin girilmesi.

Adım 2: Daha rasgele sonuçlar elde etmek için, kaotik sistemin zaman serilerine en uygun Δh örnekleme aralığının tespit edilmesi.

Adım 3: Kaotik sistemin RK4 sayısal analiz metodu ile çözülerek, zaman serilerinin elde edilmesi.

Adım 4: x, y, z fazları üzerinden belirlenen örnekleme değeri kullanılarak elde edilen kayan noktalı sayılar üzerinde mod alma işleminin gerçekleştirilmesi.

- Virgülden sonraki 15 basamak üzerinde her bir basamak için mod 2 işlemi gerçekleştirilerek, üretilen her bir sayıdan 15 adet bit elde edilmektedir.

Örnek işlem:

x fazından örnekleme sonucu elde edilen sayı 0,459742130623401 olsun.

Basamakların mod alma işlemi:

4%2=0, 5%2=1, 9%2=1, 7%2=1, 4%2=0, 2%2=0, 1%2=1, 3%2=1, 0%2=0, 6%2=0, 2%2=0, 3%2=1, 4%2=0, 0%0=0, 1%2=1

Bir sayıdan üretilen 15'lik bit dizisi: [0 1 1 1 0 0 1 1 0 0 0 1 0 0 1] olarak elde edilir. 15 bitlik bu dizi x fazından elde edilecek olan rasgele bit dizisine eklenir.

x-phase +=[0,1,1,1,0,0,1,1,0,0,0,1,0,0,1]

Adım 5: Her bir faz çıktısından (x, y, z), şifrelemede kullanılacak ve NIST testleri ile test edilecek olan 1 milyon bitin üretimi için gerekli kayan noktalı sayılar (1000000 / 15) üretilerek, bit dizileri oluşturulmaktadır.

Adım 6: Her bir fazdan oluşturulan 1 milyonluk bit dizilerine uygulanan NIST testlerini geçemedikleri tespit edildiği için, rasgele bit dizilerinin kendi aralarında ikili olarak XOR işlemine tabi tutulması.

Örnek XOR işlemi:

x-phase= [0,1,1,1,0,0,1,1,0,0,0,1,0,0,1, ... 1,0,1,1]

y-phase= [1,1,0,0,0,1,1,0,1,1,0,1,1,1,0, ... 0,1,1,0]

z-phase= [0,0,1,1,1,1,0,0,1,0,1,1,0,0,1, ... 1,0,0,1]

xy-phase= x-phase(xor) y-phase = [1,0,1,1,0,1,0,1,1,1,0,0,1,1,1, ...1,1,0,1]

xz-phase= x-phase(xor) z-phase = [0,1,0,0,1,1,1,1,0,1,0,1,0,0,0, ... 0,0,1,0]

yz-phase= y-phase(xor) z-phase = [1,1,1,1,1,0,1,0,0,1,1,0,1,1,1, ... 1,1,1,1]

Adım7: İkili fazların XOR'lanması ile oluşturulan bit dizilerine (xy, xz ve yz) NIST testlerinin uygulanması.

RSÜ-2 tasarımında RSÜ-1 tasarımında olduğu gibi kaotik sistem RK4 algoritması ile çözülerek belirlenen örnekleme adımı ile kayan noktalı sayılar elde edilmiştir. İlk

tasarımdan farklı olarak, RSÜ-2 tasarımında kayan noktalı sayıların ikilik sayı sistemine çevrimi yapılmamaktadır. RSÜ-2 tasarımında kayan noktalı sayıların virgülden sonraki 15 basamağının, basamak değerleri kullanılarak mod işlemi ile rasgele bitler oluşturulmaktadır. Fakat bu tasarımda her fazdan üretilen rasgele bit dizilerinin tek başına NIST testlerinden geçemedikleri tespit edilmiştir. Bu sebeple fazların aralarında ikili olarak XOR işlemine tabi tutularak, NIST testlerinin hepsinden geçmesi sağlanmıştır. RSÜ-2 algoritmasına ait sözde kod aşağıda verilmiştir.

```
Başla
Sistem parametreleri ve başlangıç koşullarının kaotik sisteme girilmesi
Uygun Δh değerinin belirlenmesi (Δh=0.001)
i=0;
x-phase=[]; y-phase=[]; z-phase=[];
xy-phase=[]; xz-phase=[]; yz-phase=[];

while (i=<1000000) do
   Kaotik sistemin RK4 algoritması ile çözülmesi
   x,y ve z faz değerlerinin elde edilmesi
   x − value → x, x0x1x2x3x4x5x6x7x8x9x10x11x12x13x14
   y − value → y, y0y1y2y3y4y5y6y7y8y9y10y11y12y13y14
   z − value → z, z0z1z2z3z4z5z6z7z8z9z10z11z12z13z14

   for k = 0 to 14 do
      x-phase[i]= mod (x[k],2);
      y-phase[i]= mod (y[k],2);
      z-phase[i]= mod (z[k],2);
      i=i+1;
   end for
end while

xy-phase= x-phase ⊕ y-phase;
xz-phase= x-phase ⊕ z-phase;
yz-phase= y-phase ⊕ z-phase;

xy-phase,xz-phase,yz-phase değerlerine NIST testlerinin uygulanması
if
 then {test sonucu==geçti}
   şifreleme için hazır bit dizisi
else {test sonucu==kaldı}
   önceki adımlara dönülerek yeni bit dizisinin oluşturulması (adım 3)
end if
Bitir
```

4.1.3. RSÜ-1 algoritması NIST test sonuçları

Rasgele sayı dizilerinin, NIST testlerinin tümünden geçmesi, tasarlanan yeni RSÜ' lerin şifreleme uygulamalarında rasgele sayı üretiminde kullanılabileceğini göstermektedir. Rasgele bit dizisinin testlerinden en az birinden kalması durumunda, RSÜ'nün üretmiş olduğu bit dizileri yeterli rassallığa sahip değildir. Kaos tabanlı RSÜ ile üretilen bit dizileri testleri geçtiği için, şifrelemede ihtiyaç duyulan kadar bitin üretimi için, tasarlanan RSÜ'den elde edilecek olan rasgele bit dizileri şifrelemede kullanılmıştır. RSÜ-1 ve RSÜ-2 algoritmalarında kullanılan yeni NCS ve skala edilmiş Zhongtang kaotik sisteminin başlangıç değerleri, sistem parametreleri ve örnekleme adım değerleri,

Yeni NCS kaotik sistemi sistem parametreleri:
a=1, b=1, c=2, d= -3 başlangıç koşulları: x_0 =1, y_0 = -1, z_0 = 0, 01
Δh örnekleme aralığı: 0,05
Yeni skala edilmiş Zhongtang kaotik sistemi system parametreleri:
a = 80, b = 40, c = 5, d = 10, e = 2, f = 10, g = 15 başlangıç koşulları: x_0=1, y_0=0, z_0=1 ve Δh örnekleme aralığı: 0,001 olarak kullanılmıştır.

Tablo 4.1. Yeni NCS kaotik sistemi ile RSÜ-1 NIST-800-22 Test Sonuçları (2 bit)

NIST Testleri	**P-değeri (x)**	**P- değeri (y)**	**P- değeri (z)**	**Sonuç**
Frekans testi	0.8697	0.1235	0.8633	Başarılı
Blok frekans testi	0.2621	0.5180	0.6326	Başarılı
Birikimli toplamlar testi	0.9796	0.8471	0.2040	Başarılı
Akış testi	0.3886	0.7116	0.7703	Başarılı
Bir blok içerisinde en uzun birler akış	0.7735	0.3529	0.7242	Başarılı
İkili matris derece testi	0.1608	0.6109	0.8804	Başarılı
Ayrık fourier dönüşüm testi	0.6529	0.0239	0.1988	Başarılı
Örtüşmeyen Şablon eşleştirme testi	0.4356	0.3679	0.3298	Başarılı
Örtüşen Şablon Eşleştirme Testi	0.5758	0.7760	0.1927	Başarılı
Maurer'in "Evrensel İstatistik" Testi	0.1424	0.1899	0.2508	Başarılı
Yaklaşık Entropi Testi	0.0409	0.9349	0.6270	Başarılı
Rasgele Gezinimler Testi	0.9727	0.6489	0.7345	Başarılı
Rasgele Gezinimler Değişken Testi	0.4973	0.4892	0.5346	Başarılı
Seri testi-1	0.1148	0.0423	0.5276	Başarılı
Seri testi-2	0.8163	0.0869	0.5990	Başarılı
Doğrusal Karmaşıklık Testi	0.9505	0.3667	0.8755	Başarılı

Tablo 4.2. Yeni skala edilmiş Zhongtang kaotik sistemi ile RSÜ-1 NIST-800-22 Test Sonuçları (2 bit)

NIST Testleri	**P-değeri (x)**	**P- değeri (y)**	**P- değeri (z)**	**Sonuç**
Frekans testi	0,47152	0,42836	0,27836	Başarılı
Blok frekans testi	0,31291	0,57038	0,40505	Başarılı
Birikimli toplamlar testi	0,35265	0,23846	0,39250	Başarılı
Akış testi	0,72973	0,60821	0,62047	Başarılı
Bir blok içerisinde en uzun birler akış	0,66317	0,36167	0,50450	Başarılı
İkili matris derece testi	0,26959	0,53986	0,99071	Başarılı
Ayrık fourier dönüşüm testi	0,93417	0,13235	0,76202	Başarılı
Örtüşen Şablon Eşleştirme Testi	0,81371	0,72090	0,56254	Başarılı
Maurer'in "Evrensel İstatistik" Testi	0,19866	0,40014	0,86944	Başarılı
Yaklaşık Entropi Testi	0,19206	0,42047	0,69099	Başarılı
Rasgele Gezinimler Testi	0,99812	0,32208	0,74956	Başarılı
Rasgele Gezinimler Değişken Testi	0,96797	0,40179	0,38883	Başarılı
Seri testi-1	0,69975	0,29663	0,85269	Başarılı
Seri testi-2	0,94370	0,17954	0,69698	Başarılı
Doğrusal Karmaşıklık Testi	0,21698	0,50630	0,85498	Başarılı

Tablo 4.1. ve Tablo 4.2.'de yeni geliştirilen NCS ve skala edilmiş Zhongtang kaotik sisteminin RSÜ-1 tasarım algoritmasında kullanılması sonucu elde edilen rasgele bit dizilerine uygulanan NIST rasgelelik test sonuçları görülmektedir. RSÜ-1 tasarım algoritmasında, her iki kaotik sistemin x, y ve z fazlarından rasgele 1 milyon genişliğinde bit dizileri oluşturulmuştur. Algoritma tasarımında belirtildiği üzere bu dizilerin oluşturulması sırasında, üretilen kayan noktalı sayıların ikilik sayı sistemine çevrilen bit dizilerinden yüksek hassasiyete sahip, düşük anlamlı kısımlarından 2 bit çekilerek, bit dizileri elde edilmiştir. Bu işlemde 1 milyon uzunluğunda rasgele bit dizisi oluşturmak için, RSÜ-1 algoritması 500 bin adet kayan noktalı sayı üretmiştir. Test sonuçlarına göre geliştirilen iki yeni kaotik sisteminde RSÜ-1 tasarım algoritmasında kullanılması ile üretilen rasgele bit dizilerinin tüm NIST testlerinden geçtiği görülmektedir. Geliştirilecek olan hibrit kaos tabanlı CRSA algoritmasında testlerin tümünden geçmiş olan yeni NCS kaotik sistemini kullanan RSÜ-1 algoritması kullanılmıştır.

Tablo 4.3. ve Tablo 4.4.'te ise yeni NCS kaotik sisteminin RSÜ-1 algoritmasında, farklı sayıda bit seçimi yapılarak oluşturulan rasgele bit dizilerine ait NIST test sonuçları görülmektedir. Her bir örnekleme adımında üretilen kayan noktalı değerin, 32 bitlik ikilik sayı formatına çevrilmesinden sonra, düşük anlamlı kısımından

sırasıyla 5, 8, 10, 16, 20 ve 25 bit çekilerek her biri için 1 milyonluk rasgele bit dizileri oluşturulmuş ve NIST testleri gerçekleştirilmiştir. 5, 8, 10 ve 16 bit seçilerek oluşturulan 1milyonluk rasgele bit dizisinin x, y ve z fazlarının tüm NIST testlerinden geçtiği tespit edilmiştir. Farklı sayıda bit seçimi yapılarak 1 milyon bit dizisinin üretimi için, ihtiyaç duyulan kadar sayı üretilmiştir. 20 bit seçim yapılarak üretilen rasgele bit dizisi x fazı için toplamda 4 testten, y fazı için toplamda 3 testten geçemeyerek, uygun rasgeleliğe sahip olmadıkları tespit edilmiştir. 20 bit seçim yapılarak oluşturulan z fazına ait bit dizileri ise tüm testlerden geçmiştir. 25 bit seçildiğinde oluşturulan bit dizilerinin x, y ve z fazları için birden çok testten kaldığı görülmektedir. Bunun sonucu olarak, seçilen bit sayısı arttığında, üretilen rasgele bit dizilerinin testlerden geçme oranı düştüğü görülmüştür. 32 bitin tamamının seçildiği bit dizisinin ise sadece 1-2 testten geçtiği tespit edilmiş bu sebeple bu sonuçlar tabloya dahil edilmemiştir. Geliştirilen şifreleme uygulamasında kullanılacak olan RSÜ-1 tasarımında, rassallığın yüksek olması şifreleme kalitesini etkilediğinden dolayı her üç fazın testlerin tümünü geçtiği ve güvenlik analizleri sonuçlarına göre en iyi sonuçlara sahip 2 bitlik seçim kullanılmıştır.

Tablo 4.3. Yeni NCS kaotik sistemi ile RSÜ-1 NIST-800-22 Test Sonuçları (x-y-z fazları farklı sayıda bit seçimi)

NIST Testleri	**(5 bit) p-değeri**			**(8 bit) p-değeri**			**(10 bit) p-değeri**		
Faz çıktıları	**x**	**y**	**z**	**x**	**y**	**z**	**x**	**y**	**z**
Frekans testi	0,6198	0,3575	0,6227	0,0566	0,7994	0,3975	0,2909	0,8949	0,2819
Blok frekans testi	0,7397	0,4241	0,6952	0,9487	0,3825	0,4049	0,4096	0,7053	0,3803
Birikimli toplamlar testi	0,4767	0,5578	0,7402	0,0863	0,9373	0,6029	0,3042	0,5613	0,4251
Akış testi	0,3068	0,6683	0,2034	0,3342	0,8822	0,3666	0,8392	0,9744	0,6192
Bir blok içerisinde en uzun birler akış testi	0,4269	0,262	0,4971	0,6677	0,2945	0,9406	0,9761	0,7514	0,7228
İkili matris derece testi	0,2941	0,4119	0,792	0,2153	0,662	0,3274	0,157	0,4929	0,2527
Ayrık fourier dönüşüm testi	0,7342	0,8832	0,7901	0,3733	0,3352	0,072	0,7204	0,2257	0,762
Örtüşen Şablon Eşleştirme Testi	0,3017	0,9936	0,9515	0,9742	0,074	0,3889	0,2596	0,9252	0,5903
Maurer'in "Evrensel İstatistik" Testi	0,6872	0,049	0,8451	0,1743	0,904	0,9028	0,8163	0,3173	0,441
Yaklaşık Entropi Testi	0,7646	0,9917	0,937	0,7889	0,1828	0,3212	0,9636	0,5194	0,3974
Rasgele Gezinimler Testi	0,6918	0,2652	0,7776	0,2875	0,3232	0,9568	0,6903	0,2089	0,4226
Rasgele Gezinimler Değişken Testi	0,8525	0,7639	0,9544	0,8115	0,5763	0,1864	0,3799	0,3023	0,8236
Seri testi-1	0,3308	0,8314	0,7882	0,3893	0,3137	0,1864	0,7667	0,8039	0,09
Seri testi-2	0,2436	0,2541	0,3263	0,1151	0,6805	0,445	0,2805	0,8602	0,1594
Doğrusal Karmaşıklık Testi	0,9867	0,516	0,7014	0,802	0,9689	0,8041	0,1231	0,7269	0,1962

Tablo 4.4. Yeni NCS kaotik sistemi ile RSÜ-1 NIST-800-22 Test Sonuçları (x-y-z fazları farklı sayıda bit seçimi)

NIST Testleri	(16 bit) p-değeri			(20 bit) p-değeri			(25 bit) p-değeri		
Faz çıktıları	x	y	z	x	y	z	x	y	z
Frekans testi	0,617	0,4448	0,6599	Başarısız	0,1855	0,0499	0,2946	Başarısız	Başarısız
Blok frekans testi	0,096	0,2106	0,1947	0,0671	Başarısız	0,1705	Başarısız	Başarısız	Başarısız
Birikimli toplamlar testi	0,3469	0,4744	0,986	Başarısız	0,3494	0,0938	0,2641	Başarısız	Başarısız
Akış testi	0,9651	0,7327	0,6015	0,8076	0,7746	0,676	Başarısız	Başarısız	Başarısız
Bir blok içerisinde en uzun birler akış testi	0,4672	0,4426	0,613	0,0945	0,7712	0,1416	0,6846	0,1515	0,063
İkili matris derece testi	0,2518	0,6951	0,6051	0,7124	0,877	0,662	0,6542	0,7647	0,4039
Ayrık fourier dönüşüm testi	0,2513	0,769	0,497	0,147	0,755	0,3261	Başarısız	Başarısız	Başarısız
Örtüşen Şablon Eşleştirme Testi	0,0466	0,2623	0,1808	0,9478	0,8346	0,7259	0,0786	0,0931	0,1122
Maurer'in "Evrensel İstatistik" Testi	0,6102	0,523	0,9977	0,4418	0,8306	0,2285	0,7624	Başarısız	0,1861
Yaklaşık Entropi Testi	0,5889	0,3572	0,7742	0,1432	0,9461	0,0638	0,2797	Başarısız	Başarısız
Rasgele Gezinimler Testi	0,2909	0,2235	0,2705	Başarısız	Başarısız	0,6266	Başarısız	Başarısız	Başarısız
Rasgele Gezinimler Değişken Testi	0,4669	0,3371	0,7062	Başarısız	Başarısız	0,6532	Başarısız	Başarısız	Başarısız
Seri testi-1	0,5997	0,2365	0,6641	0,1925	0,7675	0,0239	0,0613	0,2527	0,0889
Seri testi-2	0,8235	0,0812	0,8938	0,0992	0,1329	0,0132	0,0184	0,4233	0,2305
Doğrusal Karmaşıklık Testi	0,6264	0,5657	0,8003	0,8259	0,4534	0,0169	0,1589	0,4482	0,3051

4.1.4. RSÜ-2 algoritması NIST test sonuçları

RSÜ-2 tasarımında, kaotik sistemlerin RK4 algoritması ile çözülerek üretilen kayan noktalı sayıların ondalık kısımlarının mod işlemi ile oluşturulan 1 milyonluk bit dizilerinin XOR'lanması sonucu elde edilen yeni bit dizilerine NIST testleri uygulanmıştır. RSÜ-2 tasarımında üretilen x, y ve z fazlarının tek başına testleri geçmediği tespit edildiği için, fazlar kendi aralarında ikili olarak XOR'lanmış ve 3 adet 1 milyonluk bit dizileri oluşturulmuştur. Tablo 4.5.' te yeni geliştirilen skala edilmiş Zhongtang kaotik sistemi kullanılarak elde edilen rasgele bit dizilerinin NIST test sonuçları görülmektedir. Tablo 4.6.'da ise kaotik sistem analizleri sırasında tanıtımı yapılan ve literatürde şifreleme uygulamalarında yaygın olarak kullanılan Lorenz sisteminin RSÜ-2 algoritma tasarımında kullanılması ile elde edilen rasgele bit dizilerine uygulanan NIST test sonuçları görülmektedir. Tablo 4.6. incelendiğinde; x, y ve x, z fazlarının XOR'lanması ile üretilen 1milyonluk rasgele bit dizilerinin tüm NIST testlerini geçtiği ve şifreleme uygulamalarında kullanılabileceği görülmektedir. Fakat y ve z fazlarının üretmiş olduğu 1 milyonluk bit dizilerinin XOR'lanması ile oluşturulan yeni bit dizisinin frekans ve kümülatif toplam testlerini geçemediği tespit edilmiştir. Bu sebeple kullanımının uygun olmadığı görülmüştür.

Tablo 4.5. Yeni skala edilmiş zhongtang kaotik sistemi ile RSÜ-2 NIST-800-22 Test Sonuçları

NIST Testleri	P-değeri (x⊕y)	P- değeri (x⊕z)	P- değeri (y⊕z)	Sonuç
Frekans testi	0,50413	0,42371	0,29648	Başarılı
Blok frekans testi	0,49478	0,20208	0,31282	Başarılı
Birikimli toplamlar testi	0,71298	0,67735	0,54243	Başarılı
Akış testi	0,52058	0,53567	0,22054	Başarılı
Bir blok içerisinde en uzun birler akış	0,84018	0,15041	0,65301	Başarılı
İkili matris derece testi	0,54134	0,39733	0,77284	Başarılı
Ayrık fourier dönüşüm testi	0,43538	0,14708	0,40367	Başarılı
Örtüşen Şablon Eşleştirme Testi	0,15198	0,71046	0,69889	Başarılı
Maurer'in "Evrensel İstatistik" Testi	0,94045	0,17520	0,41380	Başarılı
Yaklaşık Entropi Testi	0,26715	0,71578	0,42833	Başarılı
Rasgele Gezinimler Testi	0,94621	0,74149	0,69230	Başarılı
Rasgele Gezinimler Değişken Testi	0,86405	0,62237	0,70234	Başarılı
Seri testi-1	0,12035	0,79025	0,84638	Başarılı
Seri testi-2	0,23978	0,79948	0,75705	Başarılı
Doğrusal Karmaşıklık Testi	0,50480	0,15283	0,71334	Başarılı

Tablo 4.6. Lorenz kaotik sistemi ile RSÜ-2 NIST-800-22 Test Sonuçları

NIST Testleri	P-değeri (x⊕y)	P- değeri (x ⊕ z)	Sonuç
Frekans testi	0,21869	0,32609	Başarılı
Blok frekans testi	0,90193	0,43164	Başarılı
Birikimli toplamlar testi	0,42588	0,43768	Başarılı
Akış testi	0,03112	0,50219	Başarılı
Bir blok içerisinde en uzun birler akış testi	0,35611	0,64400	Başarılı
İkili matris derece testi	0,57553	0,69615	Başarılı
Ayrık fourier dönüşüm testi	0,77604	0,53262	Başarılı
Örtüşen Şablon Eşleştirme Testi	0,33166	0,76613	Başarılı
Maurer'in "Evrensel İstatistik" Testi	0,79152	0,58340	Başarılı
Yaklaşık Entropi Testi	0,32076	0,57044	Başarılı
Rasgele Gezinimler Testi	0,91318	0,42895	Başarılı
Rasgele Gezinimler Değişken Testi	0,64626	0,51371	Başarılı
Seri testi-1	0,69885	0,57022	Başarılı
Seri testi-2	0,86204	0,81279	Başarılı
Doğrusal Karmaşıklık Testi	0,87017	0,05775	Başarılı

4.2. Yeni Kaos Tabanlı S-Box Üretim Algoritması ve Performans Testleri

Kaotik sistemler, blok şifreleme algoritmalarının en önemli kısımlarından birisi olan S-Box üretiminde de kullanılabilmektedir. Bu bölümde, tasarlanan yeni kaotik sistemleri kullanan kaos tabanlı RSÜ'lerin kullanıldığı S-Box üretim algoritması

geliştirilmiş ve üretilen S-Box'ların performans analizleri yapılmıştır. Literatürdeki kaos tabanlı S-Box üretme algoritmaları analiz edildiğinde, satır ve sütünlar üzerinde karmaşık matris işlemleri içermektedir. AES algoritmasının S-Box üretimi ise matematiksel olarak karmaşık ve çok fazla işlem yüküne sahiptir. Karmaşık matris işlemleri ve matematiksel işlem yükü, işlem zamanını ve kaynak kullanımının artmasına sebep olmaktadır. Geliştirilen yeni S-Box üretim algoritması ile, literatürdeki kaos tabanlı S-Box yapılarından kriptolojik olarak daha güçlü, saldırılara dirençli ve işlem yükü az yeni bir algoritma üretilmiştir.

4.2.1. Yeni kaos tabanlı S-Box üretim algoritması tasarımı

S-Box üretim algoritmasına ait blok diyagram Şekil 4.2.'de görülmektedir. Algoritma tasarımında kullanılacak olan kaotik sistemin üretmiş olduğu rasgele sayıların şifreleme algoritmasında kullanılabilmesi için NIST testlerine tabi tutulmuş ve tüm testleri geçmiş olması gerekmektedir. NIST testlerinin tümünden geçmiş kaotik sistem tabanlı RSÜ'den şifreleme ihtiyaç duyulduğu kadar bit üretilerek şifrelemede kullanılabilir. RSÜ tasarımında bahsedildiği gibi, kaotik sisteme başlangıç koşulları ve sistem parametrelerinin girilmesinden sonra RSÜ x ve z fazlarından üretilen 8 bitlik diziler XOR'lanarak 8 bit değer üretilmektedir. Algoritma bu şekilde değer üretmeye başlamakta ve 256 tekil elemana sahip bir S-BOX elde edilmektedir. Yeni kaos tabanlı S-Box tasarım algoritması incelendiğinde, RSÜ'nün iki fazının XOR'lanmasından elde edilen çıktıları kullanan ve her hangi bir satır, sütun dönüşüm işlemine gerek duymayan, basit operasyonlar içeren işlem yükü oldukça az bir tasarım olduğu görülmektedir. Yeni kaos tabanlı S-BOX üretim algoritmasının adımları aşağıda verilmiştir:

Adım 1: RSÜ tasarımında kullanılan, NIST testlerini geçmiş kaotik sisteme parametre ve başlangıç koşullarının girilmesi.

Adım 2: RSÜ'den ihtiyaç duyulan kadar bitin üretilmesi. (8bit)

Adım 3: RSÜ'nün x ve z fazlarından üretilen 8 adet bitin üretilmesi ve bu değerlerin XOR'lanması.

x fazından üretilen ikilik sayı sistemindeki 8 bitlik değer : “10101101”
y fazından üretilen ikilik sayı sistemindeki 8 bitlik değer: “01100110”
Elde edilen XOR’lanmış değer : “11001011”

Adım 4: XOR’lanmış 8 bitlik değerin decimal (onluk taban) değere çevrimi.

XOR’lanmış değerin onluk tabandaki karşılığı: “203”

Adım 5: Üretilen decimal değerin S-BOX’ ta daha önce üretilen değerler arasında olup olmadığı kontrol edilerek, eğer değer daha önce üretilen yani S-BOX’ ta olan bir değer ise bu sayı kullanılmamakta, S-BOX’ ta yoksa yeni bir eleman olarak eklenmektedir.

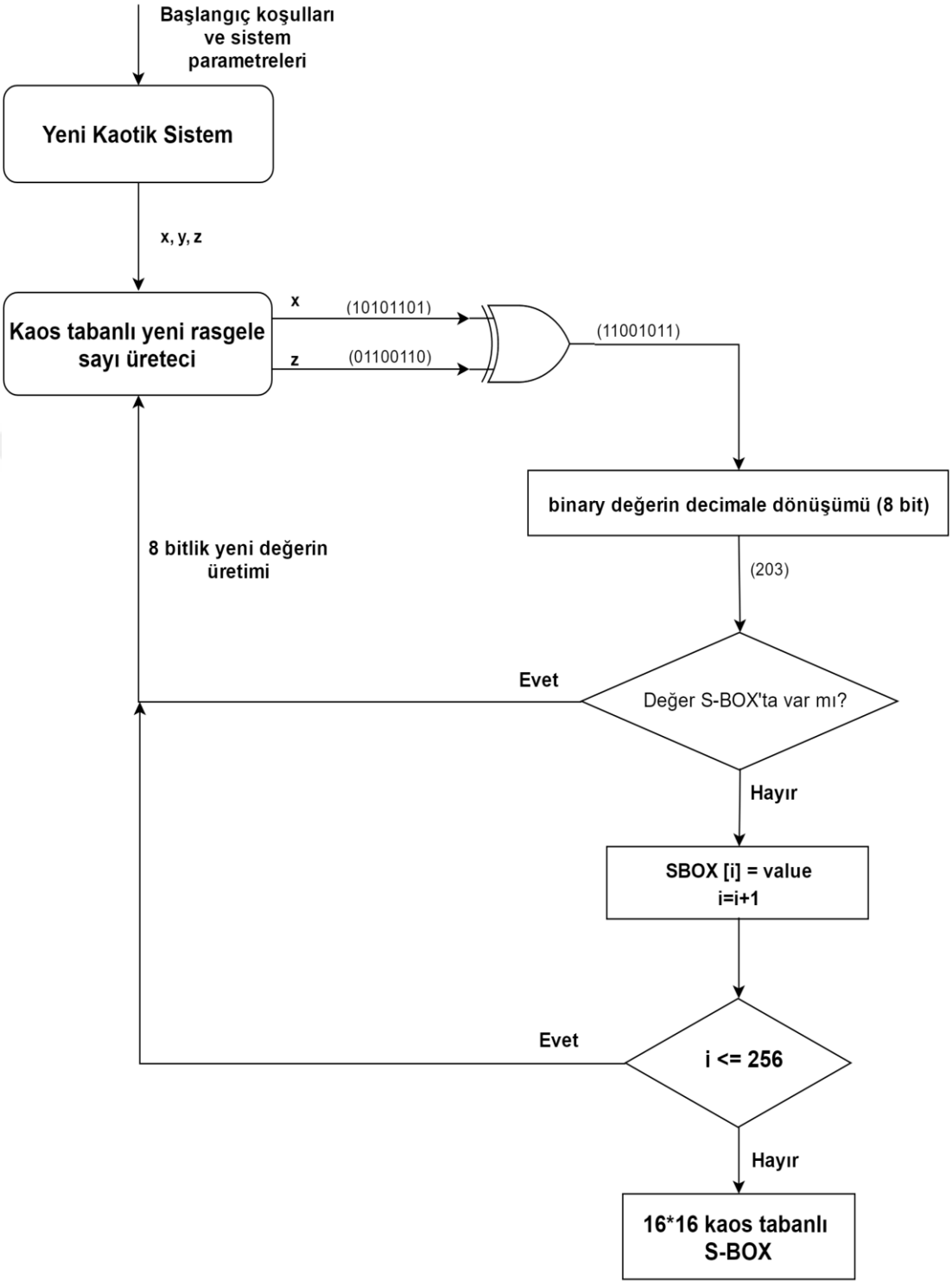
- 203 değeri daha önce üretilmedi ise S-Box’a eklenecek eğer daha önce üretildi ise bu değer kullanılmayacak.

Adım 6: Bu işlem tekil 256 adet değer S-BOX’a yerleştirilinceye kadar Adım 2’ye dönülerek devam etmektedir.

Adım 7: 0-255 arasındaki tüm değerler üretildiğinde S-BOX üretimi tamamlanır.
S-BOX üretimi tamamlandıktan sonra, S-BOX performans testleri gerçekleştirilmiştir. S-BOX eğer yeterli performans kriterlerini sağlıyor ise, şifreleme işleminde kullanılabilir, sağlamıyorsa yeni bir S-Box üretimi gerçekleştirilmektedir.

4.2.2. Önerilen S-Box’ lar ve performans testleri

Geliştirilen yeni kaos tabanlı S-Box üretim algoritması ile bu tez çalışmasında geliştirilen yeni kaotik sistemleri kullanan RSÜ-1 ve RSÜ-2 tasarımları ile 2 adet yeni S-Box önerilmiş ve bu S-Box’ların performans testleri yapılmıştır. Önerilen S-Box’ ların performans seviyesini tespit etmek için, literatürdeki kaos tabanlı uygulamalar ve diğer S-Box çalışmaları karşılaştırılmıştır. Önerilen S-Box’lar üzerinde 2. Bölümde açıklamaları yapılan, doğrusal olmama, katı çığ kriteri (SAC), çıkış bitleri bağımsızlık kriteri (BIC), giriş ve çıkış bitleri arasındaki yaklaşık fark (DP) analizleri yapılmıştır.



Şekil 4.2. Yeni kaos tabanlı S-box üretim algoritması blok diyagramı

4.2.2.1. Önerilen S-Box-1 ve performans testleri

Önerilen S-Box-1'in üretimi için, RSÜ-2 rasgele sayı üretim algoritması ve RSÜ-2 algoritmasında da kaotik sistem olarak yeni skala edilmiş Zhongtang kaotik sistemi kullanılmıştır. Yeni sakala edilmiş Zhongtang kaotik sisteminin sistem parametreleri: a = 80, b = 40, c = 5, d = 10, e = 2, f = 10, g = 15 başlangıç koşulları: x_0=1, y_0=0, z_0=1 olarak sistem kullanılmıştır. RSÜ-2 algoritmasında ise Δh örnekleme aralığı 0,001 olarak alınmıştır. Tablo 4.7.'de yeni geliştirilen kaos tabanlı S-Box üretim algoritması ile elde edilen S-Box görülmektedir.

Tablo 4.7. Önerilen S-Box-1

16	9	170	4	218	35	46	54	11	146	136	71	190	60	178	252
197	187	209	122	198	139	103	70	0	79	207	111	47	109	120	248
191	202	167	222	21	40	116	159	28	183	196	76	148	94	49	140
132	245	133	88	175	171	166	157	184	34	226	8	83	3	205	239
62	17	43	27	89	189	68	182	127	137	93	144	193	124	123	2
23	155	96	39	238	92	223	95	169	172	212	37	25	199	232	229
105	118	31	188	75	135	119	203	219	112	15	154	91	65	244	249
45	213	176	24	153	121	194	220	110	19	72	113	26	61	73	143
131	38	74	58	106	173	67	86	164	98	151	129	180	158	142	185
48	82	201	41	117	243	114	216	66	44	130	221	228	241	33	77
230	63	5	254	192	186	208	55	53	115	99	30	174	12	18	147
231	80	134	13	145	104	253	101	156	50	160	51	225	246	240	29
90	59	200	210	165	215	214	211	6	150	126	163	87	206	20	32
36	235	64	10	179	57	195	237	107	97	149	56	181	102	52	141
152	204	85	128	84	42	233	224	7	1	255	162	81	69	22	247
100	250	236	242	108	161	168	14	217	177	251	125	138	78	227	234

Çalışmada üretilen kaos tabanlı S-Box'a ait doğrusal olmama değerleri 106, 110, 104, 110, 104, 104, 106, 104 şeklindedir. S-Box-1'e ait doğrusal olmama ortalama değeri 106, minimum değer 104 ve maksimum değeri 110 olarak bulunmuştur. Üretim aşamasında en yüksek değer olan orijinal AES algoritmasının doğrusal olmama değerine yakın bir değer elde edilmesi hedeflenmiştir. Önerilen kaos tabanlı S-Box algoritmasının üretmiş olduğu S-Box' a ait ilişki matrisi Tablo 4.8.'de verilmiştir. Tablo 4.8.'de görüldüğü üzere minimum değer 0.40625 maksimum değer 0.64065, ortalama değer 0.50122 dir. Bu değerlere göre önerilen S-Box'un SAC kriterlerine göre oldukça ideal değerler taşıdığı görülmektedir.

Tablo 4.8. Önerilen S-Box-1'e ait ilişki matrisi

0	1	2	3	4	5	6	7
0.453125	0.515625	0.437500	0.531250	0.484375	0.531250	0.500000	0.531250
0.468750	0.515625	0.453125	0.500000	0.515625	0.500000	0.484375	0.453125
0.593750	0.453125	0.453125	0.515625	0.500000	0.609375	0.515625	0.484375
0.515625	0.546875	0.500000	0.515625	0.531250	0.484375	0.468750	0.468750
0.468750	0.468750	0.468750	0.484375	0.421875	0.468750	0.515625	0.562500
0.421875	0.453125	0.500000	0.500000	0.531250	0.484375	0.468750	0.515625
0.500000	0.484375	0.578125	0.546875	0.640625	0.484375	0.406250	0.484375
0.468750	0.531250	0.578125	0.546875	0.500000	0.515625	0.546875	0.500000

Tablo 4.9.'da BIC-Nonlinearity matrisi, Tablo 4.10.'da ise BIC-SAC ilişki matrisi, görülmektedir. Tablo 4.9. incelendiğinde min değerin 98, max değerin 108 ve ortalama değerin 103,5 olduğu görülmektedir. Tablo 4.10'da ise minimum değerin 0,46289 max değerin 0,53515 ortalama değerin ise ideal değer olan 0,5 e çok yakın 0,50035 olduğu görülmektedir.

Tablo 4.9. Önerilen S-Box-1'e BIC-Nonlinearity matrisi

0	1	2	3	4	5	6	7
—-	106	102	102	98	100	104	106
106	—-	104	106	104	100	100	104
102	104	—-	108	106	104	100	104
102	106	108	—-	102	104	106	102
98	104	106	102	—-	104	104	104
100	100	104	104	104	—-	102	106
104	100	100	106	104	102	—-	106
106	104	104	102	104	106	106	—-

Tablo 4.10. Önerilen S-Box-1'e ait BIC-SAC matrisi

0	1	2	3	4	5	6	7
—-	0.494141	0.496094	0.496094	0.498047	0.505859	0.498047	0.494141
0.494141	—-	0.503906	0.513672	0.515625	0.484375	0.515625	0.494141
0.496094	0.503906	—-	0.501953	0.478516	0.513672	0.486328	0.535156
0.496094	0.513672	0.501953	—-	0.488281	0.462891	0.519531	0.513672
0.498047	0.515625	0.478516	0.488281	—-	0.476562	0.498047	0.496094
0.505859	0.484375	0.513672	0.462891	0.476562	—-	0.529297	0.484375
0.498047	0.515625	0.486328	0.519531	0.498047	0.529297	—-	0.515625
0.494141	0.494141	0.535156	0.513672	0.496094	0.484375	0.515625	—-

Tablo 4.11.'de önerilen kaos tabanlı S-Box'a ait giriş çıkış XOR bitleri arasındaki fark matrisi görülmektedir. Tablodaki değerlere bakıldığında min değerin 6, max değerin

10 olduğu görülmektedir. DP değerinin olabildiğince küçük olması güçlü bir S-Box için gereklidir.

Tablo 4.11. Önerilen S-Box-1'e ait DP matrisi

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
-	6.0	6.0	6.0	6.0	6.0	6.0	8.0	6.0	8.0	6.0	6.0	8.0	6.0	6.0	8.0
6.0	6.0	6.0	8.0	6.0	6.0	8.0	8.0	6.0	8.0	10.0	8.0	6.0	6.0	6.0	6.0
6.0	8.0	6.0	4.0	6.0	6.0	6.0	8.0	8.0	8.0	6.0	8.0	6.0	6.0	6.0	10.0
8.0	8.0	6.0	6.0	4.0	6.0	6.0	8.0	6.0	8.0	6.0	8.0	6.0	6.0	6.0	8.0
6.0	6.0	6.0	6.0	6.0	8.0	8.0	6.0	6.0	6.0	6.0	8.0	8.0	8.0	6.0	8.0
8.0	6.0	6.0	6.0	6.0	6.0	6.0	6.0	6.0	8.0	6.0	6.0	8.0	6.0	8.0	8.0
8.0	6.0	8.0	8.0	8.0	6.0	8.0	6.0	6.0	6.0	6.0	6.0	6.0	8.0	8.0	8.0
6.0	6.0	6.0	6.0	6.0	6.0	8.0	6.0	8.0	6.0	6.0	6.0	6.0	6.0	6.0	6.0
8.0	6.0	8.0	6.0	6.0	6.0	6.0	6.0	8.0	6.0	8.0	8.0	6.0	6.0	6.0	6.0
6.0	6.0	10.0	6.0	6.0	6.0	6.0	8.0	8.0	6.0	10.0	6.0	6.0	6.0	6.0	6.0
6.0	6.0	6.0	6.0	6.0	6.0	8.0	8.0	6.0	6.0	10.0	8.0	6.0	8.0	8.0	6.0
6.0	4.0	6.0	6.0	8.0	6.0	6.0	8.0	6.0	6.0	8.0	8.0	6.0	6.0	10.0	6.0
8.0	8.0	6.0	8.0	8.0	8.0	8.0	8.0	6.0	6.0	8.0	8.0	6.0	4.0	8.0	8.0
6.0	10.0	6.0	8.0	6.0	10.0	8.0	6.0	6.0	6.0	6.0	8.0	6.0	6.0	8.0	8.0
6.0	6.0	8.0	8.0	10.0	8.0	6.0	6.0	6.0	8.0	8.0	8.0	8.0	6.0	6.0	6.0
6.0	6.0	6.0	6.0	8.0	6.0	6.0	8.0	6.0	6.0	6.0	8.0	8.0	6.0	8.0	8.0

Yeni kaos tabanlı S-Box tasarım algoritması incelendiğinde, RSÜ'nün iki fazının XOR'lanması ile elde edilen çıktıları kullanan ve her hangi bir satır, sütun dönüşüm işlemine gerek duymayan, işlem yükü oldukça az ve performans analiz sonuçlarına göre güvenli ve saldırılara dayanıklı bir S-Box olduğu görülmektedir. Önerilen S-Box-1 geliştirilecek olan kaos tabanlı hibrit CS-AES şifreleme algoritmasında kullanılmıştır.

4.2.2.2. Önerilen S-Box-2 ve performans testleri

Önerilen S-Box-2'nin üretimi için, RSÜ-1 rasgele sayı üretim algoritması ve RSÜ-1 algoritmasında da kaotik sistem olarak yeni NCS kaotik sistemi kullanılmıştır. Yeni NCS kaotik sisteminin sistem parametreleri a=1, b=1, c=2, d= -3 başlangıç koşulları: x_0 =1, y_0 = -1, z_0 = 0, 01 olarak kullanılmıştır. RSÜ-1 algoritmasında ise Δh örnekleme aralığı 0,05 olarak alınmıştır. Tablo 4.12.'de yeni geliştirilen kaos tabanlı S-Box üretim algoritması ile elde edilen S-Box görülmektedir.

Kaos tabanlı S-Box algoritmasının üretmiş olduğu önerilen S-Box-2' nin doğrusal olmama değerleri 108, 106, 104, 106, 108, 106, 106, 106 şeklindedir. Doğrusal

olmama ortalama değeri 106, minimum değeri 104 ve maksimum değeri 108 olarak belirlenmiştir. Tablo 4.13.'de önerilen kaos tabanlı S-Box'a ait ilişki matrisi verilmiştir. SAC minimum değer 0,3906 maksimum değer 0,5937 ve ortalama değer 0,5063 olarak bulunmuştur. Bu değerlerin ideal değerlere oldukça yakın olduğu görülmektedir.

Tablo 4.12. Önerilen S-Box-2

62	111	132	176	44	203	242	213	159	160	3	41	225	45	161	119
134	177	104	191	61	4	250	221	5	71	253	98	155	101	22	36
215	67	2	118	241	78	127	243	117	53	143	236	197	144	224	209
152	8	87	92	32	163	188	140	50	170	20	31	6	28	84	42
136	124	211	90	254	11	72	59	226	35	12	214	40	217	19	70
102	141	149	69	210	10	194	231	175	167	0	43	131	249	206	82
123	184	138	86	34	153	244	245	65	38	174	47	187	96	158	255
147	182	240	220	146	99	97	91	137	229	202	252	21	9	110	154
189	60	79	13	1	248	205	207	73	142	121	85	251	185	128	222
114	116	56	37	29	246	166	193	103	126	228	122	120	186	133	75
173	88	48	17	63	24	227	234	204	74	145	94	25	201	130	164
115	80	199	27	168	14	83	148	171	156	58	77	26	89	190	55
66	233	230	81	95	169	218	196	76	68	64	179	157	51	216	125
200	52	100	139	93	30	150	113	208	239	165	172	109	247	235	39
106	162	178	49	46	135	237	18	108	212	54	223	181	33	232	23
183	57	105	112	180	16	195	15	198	192	219	151	107	129	238	7

Tablo 4.13. Önerilen S-Box-2'ye ait ilişki matrisi

0.437500	0.562500	0.453125	0.546875	0.531250	0.562500	0.531250	0.531250
0.437500	0.500000	0.484375	0.468750	0.500000	0.468750	0.531250	0.484375
0.500000	0.515625	0.578125	0.390625	0.484375	0.500000	0.453125	0.500000
0.546875	0.546875	0.468750	0.484375	0.468750	0.546875	0.562500	0.468750
0.562500	0.531250	0.484375	0.578125	0.484375	0.437500	0.546875	0.484375
0.515625	0.437500	0.562500	0.515625	0.484375	0.515625	0.562500	0.515625
0.515625	0.515625	0.453125	0.562500	0.562500	0.515625	0.515625	0.531250
0.484375	0.421875	0.468750	0.484375	0.500000	0.484375	0.593750	0.531250

Tablo 4.14.'de BIC-Nonlinearity ve Tablo 4.15.'de ise BIC-SAC matrisi görülmektedir. Tablo 4.14. incelendiğinde minimum değerin 100, maksimum değerin 108 olduğu görülmekte ve ortalama değer ise 103.857 olarak hesaplanmıştır. Tablo 4.15.'deki BIC-SAC değerlerine bakıldığında, minimum değerin 0,4765, maksimum değerin 0,5312 ortalama değerin ise 0,4976 ile 0,5 olan ideal değere çok yakın olduğu tespit edilmiştir. Önerilen S-Box-2'nin DP değerleri Tablo 4.16.'da görülmektedir. Önerilen S-BOX-2'nin min DP değeri 6,0 ve max DP değeri 12 olarak tespit edilmiştir.

Tablo 4.14. Önerilen S-Box-2'ye ait BIC-Nonlinearity matrisi

—-	100	104	102	106	106	106	106
100	—-	108	106	104	102	106	102
104	108	—-	104	106	100	102	102
102	106	104	—-	106	104	100	108
106	104	106	106	—-	100	102	106
106	102	100	104	100	—-	104	102
106	106	102	100	102	104	—-	104
106	102	102	108	106	102	104	—-

Tablo 4.15. Önerilen S-Box-2'ye ait BIC-SAC matrisi

—-	0.482422	0.505859	0.476562	0.486328	0.525391	0.498047	0.498047
0.482422	—-	0.490234	0.494141	0.482422	0.503906	0.486328	0.480469
0.505859	0.490234	—-	0.507812	0.521484	0.496094	0.476562	0.498047
0.476562	0.494141	0.507812	—-	0.488281	0.500000	0.519531	0.490234
0.486328	0.482422	0.521484	0.488281	—-	0.484375	0.478516	0.531250
0.525391	0.503906	0.496094	0.500000	0.484375	—-	0.498047	0.505859
0.498047	0.486328	0.476562	0.519531	0.478516	0.498047	—-	0.527344
0.498047	0.480469	0.498047	0.490234	0.531250	0.505859	0.527344	—-

Tablo 4.16. Önerilen S-Box-2'ye ait DP matrisi

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
-	6.0	6.0	6.0	8.0	8.0	6.0	8.0	8.0	6.0	6.0	6.0	6.0	8.0	6.0	8.0
6.0	8.0	8.0	6.0	6.0	4.0	6.0	8.0	6.0	6.0	6.0	6.0	6.0	4.0	6.0	6.0
6.0	8.0	8.0	6.0	8.0	6.0	8.0	6.0	8.0	8.0	6.0	6.0	8.0	6.0	6.0	8.0
8.0	6.0	6.0	8.0	8.0	8.0	6.0	6.0	8.0	6.0	6.0	8.0	6.0	6.0	8.0	8.0
6.0	8.0	6.0	6.0	6.0	12.0	6.0	6.0	6.0	6.0	6.0	6.0	6.0	6.0	6.0	8.0
8.0	6.0	6.0	6.0	8.0	6.0	6.0	6.0	6.0	6.0	6.0	6.0	6.0	6.0	6.0	8.0
6.0	8.0	6.0	10.0	8.0	6.0	6.0	6.0	8.0	6.0	6.0	6.0	8.0	8.0	6.0	8.0
6.0	8.0	6.0	6.0	6.0	6.0	6.0	10.0	8.0	6.0	6.0	8.0	6.0	6.0	6.0	6.0
6.0	6.0	6.0	6.0	6.0	6.0	6.0	6.0	8.0	6.0	6.0	6.0	8.0	8.0	8.0	8.0
6.0	6.0	6.0	8.0	8.0	6.0	8.0	8.0	6.0	6.0	6.0	6.0	10.0	10.0	6.0	6.0
6.0	8.0	8.0	6.0	6.0	6.0	8.0	8.0	8.0	6.0	8.0	10.0	8.0	6.0	10.0	6.0
6.0	6.0	6.0	8.0	6.0	6.0	8.0	8.0	6.0	6.0	6.0	6.0	10.0	6.0	6.0	8.0
8.0	8.0	6.0	6.0	6.0	8.0	6.0	8.0	8.0	6.0	8.0	8.0	8.0	8.0	8.0	10.0
6.0	6.0	6.0	8.0	6.0	6.0	8.0	6.0	6.0	6.0	6.0	8.0	8.0	6.0	8.0	6.0
6.0	6.0	8.0	6.0	6.0	6.0	8.0	8.0	6.0	8.0	6.0	6.0	6.0	8.0	6.0	8.0
10.0	8.0	6.0	8.0	8.0	8.0	6.0	10.0	6.0	6.0	8.0	6.0	6.0	6.0	6.0	8.0

4.2.3. Önerilen yeni S-Box'ların performans karşılaştırması

Tez çalışmasında önerilen kaos tabanlı S-Box'lar ile literatürdeki Jakimoski [142], Tang [51], Wang [67], Chen [61], Khan [62], Ozkaynak [57], Hussain [63] tarafından

önerilen kaos tabanlı S-Box'ların ve AES algoritmasında kullanılan S-Box'un performans karşılaştırılması yapılmıştır. Tablo 4.17.'de S-Box'ların performans testi sonuçları görülmektedir.

Tablo 4.17. S-Box performans karşılaştırma tablosu

S-Box	Nonlinearity			BIC-SAC	BIC-Nonlinearity	SAC			DP
	Min	Avg	Max			Min	Avg	Max	
Önerilen S-Box-1	104	106	110	0.5003	103.5	0.4065	0.5012	0.6406	10
Önerilen S-Box-2	104	106	108	0.4976	103.8	0.3906	0.5063	0.5937	12
Jakimoski [142]	98	103.2	108	0.5031	104.2	0.3761	0.5058	0.5975	12
Tang [51]	99	103.4	106	0.4995	103.3	0.4140	0.4987	0.6015	10
Wang[67]	102	104	106	0.5070	103.8	0.4850	0.5072	0.5150	12
Chen[61]	100	103	106	0.5024	103.1	0.4218	0.5000	0.6093	14
Khan[62]	96	103	106	0.5010	100.3	0.3906	0.5039	0.6250	12
Ozkaynak[57]-1	100	104.2	109	0.4988	103.3	0.3906	0.4931	0.5703	12
Ozkaynak[57]-2	100	103.2	106	0.5009	103.7	0.4218	0.5048	0.5938	10
Hussain[63]	102	105.2	108	0.5053	104.2	0.4080	0.5050	0.5894	12
Skipjack S-Box	104	105.7	108	0.4994	104.1	0.3986	0.5032	0.5938	12
AES S-Box	112	112	112	0.5046	112	0.4531	0.5048	0.5625	4

Tablo 4.17.'de görüldüğü üzere, literatürdeki diğer kaos tabanlı S-Box algoritmaları ile karşılaştırıldığında, önerilen kaos tabanlı S-Box'un en yüksek ortalama, minimum ve maksimum doğrusal olmama değerine sahip olduğu görülmektedir. Fakat önerilen S-Box'un maksimum doğrusal olmama değerinin AES algoritmasına yakın olmasına rağmen, AES S-Box değerinden düşük olduğu tespit edilmiştir.

Tablo 4.17.'de BIC-SAC ve BIC-Nonlinearity değerlerinin literatürdeki diğer çalışmalar ile karşılaştırılması görülmektedir. BIC-SAC testinde, sonucun ideal değer olan 0,5 olması istenmektedir. Test sonuçlarına göre, önerilen S-Box'ların BIC-SAC değerleri 0,5 değerine çok yakın bir değere sahiptir. Önerilen S-Box'ların BIC-Nonlinearity değerleri 103,5 ve 103,8 olarak tespit edilmiştir. Bu değerler diğer kaos tabanlı çalışmaların değerleri ile karşılaştırıldığında genel olarak iyi bazı çalışmaların

üstünde, bazılarına ise çok yakın olduğu görülmektedir. SAC testinde önerilen S-Box'ların ortalama değerleri 0,5012 ve 0,5063 olarak bulunmuştur. Bulunan değerlerin AES algoritması ile birlikte, literatürdeki kaos tabanlı diğer çalışmalara çok yakın olduğu tespit edilmiştir. Tablo 4.17.'deki DP değerlerine bakıldığında ise, AES algoritmasına ait DP değerinin en iyi olduğu, kaotik tabanlı S-BOX yapıları içinde önerilen S-Box'ların DP değerinin Tang ve Ozkaynak' ın önerdiği sistemler ile aynı ve diğer karşılaştırılan sistemlerden daha iyi olduğu görülmektedir. Bundan dolayı geliştirilen yeni S-Box'un diferansiyel ataklara karşı dirençli bir yapıda olduğu söylenebilir.

S-Box performans test sonuçlarına göre, önerilen kaos tabanlı S-Box'ların diğer kaos tabanlı çalışmalardan, en önemli performans kriterlerinden biri olan doğrusal olmama ve DP değerleri ile öne çıktığı söylenebilir. Geliştirilen algoritmanın üretmiş olduğu S-Box' ların değerleri AES algoritması ile karşılaştırıldığında, AES algoritmasının doğrusal olmama kriterinde kaos tabanlı tüm algoritmalardan yüksek değere sahip olduğu görülmektedir. Kaos tabanlı S-Box çalışmaları, AES algoritmasının üretmiş olduğu doğrusal olmama ve DP değerlerine yaklaşmaya çalışmaktadır. Karşılaştırma tablosundaki kaos tabanlı S-Box üretim algoritmaların performans değerleri incelendiğinde, AES algoritmasının doğrusal olmama ve DP değerlerine en yakın değerlere, önerilen S-Box'ların sahip olduğu görülmektedir. SAC ve BIC-SAC değerleri incelendiğinde, önerilen S-Box'ların değerlerinin AES ve kaos tabanlı diğer S-Box'lardan daha iyi veya çok yakın olduğu tespit edilmiştir. Kaotik sistemler ile üretilen S-Box yapılarının AES algoritmasının üretim algoritmasına göre çok az işlem yükü içermesi ve güvenlik seviyesinde ise, AES S-Box' un altında fakat yakın değerler elde etmesi sebebiyle, kaos tabanlı S-Box üretim algoritmaları üzerine çalışmalar yapılmaktadır.

4.3. Yeni Kaos Tabanlı Simetrik Ve Asimetrik Hibrit Şifreleme Algoritmaları

Bu bölümde kaos tabanlı simetrik ve asimetrik hibrit şifreleme algoritmaları tasarımı gerçekleştirilmiştir. Hibrit kaos tabanlı asimetrik şifreleme algoritmasının geliştirilmesinde RSA, simetrik şifreleme algoritması tasarımında ise S-AES

algoritması kullanılmıştır. Tasarımlarda tez çalışmasında geliştirilen yeni kaotik sistemleri temel alan RSÜ algoritmaları kullanılmıştır. Kaotik sistemlerin zengin dinamik yapıları ile modern şifreleme algoritmalarının güçlü yönlerini birlikte kullanan algoritmalar geliştirilmiştir. Modern şifreleme algoritmalarında kullanılan işlemler üzerinde değişime gidilerek, daha az işlem yükü ile daha yüksek güvenliğe sahip şifreleme algoritmaları geliştirilmesi hedeflenmiştir. Sadece kaos tabanlı sistemlerin kullanıldığı şifreleme algoritmalarının zayıf ve kırılabilir olduğu, yapılan literatür taraması sonucu gösterilmiştir. Bu sebeple kaotik sistemlerin kullanıldığı hibrit tasarımlar gerçekleştirilmiştir. Literatürde geliştirilen hibrit yapılar incelendiğinde, kaotik sistemlerin bu tasarımların belli yerlerinde sınırlı olarak kullanıldığı tespit edilmiştir. Örnek olarak, kaos tabanlı RSÜ'ler algoritmalara anahtar üretmek için yaygın olarak kullanılmıştır. Literatürdeki çalışmalardan farklı olarak, geliştirilen hibrit şifreleme algoritmalarında kaos tabanlı RSÜ'ler tarafından üretilen NIST testlerini geçmiş rasgele sayı dizileri algoritmanın bir çok farklı tasarım aşamasında kullanılmıştır.

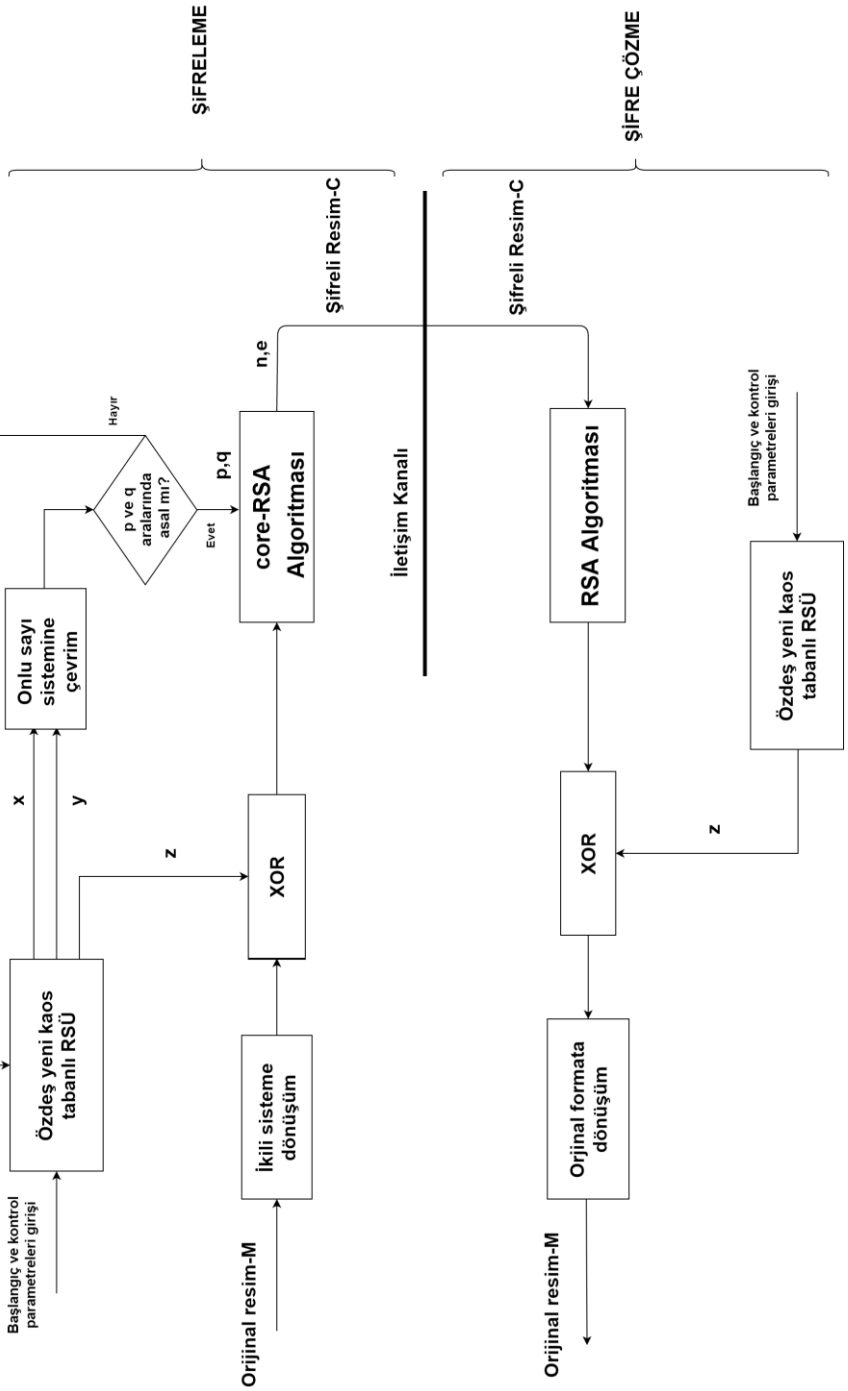
4.3.1. Yeni CRSA kaos tabanlı hibrit şifreleme algoritması tasarımı

Bu bölümde, güçlü matematiksel alt yapıya sahip RSA algoritması ile RSÜ-1 rasgele sayı üreteci algoritmasının birlikte kullanıldığı hibrit bir şifreleme algoritması geliştirilmiştir. RSÜ-1 rasgele sayı üretecinde NCS kaotik sistemi kullanılmıştır. NCS kaotik sisteminin kullanıldığı RSÜ-1 algoritmasının tüm NIST testlerinden başarılı bir şekilde geçtiği ve şifreleme uygulamalarında kullanılmak üzere yeterli rassallıkta sayılar ürettiği daha önce Tablo 4.1.'deki sonuçlara göre tespit edilmiştir. CRSA algoritması tasarımına ait blok diyagram Şekil 4.3.'de görülmektedir.

Kaos tabanlı RSÜ'nin sayısal değer üretmesi için kaotik sisteme ait başlangıç koşulları ve kontrol parametreleri sisteme girdi olarak verilmektedir. Kaos tabanlı RSÜ'den x, y ve z olmak üzere üç fazda rasgele sayılar üretilmektedir. Elde edilen bu rasgele sayılardan x ve y fazından elde edilen ikilik sayı sistemindeki değerler, RSA algoritmasının başlangıcında p ve q değerlerinin üretilmesinde kullanılmaktadır. İstenilen uzunlukta p ve q değerleri, RSÜ tarafından üretilmektedir. p ve q değerlerinin büyük olması algoritmanın zorluk derecesini artırmaktadır. Bu tasarımda p ve q

değerleri istenildiği kadar büyük seçilebilmekte ve algoritmanın şifreleme gücü artırılabilmektedir. x ve y fazından alınan bit dizileri onlu sayı sistemine dönüştürülerek, aralarında asallık kontrolü yapılmaktadır. Aralarında asal olmamaları durumunda, RSÜ üzerinden tekrar aynı sayıda bit alınarak, dönüşüm gerçekleştirilip aralarında asallık kontrolü yapılmakta, aralarında asal sayı üretimi gerçekleşinceye kadar bu işlem devam etmektedir. p ve q değerleri üretiminin ardından, şifrelenecek olan veri ikilik sisteme dönüştürülerek, verinin boyutu kadar bit kaos tabanlı RSÜ'nün z fazından elde edilmekte ve üretilen anahtar ile veri bit bazında XOR işlemine tabi tutulmaktadır. XOR işlemine tabi tutulan veri bir ön şifreleme işleminden geçirilmektedir. XOR işleminden geçirilmiş olan veri core-RSA algoritması ile şifrelenmekte ve şifreli veri elde edilmektedir. core-RSA algoritmasına p ve q değerleri RSÜ tarafından üretilen değerlerden verilmekte, diğer işlemler RSA algoritmasında olduğu gibi gerçekleştirilmektedir. Gönderici taraf RSA algoritmasının üretmiş olduğu n ve e değerleri ile şifreleme işlemini yapmakta ve veriyi alıcı tarafına ulaştırmaktadır. Alıcı taraf ise kendisine ulaştırılan n ve e değerlerini kullanarak, d değerini hesaplamakta, daha sonra n ve d değerini kullanarak şifreli veriyi çözmektedir. Çözülmüş olan şifreli verinin orijinal veriye dönüşümü için, gönderici tarafta kullanılan özdeş RSÜ kullanılarak aynı anahtar ile XOR'lanıp, RSA algoritmasından elde edilen veriye uygulanarak orijinal veri elde edilmektedir. Bu tasarımda kaos tabanlı RSÜ kullanılarak RSA algoritması güçlendirilmiştir. Veri üzerinde, üretilen rasgele bitler ile XOR işlemi yapılmış ve RSA algoritmasının kullandığı p ve q değerlerinin kaos tabanlı RSÜ kullanılarak istenilen büyüklükte ve daha rassal olarak üretimi sağlanmıştır.

CRSA şifreleme algoritmasının uygulaması Matlab ortamında gerçekleştirilmiştir. CRSA algoritmasının başlangıcında, Şekil 4.4.'de görüldüğü gibi algoritmanın çalışması için gerekli değerler hesaplanmıştır. Şifreleme algoritmasında kullanılan p ve q kendi aralarında asal olan değerleri kaos tabanlı RSÜ kullanılarak hesaplanmıştır. p ve q değerlerinin hesaplanmasının ardından n mod değeri, $\varphi(n)$, e ve d değerleri hesaplanmıştır. Bu değerlerden n ve e genel anahtar olarak şifrelemede, d ve e çözme işleminde kullanılmaktadır.



Şekil 4.3. CRSA algoritması blok diyagramı

```
RSA algoritması için değerlerin üretilmesi:

     p=9749 - ilk asal deger (özel)
     q=1439 - ikinci asal deger (özel)
     n=14028811 - modül (genel)
     phi(n)=14017624 - Euler fonksiyonunun degeri (özel)
     e=3903 - kriptolama için genel anahtar (genel)
     d=7183 - gizli kripto cozme anahtari (özel)
```

Şekil 4.4. CRSA algoritmasında değerlerin üretilmesi

4.3.2. Yeni CS-AES kaos tabanlı hibrit şifreleme algoritması tasarımı

Yeni CS-AES kaos tabanlı hibrit blok şifreleme algoritması, önceki bölümlerde açıklanan yeni skala edilmiş Zhongtang kaotik sistemini kullanan RSÜ-2 rasgele sayı üreteci, kaos tabanlı S-Box üretim algoritması ve S-AES şifreleme algoritması kullanılarak geliştirilmiştir. Geliştirilen yeni şifreleme algoritması blok şifreleme gerçekleştiren simetrik tabanlı bir algoritmadır. CS-AES algoritmasında, kaos tabanlı sistemler algoritmada farklı işlemler için kullanılmıştır.

Algoritma tasrımında RSÜ-2'nin üretmiş olduğu rasgele değerler kullanılarak aşağıdaki işlemler gerçekleştirilmiştir.

- Şifreleme algoritmasında kullanılacak olan S-Box, yeni kaos tabanlı S-Box üretim algoritması kullanılarak üretilmiştir.
- Şifrelemede S-AES algoritmasındaki döngülere geçilmeden önce, RSÜ tarafından üretilen rasgele bir dizileri ile bir ön şifreleme işlemi gerçekleştirilmiştir.
- Algoritmada kullanılacak döngü anahtarları kaos tabanlı RSÜ kullanılarak üretilmiştir.

Yeni kaos tabanlı CS-AES şifreleme algoritması tasarımında kullanılan RSÜ-2 rasgele sayı üretecinde, zengin dinamik özelliklere sahip yeni skala edilmiş Zhongtang kaotik sistemi kullanılmıştır. Şifrelemede kullanılacak olacak RSÜ-2'nin üretmiş olduğu bit

dizileri tüm NIST testlerinden geçmektedir. Şekil 4.5.'te şifreleme, Şekil 4.6.'da ise şifre çözme algoritmasına ait blok diyagram görülmektedir. CS-AES şifreleme algoritmasında ilk olarak yeni skala edilmiş Zhongtang kaotik sistemine başlangıç koşulları ve sistem parametreleri girilerek, RSÜ-2'nin rasgele sayı dizileri üretimi gerçekleştirilmektedir. Kaotik sisteme ait başlangıç koşulları ve sistem parametreleri şifreleme algoritmasının anahtarı olarak kullanılmaktadır. Kaotik sistemler başlangıç koşullarına ve sistem parametrelerine hassas bağımlı olduklarından dolayı yapılacak en ufak bir değişiklik tüm şifreleme ve çözme işlemi sonuçlarını tamamen değiştirecektir. Kaotik sistemin başlangıç koşulları ve sistem parametreleri alıcı tarafa güvenlik seviyesi yüksek RSA algoritması ile iletilmektedir. Şifreleme sistemi tamamen bilinse bile, sistem parametrelerini ve başlangıç koşulları bilinmeden sistemin çözülmesi mümkün olmayacaktır. Şifreleme ve çözme işlemleri sırasında, blok diagramlarda gösterilen adımlar sırası ile gerçekleştirilmektedir. Şifre çözme işlemi sırasında, şifrelemenin tersi işlemler uygulanmaktadır. Blok diyagramlarda görülen Nr döngü sayısı S-AES algoritması için 2 dir. CS-AES şifreleme algoritmasında yer alan modüller aşağıda detaylı olarak açıklanmıştır. Aşağıda anlatılan modüllerin dışındaki blok diyagramda görülen işlemler orijinal S-AES algoritmasında olduğu gibi gerçekleştirilmektedir.

Yeni kaos tabanlı RSÜ: RSÜ-2 rasgele sayı üretecinin üretmiş olduğu, NIST testlerini geçmiş rasgele sayılar şifreleme işleminde kullanılmıştır. RSÜ-2'de kullanılan yeni skala edilmiş Zhongtang kaotik sistemine sistem parametreleri ve başlangıç koşullarının girilmesinin ardından, RSÜ'nün fazları tasarımda anlatıldığı gibi ikili olarak XOR işlemine tutulmuştur. RSÜ'nün x ve z fazlarından elde edilen rasgele bit dizileri yeni kaos tabanlı S-Box üretim algoritmasında, y ve z fazından elde edilen bit dizileri ön şifreleme işleminde, x ve y fazlarından elde edilen bit dizileri ise döngü anahtarı üretiminde kullanılmıştır. RSÜ, şifreleme algoritmasında gerçekleştirdiği işlem için ihtiyaç duyulan uzunlukta rasgele sayı dizisi üretmektedir. RSÜ aynı değerleri çözme işleminde kullanılmak üzere üretmektedir.

Ön şifreleme işlemi: CS-AES şifreleme algortiması ön şifreleme işleminde, şifreleme işlemine tabi tutulacak blok uzunluğu kadar, RSÜ'nün y ve z fazlarından rasgele bit

dizisi üretilerek XOR işlemine tabi tutulmaktadır. CS-AES şifreleme algoritması 128 bitlik veri üzerinde bit bazında XOR işlemi gerçekleştirmektedir. Şifre çözme işleminde ise aynı 128 bitlik blok anahtarı ile şifreli veri XOR'lanarak orijinal veri elde edilmektedir. Ön şifreleme işleminde her bir 128 bitlik blok için RSÜ tarafından yeni üretilen 128 bit rasgele bit dizisi kullanılmaktadır.

Döngü anahtarlarının üretimi: CS-AES şifreleme algoritmasında döngülerde kullanılacak olan anahtarların üretimi RSÜ üretecinden elde edilen rasgele sayılar kullanılarak üretilmektedir. AES algoritmasında döngü anahtarlarının elde edilmesi anahtar genişletme adı verilen bir operasyon sonucu elde edilmektedir. Bu işlem sırasında, AES algoritması şifreleme anahtarı, üretilen S-BOX ve rCon matrisi kullanılmaktadır. İşlem sonucunda tek bir anahtar kullanılarak döngü sayısınca her döngüde kullanılmak üzere anahtarlar elde edilmektedir. Anahtar genişletme operasyonu 2. Bölümde detaylı bir şekilde anlatılmıştır. Şifreleme algoritmasında üretilen döngü anahtarları anahtar ekleme adımında kullanılmaktadır. CS-AES şifreleme algoritmasında ise döngü anahtarları RSÜ-2'nin üretmiş olduğu x ve y fazlarının üretmiş olduğu rasgele sayıların XOR'lanması ile elde edilmektedir. AES algoritması için toplamda (11x128 bit) [44,4]'lük matris, S-AES algoritması için ise (3x128 bit) [12,4]'lük matris döngü anahtarları gerekmektedir. CS-AES algoritması için (3x128 bit) [12,4]'lük matris döngü anahtarları sistem tarafından oluşturulmaktadır. Alıcı tarafta şifre çözme işlemi için, aynı anahtar takımının oluşturulması, özdeş RSÜ tarafından sağlanmaktadır.

AES ve S-AES algoritmasının anahtar üretimi mekanizmalarında satır kaydırma ve S-Box' un kullanıldığı bayt değişim işlemi ve matris işlemleri bulunmaktadır. Bu işlem zaman ve kaynak kullanımını artıran bir işlemdir. CS-AES algoritmasının anahtar üretiminde ise bu işlemin yerine kaos tabanlı RSÜ'nün kullanıldığı basit operasyonlar ile güçlü rassallığa sahip döngü anahtarları oluşturulmaktadır. Bunun sonucu olarak algoritma hızlanmakta ve işlem yükünden kurtulmaktadır.

Yeni kaos tabanlı S-BOX üretim algoritması: CS-AES şifreleme algoritmasında bayt değişim işleminde kullanılan S-Box'un üretimi, yeni kaos tabanlı RSÜ'nün üretmiş

olduğu x ve z fazlarından elde edilen rasgele sayıları kullanan S-Box üretim algoritması tarafından gerçekleştirilmektedir. Bölüm 4.2'de S-Box tasarım algoritması detaylı olarak anlatılmış, şifreleme algoritmasında kullanılan S-Box'un detaylı performans analizleri gerçekleştirilmiştir. S-Box üretimi orijinal S-Box algoritmasının üretiminden farklı olarak kaos tabanlı sistemlerin güçlü rassallık özellikleri kullanılarak geliştirilmiştir. AES ve S-AES algoritmalarındaki S-Box üretimi 2. Bölümde açıklandığı gibi karmaşık matematiksel işlemler kullanılarak gerçekleştirilmektedir. Şifreleme işlemi için bir S-Box ve çözme işleminde ise şifrelemede kullanılan S-Box'un çarpma ve mod işlemlerine göre tersi olan ters S-Box kullanılmaktadır. Geliştirilen kaos tabanlı algoritmada ise, şifreleme ve çözme işlemlerinde aynı S-Box kullanılmıştır. Kaos tabanlı S-Box üretim algoritması daha basit işlemler ile saldırılara dayanıklı ve güçlü kriptolojik özelliklere sahip S-Box üretimini hedeflemektedir.

Satır karıştırma: Satır karıştırma işlemi AES ve S-AES algoritmasında bulunmayan ve satır bazında bir karıştırma için tasarıma yeni eklenen bir bölümdür. Bu adımda satır öteleme işleminin ardından, elde edilen [4x4] lük durum matrisi üzerinde satırlar üzerinde karıştırma işlemi gerçekleştirilmektedir. Karıştırma işlemi sırasında döngüde kullanılan, döngü anahtarının modu alınarak döngü anahtarına bağlı bir öteleme işlemi gerçekleştirilmektedir. Böylece satır kaydırma işleminde olduğu gibi sabit bir kaydırma değil, dinamik bir karıştırma işlemi yapılmaktadır. Çözme işleminde ise, çözme blok diyagramında görülen döngü içindeki sırada satır karıştırma işlemi gerçekleştirilmektedir. Satır karıştırma işlemine ait kod parçası aşağıdadır.

```
shft = mod(round_key(i),3);
state = mix_rows(state, shft+1);
```

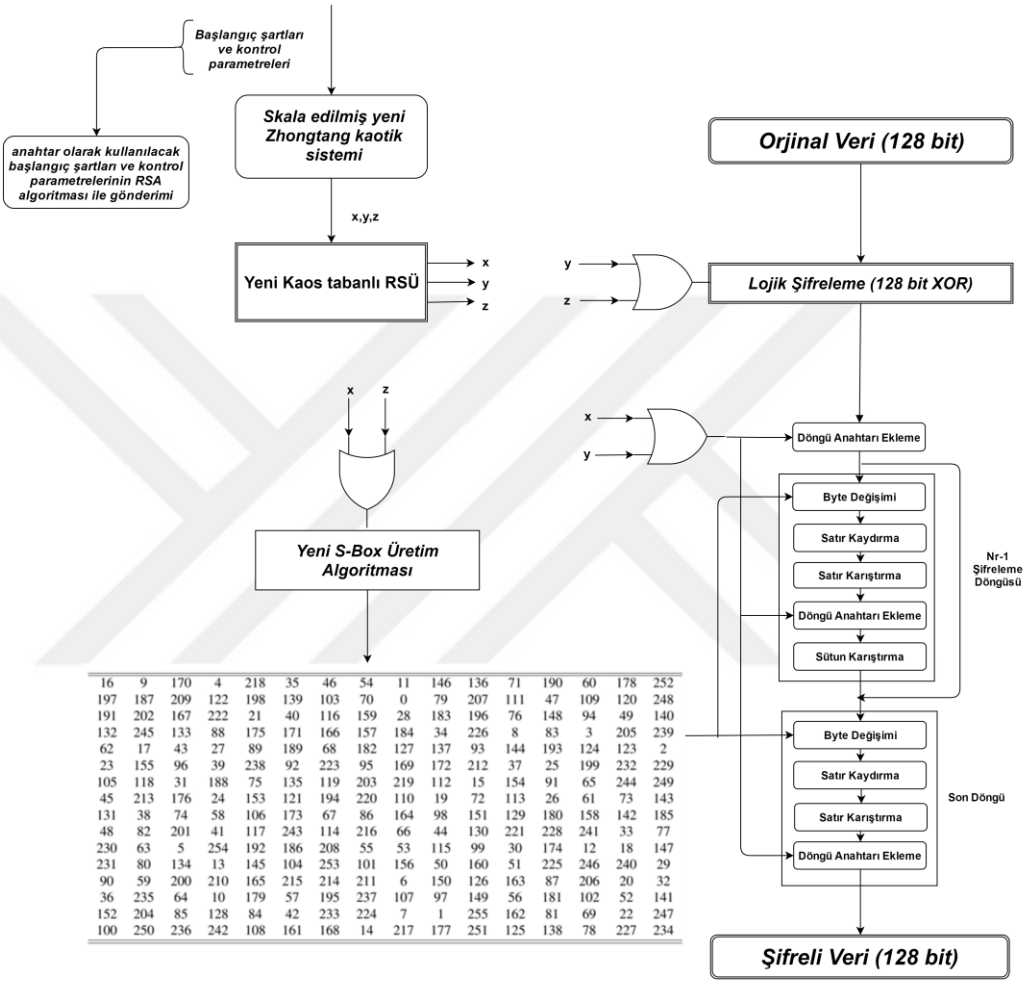
Bayt değişimi: CS-AES algoritmasında bayt değişim işlemi, gönderici ve alıcı tarafında, kaos tabanlı S-Box üretim algoritması tarafından üretilen aynı S-Box üzerinden gerçekleştirilmektedir. Algoritmada gönderici tarafından şifrelenecek olan bayt satır ve sütun üzerinde değerleri bulunarak ikisinin kesişim noktasında bulunan 16x16 S-Box matrisi üzerinde bulunan değer ile değiştirilmektedir. Alıcı tarafta ise,

şifresi çözülecek olan veri, algoritmadaki döngü işlem sırasında, şifreli olan bayt matris üzerinde bulunarak, bu değerin matris üzerindeki satır ve sütun değerleri ile değiştirilerek şifre çözme işlemine devam edilmektedir.

CS-AES algoritmasında, anahtar ekleme adımı RSÜ'nün üretmiş olduğu döngü anahtarları ile, bayt değişim işlemi ise, kaos tabanlı S-BOX üretim algoritmasının üretmiş olduğu S-Box kullanılarak gerçekleştirilmektedir. Satır kaydırma ve sütun karıştırma işlemleri orijinal algoritma da olduğu gibi uygulanmaktadır. Geliştirilen algoritmaya orijinalinden farklı olarak karıştırmayı artırması maksadıyla satır karıştırma adımı eklenmiştir. Özetle hibrit CS-AES algoritmasında yeni kaos tabanlı RSÜ, yeni kaos tabanlı S-Box üretim algoritması ve S-AES algoritması kullanılmıştır. CS-AES algoritmasının işlem basamakları özetle aşağıdaki gibidir.

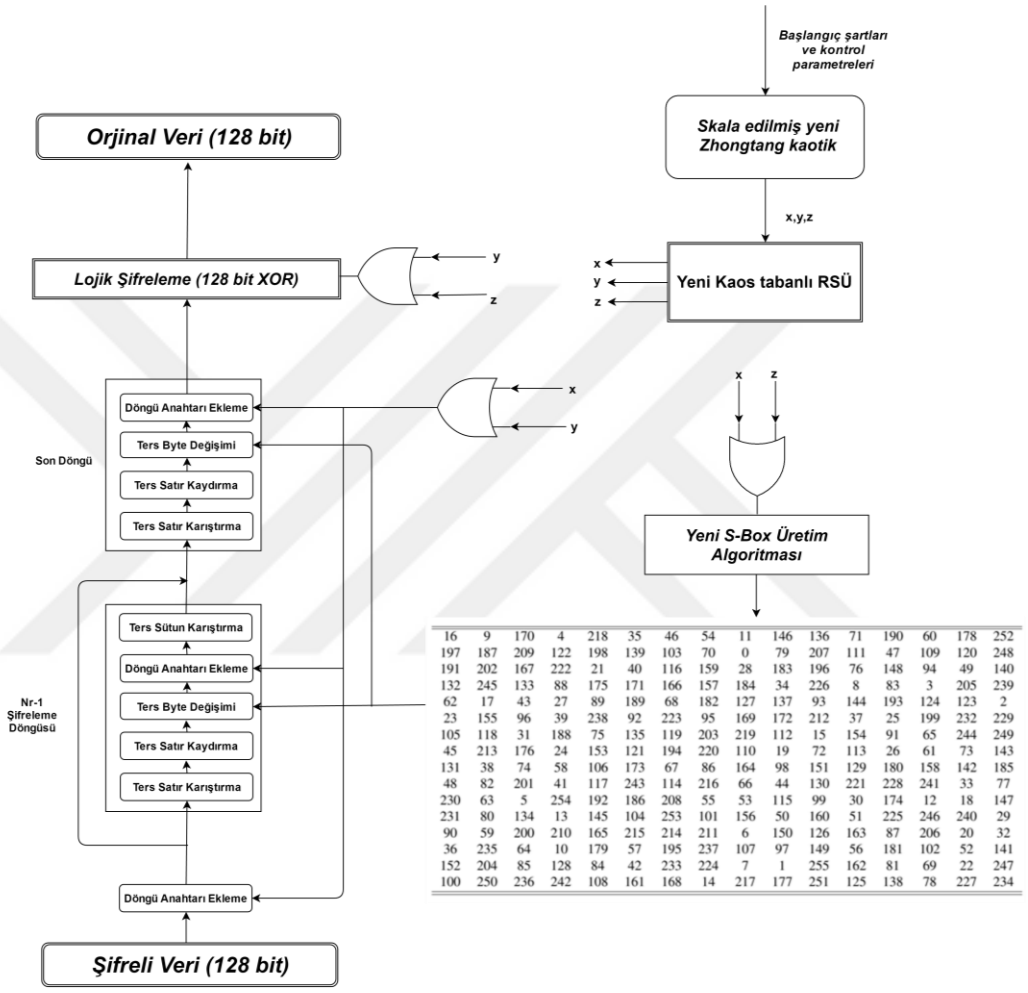
- Şifrelenecek olan 128 bit orijinal verinin şifreleme algoritmasına verilmesi.
- Kaos tabanlı RSÜ'de kullanılan yeni skala edilmiş Zhongtang kaotik sistemine başlangıç şartları ve sistem parametrelerinin girilmesi
- RSÜ tarafından x, y, z fazlarına ait rasgele sayıların üretimi
- Skala edilmiş Zhongtang kaotik sisteminin x ve z fazı kullanılarak RSÜ'den elde edilen rasgele sayıların XOR işlemine tabi tutulup, kaos tabanlı S-BOX üretim algoritması tarafından şifreleme işleminde kullanılacak S-Box'un üretilmesi
- Skala edilmiş Zhongtang kaotik sisteminin x ve y fazı kullanılarak RSÜ'den elde edilen rasgele sayıların XOR işlemine tabi tutulması ile döngü anahtarlarının elde edilmesi
- Skala edilmiş Zhongtang kaotik sisteminin y ve z fazı kullanılarak RSÜ'den elde edilen rasgele sayıların XOR işlemine tabi tutulması ile her blok şifreleme işleminde kullanılacak 128 bit rasgele sayının ön şifreleme işlemi için üretilmesi (128 bitlik değer her blok için ayrı üretilmektedir.)
- Döngüye girilmeden önce ilk anahtar ekleme işleminin gerçekleştirilmesi
- Kaos tabanlı S-Box kullanılarak bayt değişim işleminin gerçekleştirilmesi
- Satır kaydırma işlemi (4x4 durum matrsinin satırlarının sırası ile (0-1-2-3) kere öteleme işlemi)

- Satır karıştırma işlemi (satır karıştırma döngü anahtarının mod işlemine tabi tutulması ile her döngüde dinamik olarak farklı şekilde gerçekleştirilmektedir.)
- Döngü içinde anahtar ekleme işleminin gerçekleştirilmesi.
- Sütun karıştırma işlemi AES algoritmasında olduğu gibi gerçekleştirilmektedir.
- Son döngüde sütun karıştırma işlemi hariç tüm işlemlerin tekrarlanması
- Şifreli 128 bitlik verinin elde edilmesi ve alıcıya gönderimi
- Şifre çözme işleminde kullanılmak üzere RSA algoritması kullanılarak, RSÜ'de kullanılan kaotik sistemin başlangıç koşulları ve sistem parametrelerinin alıcıya gönderimi
- Alıcı tarafta, şifre çözme işleminde kullanılacak S-Box, döngü anahtarları ve ön şifreleme işleminde kullanılmak üzere her döngüde 128 bitlik rasgele değerlerin üretimi
- Şifre çözme işleminde Şekil 4.6.'da görüldüğü gibi tersi sırada işlemler gerçekleştirilmekte ve orijinal veri elde edilmektedir.



16	9	170	4	218	35	46	54	11	146	136	71	190	60	178	252
197	187	209	122	198	139	103	70	0	79	207	111	47	109	120	248
191	202	167	222	21	40	116	159	28	183	196	76	148	94	49	140
132	245	133	88	175	171	166	157	184	34	226	8	83	3	205	239
62	17	43	27	89	189	68	182	127	137	93	144	193	124	123	2
23	155	96	39	238	92	223	95	169	172	212	37	25	199	232	229
105	118	31	188	75	135	119	203	219	112	15	154	91	65	244	249
45	213	176	24	153	121	194	220	110	19	72	113	26	61	73	143
131	38	74	58	106	173	67	86	164	98	151	129	180	158	142	185
48	82	201	41	117	243	114	216	66	44	130	221	228	241	33	77
230	63	5	254	192	186	208	55	53	115	99	30	174	12	18	147
231	80	134	13	145	104	253	101	156	50	160	51	225	246	240	29
90	59	200	210	165	215	214	211	6	150	126	163	87	206	20	32
36	235	64	10	179	57	195	237	107	97	149	56	181	102	52	141
152	204	85	128	84	42	233	224	7	1	255	162	81	69	22	247
100	250	236	242	108	161	168	14	217	177	251	125	138	78	227	234

Şekil 4.5. CS-AES şifreleme algoritması blok diyagramı



16	9	170	4	218	35	46	54	11	146	136	71	190	60	178	252
197	187	209	122	198	139	103	70	0	79	207	111	47	109	120	248
191	202	167	222	21	40	116	159	28	183	196	76	148	94	49	140
132	245	133	88	175	171	166	157	184	34	226	8	83	3	205	239
62	17	43	27	89	189	68	182	127	137	93	144	193	124	123	2
23	155	96	39	238	92	223	95	169	172	212	37	25	199	232	229
105	118	31	188	75	135	119	203	219	112	15	154	91	65	244	249
45	213	176	24	153	121	194	220	110	19	72	113	26	61	73	143
131	38	74	58	106	173	67	86	164	98	151	129	180	158	142	185
48	82	201	41	117	243	114	216	66	44	130	221	228	241	33	77
230	63	5	254	192	186	208	55	53	115	99	30	174	12	18	147
231	80	134	13	145	104	253	101	156	50	160	51	225	246	240	29
90	59	200	210	165	215	214	211	6	150	126	163	87	206	20	32
36	235	64	10	179	57	195	237	107	97	149	56	181	102	52	141
152	204	85	128	84	42	233	224	7	1	255	162	81	69	22	247
100	250	236	242	108	161	168	14	217	177	251	125	138	78	227	234

Şekil 4.6. CS-AES şifre çözme algoritması blok diyagram

BÖLÜM 5. YENİ HİBRİT ŞİFRELEME ALGORİTMALARI UYGULAMALARI VE PERFORMANS ANALİZLERİ

Bu bölümde geliştirilen kaos tabanlı hibrit asimetrik şifreleme algoritması CRSA ve simetrik şifreleme algoritması CS-AES ile resim şifreleme işlemleri yapılmıştır. Gerçekleştirilen şifreleme işlemlerinin güvenlik ve performans analizleri gerçekleştirilmiştir. Resim şifreleme uygulamaları ve analizler yapılmadan önce performans ve güvenlik analizleri ile ilgili bilgi verilmiştir.

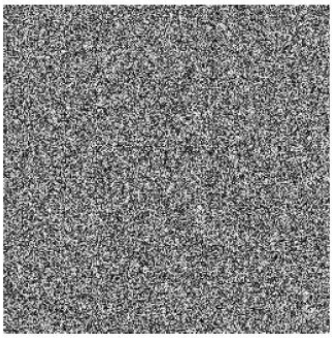
5.1. CRSA Şifreleme Algoritması ve Uygulaması

Geliştirilen CRSA algoritması ile Şekil 5.1.a'da görülen 256x256 boyutundaki 'taraftar. jpg' resmi şifrelenmiş ve çözülmüştür. Resim şifreleme uygulaması, CRSA algoritması tasarımında anlatıldığı şekilde şifreleme ve çözme işlemleri gerçekleştirilmiştir. RSA algoritması için gerekli olan aralarında asal p ve q değerleri kaos tabanlı RSÜ tarafından üretilmiş, üretilen p ve q değerleri üzerinden n, $\varphi(n)$, e ve d değerleri hesaplanmıştır. Şifreleme işlemi için ilk önce gönderici tarafta 256x256 boyutundaki resim RSÜ tarafından üretilen rasgele bit dizisi ile resme XOR işlemi uygulanmaktadır. Ardından 256x256 boyutundaki matristen 16 bayt'lık bloklar şeklinde alınan veri RSA algoritması tarafından şifrelenmekte ve alıcıya iletilmektedir. Şifrelenmiş olan resme ait görüntü Şekil 5.1.b'de görülmektedir. Alıcı tarafında RSA algoritması ile çözülen veri son olarak, gönderici tarafında RSÜ'nün üretmiş olduğu eş değer bit dizisi ile XOR'lanarak orijinal resim elde edilmektdir.

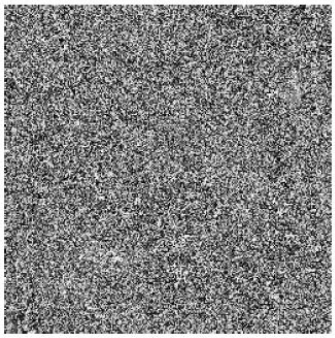
CRSA algoritmasının güvenlik ve performans analizlerini gerçekleştirmek için aynı resim RSA algoritması ile de şifreleme ve çözme işlemine tabi tutulmuştur. Şekil 5.1.c' de ise sadece RSA algoritması ile gerçekleştirilen şifreleme işlemi sonucunda elde edilen resim görülmektedir. Şekil 5.1.d'de ise CRSA ve RSA algoritmaları ile

gerçekleştirilen şifre çözme işlemlerinin sonucunda elde edilen orijinal resim görülmektedir. Şekil 5.1.a ve 5.1.d incelendiğinde her iki şifreleme uygulamasında da orijinal resmin elde edildiği görülmektedir.

a) Orijinal resim



b) CRSA şifreli resim



c) RSA şifreli resim

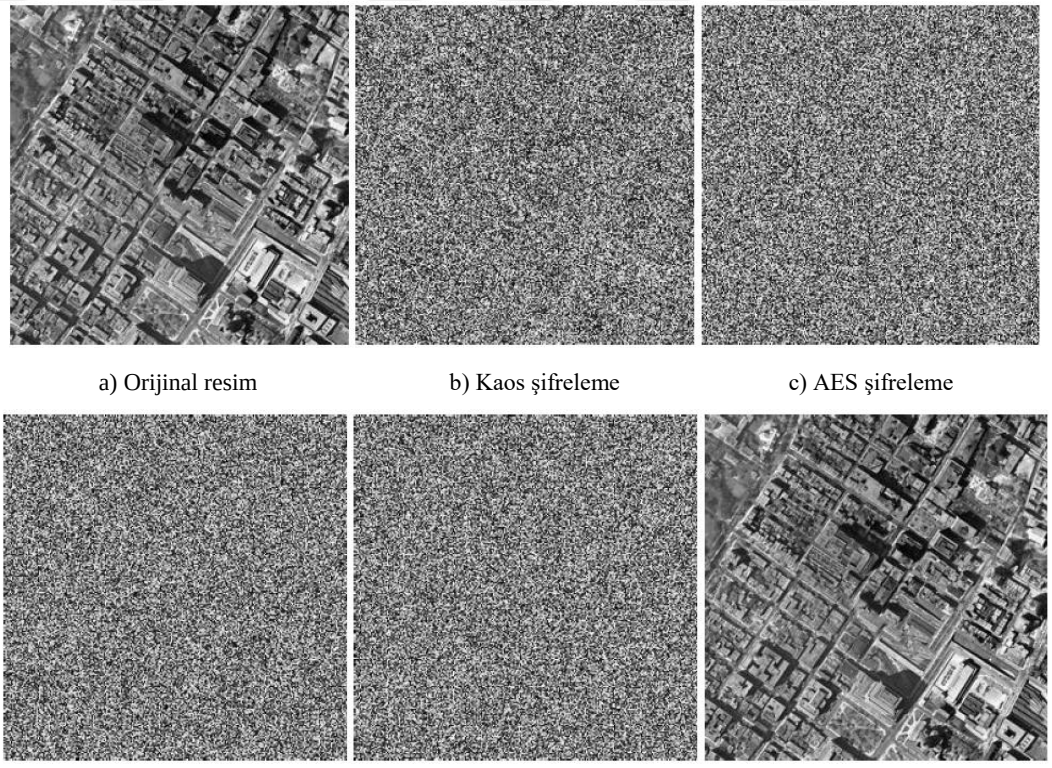
d) Çözülmüş resim

Şekil 5.1. Resim şifreleme ve çözme uygulaması sonuçları

5.2. CS-AES Şifreleme Algoritması ile Şifreleme Uygulaması

Bu bölümde CS-AES şifreleme algoritması kullanılarak 256x256 boyutundaki satellite. jpg resmi üzerinde şifreleme ve çözme işlemleri gerçekleştirilmiştir. Ayrıca aynı resim üzerinde, CS-AES şifreleme algoritmasının performansını değerlendirmek için, sadece kaotik sistem, AES ve S-AES algoritması ile 3 farklı şifreleme daha yapılmıştır. Şekil 5.2.a'da şifreleme işleminde kullanılan 256x256 boyutundaki satellite. jpg resmi görülmektedir. Resim şifreleme işlemlerini gerçekleştirmek için, resim bit bazında dönüşüm işlemine tabi tutulmuştur. Kaos tabanlı şifreleme için, RSÜ x ve y fazlarından elde edilen rasgele bit dizileri XOR işlemine tabi tutularak 256x2048 bitlik şifre matris elde edilmiştir. Elde edilen şifreleme matris ile resim bit

bazında XOR işlemine tabi tutularak kaos tabanlı şifreleme işlemi gerçekleştirilmiştir. Kaos tabanlı şifreleme işlemine ait şifrelenmiş resim Şekil 5.2.b'de görülmektedir. Daha sonra sırasıyla AES ve S-AES algoritmaları kullanılarak resim üzerinde şifreleme gerçekleştirilmiştir. Şekil 5.2.c'de AES şifreleme, Şekil 5.2.d'de ise S-AES algoritması ile yapılan şifreleme sonucu elde edilen şifreli resimler görülmektedir. Son olarak geliştirilen CS-AES algoritması ile algoritma tasarımında anlatıldığı gibi, resim 128 bitlik bloklar halinde şifrelenmiş ve Şekil 5.2.e'de şifreleme sonucu elde edilen resim verilmiştir. Yapılan tüm şifreleme işlemlerinden sonra çözme işlemi gerçekleştirilerek Şekil 5.2.f'de görülen orijinal resim elde edilmiştir. Şifreleme işlemine ait güvenlik ve performans analizleri bir sonraki bölümde gerçekleştirilmiştir.



a) Orijinal resim b) Kaos şifreleme c) AES şifreleme

d) S-AES şifreleme e) CS-AES şifreleme f) Çözülmüş resim

Şekil 5.2. Resim şifreleme ve çözme uygulaması sonuçları

5.3. Güvenlik ve Performans Analizleri

Şifreleme algoritmalarının kalitesi, ataklara ve saldırılara karşı dayanıklı olması ve uygun performans ile işlemleri gerçekleştirmesine bağlıdır. Tüm saldırılara dayanıklı

fakat performans bakımından zayıf algoritmalar güvenlik uygulamalarında tercih edilmemektedir. Çünkü bu tür algoritmalar, yüksek şifreleme ve çözme zamanlarına ve aşırı kaynak kullanımına ihtiyaç duymaktadır. Bu sebeple pratikte tercih edilen algoritmalar hem güçlü ve kırılması zor güvenlik seviyelerine aynı zamanda uygun performansa sahip olmalıdırlar. Geliştirilen hibrit şifreleme algoritmaları ile gerçekleştirilen şifreleme işlemlerine ait güvenlik ve performans değerlendirmeleri için bazı analizler gerçekleştirilmiştir. Test işlemleri Matlab ortamında yapılmıştır. Analiz işlemlerine geçilmeden önce güvenlik ve performans testleri hakkında bilgi verilmiştir.

5.3.1. Güvenlik analizleri

5.3.1.1. Histogram analizi

Histogram analizi, bir resim içindeki renk değerlerinin sayısını gösteren grafiksel bir gösterim şeklidir. Orijinal bir resimde renk dağılımları, resmin renklerine göre belli bölgelerde yoğunlaşmakta, dengesiz bir dağılım göstermektedir. Şifreleme işleminde, bu renk dağılımı eşitlenmeye çalışılmaktadır. Histogram dağılım dengesinin bir birine yakın olması şifrelemenin kaliteli olduğunu göstermekte ve şifrelenen verinin kırılmasını güçleştirmektedir. Tüm değerler birbirine yakın olduğu durumda, şifreli verinin histogramından bir çıkarım yapmak mümkün olmayacaktır.

5.3.1.2. Korelasyon analizi

Korelasyon analizi [143], iki rassal değişken arasında ilişkinin hesaplanması temeline dayanır. Kovaryans, iki rasgele değişkenin birlikte değişim değerini hesaplamaktadır. Korelasyon analizinde korelasyon katsayısı tespit edilmektedir. Korelasyon katsayısı bu iki değişken arasındaki ilişkinin, bağımsızlık durumunu göstermektedir. Korelasyon değeri, bu iki değerin kovaryansının, standart sapmalarının çarpım değerine bölümü ile bulunmaktadır. Resim üzerinde ilişki yatay, dikey ve çapraz pikseller arasındaki ilişki incelenerek tespit edilebilir. Orijinal resimde değişkenler arası ilişki doğrusal iken, analiz sonucu değişkenler arası ilişkinin doğrusal olmaması

(dağınık olması), oldukça karmaşık dağılım göstermesi, analiz sonucunun iyi olduğunu, iki resim arasında ilişki olmadığını göstermektedir. Bu değer -1 ile +1 değer arasında bir değer almaktadır. Pozitif değerler doğru yönlü doğrusal ilişkiyi, negatif değerler ters yönlü doğrusal ilişkiyi ifade etmektedir. Eğer katsayı 0 ise değişkenler arasında ilişki bulunmamaktadır. Rasgele herhangi bir sayıdaki çift yakın piksel, resimden alınarak, Denklem 5.1'de verilen formül yardımıyla her çiftin korelasyon katsayısı hesaplanabilir [144]. Denklemde x ve y resimdeki bitişik iki pikselin değerleri ve N seçilen piksel çiftinin sayısını göstermektedir.

$$
\begin{aligned}
E(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i \\
D(x) &= \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \\
\mathrm{cov}(x,y) &= \frac{1}{N}(\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y))) \\
r_{xy} &= \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)D(y)}}
\end{aligned}
\tag{5.1}
$$

5.3.1.3. Diferansiyel atak analizi (NPCR-UACI)

Biham ve Shamir [131] tarafından ortaya atılan diferansiyel kriptoanaliz, orijinal resim üzerindeki küçük değişimlerin şifreli resimler üzerinde nasıl bir etki meydana getirdiğini incelemektedir. Rasgele seçilmiş orijinal resim ve değiştirilmiş pikselinin aynı anahtar kullanılarak gerçekleştirilen şifreleme sonuçları karşılaştırmakta, bu değişimlerden elde ettiği bilgiyi kullanarak şifreyi çözmeyi denemektedir. Orijinal resimdeki küçük değişimler, şifreli resim üzerinde büyük değişimlere yol açıyor ise, şifrelemenin diferansiyel atak saldırılarına karşı dirençli olduğunu göstermektedir. Bu saldırılara karşı NPCR (Number of Pixels Change Rate) ve UACI (Unified Average Changing Intensity) diferansiyel ve lineer atak dayanıklılık performansını ölçmek için en sık kullanılan yöntemlerdir. NPCR ve UACI değerlerinin en uygun değerleri şu şekildedir: $NPCR_{opt}$ = 99.61% ve $UACI_{opt}$ =33.46% [145]. İki resim arasındaki ilişkiyi belirleyen NPCR değeri Denklem 5.2'de verildiği gibi hesaplanmaktadır. Denklem 5.2'de görülen D(i,j) matrisi Denklem 5.3'den elde edilmektedir. Bir önceki pikselde

hesaplanan veri ile sonraki veri birbirine eşitse 0, eşit değilse 1 üretilmektedir. Denklemde verilen N değeri ise resimdeki toplam piksel sayısıdır.

$$NPCR(A,B) = (\sum_{(i,j)} \frac{D(i,j)}{N}) * 100\% \tag{5.2}$$

$$D(i,j) = \begin{cases} 1 \leftarrow if \cdots A(i,j) \neq B(i,j) \\ 0 \leftarrow if \cdots A(i,j) = B(i,j) \end{cases} \tag{5.3}$$

İki resim arasındaki ortalama yoğunluğu ifade eden UACI değerinin hesaplanması için kullanılan formül Denklem 5.4'te verilmiştir. Denklemde verilen A(i,j) ve B(i,j) değerleri önceki ve sonraki pikselleri ifade ederken, L değeri ise resmin pikselini ifade eden bit sayısıdır. N değeri ise NPCR'de olduğu gibi toplam piksel sayısını ifade etmektedir.

$$UACI(A,B) = \frac{1}{N} (\frac{\sum_{(i,j)} (|A(i,j) - B(i,j)|)}{(2^L - 1)}) * 100\% \tag{5.4}$$

5.3.1.4. Bilgi entropi analizi

Şifrelemedeki asıl amaçlardan birisi şifrelenmek istenen veriyi olabildiğince karmaşık hale getirmeye çalışmaktır. Şifrelenmiş olan verinin karmaşıklığı şifrelemenin kalitesini ölçen kriterlerden birisidir. Şifrelenen veriler ne kadar çok karmaşık olursa o kadar iyi şifrelenmiş denilebilir. Bu karmaşıklık analizini yapmak için Shannon, Norm, Eşik, Logaritmik, Sample gibi birçok entropi hesaplama yöntemi mevcuttur. Şifrelenmiş veri orijinal veri hakkında tahmin yürütülemeyecek şekilde olmalıdır. Shanon [99] tarafından ortaya atılan bilgi entropi analizi şifreli verinin karmaşıklığını ölçmek için kullanılan metotlardan birisidir. Çalışmada bu analiz için Shannon Entropi metodu kullanılmıştır. Denklem 5.5'te Shanon bilgi entropi formülü verilmiştir. Formülde N olasılık kütle fonksiyonun değerlerinin sayısı, $p_i(x)$ i. sıradaki olasılık kütle fonksiyonu değeridir. Literatürdeki şifreleme çalışmalarında resim verileri için genellikle 256x256 resimler kullanılmaktadır. 256x256 resimler için ideal entropi

değeri 8 olması beklenmektedir. Şifrelenen verinin entropi değeri 8'e ne kadar yakınsa şifreleme işlemi o kadar iyi bir entropi değerine sahiptir.

$$ShanEn(x) = -\sum_{i=1}^{N}(p_i(x))^2(\log_2 p_i(x))^2 \tag{5.5}$$

5.3.1.5. Şifreleme kalitesi analizi

Şifreleme kalitesi analizinde [146,147], şifreleme işleminden önceki ve sonraki piksel değişim değerleri karşılaştırılarak, şifreleme kalitesi ölçülmektedir. Şifreleme işleminin ardından hemen hemen bütün piksellerde değişim gerçekleşmektedir. Piksel değişim değerleri ne kadar fazlaysa, şifreleme kalitesi artmaktadır. Denklem 5.6'da görüldüğü üzere, orijinal resim ve şifreli resim arasındaki sapma şifreleme kalite değerini belirlemektedir. Denklemde P orijinal resmi C ise şifreli resmi ifade etmektedir. L değeri 0 ile 255 arasında değişerek, bu değerin şifreli ve orijinal resimdeki bulunma miktarlarının farkının mutlak değerinin toplamını bulmak için kullanılmaktadır. Bulunan toplam değer 256'ya bölünerek şifreleme işlemine ait kalite analiz değeri elde edilmektedir.

$$Şifreleme\_Kalitesi = \frac{\sum_{L=0}^{255}\left|H_L(C) - H_L(P)\right|}{256} \tag{5.6}$$

5.3.1.6. Anahtar uzayı analizi

Güvenli bir şifreleme kaba kuvvet saldırılarına dayanıklı olacak yeterli bir anahtar uzayına sahip olmalıdır. Bilgisayar teknolojileri geliştikçe, daha büyük anahtar uzayına sahip şifrelemelere ihtiyaç duyulmaktadır. Alvarez ve Li [6], kaba kuvvet saldırılarına karşı koyabilecek bir şifreleme sisteminin anahtar havuzunun min. 2^{100} büyüklüğünde olması gerektiğini ifade etmişlerdir. Kaotik sistemler başlangıç koşullarına ve sistem parametrelerine hassas bağımlı olduklarından dolayı, kaotik şifreleme sistemlerinde bu değerler genellikle anahtar olarak kullanılmaktadır. Kaotik

şifrelemede anahtar uzunluğu analizinde, kaotik sistemin boyutu ve sistem parametrelerinin sayısı anahtar uzayının genişliğini belirlemektedir.

5.3.1.7. Anahtar hassasiyet analizi

Anahtar hassasiyet analizi, şifreleme ve çözme işlemlerinde kullanılan anahtarlardaki çok küçük değişimlerin şifreleme ve çözme işlemlerinde çok farklı sonuçların alınmasına sebep olmasıdır. Anahtar üzerindeki en küçük bir değişim sonucu elde edilen değer ile gerçekleştirilen şifreleme ve çözme işlemi sonucunda, gerçeğinden çok farklı şifreli ve orijinal veriler elde edilmektedir. Güvenli bir şifrelemede, anahtarlardaki çok küçük değişimler ataklara ve saldırılara karşı güvenli bir şifreleme ortaya koymalıdır. Kaotik tabanlı şifrelemede anahtar olarak sistem başlangıç koşulları ve sistem parametreleri kullanılmaktadır. Dolayısıyla kaotik sistemler, bu değerlere hassas bağımlı olduklarından dolayı, değerler üzerindeki en küçük bir değişim tüm şifreleme ve çözme işlemleri sonucu elde edilen sonuçları değiştirecektir. Özetle kaotik sistem tabanlı şifreleme sistemleri anahtara aşırı hassas bağımlı sistemlerdir.

5.3.2. Performans analizleri

Güvenlik testlerini geçmiş bir şifreleme sisteminin, gerçek ortamda kullanılması için iyi performans değerlerine sahip olması gerekmektedir. Özellikle gerçek zamanlı uygulamalarda ve büyük boyutlu verilerin şifreleme ve çözme işlemlerinde, ağır işlem ve aşırı kaynak tüketimine sahip, uzun çalışma zamanı olan algoritmalar tercih edilmemektedir. Şifreleme algoritmalarının performans analizinde en çok kullanılan yöntemler, şifreleme ve çözme hızı yani zaman analizi ve kaynak kullanım analizleridir. Algoritmaların değerlendirilmesinde güvenlik ve performans analizlerinin birlikte incelenmesi gerekmektedir.

5.3.2.1. Şifreleme hızı analizi

Bir şifreleme sisteminde, özellikle büyük boyutlu ve gerçek zamanlı uygulamalarda, şifreleme hızı güvenlik gereksinimlerinden sonra, dikkat edilmesi gereken en önemli

kriterlerden birisidir. Büyük boyutlu verilerin karmaşık işlemlere sahip algoritmalarda kullanımı ile şifreleme ve çözme süreleri çok uzamaktadır. Bu da şifreleme uygulamasının performansını olumsuz yönde etkilemektedir. Geliştirilen şifre algoritmalarının iyi güvenlik seviyesine sahip olmasının yanında, kullanılacak olan ortam ve sisteme uygun şifreleme ve çözme değerlerine sahip olmaları gerekmektedir.

5.3.2.2. Kaynak kullanım analizi

Şifreleme algoritmasının üzerinde çalıştığı donanımsal yapının kaynaklarını kullanım oranlarıda algoritmanın performans değerlendirilmesinde kullanılmaktadır. Kaynak kullanımının tespiti için, işlemci kullanım yüzdesi, bellek kullanım miktarı ve enerji tüketim değerleri gibi ölçümler gerçekleştirilmektedir. Şifreleme algoritmalarının performans değerlendirmesinde en önemli kriterlerden biri bellek kullanımıdır. Özellikle kısıtlı kaynaklara sahip cihazlar üzerinde gerçekleştirilecek şifreleme işlemlerinde daha az kaynağa ihtiyaç duyan uygulamalar tercih edilmektedir. Büyük boyutlu bellek işlemleri gerektiren algoritmalar aşırı bellek tüketim ihtiyacı sebebiyle, sınırlı bellek ve işlemci kapasitesine sahip donanımlarda sistemi yavaşlatmakta ve hantal bir yapının ortaya çıkmasına sebep olmaktadırlar. Sınırlı güç ve bataryaya sahip küçük ve mobil donanımlar üzerinde ise aşırı işlem yüküne sahip algoritmalar, aşırı kaynak tüketimi ile bataryaların kullanım sürelerinin kısalmasına sebep olmaktadırlar.

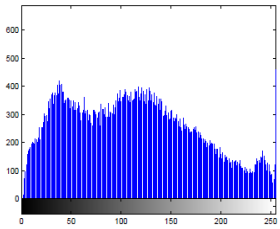
5.4. CRSA Şifreleme Uygulaması Analiz Sonuçları

Bu bölümde CRSA algoritması ile gerçekleştirilen şifreleme işlemine ait analizler yapılmıştır. Şifreleme işleminin analiz sonuçlarını değerlendirmek için, orijinal RSA algoritması ile gerçekleştirilen şifreleme işlemine ait sonuçlar karşılaştırılmıştır.

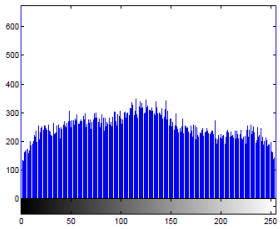
5.4.1. Histogram analizi

Geliştirilen CRSA hibrit şifreleme algoritması ve RSA algoritması ile gerçekleştirilen resim şifreleme işlemine ait histogram analizi yapılmıştır. Histogram analizinde renk dağılım değerlerinin birbirine yakın olması iyi bir şifreleme yapıldığını

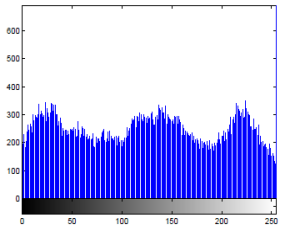
göstermektedir. Şekil 5.3.a'da orijinal resme ait histogram grafiği görülmektedir. Şekil 5.3.a incelendiğinde orijinal resimdeki renk değerlerinin düzensiz bir dağılıma sahip olduğu görülmektedir. Şekil 5.3.b'de CRSA, Şekil 5.3.c'de ise RSA algoritması tarafından şifrelenmiş resimlere ait histogram dağılımları görülmektedir. Şekil 5.3.b ve 5.3.c karşılaştırıldığında, CRSA algoritması ile yapılan şifreleme işlemi histogram dağılımı sonucunun, RSA algoritması ile yapılan şifrelemeden daha iyi olduğu görülmektedir. Şekil 5.3.b'de görüldüğü gibi, CRSA algoritması ile eşit dağılımlı sonuçlar elde edilmiştir. Ayrıca Şekil 5.3.a ve 5.3.d'de orijinal resim verisinin ve çözülmüş resim verisinin histogram dağılımları incelendiğinde, benzer sonuçların elde edildiği yani, şifreli verinin düzgün olarak çözüldüğü görülmektedir.



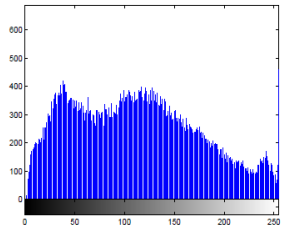
a) Orijinal resim



b) CRSA şifreli resim



c) RSA şifreli resim



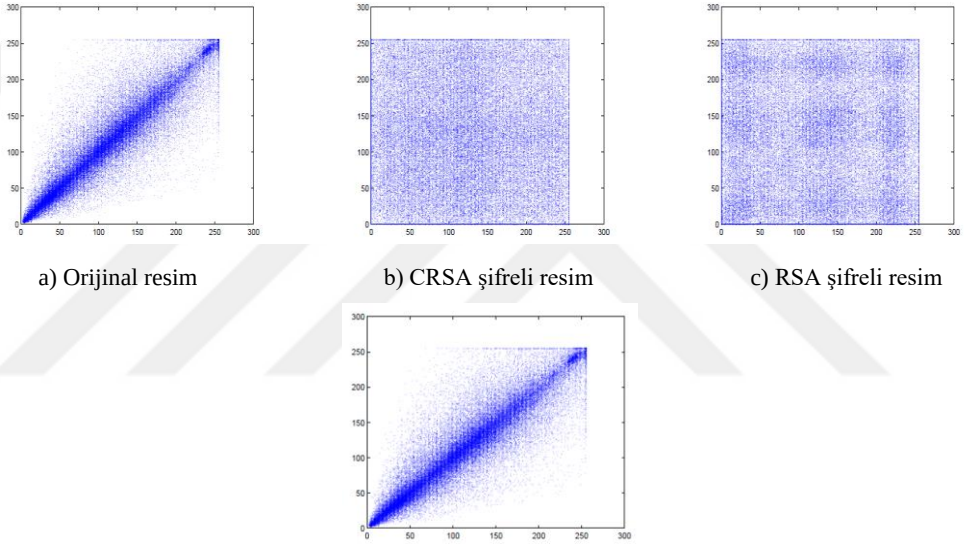
d) Çözülmüş resim

Şekil 5.3. Şifreleme işlemi histogram analizi sonuçları

5.4.2. Korelasyon analizi

Korelasyon analizinde resimdeki bitlerin doğrusallık durumu incelenmektedir. Şifreleme işleminde doğrusallığın kaybolması olabildiğince doğrusal olmayan bir yapının ortaya çıkması hedeflenmektedir. Şekil 5.4.a'da görüldüğü üzere, orijinal resimde doğrusallık varken, şifreleme işlemleri sonucunda doğrusallık bozulmuştur. Şekil 5.4.b'de CRSA hibrit şifreleme algoritması, Şekil 5.4.c'de ise RSA şifreleme algoritması ile gerçekleştirilen şifreleme işlemlerinin korelasyon analizi grafiği görülmektedir. Şifresi çözülmüş resime ait korelasyon analiz grafiği Şekil 5.4.d'dedir.

Şekil 5.4.a ve Şekil 5.4.d incelendiğinde, eş değer bir grafik elde edildiği, şifre çözme işleminin başarılı bir şekilde gerçekleştirildiği görülmektedir. Hem RSA hem de CRSA ile gerçekleştirilen şifrelemede doğrusallığın büyük oranda bozulduğu tespit edilmiştir. Tespit edilen korelasyon değerleri incelendiğinde, orijinal resme ait r_{xy} değeri 0,9259 CRSA ile şifreleme sonucu elde edilen ve Şekil 5.4.b'de görülen resime ait $_{rxy}$ değeri 0,5145 ve RSA ile şifreleme sonucu elde dilen ve Şekil 5.4.c'de görülen resme ait r_{xy} değeri 0,5445 olarak bulunmuştur. Bu değerlere göre, CRSA ile gerçekleştirilen şifrelemeye ait korelasyon değeri 0,5'e yakın ve RSA algoritmasının sonucundan daha iyi bir sonuca sahiptir.



a) Orijinal resim b) CRSA şifreli resim c) RSA şifreli resim

d) Çözülmüş resim

Şekil 5.4. Şifreleme işlemine ait korelasyon analizi sonuçları

5.4.3. Diferansiyel atak analizi (NPCR-UACI)

Diferansiyel atak analizinde, şifreli resim ile orijinal resim arasındaki ilişki tespit edilerek, şifre kırılmaya çalışılmaktadır. Bu analizde, piksel değişim oranı ve bileşik ortalama yoğunluk değerini tespit eden yöntemler kullanılmaktadır. Geliştirilen CRSA şifreleme algoritmasının diferansiyel atak analizinde, NPCR ve UACI testleri uygulanmıştır. CRSA algoritması ile karşılaştırmak için, RSA algortiması ile gerçekleştirilen şifreleme işlemi içinde analizler gerçekleştirilmiştir. Tablo 5.1.'den görüldüğü üzere RSA algoritması ile gerçekleştirilen şifreleme işleminde NPCR

99,6078 %, UACI 30,9862 % olarak elde edilirken, CRSA algoritması ile yapılan şifreleme işleminde NPCR 99,6093 %, UACI 32,2612 % olarak elde edilmiştir. Sonuçlara göre CRSA algoritması ile gerçekleştirilen şifreleme işleminin NPCR ve UACI analiz sonuçlarının RSA algoritması ile yapılan şifreleme işlemine göre daha iyi olduğu görülmektedir. Bu sonuçlara göre geliştirilen şifreleme algoritmasının diferansiyel ataklara dayanıklı bir yapıya sahip olduğu tespit edilmiştir.

Tablo 5.1. Şifreleme işlemine ait NPCR-UACI analiz sonuçları

Algoritma /NPCR-UACI	**NPCR**	**UACI**
RSA Algoritması	99,6078	30,9862
CRSA Algoritması	99,6093	32,2612

5.4.4. Bilgi entropi analizi

Entropi bir sistemdeki belirsizliğin seviyesini değerlendirmek için kullanılan bir yöntemdir. Geliştirilen CRSA ve RSA şifreleme algoritmaları ile gerçekleştirilen şifreleme işlemlerine ait entropi değerleri Tablo 5.2.'de görülmektedir. Şifreleme işlemlerine ait entropi değerlerinin ideal değer olan 8'e oldukça yakın olduğu görülmektedir. Orijinal resmin entropi değeri ise 6,9525 olarak bulunmuştur. Bu değerlere göre geliştirilen şifreleme algoritması ile yapılan şifreleme işleminin entropi değerinin RSA algoritmasından daha iyi ve güvenli şifreleme için yeterli seviyede olduğu görülmektedir.

Tablo 5.2. Şifreleme işlemine ait bilgi entropi analizi sonuçları

Algoritma	**Bilgi entropi değeri**
Orijinal resim	6,9525
RSA algoritması-şifreli resim	7,9279
CRSA algoritması-şifreli resim	7,9342

5.4.5. Şifreleme kalitesi analizi

Şifreleme kalite analizi, şifrelenmiş resim ile orijinal resim arasındaki değişen piksel değerleri karşılaştırılarak yapılmaktadır. Geliştirilen CRSA ve RSA şifreleme algoritmalarının şifreleme kalite analizi gerçekleştirilmiştir. Uygulama kısmında

gerçekleştirilen resim şifreleme işlemine ait şifreleme kalite analiz sonuçları RSA algoritması için 27,4453 ve CRSA algoritması için 35,4179 olarak bulunmuştur. Bu sonuçlara göre geliştirilen CRSA şifreleme algoritmasının RSA algoritmasından daha iyi bir şifreleme kalitesine sahip olduğu görülmektedir.

5.4.6. Anahtar uzayı analizi

Şifreleme uygulamalarının kaba kuvvet saldırılarına dayanıklı olabilmesi için yeterli genişlikte anahtar uzayına sahip olması gerekmektedir. Anahtar uzay analizinde, şifreleme algoritmasının mevcut anahtar uzayının genişliği tespit edilmektedir. Kaos tabanlı şifreleme uygulamalarında anahtar olarak, başlangıç şartları ve sistem parametreleri kullanılmaktadır. Geliştirilen kaos tabanlı şifreleme uygulamasında kaotik sistem olarak, Denklem 5.7'de görülen NCS kaotik sistemi kullanılmıştır.

$$\begin{aligned} x' &= cy - x - bz \\ y' &= axz - xy - bx \\ z' &= dxy + b \end{aligned} \tag{5.7}$$

Bir parametre 10^{14} farklı değer alabilmektedir. 3 boyutlu sürekli yeni NCS kaotik sistemi, her boyut için farklı bir değere (x, y ve z) 10^{42} ve 4 farklı sistem parametresine (a, b, c ve d) sahip olduğu için 10^{56} uzunluğunda bir anahtar uzunluğuna sahiptir. Başlangıç koşullarının ve sistem parametrelerinin anahtar uzayının toplamı 10^{98} ise sistemin toplam anahtar uzunluğunu vermektedir. NCS kaotik sistemini kullanan, CRSA şifreleme algoritmasının geniş ve kaba kuvvet saldırılarına dayanıklı bir anahtar havuzuna sahip olduğu tespit edilmiştir.

5.4.7. Anahtar hassasiyet analizi

Anahtar hassasiyet analizinde, sistemin şifrelemede kullandığı anahtara olan bağımlılığı incelenmektedir. Geliştirilen şifreleme algoritması, kaos tabanlı bir RSÜ tarafından üretilen rasgele sayıları kullandığı için, anahtar olarak kullanılan kaotik sistemin başlangıç şartlarına ve sistem parametrelerine oldukça hassas bağımlı bir yapıya sahiptir. CRSA şifreleme algortimasında NCS kaotik sistemi ve RSÜ-1 rasgele

sayı üreteci kullanılmıştır. Şifreleme sırasında üretilen rasgele değerlerin, şifre çözme aşamasında da aynı şekilde üretimi gerekmektedir. Şifreleme esnasında kullanılan NCS sistemine ait başlangıç koşulları ve sistem parametrelerinin aynı şekilde şifre çözme işleminde kullanımı zorunludur. Bu değerler üzerindeki en küçük değişiklik, şifre çözme esnasında farklı rassal sayı dizilerinin üretimine sebep olacağından şifre çözme işlemi başarılı bir şekilde gerçekleştirilemeyecektir.

RSÜ-1 tasarımında kaotik sistem çözümlemesi için RK-4 numerik analiz yöntemi kullanılmıştır. Bu yöntemde bir sonraki üretilecek olan değer bir önceki üretilmiş olan değere bağlıdır. Dolayısıyla bir adımdaki hata veya farklılık, diğer adımların tamamını etkilediğinden RSÜ tasarımı da değer değişimine hassas bağımlılık göstermektedir. Özetle, geliştirilen CRSA şifreleme algoritmasının tüm geliştirme süreçleri incelendiğinde, anahtar değişimine hassas bağımlı bir yapıya sahip olduğu görülmektedir.

5.4.8. Şifreleme hızı analizi

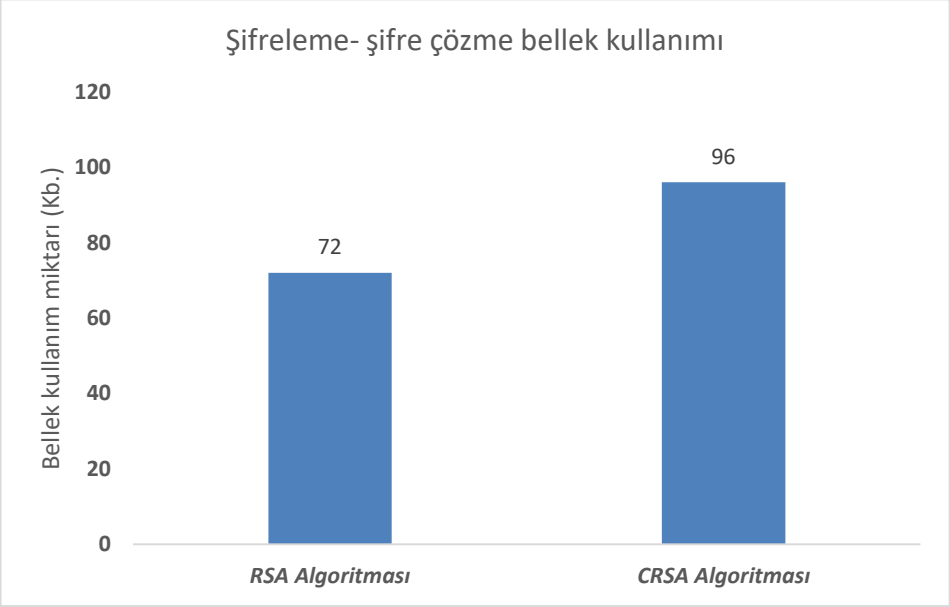
CRSA ve RSA algoritmaları ile gerçekleştirilen 256x256 boyutundaki ‘taraftar. jpg’ resmine ait şifreleme ve çözme işlemleri süreleri Tablo 5.3.’te verilmiştir. Şifreleme ve çözme işlemleri Matlab ortamında yapılan kodlama ile gerçekleştirilmiştir. RSA algoritması toplamda şifreleme ve çözme işlemlerini toplamda 32,8527 sn’de gerçekleştirmiştir. CRSA algoritması ise şifreleme ve çözme işlemlerini 29,0413 sn’de tamamladığı tespit edilmiştir. Şifreleme zamanları karşılaştırıldığında, CRSA algoritmasının RSA algoritmasından daha kısa sürede işlemleri tamamladığı görülmektedir. Şifreleme zamanları birbirine daha yakın iken, şifre çözme zamanları arasında fark daha fazladır.

Tablo 5.3. Şifreleme ve çözme süreleri karşılaştırma tablosu

Algoritma / Süre	Şifreleme zamanı (sn.)	Şifre çözme zamanı (sn.)	Toplam zaman (sn.)
RSA	8,7414	24,1113	32,8527
CRSA	9,8616	19,1797	29,0413

5.4.9. Bellek kullanım analizi

Geliştirilen şifreleme algoritmasının kaynak kullanım analizinde, şifreleme algoritmalarının bellek kullanım analizleri yapılmıştır. Matlab ortamında profile viewer eklentisi kullanılarak, şifreleme ve çözme işlemlerinde kullanılan bellek miktarları tespit edilmiştir. Şifreleme algoritmalarının bellek kullanım miktarları Şekil 5.5'te görülmektedir. RSA algoritması şifreleme işlemi için 72 Kb. bellek kapasitesi kullanırken, CRSA algoritması 96 Kb. bellek kullanmına sahiptir. CRSA algoritmasının bellek kullanımının biraz daha fazla olduğu tespit edilmiştir. Şifreleme algoritmaları bellek kullanım farkının, RSÜ'de p ve q değerleri için rasgele sayı üretimi ve üretilen sayılar ile şifrelenecek ve çözülecek verilerin XOR işlemlerinden kaynaklanmaktadır.



Şekil 5.5. Şifreleme ve çözme işlemleri toplam bellek kullanımı

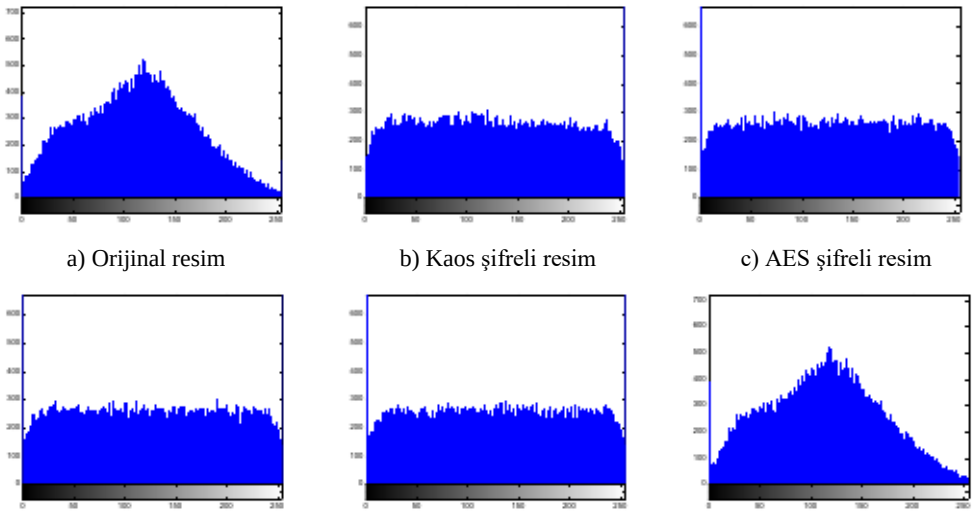
5.5. CS-AES Şifreleme Uygulaması Analiz Sonuçları

Bu bölümde skala edilmiş Zhongtang sistemi ile tasarlanan RSÜ-2 rasgele sayı üretecinin kullanıldığı CS-AES şifreleme algoritmasının güvenlik ve performans analizleri gerçekleştirilmiştir. Uygulama bölümünde gerçekleştirilen sadece kaos

tabanlı şifreleme, AES ve S-AES algoritmaları ile yapılan resim şifreleme işlemlerine ait analiz sonuçları CS-AES algoritmasının sonuçları ile karşılaştırılmıştır.

5.5.1. Histogram analizi

Şekil 5.6.a'da orijinal resime ait histogram dağılım grafiği görülmektedir. Şekil 5.6.b'de kaos şifreleme, Şekil 5.6.c'de AES şifreleme algoritması, Şekil 5.6.d'de S-AES şifreleme algoritması ve Şekil 5.6.e'de ise çalışmada geliştirilen CS-AES şifeleme algoritması ile şifrelenen resimlere ait histogram dağılım grafikleri görülmektedir. Şekil 5.6.f'de çözme işlemi sonucunda elde edilen orijinal resme ait histogram dağılım grafiği verilmiştir. Şekil 5.6.a'daki orijinal resim histogram grafiği ile, Şekil 5.6.f'deki çözülmüş resmin histogram grafiklerinin aynı olduğu tespit edilmiştir. Histogram grafikleri incelendiğinde, kullanılan tüm şifreleme algoritmalarında dengeli bir dağılım olduğu ve iyi bir histogram dağılımına sahip olduğu görülmektedir.



a) Orijinal resim b) Kaos şifreli resim c) AES şifreli resim

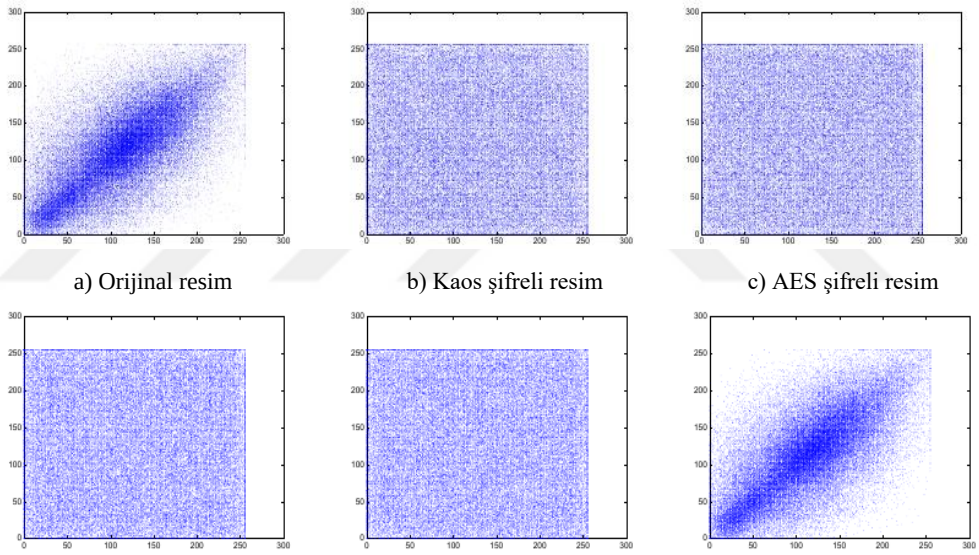
d) S-AES şifreli resim e) CS-AES şifreli resim f) Çözülmüş resim

Şekil 5.6. Şifreleme işlemine ait histogram analizi sonuçları

5.5.2. Korelasyon analizi

Korelasyon analizinde, orijinal resimdeki doğrusallığın bozulma durumu tespit edilmektedir. Doğrusallığın bozulması kaliteli bir şifrelemenin şartlarından birisidir.

Şekil 5.7.a'da orijinal resme ait korelasyon grafiği görülmektedir. Şekil 5.7.b'de kaos şifrelemeye, Şekil 5.7.c'de AES şifrelemeye, Şekil 5.7.d'de S-AES şifrelemeye ve Şekil 5.7.e'de geliştirilen CS-AES şifreleme algoritması ile gerçekleştirilen şifrelemeye ait korelasyon ilişki grafikleri, Şekil 5.7.f'de ise şifre çözme işlemi sonucu elde edilen resmin korelasyon dağılım grafiği görülmektedir. Gerçekleştirilen şifreleme işlemleri sonucu elde edilen şifreli resimlerin Denklem 5.1'deki formül kullanılarak hesaplanan korelasyon katsayı (r_{xy}) değerleri kaos tabanlı şifreleme için 0,5237, AES algoritması için 0,5236, S-AES algoritması için 0,5369 ve CS-AES algoritması için 0,5226 olarak bulunmuştur. Şekil 5.7. ve korelasyon katsayı değerleri incelendiğinde, CS-AES algoritması ile gerçekleştirilen şifrelemenin diğer şifreleme algoritmalarından daha iyi bir dağılım gösterdiği söylenebilir.



a) Orijinal resim b) Kaos şifreli resim c) AES şifreli resim

d) S-AES şifreli resim e) CS-AES şifreli resim f) Çözülmüş resim

Şekil 5.7. Şifreleme işlemine ait korelasyon analizi sonuçları

5.5.3. Diferansiyel atak analizi (NPCR-UACI)

Tablo 5.4.'te geliştirilen şifreleme algoritması ve karşılaştırma yapılan diğer tüm algoritmalara ait diferansiyel atak testleri sonucunda hesaplanan NPCR ve UACI test sonuçları görülmektedir. Tablo 5.4.'teki NPCR-UACI değerleri incelendiğinde, geliştirilen CS-AES şifreleme algoritmasının karşılaştırılan diğer algoritmalardan daha iyi ve optimal değere yakın NPCR ve UACI değerine sahip olduğu tespit edilmiştir. Sadece kaos tabanlı şifreleme ile gerçekleştirilen uygulamaya ait NPCR değerinin iyi

fakat UACI değerinin diğer algoritmalardan daha düşük olduğu görülmektedir. AES ve S-AES şifreleme algoritmalarının değerleri ise birbirine yakındır. Bu sonuçlara göre geliştirilen CS-AES şifreleme algoritmasının diferansiyel atak saldırılarına karşılaştırılan diğer algoritmalardan daha dirençli olduğu görülmüştür.

Tablo 5.4. Şifreleme algoritmaları NPCR-UACI test sonuçları

Algoritma / NPCR-UACI	NPCR	UACI
Kaos şifreleme	99,3524	27,0803
AES algoritması	99,6357	31,3142
S-AES algoritması	99,6018	30,0706
CS-AES algoritması	99,6368	31,6238

5.5.4. Bilgi entropi analizi

Tablo 5.5.'te şifreleme algoritmalarına ait bilgi entropi analiz sonuçları görülmektedir. CS-AES algoritmasının bilgi entropi analiz değeri diğer algoritmalardan daha iyi ve optimum değer olan 8'e çok yakındır. Analizi yapılan diğer şifreleme algoritmalarının entropi değerlerinin de iyi seviyelerde olduğu görülmektedir. Bu sonuçlara göre geliştirilen şifreleme algoritmasının resim üzerinde gerçekleştirdiği şifreleme işlemi sonucunda, yeterli bir entropi sonucu elde ettiği tespit edilmiştir.

Tablo 5.5. Şifreleme algroritmaları bilgi entropi değerleri

Algoritma	Bilgi entropi değeri
Kaos şifreleme	7,9553
AES algoritması	7,9587
S-AES algoritması	7,9572
CS-AES algoritması	7,9564

5.5.5. Şifreleme kalitesi analizi

Şifreleme kalite analizi için, CS-AES ve diğer şifreleme algoritmaları ile gerçekleştirilen şifreleme işlemleri sonucunda elde edilen şifreli resim ile üzerinde şifreleme yapılan orijinal resim piksel değerleri karşılaştırılmıştır. Tüm algoritmalar

için şifreleme kalite analizi yapılmılştır. Tablo 5.6.'da şifreleme algoritmalarının şifreleme kalite değerleri görülmektedir. Kaos tabanlı şifreleme uygulamasının şifreleme kalite değeri en düşük, CS-AES algoritmasının değeri ise en yüksektir. AES ve S-AES algoritmalarının şifreleme kalite değeri ise CS-AES algoritmasına yakındır. Bu sonuçlara göre geliştirilen CS-AES şifreleme algoritmasının iyi bir şifreleme kalite analiz sonucuna sahip olduğu tespit edilmiştir.

Tablo 5.6. Şifreleme algroritmaları şifreleme kalitesi analizi sonuçları

Algoritma	**Şifreleme kalitesi analizi sonucu**
Kaos şifreleme	26,5742
AES algoritması	31,1527
S-AES algoritması	30,5390
CS-AES algoritması	31,6329

5.5.6. Anahtar uzayı analizi

Kaos tabanlı şifreleme sistemlerinde anahtar olarak sistemin başlangıç şartları ve sistem parametreleri kullanılmaktadır. CS-AES şifreleme algoritmasının, anahtar uzayı analizinde, algoritma tasarımında anlatıldığı üzere, şifreleme algoritmasında anahtar olarak kullanılan ve RSÜ tasarımının gerçekleştirildiği yeni skala edilmiş Zhongtang kaotik sistemi başlangıç şartları ve kontrol parametreleri incelenecektir. Geliştirilen şifreleme algoritmasında kullanılan kaotik sistem Denklem 5.8'de verilmiştir. Denklemdeki parametrelerin değerleri ve başlangıç şartları şu şekildedir: (a = 80, b = 40, c = 5, d = 10, e = 2, f = 10, g = 15) (x_0=1, y_0=0, z_0=1).

$$\begin{aligned} x' &= ay - bx \\ y' &= cx + dy - exz^2 \\ z' &= -fx - gz + x^2 z \end{aligned} \tag{5.8}$$

Yeni skala edilmiş Zhongtanhg kaotik sistemi, 3 boyutlu sürekli bir kaotik sistem olduğu için başlangıç koşulları (x_0, y_0, z_0) olmaktadır. Başlangıç koşulları ve sistem parametresindeki her bir değişken için 10^{14}, 3 adet başlangıç koşulu için toplamda 10^{42}, sistem değişkenleri a, b, c, d, e, f, g olmak üzere toplamda 7 farklı sistem parametresine ve toplamda 10^{84} anahtar uzayına sahiptir. Başlangıç koşulları ve sistem parametreleri

birlikte değerlendirildiğinde toplamda 10^{126} gibi geniş bir anahtar uzayına sahip olduğu görülmektedir. CS-AES şifreleme algoritmasının bu analiz sonucunda oldukça geniş ve saldırılara dayanıklı bir anahtar uzayına sahip olduğu görülmektedir.

5.5.7. Anahtar hassasiyet analizi

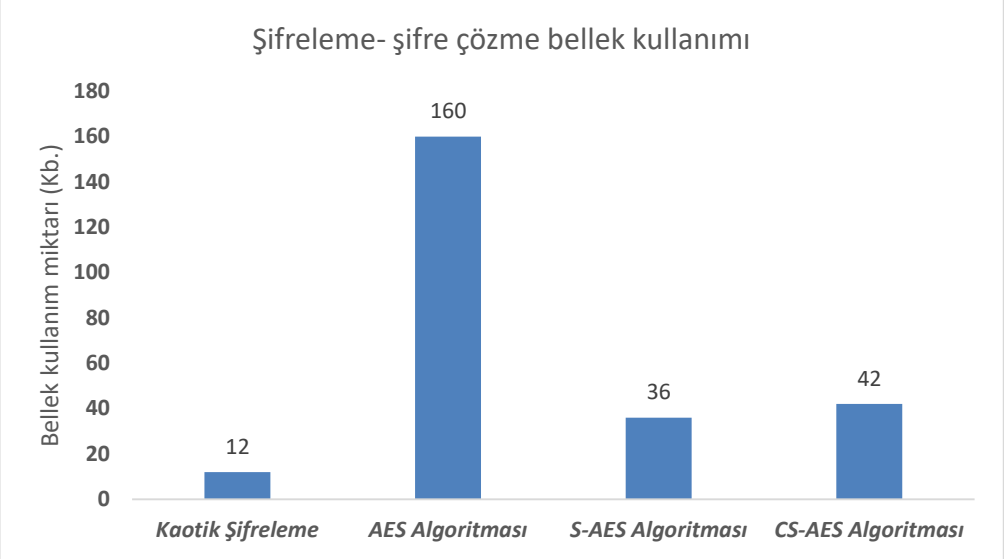
CS-AES şifeleme algoritması anahtar hassasiyet analizinde, anahtar uzayı analizinde belirtilen ve anahtar olarak kullanılan kaotik sisteme ait başlangıç şartları ve sistem parametrelerindeki küçük değişimler sonucu, şifreleme ve çözme işlemine ait sonuçlar irdelenmiştir. Bu değer ve parametrelerinin her hangi birinde gerçekleştirilen en ufak bir değişimin tamamen farklı bir şifreleme sonucu ürettiği tespit edilmiştir. Şifrelenmiş olan verinin çözümü sırasında kullanılacak olan, şifrelemede kullanılmış RSÜ tarafından üretilen özdeş rasgele bit dizilerinin, parametreler üzerindeki en ufak bir değişimin tamamen farklı rasgele diziler ürettiği ve şifreli resmi çözemediği görülmüştür. Bu sebeple geliştirilen kaos tabanlı hibrit CS-AES algoritması kaos tabanlı sistemlerin başlangıç değerlerine yüksek hassasiyetinden anahtarlar üzerindeki değişimlere hassas bağımlıdır.

5.5.8. Şifreleme hızı analizi

Şifreleme uygulmasında 256x256 boyutundaki satallite. jpg resminin kaos tabanlı, AES, S-AES ve CS-AES algoritmalarına ait şifreleme ve çözme süreleri Matlab ortamında yapılan kodlamalar ile tespit edilmiştir. Tablo 5.7.'de 65536 bayt değerindeki resme ait şifreleme, çözme ve toplam zamanları görülmektedir. Tablodaki değerler karşılaştırıldığında daha düşük güvenlik seviyesine sahip sadece XOR işlemi ile gerçekleştiren kaotik şifrelemenin şifreleme ve çözme zamanlarının en düşük değerler olduğu, ağır işlem yüküne sahip AES algoritmasının sürelerinin çok yüksek olduğu görülmektedir. S-AES şifreleme algoritmasının resmi yaklaşık 9,29 sn. de şifreleyip çözdüğü, daha yüksek güvenlik seviyesine sahip geliştirilen CS-AES algoritmasının ise yaklaşık 8,67 sn. de bu işlemleri gerçekleştirdiği tespit edilmiştir. Bu değerlere göre, geliştirilen CS-AES şifreleme algoritmasının güvenli ve verimli şifreleme için iyi bir zaman performansına sahip olduğu söylenebilir.

Tablo 5.7. Şifreleme ve çözme süreleri karşılaştırma tablosu

Algoritma	Şifreleme zamanı (sn.)	Çözme zamanı (sn.)	Toplam zaman (sn.)
Kaos şifreleme	2,627	1,759	4,386
AES algoritması	29,344	36,502	65,846
S-AES algoritması	3,984	5,313	9,297
Önerilen CS-AES algoritması	3,436	5,236	8,672



Şekil 5.8. Şifreleme ve çözme işlemleri toplam bellek kullanımı (128 bitlik şifreleme)

5.5.9. Bellek kullanım analizi

Geliştirilen şifreleme algoritmasının bellek kullanım miktarının belirlenmesi ve diğer şifreleme algoritmaları ile karşılaştırmak için, satallite. jpg resmi (65536 bayt) şifreleme ve çözme işlemine tabi tutularak, bir blok için (128 bit) algoritmaların bellek kullanım miktarları Matlab profile viewer ile ölçülmüştür. Şekil 5.8.'de kaos tabanlı, AES, S-AES ve CS-AES şifreleme algoritmalarının, şifreleme ve çözme işlemleri için ihtiyaç duydukları bellek miktarları görülmektedir. Sadece XOR işlemi ile gerçekleştirilen kaotik şifreleme 12 Kb. ile en düşük bellek gereksinimine, AES algoritması 160 Kb. ile en yüksek bellek gereksinimine sahip algoritmalardır. S-AES ve CS-AES algoritması ise 36 ve 42 Kb. ile birbirine çok yakın ve güvenlik seviyelerine göre iyi bir bellek kullanımına sahip oldukları görülmektedir.

BÖLÜM 6. SONUÇLAR, DEĞERLENDİRME VE ÖNERİLER

Kaotik sistemler sahip oldukları rasgelelik, ergodiklik ve başlangıç şartlarına olan hassas bağımlılık gibi özelliklerinden dolayı, kriptolojik uygulamaların temel gereksinimleri olan karıştırma ve yayılma özelliklerini sağlamaktadırlar. Literatürdeki sadece kaotik sistemler ile gerçekleştirilen şifreleme uygulamalarının bazı zafiyetler taşıdığı ve saldırılara yeterince dayanıklı olmadığı gösterilmiştir. Modern şifreleme algoritmaları incelendiğinde ise, gün geçtikçe daha büyük anahtar uzunlukları ile şifreleme yükleri artmakta özellikle büyük boyutlu verilerin şifrelenmesinde ve gerçek zamanlı uygulamalarda, şifreleme sürelerinin uzamasına ve aşırı kaynak tüketimine sebep olduğu görülmektedir.

Bu tez çalışmasında; kaotik sistemlerin zengin dinamik özelliklerinin ve modern şifreleme algoritmalarının birlikte kullanıldığı yeni kaos tabanlı hibrit şifreleme algoritma tasarımları önerilerek, geliştirilen şifreleme algoritmaları ile saldırılara karşı güçlü, dayanıklı ve yüksek performanslı resim şifreleme uygulamaları gerçekleştirilmiştir. Şifreleme uygulamalarına ait güvenlik ve performans analizleri yapılarak, sonuçları ortaya konulmuştur.

Yeni şifreleme algoritmalarının geliştirilebilmesi için, literatürde kullanılan ve dinamik yapıları çok iyi bilinen kaotik sistemler yerine, dinamik özellikleri daha zengin ve yüksek rasgelelik taşıyan yeni kaotik sistem tasarımları gerçekleştirilmiştir. Yeni kaotik sistemlerin tasarımlarından önce faz portresi analizi, zaman serisi analizi, denge noktası analizi, Lyapunov üstelleri spektrum analizi, çatallaşma analizi, frekans spekturum analizi gibi dinamik analiz yöntemleri açıklanmıştır. Daha sonra yeni NCS kaotik sistemi tanıtılarak, analizleri gerçekleştirilmiştir. Analiz sonuçlarına göre yeni NCS kaotik sisteminin zengin dinamik özellikler taşıdığı gösterilmiştir. İkinci kaotik sistemin tasarımında, daha zengin dinamik özellikler elde etmek için, orijinal Zhongtang sistemi skala edilmiştir. Yeni skala edilmiş Zhongtang sisteminin analizleri

yapılmıştır. Kaotik sistem analizlerine göre; yeni sistemin oldukça rasgele sinyaller ürettiği, 5 adet denge noktasına sahip olduğu, a ve b parametrelerine göre yapılan Lyapunov ve çatallaşma analizlerinden çok geniş bir aralıkta kaotik özellikler sergilediği ve daha yüksek frekans aralığında çıkışlar ürettiği tespit edilmiştir. Analiz sonuçlarından her iki kaotik sistemin de şifreleme uygulamalarında rasgele sayı üretimi için kullanılabileceği sonucuna varılmıştır.

Zengin dinamik özelliklere sahip yeni kaotik sistem tasarımlarının ardından bu kaotik sistemlerin kullanıldığı iki adet yeni RSÜ tasarımı yapılmıştır. RSÜ tasarımlarında kaotik sistemlerin çözümlenmesi için RK-4 sayısal analiz yöntemi kullanılmıştır. RSÜ-1 algoritma tasarımında kaotik sistemden örnekleme adım değer aralığı kullanılarak kayan noktalı sayılar elde edilmektedir. Her bir kayan noktalı sayı ikili sisteme çevrilerek, elde edilen bit dizisinin yüksek hassasiyete sahip olan bitlerinden, belirlenen sayıda bitler alınmaktadır. İstenilen sayıda ragele bit dizisi tamamlanıncaya kadar bu işleme devam edilerek rasgele bit dizileri elde edilmektedir. RSÜ-1 algoritmasında farklı sayıda bitlerin alınması ile oluşturulan rasgele bit dizilerine ait NIST rasgelelik test sonuçları tablo halinde sunulmuştur. RSÜ-2 algoritma tasarımında, kaotik sistemin üretmiş olduğu kayan noktalı değerlerin ondalık kısmının basamak değerlerine mod işlemi uygulanması ile rasgele bit dizileri elde edilmektedir. RSÜ-2 tasarımında tek bir fazdan elde edilen bit dizileri NIST testlerini geçemediğinden dolayı faz çıkışlarına ikişerli olarak XOR işlemi uygulanmıştır.

RSÜ-1 tasarımında NCS ve skala edilmiş Zhongtang sistemleri ile rasgele bit dizileri üretilerek NIST rasgelelik testleri yapılmıştır. RSÜ-2 tasarımında ise skala edilmiş Zhongtang ve Lorenz kaotik sistemleri ile rasgele bit dizilerinin üretimi gerçekleştirilmiştir. RSÜ-1 ve RSÜ-2 rasgele sayı üreteci tasarım algoritmalarının her iki kaotik sistem kullanılarak ürettikleri bit dizileri tüm NIST testlerinden geçmiştir. Tasarlanan her iki RSÜ'nünde şifreleme uygulamalarında rasgele sayı üretimi için kullanılabileceği gösterilmiştir. RSÜ-1 tasarımında üretilen 32 bitten belli bitlerin çekilmesi ve fazla bit çekilmesi durumunda üretilen rasgele bit dizilerinin NIST testlerinden geçememesi olumsuz olarak değerlendirilirken, RSÜ-2 tasarımında ise tek bir faza ait üretilen bit dizileri testleri geçememekte ve en az iki faza ait bit çıktılarının

XOR işlemine tabi tutulması gerekmektedir. RSÜ tasarımlarında basit operasyonlar kullanılarak, NIST testlerinin tamamından geçen daha rassal sayıların üretimi gerçekleştirilmiştir.

CS-AES şifreleme algoritmasında kullanılacak, S-Box'un üretimi için, kaos tabanlı S-Box üretim algoritması tasarlanmıştır. Çalışmada S-Box üretim algoritması kullanılarak elde edilen iki adet S-Box önerilmiştir. Önerilen S-Box-1 RSÜ-2 algoritması ve yeni skala edilmiş Zhongtang sistemi kullanılarak üretilmiştir. CS-AES algoritma tasarımında S-Box-1 kullanılmıştır. S-Box-1'in performans test sonuçlarına göre, kaos tabanlı S-Box'lar içinde en yüksek doğrusal olmama değerine sahip olduğu, ideal BIC ve SAC değerleri taşıdığı görülmektedir. Önerilen S-Box-2 ise RSÜ-1 ve NCS kaotik sisteminin kullanımı ile üretilmiştir. Çalışmada önerilen S-Box'lar literatürdekiler ile karşılaştırılmıştır. Önerilen her iki S-Box'ında en önemli değerlendirme kriterlerinden olan doğrusal olmama ve DP değerlerinin literatürdeki karşılaştırılan kaos tabanlı S-Box'lardan daha iyi olduğu görülmektedir. AES algoritmasında kullanılan S-Box'ın performans değerlerinin, diğer tüm kaos tabanlı S-Box'lardan daha iyi olduğu gösterilmiştir. Daha az işlem yükü olması ve AES S-Box'ına yakın performans değerleri elde etmesi sebebiyle, kaos tabanlı S-Box algoritmaları tercih edilmektedir. Tasarlanan S-Box üretim algoritması sadece kaotik sistem çıktılarını kullanan, işlem yükü az, matris dönüşüm işlemlerine ihtiyaç duymayan fakat kriptolojik olarak güçlü S-Box yapıları üretmektedir.

RSÜ ve S-Box algoritmalarının tasarımından sonra, kaos tabanlı hibrit şifreleme algoritmalarının tasarımları gerçekleştirilmiştir. CRSA kaos tabanlı hibrit asimetrik şifreleme algoritması tasarımında NCS kaotik sistemini kullanan RSÜ-1 algoritması kullanılmıştır. CS-AES kaos tabanlı hibrit simetrik şifreleme algoritmasında skala edilmiş Zhongtang kaotik sistemini kullanan RSÜ-2 rasgele sayı üreteci kullanılmıştır. Geliştirilen şifreleme algoritmalarının güvenlik ve performans değerlendirmelerinin yapılması için her iki algoritma ile görüntü şifreleme işlemi gerçekleştirilmiştir. CRSA şifreleme algoritması ve RSA algoritmasının analiz sonuçlarının karşılaştırılması Tablo 6.1.'de görülmektedir. Gerçekleştirilen şifreleme uygulamaları üzerinde, güvenlik analizleri olarak histogram analizi, korelasyon analizi, NPCR ve UACI,

anahtar hassasiyet ve uzunluk analizleri, entropi testleri ve şifreleme kalitesi; performans analizi olarak ta şifreleme hızı ve bellek kullanım testleri yapılmıştır. Güvenlik analizi sonuçları değerlendirildiğinde CRSA şifreleme algoritmasının oldukça iyi bit dağılımı ve korelasyon dağılımı sağladığı, NPCR değerinin 100'e yakın olduğu, anahtar hassasiyet analizi sonuçlarına göre, anahtar değişimine oldukça hassas ve geniş bir anahtar uzayı bulunduğu, entropi değerinin 8'e yakın olduğu, şifreleme kalitesinin RSA algoritmasından daha iyi olduğu tespit edilmiştir. Güvenlik analiz sonuçları, RSA algoritmasından elde edilen sonuçlar ile karşılaştırıldığında, CRSA algoritmasının tüm güvenlik testlerinde, RSA algoritmasından daha iyi sonuçlar elde ettiği görülmüştür. Performans testlerinde ise CRSA algoritmasının RSA algoritmasından daha kısa sürede şifreleme ve çözme işlemlerini gerçekleştirdiği fakat daha fazla bellek kullanımına sahip olduğu görülmektedir. CRSA algoritması, RSA algoritmasının güçlü şifreleme yeteneğini ve kaotik sistemlerin oldukça karmaşık dinamik yapılarını birlikte kullanıldığı bir şifreleme algoritmasıdır. Geliştirilen şifreleme algoritmasının güçlü bir şifreleme gerçekleştirdiği ortaya konulmuştur.

Tablo 6.1. RSA ve CRSA algoritması analiz sonuçları karşılaştırması

Testler / Algoritmalar	**RSA**	**CRSA**
Histogram	İyi	Daha iyi
Korelasyon	r_{xy}=0,5445	r_{xy}=0,5145
NPCR	99,6078	99,6093
UACI	30,9862	32,2612
Bilgi Entropi Analizi	7,9279	7,9342
Şifreleme Kalitesi Analizi	27,4453	35,4179
Anahtar Uzayı Analizi	Geniş	Daha geniş
Anahtar Hassasiyet Analizi	Hassas	Aşırı hassas
Bellek kullanımı (Kb)	72	96
Zaman Analizi (sn.) (şifreleme+çözme)	32,8527 (8,7414+24,1113)	29,0413 (9,8616+19,1797)

Geliştirilen CS-AES şifreleme algoritması, sadece kaotik sistem tabanlı şifreleme, AES ve S-AES şifreleme algoritmaları ile gerçekleştirilen şifreleme uygulamalarına ait performans ve güvenlik analiz sonuçları Tablo 6.2.'de verilmiştir. Güvenlik analizleri sonuçları incelendiğinde, geliştirilen CS-AES algoritmasının karşılaştırılan

kaos tabanlı şifreleme, AES ve S-AES algoritmalarından daha iyi güvenlik seviyesine sahip olduğu ispatlanmıştır. Geliştirilen şifreleme algoritmasının performans analizleri için, şifreleme ve çözme süreleri, bellek kullanım miktarları ölçülerek diğer algoritmalar ile karşılaştırılmıştır. CS-AES algoritmasının zaman ve bellek değerlerinin S-AES algoritmasına yakın ve AES algoritmasından oldukça düşük ve iyi değerlere sahip olduğu tespit edilmiştir. CS-AES şifreleme algoritmasının, sadece kaos tabanlı yapılan şifreleme işleminden oldukça iyi güvenlik sonuçlarına sahip olduğu görülmektedir. Sonuç olarak, tüm geliştirme aşamaları, güvenlik ve performans analizleri incelendiğinde, geliştirilen CS-AES algoritmasının kaotik sistemlerin güçlü rassallık özelliklerini ve modern S-AES algoritmasının şifreleme tekniklerini kullanan güçlü, saldırılara dayanıklı, hızlı ve az kaynak tüketimine sahip hibrit bir algoritma olduğu sonucuna varılmıştır. Özellikle resim şifrelemede güvenli ve hızlı bir şifreleme için kullanılabileceği gösterilmiştir. Sonuç olarak geliştirilen kaos tabanlı hibrit şifreleme algoritmalarının görüntü şifrelemede güvenli bir şekilde kullanılabileceği ispat edilmiştir.

Tablo 6.2. Kaos tabanlı şifreleme, AES, S-AES ve CS-AES algoritmaları analiz sonuçları karşılaştırması

Testler / Algoritmalar	**Kaos tabanlı**	**AES**	**S-AES**	**CS-AES**
Histogram	İyi	İyi	İyi	İyi
Korelasyon	r_{xy}=0,5237	r_{xy}=0,5236	r_{xy}=0,5369	r_{xy}=0,5226
NPCR	99,3524	99,6357	99,6018	99,6368
UACI	27,0803	31,3142	30,0706	31,6238
Bilgi Entropi Analizi	7,9553	7,9587	7,9572	7,9564
Şifreleme Kalitesi Analizi	26,5742	31,1527	30,539	31,6329
Anahtar Uzayı Analizi	Daha geniş	Geniş	Geniş	Daha geniş
Anahtar Hassasiyet Analizi	Aşırı hassas	Hassas	Hassas	Aşırı hassas
Bellek kullanımı (Kb)	12	160	36	42
Zaman Analizi (sn.) (şifreleme+çözme)	4,386 (2,627+1,759)	65,846 (29,344+36,502)	9,297 (3,984+5,313)	8,672 (3,436+5,236)

İleriki çalışmalarda, tez çalışması sırasında geliştirilen kaotik sistemler, RSÜ ve S-Box üretim algoritmaları yeni şifreleme çalışmalarında veya farklı alanlarda kullanılabilir. Geliştirilen şifreleme algoritmalarının, gerçek ortamda kullanımı için uygulamaların geliştirilmesi, farklı şifreleme algoritmaları ile kaotik sistemlerin bir arada kullanılabileceği yapıların tasarlanması planlanmaktadır.

KAYNAKLAR

[1] Ott, E., Chaos in Dynamical Systems Second Edition. Cambridge University Press, 1979.

[2] Katz, J.ve Lindell, Y., Introduction to Modern Cryptography : Principles and Protocols. Chapman & Hall/CRC, 2008.

[3] Stallings, W., Cryptography and Network Securuty: Principles and Practice. Fifth ed. Ed., Prentice Hall, 2006.

[4] Amigo, J. M., Kocarev, L., Szczepanski, J., Theory and practice of chaotic cryptography. Physics Letters, Section A: General, Atomic and Solid State Physics, 366 (3), 211–216, 2007.

[5] Jakimoski, G., Kocarev, L., Chaos and cryptography: Block encryption ciphers based on chaotic maps. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 48 (2), 163–169, 2001.

[6] Alvarez, G., Li, S., Some basic cryptographic requirements for chaos-based cryptosystems. International Journal of Bifurcation and Chaos, 16 (8), 2129–2151, 2006.

[7] Bakhache, B., Ghazal, J. M., El Assad, S., Improvement of the security of ZigBee by a new chaotic algorithm. IEEE Systems Journal, 8 (4), 1021–1030, 2014.

[8] Wang, Y., Wong, K.-W., Liao, X., Chen, G., A new chaos-based fast image encryption algorithm. Applied Soft Computing, 11 (1), 514–522, 2011.

[9] Liu, Y., Tian, S., Hu, W., Xing, C., Design and statistical analysis of a new chaotic block cipher for Wireless Sensor Networks. Communications in Nonlinear Science and Numerical Simulation, 17 (8), 3267–3278, 2012.

[10] Chen, S., Zhong, X., Wu, Z., Chaos block cipher for wireless sensor network. Science in China, Series F: Information Sciences, 51 (8), 1055–1063, 2008.

[11] Mohammed, M. T., Rohiem, A. E., El-Moghazy, A., Confidentiality enhancement of Secure Real Time Transport Protocol. 2012 8th International Computer Engineering Conference: Today Information Society What's Next, ICENCO 2012, (M), 43–48, 2013.

[12] Kocarev, L., Jakimoski, G., Logistic map as a block encryption algorithm. Physics Letters, Section A:General, Atomic and Solid State Physics, 289 (4-5), 199–206, 2001.

[13] Tong, X.-J., Wang, Z., Zuo, K., A novel block encryption scheme based on chaos and an S-box for wireless sensor networks. Chinese Physics B, 21 (2), 20506, 2012.

[14] Tong, X.-J., Wang, Z., Liu, Y., Zhang, M., Xu, L., A novel compound chaotic block cipher for wireless sensor networks. Communications in Nonlinear Science and Numerical Simulation, 22 (1–3), 120–133, 2015.

[15] Çavuşoğlu Ü., Akgül A., Kaçar S., Pehlivan İ., Z. A., A novel chaos-based encryption algorithm over TCP data packet for secure communication. Security and Communication Networks., 9, 1285–1296, 2016.

[16] Noura, H., El Assad, S., Vldeanu, C., Design of a fast and robust chaos-based crypto-system for image encryption. 2010 8th International Conference on Communications, COMM 2010, (1), 423–426, 2010.

[17] Mansour, I., Chalhoub, G., Bakhache, B., Evaluation of a Fast Symmetric Cryptographic Algorithm Based on the Chaos Theory for Wireless Sensor Networks. Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, (i), 913–919, 2012.

[18] Assad, S. El, Farajallah, M., Vladeanu, C., Chaos-based Block Ciphers : An Overview., 4–7, 2014.

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

[20] Zhang, Z., Sun, S., Image encryption algorithm based on Logistic chaotic system and s-box scrambling. Proceedings - 4th International Congress on Image and Signal Processing, CISP 2011, 1, 177–181, 2011.

[21] Faculty, I. P., Dhar-mahraz, S., Benchmarking AES and Chaos Based Logistic Map for Image Encryption. , Computer Systems and Applications (AICCSA), 2013 ACS International Conference on. IEEE, 2013.

[22] Gao, T., Chen, Z., Image encryption based on a new total shuffling algorithm. Chaos, Solitons and Fractals, 38 (1), 213–220, 2008.

[23] Ren, H., Wang, Y., Xie, Q., Yang, H., A novel method for one-way hash function construction based on spatiotemporal chaos. Chaos, Solitons & Fractals, 42 (4), 2014–2022, 2009.

[24] Wang, X. yuan, Yu, Q., A block encryption algorithm based on dynamic sequences of multiple chaotic systems. Communications in Nonlinear Science and Numerical Simulation, 14 (2), 574–581, 2009.

[25] Tang, Y., Wang, Z., Fang, J., Image encryption using chaotic coupled map lattices with time-varying delays. Communications in Nonlinear Science and Numerical Simulation, 15 (9), 2456–2468, 2010.

[26] Masuda, N., Jakimoski, G., Aihara, K., Kocarev, L., (Read this for finite state tent) Chaotic block ciphers: From theory to practical algorithms. IEEE Transactions on Circuits and Systems I: Regular Papers, 53 (6), 1341–1352, 2006.

[27] Usama, M., Khan, M. K., Alghathbar, K., Lee, C., Chaos-based secure satellite imagery cryptosystem. Computers & Mathematics with Applications, 60 (2), 326–337, 2010.

[28] Guan, Z.-H., Huang, F., Guan, W., Chaos-based image encryption algorithm. Physics Letters A, 346 (1–3), 153–157, 2005.

[29] Wei, J., Liao, X., Wong, K. wo, Xiang, T., A new chaotic cryptosystem. Chaos, Solitons and Fractals, 30 (5), 1143–1152, 2006.

[30] Xiao, D., Liao, X., Wang, Y., Parallel keyed hash function construction based on chaotic neural network. Neurocomputing, 72 (10–12), 2288–2296, 2009.

[31] Yang, D., Liao, X., Wang, Y., Yang, H., Wei, P., A novel chaotic block cryptosystem based on iterating map with output-feedback. Chaos, Solitons and Fractals, 41 (1), 505–510, 2009.

[32] Wong, K. W., Ho, S. W., Yung, C. K., A chaotic cryptography scheme for generating short ciphertext. Physics Letters, Section A: General, Atomic and Solid State Physics, 310 (1), 67–73, 2003.

[33] Khan, M., Investigation on Pseudorandom Properties of Chaotic Stream Ciphers. 2006 IEEE International Conference on Engineering of Intelligent Systems, 1–5, 2006.

[34] Ozkaynak, F., Cryptographically secure random number generator with chaotic additional input. Nonlinear Dynamics, 78 (3), 2015–2020, 2014.

[35] Avaroğlu, E., Koyuncu, İ., Özer, A. B., Türk, M., Hybrid pseudo-random number generator for cryptographic systems. Nonlinear Dynamics, 82 (1–2), 239–248, 2015.

[36] Hu, H., Liu, L., Ding, N., Pseudorandom sequence generator based on the Chen chaotic system. Computer Physics Communications, 184 (3), 765–768, 2013.

[37] Angulo, J. A. A., Kussener, E., Barthelemy, H., Duval, B., A new oscillator-based Random Number Generator. 2012 IEEE 10th International New Circuits and Systems Conference, NEWCAS 2012, , 21–24, 2012.

[38] Avaro, E., Çok Modlu Kaotik Sarmal Kullanılarak Rasgele Sayı Üretimi Random Number Generation Using Multi-mode Chaotic Attractor, 0–3, 2013.

[39] Zhu, H., Zhao, C., Zhang, X., Yang, L., A novel iris and chaos-based random number generator. Computers and Security, 36, 40–48, 2013.

[40] Stojanovski, T., Kocarev, L., Chaos-based random number generators - Part I: Analysis. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 48 (3), 281–288, 2001.

[41] Li, P., Li, Z., Halang, W. A., Chen, G., A multiple pseudorandom-bit generator based on a spatiotemporal chaotic map. Physics Letters, Section A: General, Atomic and Solid State Physics, 349 (6), 467–473, 2006.

[42] Hu, Y., Liao, X., Wong, K. wo, Zhou, Q., A true random number generator based on mouse movement and chaotic cryptography. Chaos, Solitons and Fractals, 40 (5), 2286–2293, 2009.

[43] Sun, F., Liu, S., Cryptographic pseudo-random sequence from the spatial chaotic map. Chaos, Solitons and Fractals, 41 (5), 2216–2219, 2009.

[44] Ergün, S., Özoğuz, S., Truly random number generators based on a non-autonomous chaotic oscillator. AEU - International Journal of Electronics and Communications, 61 (4), 235–242, 2007.

[45] Cicek, I., Pusane, A. E., Dundar, G., A novel design method for discrete time chaos based true random number generators. Integration, the VLSI Journal, 47 (1), 38–47, 2014.

[46] Cicek, I., Pusane, A. E., Dundar, G., A novel dual entropy core true random number generator. 8th International Conference on Electrical and Electronics Engineering (ELECO), (February), 332–335, 2013.

[47] Pareschi, F., Setti, G., Rovatti, R., Implementation and Testing of High-Speed CMOS True Random Number Generators Based on Chaotic Systems. IEEE Transactions on Circuits and Systems I: Regular Papers, 57 (12), 3124–3137, 2010.

[48] Kanso, A., Smaoui, N., Logistic chaotic maps for binary numbers generations. Chaos, Solitons and Fractals, 40 (5), 2557–2568, 2009.

[49] Zhao, L., Liao, X., Xiao, D., Xiang, T., Zhou, Q., Duan, S., True random number generation from mobile telephone photo based on chaotic cryptography. Chaos, Solitons & Fractals, 42 (3), 1692–1699, 2009.

[50] Nian-sheng, L., Pseudo-randomness and complexity of binary sequences generated by the chaotic system. Communications in Nonlinear Science and Numerical Simulation, 16 (2), 761–768, 2011.

[51] Tang, G., Liao, X., Chen, Y., A Novel Method for Designing S-boxes based on Chaotic Maps. Chaos, Solitons & Fractals, 23 (2), 413–419, 2005.

[52] Peng, J., Jin, S., Lei, L., Liao, X., Construction and Analysis of Dynamic S-boxes Based on Spatiotemporal Chaos. Cognitive Informatics & Cognitive Computing (ICCI* CC), 2012 IEEE 11th International Conference on. IEEE, 2012.

[53] Özkaynak, F., Özer, A. B., A method for designing strong S-Boxes based on chaotic Lorenz system. Physics Letters, Section A: General, Atomic and Solid State Physics, 374 (36), 3733–3738, 2010.

[54] Zaïbi, G., Kachouri, A., Peyrard, F., Foumier-Prunaret, D., On dynamic chaotic S-BOX. 2009 Global Information Infrastructure Symposium, GIIS ’09, (2), 1–5, 2009.

[55] Zaibi, G., Peyrard, F., Kachouri, A., Fournier-Prunaret, D., Samet, M., Efficient and secure chaotic S-Box for wireless sensor network. Security and Communication Networks, 7 (2), 279–292, 2014.

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

[57] Ozkaynak, F., Yavuz, S., Designing chaotic S-boxes based on time-delay chaotic system. Nonlinear Dynamics, 74 (3), 551–557, 2013.

[58] Asim, M., Jeoti, V., Hybrid chaotic image encryption scheme based on S-box and ciphertext feedback. 2007 International Conference on Intelligent and Advanced Systems, ICIAS 2007, , 736–741, 2007.

[59] Peyrard, F., Kachouri, A., Samet, M., A new design of dynamic S - Box based on two chaotic maps. ACS/IEEE International Conference on Computer Systems and Applications-AICCSA 2010. IEEE, 2010.

[60] Tang, G., Liao, X., A method for designing dynamical S-boxes based on discretized chaotic map. Chaos, Solitons and Fractals, 23 (5), 1901–1909, 2005.

[61] Chen, G., Chen, Y., Liao, X., An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps. Chaos, Solitons and Fractals, 31 (3), 571–579, 2007.

[62] Khan, M., Shah, T., Mahmood, H., Gondal, M. A., Hussain, I., A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems. Nonlinear Dynamics, 70 (3), 2303–2311, 2012.

[63] Hussain, I., Shah, T., Gondal, M. A., A novel approach for designing substitution-boxes based on nonlinear chaotic algorithm. Nonlinear Dynamics, 70 (3), 1791–1794, 2012.

[64] Hussain, I., Shah, T., Mahmood, H., Gondal, M. A., Construction of S8 Liu J S-boxes and their applications. Computers & Mathematics with Applications, 64 (8), 2450–2458, 2012.

[65] Hussain, I., Gondal, M. A., Hussain, A., Construction of Substitution Box Based on Piecewise Linear Chaotic Map and S8 Group. 3D Research, 6 (1), 2015.

[66] Chen, G., A novel heuristic method for obtaining S-boxes. Chaos, Solitons and Fractals, 36 (4), 1028–1036, 2008.

[67] Wang, Y., Wong, K. W., Liao, X., Xiang, T., A block cipher with dynamic S-boxes based on tent map. Communications in Nonlinear Science and Numerical Simulation, 14 (7), 3089–3099, 2009.

[68] Wang, Y., Xie, Q., Wu, Y., Du, B., A software for S-box performance analysis and test. Proceedings - 2009 International Conference on Electronic Commerce and Business Intelligence, ECBI 2009, 125–128, 2009.

[69] Arroyo, D., Li, C., Li, S., Alvarez, G., Halang, W. A., Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm. Chaos, Solitons and Fractals, 41 (5), 2613–2616, 2009.

[70] Alvarez, G., Li, S., Cryptanalyzing a nonlinear chaotic algorithm (NCA) for image encryption. Communications in Nonlinear Science and Numerical Simulation, 14 (11), 3743–3749, 2009.

[71] Rhouma, R., Belghith, S., Cryptanalysis of a spatiotemporal chaotic cryptosystem. Chaos, Solitons and Fractals, 41 (4), 1718–1722, 2009.

[72] Arroyo, D., Alvarez, G., Amigó, J. M., Li, S., Cryptanalysis of a family of self-synchronizing chaotic stream ciphers. Communications in Nonlinear Science and Numerical Simulation, 16 (2), 805–813, 2011.

[73] Solak, E., Çokal, C., Algebraic break of a cryptosystem based on discretized two-dimensional chaotic maps. Physics Letters, Section A: General, Atomic and Solid State Physics, 373 (15), 1352–1356, 2009.

[74] Li, C., Li, S., Alvarez, G., Chen, G., Lo, K. T., Cryptanalysis of a chaotic block cipher with external key and its improved version. Chaos, Solitons and Fractals, 37 (1), 299–307, 2008.

[75] Solak, E., Rhouma, R., Belghith, S., Cryptanalysis of a multi-chaotic systems based image cryptosystem. Optics Communications, 283 (2), 232–236, 2010.

[76] Li, C., Li, S., Lo, K. T., Breaking a modified substitution-diffusion image cipher based on chaotic standard and logistic maps. Communications in Nonlinear Science and Numerical Simulation, 16 (2), 837–843, 2011.

[77] Özkaynak, F., Bedri, A., Cryptanalysis of a new image encryption algorithm based on chaos. Optik- International journal for light and electron optics., 127 (13), 5190–5192, 2016.

[78] Çokal, C., Solak, E., Cryptanalysis of a chaos-based image encryption algorithm. Physics Letters, Section A: General, Atomic and Solid State Physics, 373 (15), 1357–1360, 2009.

[79] Silva, R. M., Crespo, R. G., Nunes, M. S., Enhanced chaotic stream cipher for WSNs. ARES 2010 - 5th International Conference on Availability, Reliability, and Security, , 210–215, 2010.

[80] Dillak, R. Y., Digital Color Image Encryption Using RC4 Stream Cipher and Chaotic Logistic Map. Information Technology and Electrical Engineering (ICITEE), 2013 International Conference on, , 2013.

[81] Jolfaei, A., Mirghadri, A., Image Encryption Using Chaos and Block Cipher. Computer and Information Science, 4 (1), 172–185, 2011.

[82] Atteya, A. M., Madian, A. H., A Hybrid Chaos-AES Encryption Algorithm and Its Implemention Based on FPGA. 2014 IEEE 12th International New Circuits and Systems Conference (NEWCAS), 217–220, 2014.

[83] Xiao, H., Qiu, S., Deng, C., A composite image encryption scheme using AES and chaotic series. Proceedings of the 1st International Symposium on Data, Privacy, and E-Commerce, ISDPE 2007, 277–279, 2007.

[84] Challita, N., Enhancement of S-AES using chaos for the support of biomedical applications. 2013 2nd International Conference on Advances in Biomedical Engineering, 175–178, 2013.

[85] Chen, D., Qing, D., Wang, D., AES Key Expansion Algorithm Based on 2D Logistic Mapping. 2012 Fifth International Workshop on Chaos-fractals Theories and Applications, 207–211, 2012.

[86] Pradhan, C., Bisoi, A. K., Chaotıc varıatıons of AES algorithm. International Journal of Chaos, Control, Modelling and Simulation (IJCCMS), 19–25, 2013.

[87] Muhaya, F. T. Bin, Chaotic and AES cryptosystem for satellite imagery. Telecommunication Systems, 52 (2), 573–581, 2013.

[88] Ashtiyani, M., Birgani, P. M., Hosseini, H. M., Chaos-Based Medical Image Encryption Using Symmetric Cryptography. 2008 3rd International Conference on Information and Communication Technologies: From Theory to Applications, 2008.

[89] Yuan, K., Zhang, H., Li, Z., An improved AES algorithm based on chaos. 1st International Conference on Multimedia Information Networking and Security, MINES 2009, 2, 326–329, 2009.

[90] Zeghid, M., Machhout, M., Khriji, L., A modified AES based algorithm for image encryption. World Academy of Science, Engineering and Technology, 1 (1), 70–75, 2007.

[91] Acharya, A., Image encryption using a new chaos based encryption algorithm. Proceedings of the 2011 International Conference , 1–5, 2011.

[92] Stinson, D., R., Cryptography: Theory and Practice, Discrete Mathematics and Its Application. Chapman & Hall/CRC, Third Edt. , 2006.

[93] Diffie, W., Hellman, M., New directions in cryptography. IEEE transactions on Information Theory, 22(6), 644-654,1976.

[94] Mohammed, R. S., Chaos based Cryptography for Voice Encryption in Wireless Communication, Electrical, Communication, Computer, Power, and Control Engineering (ICECCPCE), 2013 International Conference on. IEEE 2013.

[95] Van Tilborg, H., Fundamentals of Cryptology. Kluwer Academic Publishers, 2000.

[96] Schneier, B., Applied Cryptography. Second Edt. Ed., John Wiley And Sons, 1996.

[97] Menezes, A., Van Oorschot, P., C. and Vanstone, S., A., Handbook of Applied Cryptography. CRC Press, 1996.

[98] Kerckhoffs, A., La cryptographie militaire. Journal des sciences militaires, 9, 5–38, 1883.

[99] Shannon CE., Communication theory of secrecy system. Bell Syst. Tech. J., 28, 656–715, 1949.

[100] Delfs, H., Knebl, H., & Knebl, H., Introduction to Cryptography. Berlin Etc.: Springer, 2002.

[101] National Institute of Standards and Technology (NIST), Data encryptıon standard (des)-fıps pub 46-3. http://csrc.nist.gov/publications/fips /fips46-3/fips46-3.pdf .

[102] National Institute of Standards and Technology (NIST), Triple Data Encryption Algorithm. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecial publication800-67ver1.pdf .

[103] National, (NIST), I. of S. and T., Advanced Encryption Standart. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf .

[104] L. Keliher, Linear Cryptanalysis of Substitution-Permutation Networks, PhD Thesis, Queen's University, 2003.

[105] Internet: Ronald L. Rivest, RC5 Encryption Algorithm. http://people.csail.mit.edu/rivest/Rivest-rc5rev.pdf .

[106] Rivest, R. L., Shamir, A., Adleman, L., A Method for Obtaining Digital Signatures and Public- Key Cryptosystems. 21 (2), 1978.

[107] Koblitz, B. N., Elliptic Curve Cryptosystems. Mathematics of computation, 4 (177), 203–209, 1987.

[108] Alvarez, G., Montoya, F., Romera, M., Pastor, G., Cryptanalysis of a chaotic secure communication system, Physics Letters A, 306 (4), 200–205, 2003.

[109] V. Rijmen, Cryptanalysis and Design of Iterated Block Ciphers, PhD Thesis, 1997.

[110] Kocher, P., Jaffe, J., Jun, B., Introduction to differential power analysis, Journal of Cryptographic Engineering, 1 (1), 5–27, 2011.

[111] Lorenz, E., Deterministic nonperiodic flow. J. Atmos. Sci., 20 (2), 130–141, 1963.

[112] Rössler, O. E., An equation for continuous chaos. Physics Letters A, 57 (5), 397–398, 1976.

[113] Chua, L. O., Wu, C. W., Huang, A., Zhong, G. Q., A Universal Circuit for Studying and Generating Chaos Part II: Strange Attractors. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 40 (10), 745–761, 1993.

[114] Lü J., Chen G., Zhang, S., Dynamical analysis of a new chaotic attractor. International Journal of Bifurcation and Chaos, 12 (5), 1001–1015, 2002.

[115] Chen G., Yet another chaotic attractor. International Journal of Bifurcation and chaos, 9 (7), 1465–1466, 1999.

[116] Sprott, J. C., Simplest Dissipative Chaotic Flow. Physics Letters A, 228 (April), 271–274, 1997.

[117] Chen C. K., Lin C. L., Lin S. L., Chiu Y. M., A chaotic theorectical approach to ECG-based identity recognition. IEEE Computational Intelligence Magazine, 1 (9), 53–63, 2014.

[118] Gagnon, F., Kaddoum, G., Lower bound on the bit error rate of a decode-and-forward relay network under chaos shift keying communication system. IET Communications, 8 (2), 227–232, 2014.

[119] Ma, X., Chen, Y., DDoS detection method based on chaos analysis of network traffic entropy. IEEE Communications Letters, 18 (1), 114–117, 2014.

[120] Kang, Z., Sun, J., Ma, L., Qi, Y., Jian, S., Multimode synchronization of chaotic semiconductor ring laser and its potential in chaos communication. IEEE Journal of Quantum Electronics, 50 (3), 148–157, 2014.

[121] Anees, A., Siddiqui, A. M., Ahmed, F., Chaotic substitution for highly autocorrelated data in encryption algorithm. Communications in Nonlinear Science and Numerical Simulation, 19 (9), 3106–3118, 2014.

[122] Belazi, A., Hermassi, H., Rhouma, R., Belghith, S., Algebraic analysis of a RGB image encryption algorithm based on DNA encoding and chaotic map. Nonlinear Dynamics, 76 (4), 1989–2004, 2014.

[123] Parashar, A., Singh, R., Panigrahi, P. K., Muralidhar, K., Chaotic flow in an aortic aneurysm. Journal of Applied Physics, 113 (21), 2013.

[124] Lones, M. A., Fuente, L. A., Turner, A. P., Caves, L. S. D., Stepney, S., Smith, S. L., Tyrrell, A. M., Artificial biochemical networks: Evolving dynamical systems to control dynamical systems. IEEE Transactions on Evolutionary Computation, 18 (2), 145–166, 2014.

[125] Hilborn, R., Chaos and Nonlinear Dynamics. Oxford University Press, 2003.

[126] Parker T., C. L., Practical Numerical Algorithms for Chaotic Systems. Springer-Verlag, 1989.

[127] Alvarez, G., Li, S., Some basic cryptographic requirements for chaos-based cryptosystems. 16 (8), 2129–2151, 2006.

[128] Kohlbrenner, P. W., The Design and Analysis of a True Random Number Generator in a Field Programmable Gate Array. Carnegie Mellon University, PhD Thesis, 2003.

[129] Marton, K., Suciu, A., Sacarea, C., Cret, O., Generation and testing of random numbers for cryptographic applications. Proceedings of the Ramanian Academy Series A, 13 (4), 368–377, 2012.

[130] Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., Vo, S., NIST Special Publication 800-22. 22, 2001.

[131] Biham, E., Shamir, A., Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, 4 (1), 3–72, 1991.

[132] Adams C. G., Tavares, S., The Structured Design of Cryptographically Good S-Boxes. The Structured Design of S-boxes, 27–41, 1990.

[133] Musa, M. A., Schaefer, E. F., Wedig, S., A simplified AES algorithm and its linear and differential cryptanalyses. Cryptologia, 27 (2), 148–177, 2003

[134] Pehlivan İ., Yeni kaotik sistemler: Elektronik devre gerçeklemeleri, senkronizasyon ve güvenli haberleşme uygulamaları. Doktora tezi, Sakarya Üniversitesi, 2007.

[135] Hilborn, R. C., Coppersmith, S., Mallinckrodt, A. J., McKay, S., Chaos and nonlinear dynamics: an introduction for scientists and engineers. Computers in Physics, 8 (6), 1994.

[136] Zhongtang, W., Wang, M., Jianxiu, J., Jiuchao, F., A Novel Strange Attractor and its Dynamic Analysis. 9 (3), 408–415, 2014.

[137] Chen, S., Synchronization of an uncertain unified chaotic system via adaptive control. Chaos, Solitons & Fractals, 14, 643–647, 2002.

[138] Baptista, M. S., Cryptography with chaos. Physics letters A, 9601 (98), 1998.

[139] Pecora, L. M., Carroll, T. L., Synchronization in Chaotic Systems. Physical Review Letters, 64 (8), 821–825, 1990.

[140] Koyuncu, İ., Kriptolojik Uygulamalar İçin Fpga Tabanlı Yeni Kaotik Osilatörlerin Ve Gerçek Rasgele Sayı Üreteçlerinin Tasarımı Ve Gerçeklenmesi. Doktora tezi, Sakarya Üniversitesi, 2014.

[141] Akgül A., Yeni kaotik sistemler ile rasgele sayı üreteci tasarımı ve çoklu-ortam verilerinin yüksek güvenlikli şifrelenmesi. Doktora tezi, Sakarya Üniversitesi, 2015.

[142] Jakimoski, G., Kocarev, L., Chaos and cryptography: Block encryption ciphers based on chaotic maps. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 48 (2), 163–169, 2001.

[143] Cohen, J., Statistical Power Analysis for the Behavioral Sciences. New York: Academic Press, 1977.

[144] Pareek, N. K., Patidar, V., Sud, K. K., Image encryption using chaotic logistic map. Image and Vision Computing, 24 (9), 926–934, 2006.

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

[146] Jolfaei A.; Mirghadri A., Encryption A New Approach to Measure Quality of Image Encryption. International Journal of Computer and Network Security, 2 (8), 38–43, 2010.

[147] Ahmed, H. E. D. H., Kalash, H. M., Allah, O. S. F., Encryption quality analysis of the RC5 block cipher algorithm for digital images. Optical Engineering, 45 (10), 2006.

ÖZGEÇMİŞ

Ünal ÇAVUŞOĞLU, 18.11.1981 tarihinde Akhisar'da doğdu. İlkokul, ortaokul ve lise eğitimini Akhisar'da tamamladı. 2007 yılında başladığı Yıldız Teknik Üniversitesi Bilgisayar Mühendisliği Bölümü'nden 2011 yılında mezun oldu. 2014 yılında Sakarya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar ve Bilişim Mühendisliği Anabilim Dalı'nda yüksek lisansını tamamladı. Doktora eğitimine Sakarya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar ve Bilişim Mühendisliğinde 2014 yılında başladı. Halen Sakarya Üniversitesi Bilgisayar ve Bilişim Bilimleri Fakültesi Bilgisayar Mühendisliği Bölümünde Araştırmacı olarak çalışmaktadır.