T.C.

FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

HİBRİT VERİ SIKIŞTIRMA ALGORİTMALARININ GELİŞTİRİLMESİ VE PRATİK UYGULAMALARI

Fırat ARTUĞER

Doktora Tezi

YAZILIM MÜHENDİSLİĞİ ANABİLİM DALI

TEMMUZ 2022

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Yazılım Mühendisliği Anabilim Dalı

Doktora Tezi

HİBRİT VERİ SIKIŞTIRMA ALGORİTMALARININ GELİŞTİRİLMESİ VE PRATİK UYGULAMALARI

Tez Yazarı
Fırat ARTUĞER

Danışman
Doç. Dr. Fatih ÖZKAYNAK

TEMMUZ 2022
ELAZIĞ

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Yazılım Mühendisliği Anabilim Dalı

Doktora Tezi

Başlığı:	Hibrit Veri Sıkıştırma Algoritmalarının Geliştirilmesi ve Pratik Uygulamaları
Yazarı:	Fırat ARTUĞER
İlk Teslim Tarihi:	02.06.2022
Savunma Tarihi:	04.07.2022

TEZ ONAYI

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına göre hazırlanan bu tez aşağıda imzaları bulunan jüri üyeleri tarafından değerlendirilmiş ve akademik dinleyicilere açık yapılan savunma sonucunda OYBİRLİĞİ ile kabul edilmiştir.

		İmza
Danışman:	Doç. Dr. Fatih ÖZKAYNAK Fırat Üniversitesi, Teknoloji Fakültesi	Onayladım
Başkan:	Prof. Dr. Davut HANBAY İnönü Üniversitesi, Mühendislik Fakültesi	Onayladım
Üye:	Prof. Dr. Burhan ERGEN Fırat Üniversitesi, Mühendislik Fakültesi	Onayladım
Üye:	Prof. Dr. Erkan TANYILDIZI Fırat Üniversitesi, Teknoloji Fakültesi	Onayladım
Üye:	Dr. Öğr. Üyesi Ali ARI İnönü Üniversitesi, Mühendislik Fakültesi	Onayladım

Bu tez, Enstitü Yönetim Kurulunun ...../...../20..... tarihli toplantısında tescillenmiştir.

İmza

Prof. Dr. Kürşat Esat ALYAMAÇ
Enstitü Müdürü

BEYAN

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım "Hibrit Veri Sıkıştırma Algoritmalarının Geliştirilmesi ve Pratik Uygulamaları" Başlıklı Doktora Tezimin içindeki bütün bilgilerin doğru olduğunu, bilgilerin üretilmesi ve sunulmasında bilimsel etik kurallarına uygun davrandığımı, kullandığım bütün kaynakları atıf yaparak belirttiğimi, maddi ve manevi desteği olan tüm kurum/kuruluş ve kişileri belirttiğimi, burada sunduğum veri ve bilgileri unvan almak amacıyla daha önce hiçbir şekilde kullanmadığımı beyan ederim.

04.07.2022

Fırat ARTUĞER

ÖNSÖZ

Veri sıkıştırma ve şifreleme günümüzün dijital dünyasında pratik uygulamalardaki en temel gereksinimlerden ikisidir. Veriyi şifrelemek için kullanılabilecek yaklaşımlardan biri blok şifreleme algoritmalarıdır. Blok şifreleme algoritmalarında yer değiştirme kutuları (substitution boxes / s-boxes) bilgi güvenliği açısından kritik bir öneme sahiptir. Çünkü yer değiştirme kutuları, bir blok şifreleme algoritmasının doğrusal olmayan bileşenidir. Bu yüzden etkili yer değiştirme kutularının tasarlanması bilgi güvenliği çalışmalarında önemli bir role sahiptir. Bu alandaki etkili çalışmalardan bir tanesi kaos tabanlı s-box yapılarıdır. Ancak kaos tabanlı s-box yapılarının en önemli dezavantajı, doğrusal olmama özelliğinin matematiksel temelli yaklaşımlara göre düşük olmasıdır. Bu tez çalışmasının önemli katkılarından biri, kaos tabanlı s-box yapılarının doğrusal olmama değerinin arttırılması için yeni yaklaşımların önerilmiş olmasıdır.

Tez çalışmasının bir diğer katkısı veri sıkıştırma alanında gerçekleştirilmiştir. Görüntülerin sıkıştırılması için en etkili çözümlerden biri JPEG algoritmasıdır. JPEG algoritmasının sıkıştırma oranını etkileyen en önemli süreçlerden bir tanesi niceleme sürecidir. Niceleme sürecinde kullanılan niceleme tablosu sıkıştırma oranına önemli etki etmektedir. Bu çalışmada alternatif niceleme tabloları tasarlanarak, sıkıştırma performansının nasıl etkileneceği incelenmiştir. Bu süreçte temel alınan hipotez kaos tabanlı s-box yapılarının üretilmesinde kullanılan mekanizmanın niceleme tablosu üretimine uyarlanmasıdır. Elde edilen sonuçlar JPEG algoritmasının performansının önerilen yöntem ile iyileştirilebileceğini göstermiştir. Önerilen yaklaşım, özellikle patoloji biliminde kullanılan tüm slayt görüntülerinin sıkıştırılmasında etkili sonuçlar vermiştir.

Bu çalışmanın her aşamasında bilgilerini, tecrübelerini ve değerli zamanını esirgemeyerek bana her fırsatta yardımcı olan doktora tez danışmanım sayın Doç. Dr. Fatih ÖZKAYNAK ‘a sonsuz teşekkürlerimi sunarım. Bilimin ve bilim insanının destekçisi olan Tübitak 'a 2211/A programı kapsamında sağladığı destekler için teşekkür ederim. Hayatım boyunca üzerimdeki emeklerini ödeyemeyeceğim Anne ve Babama teşekkür ve minnetimi özellikle belirtmek istiyorum.

Fırat ARTUĞER
ELAZIĞ, 2022

İÇİNDEKİLER

Sayfa

ÖZET

Hibrit Veri Sıkıştırma Algoritmalarının Geliştirilmesi ve Pratik Uygulamaları

Fırat ARTUĞER

Doktora Tezi

FIRAT ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü

Yazılım Mühendisliği Anabilim Dalı

Temmuz 2022, Sayfa: xii + 76

Son yılların en önemli problemleri hiç şüphesiz verilerin yüksek boyutu ve güvensiz ağlar üzerinden uzaklara iletilmesi ya da depolanmasıdır. Bu problemlerin üstesinden gelmek için genellikle sıkıştırma ve şifreleme algoritmaları kullanılmaktadır. Günümüzde şifreleme için kullanılan yaklaşımlardan biri, blok şifreleme algoritmalarıdır. Blok şifreleme algoritmalarında karıştırma gereksinimini sağlamak için en önemli kriptolojik bileşenlerden biri yer değiştirme kutularıdır (s-box). Çünkü s-box 'lar doğrusal olmayan yapılar olup, bu sayede diferansiyel kriptanalize karşı algoritmayı dirençli hale getirmektedir. Bu yüzden s-box 'ın doğrusal olmama değeri ne kadar yüksek olursa o kadar saldırılara karşı dirençli olacaktır. Kaos tabanlı s-box yapılarının en önemli dezavantajı doğrusal olmama özelliğinin matematiksel temelli s-box yapılarına göre düşük olmasıdır. Bu tez çalışmasında ilk olarak kaos tabanlı s-box yapılarının doğrusal olmama değerlerinin arttırılması için yedi farklı yaklaşım önerilmiştir. Bu yaklaşımların tamamında s-box 'ların performansı iyileştirilmiştir.

JPEG algoritmasının birçok platformda yaygın olarak kullanılmasından dolayı önemi yadsınamaz bir gerçektir. Ancak, kullanıcıların daha fazla veri depolama ve daha hızlı veri iletimi/işleme ihtiyaçlarını karşılamaya yönelik yapılabilecek iyileştirmeler dijital dönüşümle birlikte ivme kazanmıştır. Bu çalışmalardan niceleme tabloları algoritmanın başarısını etkileyen kritik bir bileşen olduğundan bu alandaki iyileştirme çalışmaları farklı niceleme tablolarının tasarımına odaklanmıştır. Bu çalışmada farklı niceleme tabloları oluşturmak için ilk kez kaotik sistemler temel alınarak bir yöntem önerilmiştir. Önerilen yöntem basit bir yapıya sahiptir ve yüksek sıkıştırma oranları elde etmektedir. Yüksek sıkıştırma oranı elde edilmesine rağmen görüntü kalitesinden ödün verilmemesi önerilen yöntemin bir diğer avantajı ve özgün yönüdür. JPEG algoritmasının performansını iyileştirmek için literatürde kullanılan bir diğer yaklaşım, niceleme tablolarının optimizasyon yöntemleri ile üretilmesidir. Önerilen yöntem bu yaklaşımlarla karşılaştırıldığında hesapsal karmaşıklığının daha düşük olması önerilen yöntemin bir diğer avantajı olarak ön plana çıkmaktadır. Bu sonuçlar, nesnelerin interneti, endüstri 4.0 ve yapay zekâ çalışmaları gibi birçok uygulama alanı için gelecekte yapılacak çalışmalarda iyileştirmeler yapılabileceğini, önemli depolama tasarrufları ve daha hızlı veri iletimi/işleme sağlanabileceğini göstermektedir.

Anahtar Kelimeler: JPEG, Kaos, Niceleme tablosu, Yer değiştirme kutusu (s-box),

ABSTRACT

Improvement of Hybrid Data Compression Algorithms and Practical Applications

Fırat ARTUĞER

Ph.D. Thesis

FIRAT UNIVERSITY
Graduate School of Natural and Applied Sciences

Department of Software Engineering

July 2022, Pages: xii + 76

The most important problems of recent years are undoubtedly the high size of data and the transmission or storage of data over insecure networks. Compression and encryption algorithms are generally used to overcome these problems. One of the approaches used for encryption today is block cipher algorithms. One of the most important cryptological components to meet the confusion requirement in block cipher algorithms is s-boxes. Because s-boxes are nonlinear structures, making the algorithm resistant to differential cryptanalysis. Therefore, the higher the nonlinearity of the s-box, the more attack resistant it will be. The most important disadvantage of chaos-based s-box structures is that their nonlinearity is lower than mathematically-based s-box structures. In this thesis, firstly, seven different approaches are proposed to increase the nonlinearity values of chaos-based s-box structures. All of these approaches have improved the performance of s-boxes.

Since the JPEG algorithm is widely used on many platforms, its importance is an undeniable fact. However, improvements that can be made to meet users' needs for more data storage and faster data transmission/processing have gained momentum with the digital transformation. As quantization tables from these studies are a critical component that affects the success of the algorithm, improvement studies in this area have focused on the design of different quantization tables. In this study, a method based on chaotic systems is proposed for the first time to create different quantization tables. The proposed method has a simple structure and achieves high compression ratios. Despite achieving a high compression ratio, not sacrificing image quality is another advantage and unique aspect of the proposed method. Another approach used in the literature to improve the performance of the JPEG algorithm is to generate quantization tables using optimization methods. When the proposed method is compared with these approaches, the lower computational complexity stands out as another advantage of the proposed method. These results show that improvements can be made in future studies for many application areas such as the internet of things, industry 4.0 and artificial intelligence studies, significant storage savings and faster data transmission/processing can be achieved.

Keywords: JPEG, Chaos, Quantization table, Substitution box (S-box),

ŞEKİLLER LİSTESİ

Sayfa

TABLOLAR LİSTESİ

Sayfa

SİMGELER VE KISALTMALAR

Simgeler

$f_{threshold}$	: Eşik değeri
B	: Mavi
G	: Yeşil
m	: Satır
n	: Sütun
Q	: Kalite faktörü
R	: Kırmızı
U	: Renklilik
V	: Renklilik
Y	: Parlaklık

Kısaltmalar

AES	: Gelişmiş şifreleme standardı
BIC	: Bitlerinden bağımsızlık kriteri
Bpp	: Piksel başına bit sayısı
DCT	: Ayrık kosinüs dönüşümü
DWT	: Ayrık dalgacık dönüşümü
GA	: Genetik algoritma
HP	: Üst geçişli
I1DS	: Bir boyutlu kaotik sistem
IFS	: Tekrarlı fonksiyon sistemleri
JPEG	: Birleşmiş fotoğraf uzmanları grubu
LP	: Alt geçişli
MSE	: Ortalama karesel hata
PSNR	: En yüksek sinyal gürültü oranı
QF	: Kalite faktörü
RGB	: Bir renk modeli
RLE	: Çalıştırma uzunluğu kodlaması
RMSE	: Kare ortalamaların karekökü hatası
ROI	: İlgi alanı
SAC	: Katı çığ kriteri
S-box	: Yer değiştirme kutusu
SSIM	: Yapısal benzerlik endeksi
WSI	: Tüm slayt görüntü
YUV	: Bir renk modeli

1. GİRİŞ

Bilim ve mühendislik çalışmaları tarih boyunca hep yeni şeylerin arayışı içerisinde olmuştur. Bu arayış serüveni boyunca araştırmacılar sürekli yeni bilgiler elde etmiş ve bu bilgi birikimini daha sağlıklı, daha rahat, daha huzurlu ve daha kaliteli yaşayabilmek için insanoğlunun hizmetine sunmuşlardır. Yaşadığımız yüzyılda ise; bu yeni bilgileri elde etme süreci üstel bir hızla ilerlemektedir. Endüstri 4.0, yapay zekâ ve nesnelerin interneti gibi kavramlar artık tüm varlıkların birbiri ile etkileşim içerisinde olduğu devasa bir bilgi kümesini ortaya çıkarmıştır. Büyük veri olarak tanımlanan bu devasa bilgi kümesi birçok alanı derinden etkilemiş ve etkilemeye de devam etmektedir [1]. Hiç şüphesiz bu etkileşimden en fazla pay alan disiplinlerden biri tıp bilimi olmuştur. Çünkü günümüzde neredeyse bilişim teknolojilerinden bağımsız bir tıp bilimi düşünmek mümkün değildir. Dijital görüntüleme teknolojilerindeki gelişmeler, tanı ve teşhis süreçlerinde akıllı yaklaşımların kullanılması, cerrahi alanında robotlardan faydalanılması, bilgisayarların hesaplama kabiliyetlerindeki iyileşmeler, modelleme ve benzetim teknolojileri ile birçok operasyonun etkilerinin önceden analiz edilebilmesi gibi sayısız yenilik bu güçlü bağın sadece birkaç örneğidir [2].

1.1. Problemin Tanımı

Her dönemin kendine has gereksinimleri bulunmaktadır. Hayatlarımızın dijitalleştiği günümüz bilgi toplumunda ise en önemli gereksinimler arasında bilginin hızlı bir şekilde iletilmesi ve efektif bir şekilde depolanabilmesi yer almaktadır. Her iki gereksinim içinde öne çıkan önemli araştırma alanlarından biri veri sıkıştırmadır. Bilgisayarlarım kullanılmaya başlandığı 1950'lerden günümüze kadar bu gereksinimleri karşılayabilmek için araştırmacılar yeni arayışlar içerisinde olmuştur. En genel ifade ile sıkıştırma, dijital ortamlarda veriyi temsil edebilmek için gerekli veri miktarını azaltma işlemidir. Veri sıkıştırma için iki temel alt dal bulunmaktadır. Kayıpsız ve kayıplı sıkıştırma olarak adlandırılan bu alt dallar aslında kullanıcı gereksinimine göre konumlandırılmıştır. Kayıpsız sıkıştırma olarak adlandırılan tekniklerde orijinal veriye tam olarak tekrar ulaşılabilmektedir. Veri kaybının kritik problemlere yol açabileceği uygulamalarda bu özellik her ne kadar kritik bir gereksinim olsa da kayıpsız sıkıştırma algoritmalarında sıkıştırma performansının düşük olması bir problemdir. Bu problem veri sıkıştırma disiplininin diğer bir alt dalı olan kayıplı sıkıştırma algoritmalarının popüler olmasına yol açmıştır. Bir miktar veri kaybının süreci etkilemeyeceği durumlarda çok daha yüksek sıkıştırma oranlarının elde edilebileceğinin gösterilmesi; araştırmacıları bu alanda yeni algoritmalar geliştirerek kaliteyi bozmadan performansın nasıl artırılabileceği sorusu üzerine araştırma yapmaya yöneltmiştir.

Ayrıca tıbbi görüntüleme yöntemlerinin son yirmi yılda dijital hale gelmesi ile birlikte tıbbi görüntüleme departmanlarında dijital görüntülerin boyutunu ve sayısını önemli ölçüde artırmıştır. Azalan depolama çözümlerinin maliyetleri, artan dijital görüntü miktarıyla eşitlenmiş veya aşılmıştır. Teletıpta, sınırlı bant genişliği ve büyük araştırmalar için ortaya çıkan görüntü aktarım süresi ciddi bir problem haline gelmiştir [3]. Örneğin 40 kat büyütmede taranan 15×15 mm 'lik bir tam slayt görüntü (Whole Slide Image - WSI) numunesi 60000×60000, 24 bit RGB renkli görüntü için 10 gigabayt (GB) 'ın üzerinde ham veriye karşılık gelmektedir. Daha düşük, daha yaygın 0,5 µm çözünürlükte bile, görüntüler 30000×30000 boyutlarında ve yaklaşık olarak 2,5 GB sıkıştırılmamış veriye karşılık gelmektedir. Ayrıca, vaka başına yaklaşık 35 tane WSI üretildiği göz önüne alınırsa her yıl onlarca veya yüzlerce terabayt görüntü verisi oluşturur. WSI 'leri depolamanın yüksek maliyetleri nedeniyle, bir klinik ortamda dijital arşivleme kullanılması, eski WSI 'lerin sabit disklerden silinmesi veya taşınması gibi bir tür görüntü yaşam döngüsü yönetimi gerektirebilir. Manyetik disk gibi daha ucuz depolama ortamlarına yedekleme ise WSI 'lerin cam slaytlara göre temel avantajlarından biri olan erişim kolaylığını ortadan kaldırmaktadır [4].

Her gün hasta kişisel sağlık bilgilerini içeren milyonlarca yeni görüntüye internet üzerinden erişilebilmektedir. Yüzlerce hastane, tıbbi ofis ve görüntüleme merkezi, güvenli olmayan depolama sistemleri çalıştırdığı için sadece internet bağlantısı ve ücretsiz indirilebilen yazılımlar kullanarak dünya genelinde 1 milyardan fazla tıbbi görüntüleme ile alakalı araştırmaya erişilebileceğini göstermiştir. Sayılar gerçekten de ürkütücü boyuttadır. Greenbone isimli firma tarafından 2019 yılının Eylül ayında 720 milyondan fazla tıbbi görüntü saklayan 24 milyon hasta muayenesinin erişilebilir olduğu gösterilmiştir. İstatistiki verilerin ölçeğinin ne kadar büyük olduğuna işaret eden bir diğer sonuç ise sadece bu çalışmadan iki ay sonra tekrarlanan analiz çalışması ile ortaya çıkarılmıştır. Erişilebilen sunucuların sayısının yarıdan fazla artarak 35 milyon hasta muayenesine ve 1,19 milyar tıbbi görüntünün erişilebilir olduğu göstermiştir [5]. Ne yazık ki bu analizler hasta mahremiyeti ihlalinin alarm verici seviyede olduğunu ve birçok kişinin sağlık sigortası dolandırıcılığı ve kimlik hırsızlığının muhtemel kurbanları olma riski taşındığını doğrulamaktadır. ABD yasaları kapsamında olan Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (HIPAA) ile tıbbi kayıtların gizli ve güvenli tutulmasını ve elektronik kişisel sağlık bilgilerinizi korumak için "güvenlik kuralı" oluşturmuştur [6]. Yasa ayrıca sağlık hizmeti sağlayıcılarını herhangi bir güvenlik açığından sorumlu tutmakta ve kanuna aykırı durumlarda cezai müeyyideler uygulamaktadır. Örneğin; ABD hükümeti Tennessee merkezli bir tıbbi izleme firmasına 300.000 'den fazla hasta verisi içeren bir izleme ifşa ettiği için 3 milyon dolar para cezası vermiştir. Ne yazık ki Ülkemiz içinde istatistikler hiç iç açıcı değildir. Sadece tarafımızdan yapılan analizler 75 milyondan fazla hasta verisinin yetkisiz şekilde erişilebilir olduğunu göstermektedir.

Bu görüntülerin etkili ve güvenli bir şekilde depolanması ve bir iletişim ağı üzerinden uzaklara iletilmesi için yeni sıkıştırma ve şifreleme algoritmalarına ihtiyaç duyulmaktadır.

1.2. Tezin Amacı

Yukarıda bahsedilen araştırma çalışmaları arasında ciddi bir popülariteye sahip algoritmalardan biride JPEG algoritması olmuştur. Bir standart olması ve birçok sayısal kamerada yaygın biçimde kullanılması JPEG algoritmasını araştırmacıların ilgi odağı haline getirmiştir. JPEG kayıplı bir sıkıştırma algoritması olduğu için ödünleşim kavramı hep ön planda olmuştur. Başka bir ifade ile algoritmanın her bir adımında yapılan seçimler/değişiklikler sıkıştırma performansı üzerine etkileri dikkate değer bir çalışma konusu olmuştur. Bu çalışmalar arasında dikkat çeken bir konu, niceleme tablosunun sıkıştırma performansı üzerinde etkisinin incelenmesi olmuştur. Bu yüzden, en iyi sıkıştırma performansını elde edebilmek için en uygun niceleme tablosunun elde edilmesi sıcak bir araştırma sorusu olmuştur. Bu tez çalışmasında bu araştırma sorusuna cevap bulmak için yeni bir alternatif önerilmektedir.

Tezin çıkış noktası kaotik sistemlerin kriptolojik yer değiştirme kutularının (substitution box / s-box) tasarımı için etkili bir alternatif olmasıdır. Yer değiştirme kutuları n-bit uzunluklu bir girişi m-bit uzunluk bir çıkışa haritalayan doğrusal olmayan bir fonksiyondur. Bu yönü ile s-box yapıları ile JPEG algoritmasının kalbi konumundaki niceleme tabloları aralında bir benzerlik vardır. Bu benzerlikten hareketle kaos temelli niceleme tabloları oluşturma ve orijinal niceleme tablosu yerine kaotik niceleme tabloları kullanılarak sıkıştırma performansına etkilerinin araştırılması tezin temel odağıdır.

JPEG ile sıkıştırılan bu görüntülerin güvenliğinin sağlanmasının en etkili yolu şifreleme yöntemleridir. Şifreleme yöntemlerinin en önemli birimlerinden bir tanesi yer değiştirme kutularıdır. Bu tezin bir diğer amacı ise, etkili s-box üretme yöntemleri geliştirmektir. Kısaca bu tez çalışmasında etkili veri yönetimi için, yeni ve güçlü niceleme ve s-box tabloları geliştirmek amaçlanmıştır.

1.3. Tezin Özgün Yönü

Literatürde var olan yöntemlerden farklı olarak kaotik sistemleri temel alan yeni niceleme tablosu üretim yöntemleri önerilmiştir. Kaos temelli niceleme tabloları oluşturma fikri ilk defa bu tez çalışmasında önerilmiştir. Önerilen yöntemler kullanılarak birçok farklı niceleme tablosunun üretilebileceği gösterilmiştir. Analiz sonuçları önerilen niceleme tabloları kullanılarak gerçekleştirilecek sıkıştırma süreci sonucunda yüksek performans değerlerinin elde edilebileceğini

göstermiştir. Ek olarak mevcut yöntemlerle kıyaslandığında hesaplama yükünün düşük olması ve basit yapısı önerilen yöntemlerin diğer avantajlarıdır.
Tezin diğer özgün yönleri ise, birçok yeni s-box üretme yöntemi ve yeni bir kaotik sistem geliştirilmiştir.

1.4. Tezin Organizasyonu

İkinci bölümde kaos tabanlı kriptolojiye değinilmiş olup, modern kriptoloji, kaos teorisi ve kaos tabanlı s-box yapıları açıklanmıştır. Üçüncü bölümde görüntü sıkıştırma yöntemleri özelinde, kayıplı sıkıştırma yöntemleri detaylı bir şekilde verilmiştir. Dördüncü bölümde tez kapsamında geliştirilen yeni s-box üreteç algoritmaları ve performans değerleri verilmiştir. Beşinci bölümde, geliştirilen kaos tabanlı niceleme tablosu üreteçleri ve performans analizleri verilmiştir. Altıncı bölümde sonuçlar tartışılmış olup gelecek çalışmalar için önerilerde bulunulmuştur.

2. KAOS TABANLI KRİPTOLOJİ

Endüstri 4.0, nesnelerin interneti ve yapay zekâ alanlarında yaşanan gelişmeler hayatımızı önemli ölçüde değiştirmiştir. Bu değişiklik birçok açıdan hayatımızı kolaylaştırmasına rağmen büyük veri olarak adlandırılan devasa bilgi kümesinin güvenliğinin nasıl garanti edileceği ciddi bir problemdir. Bu problemi adresleyebilmek için güçlü kriptolojik protokollere gereksinim duyulmaktadır. Ancak kriptoloji bilimi zor bir disiplindir. Sadece belirli güvenlik gereksinimlerinin sağlandığının gösterilmesi yeterli değildir. Geliştirilen yeni saldırılar var oldukça yeni yöntemler ve karşı önlemler sürekli olarak araştırılmalıdır. Uygulama saldırıları mevcut şifreleme protokollerini tehdit eden önemli bir kriptanaliz tekniğidir. Yan kanal analizleri olarak adlandırılan saldırı tekniği, şifreleme protokolünün bilgisayar, cep telefonu veya FPGA kartı gibi bir donanım üzerinde gerçekleştirilmesinin (implemente edilmesinin) ardından donanınım yaydığı ses, ısı, ışık ve güç tüketimi gibi ölçümleri yardımıyla algoritmanın gizli anahtarının elde edilmesi prensine dayanmaktadır.

Son zamanlarda yapılan çalışmalar kaos temelli şifreleme protokollerinin matematiksel temelli şifreleme protokollerine göre yan kanal saldırılarına karşı daha dirençli olabileceğini göstermiştir. Analizlerin ikinci aşamasında Nyberg tarafından önerilen matematiksel yöntemleri temel alan s-box yapısı yerine kaotik s-box yapıları kullanılarak AES blok şifreleme algoritmasının yan kanal analizi gerçekleştirilmiştir. İkinci tasarımın standart AES algoritmasına göre yan kanal saldırılarına karşı daha dirençli olduğu gösterilmiştir. Bir başka ifade ile; kaos tabanlı s-box yapıları bilinen en iyi s-box tasarım ölçütlerine sahip AES s-box yapısına göre yan kanal saldırılarına karşı daha dirençlidir. Ancak literatürde bu güne kadar yapılan çalışmalar incelendiğinde en iyi s-box performans ölçütlerine sahip kaos tabanlı tasarımların bile Nyberg s-box yapısına kıyasla daha kötü olduğudur. Örneğin karıştırma ve yayılma gereksinimlerinde önemli rol oynayan doğrusal olmama ölçümü için kaos temelli tasarımlarda ulaşılabilen en iyi değer 106.75 iken Nyberg yönteminde bu değer 112'dir. Ayrıca 112 değeri ulaşılabilecek üst sınır değeridir.

Kaos temelli tasarımların yan kanal saldırılarına karşı matematiksel tasarımlara göre daha dirençli olması bir fırsat iken s-box performans ölçütlerinin kötü olması bir problemdir. Aslında literatürde optimizasyon algoritmaları yardımı ile performans ölçütlerinin iyileştirilebileceğini gösteren çeşitli çalışmalar yayınlanmıştır. Ancak bu yaklaşımlarında; optimizasyon algoritmalarının getirdiği ek işlem maliyetinden dolayı diğer bir tasarım problemi bulunmaktadır. Bu tez çalışmasında kaos temelli s-box tasarımlarına çeşitli son işlem teknikleri uygulanarak s-box performans ölçütlerinin iyileştirilebileceği gösterilmiştir. Önerilen yöntemlerin pratik uygulanabilirliğinin yüksek olması, basit yapısı ve hızlı sonuç vermesi yöntemlerin avantajları olarak değerlendirilmiştir. Ayrıca ileride

farklı son işlem teknikleri kullanılarak daha iyi performans ölçütlerine sahip s-box yapılarının elde edilebileceğine ilişkin yeni bir araştırma sorusunu ortaya koymuştur.

2.1. Modern Kriptoloji

Günümüz gelişen teknolojileriyle birlikte verilerin korunma ihtiyacı her geçen gün artmaktadır. Bu verilerin güvenliğini sağlamak gün geçtikçe zorlaşmaktadır. Kriptoloji, bu verilerin korunması için en yaygın kullanılan disiplinlerin başında gelmektedir. Bu sayede veriler, saldırganlar tarafından ele geçilse bile anlamsız bir kelime topluluğundan oluşacaktır. Şifreleme için genellikle blok şifreleme yapıları kullanılmaktadır. Blok şifreleme yapıları, Shannon 'un karıştırma ve yayılma felsefesine dayanmaktadır [7,8]. Veri eşit bloklara bölünür ve her blok ayrı ayrı şifrelenir. Daha sonra bu bloklar birleştirilerek şifreli veri elde edilmiş olur. Blok şifreleme algoritmalarına bakıldığında, 2001 yılından beri AES [9] algoritması kullanılmaktadır. Bunun yanında en çok DES [10] algoritması kullanılmaktadır. AES algoritması verileri 128 bitlik bloklar halinde, 10, 12 veya 14 turda şifrelemektedir. Anahtar uzunluğu 128, 192, 256 bitten oluşmaktadır. Buda kaba kuvvet saldırılarını imkânsız hale getirmektedir. Kaba kuvvet saldırılarının yanı sıra AES algoritmasına şu ana kadar bilinen bir saldırı bulunmamaktadır. AES algoritmasının çok uzun yıllar kırılamaması ve blok şifreleme standardı olarak kullanılması öngörülmektedir.

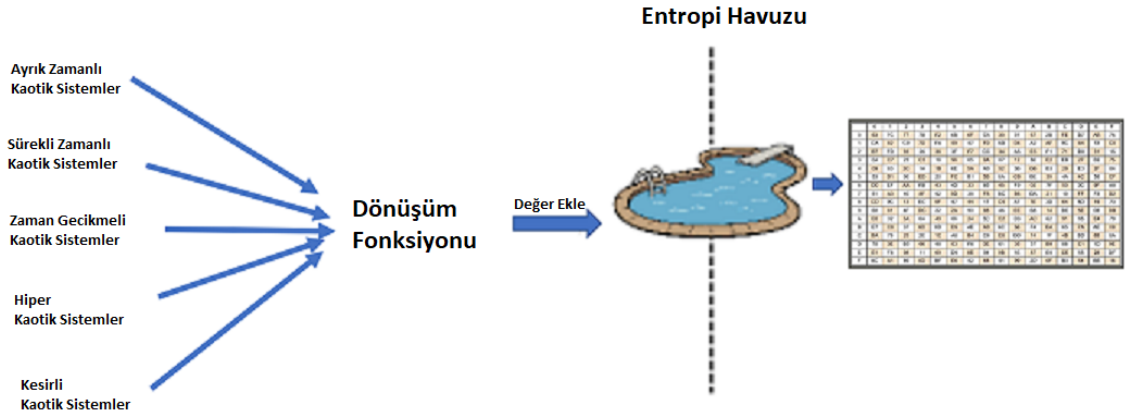
2.2. Kaos Teorisi

Bilimin gelişmesinde, doğrusal olmayan sistemler oldukça önemli bir yere sahiptir. Doğrusal olmayan sistemlere olan ihtiyaç son yıllarda ciddi bir şekilde artmıştır. Artan bu ilginin sebeplerinden bir tanesi kaos teorisinin keşfedilmesidir. Kaotik sistemlerin en önemli özelliği rastgele davranış göstermesidir [11]. Bu davranışından dolayı kaos teorisi özellikle doğrusal olmayan sistemlerde kullanılmaktadır. Ancak günümüz gelişen teknolojisi ile birlikte farklı alanlarda da uygulanabileceği düşünülmektedir.

2.3. Kaos Tabanlı S-box Yapıları

Kaos teorisi araştırmacılara bilimin birçok alanında çeşitli fırsatlar sunmaktadır. [12] İçerdiği zengin dinamikler, kaotik sistemleri her zaman ilgi odağı haline getirmiştir. Modelleme ve kontrol alanlarında kullanımının yanı sıra rastgele davranışı kriptografi uzmanlarının bu alana odaklanmasına neden olmuştur [13]. Bu ilginin arkasındaki temel fikir, karışıklık ve difüzyon gereksinimlerinin, başlangıç koşullarına ve kontrol parametrelerine duyarlı bağımlılık ilkesi ile karşılanabilmesidir. Araştırmacılar, kriptografik tasarımlarda entropi kaynağı olarak kaotik sistemleri kullanmışlardır. Kaotik sistemlerin başlangıç koşul ve kontrol parametrelerini kriptografik protokollerin gizli anahtarı olarak kullandılar. Başlangıç koşullarında ve kontrol

parametrelerinde meydana gelebilecek küçük değişikliklerle farklı çıktılar üreteceğinden, farklı başlangıç koşulları ve kontrol parametreleri kullanılarak farklı entropi kaynaklarının üretilebileceği önerilmiştir. Şekil 2.1 'de görselleştirilmeye çalışılan bu tasarım fikri kullanılarak görüntü şifreleme algoritmaları [14, 15], anahtar üreteçleri [16, 17] ve s-box tasarımları [18] gibi birçok kriptografik protokol önerilmiştir.



Şekil 2.1. Kaos tabanlı kriptografik protokol tasarımları için genel tasarım yaklaşımı

Bazı önerilerin güvenlik analizlerinin belirli kriterlere göre yapılmamış olması çeşitli güvenlik problemlerine neden olmuştur. Kaos temelli s-box tasarımları ise bu problemlerden etkilenmeyen tasarım sınıfı olmuştur. Çünkü s-box performans analizleri için kullanılan gereksinimler neredeyse standartlaşmıştır.

En basit ifade ile s-box yapıları denklem 2.1'de verilen matematiksel modele sahiptir. Başka bir ifade ile sınırlı bir aralıktaki değerleri yine sınırlı bir aralıktaki değerlere eşleştiren bijektif bir fonksiyondur. AES s-box yapısı 0 ile 255 arasındaki 256 değeri yine 0 ile 255 arasında 256 değere eşleştiren doğrusal olmayan bir fonksiyondur. Bu yüzden literatürde kaotik sistem çıkışları 256 farklı değere dönüştürülerek farklı s-box yapıları elde edilmeye çalışılmıştır. Başlangıç koşulları ve kontrol parametreleri değiştirilerek birçok farklı s-box yapısı üretilmiştir. Ayrıca s-box performans ölçütlerini iyileştirmek için farklı kaotik sistem sınıfları veya farklı dönüşüm algoritmaları da kullanılmıştır.

$$S: \begin{matrix} F_2^n \\ (x_1, \dots, x_n) \end{matrix} \rightarrow \begin{matrix} F_2^m \\ (y_1, \dots, y_m) \end{matrix} \tag{2.1}$$

Tasarım çalışmaları kaotik sistem türleri açısından sınıflandırıldığında iki genel sınıf vardır: kesikli ve sürekli zamanlı kaotik sistemler. Ayrık zamanlı sistemler tasarım sürecinde araştırmacılar için

en çok tercih edilen sistemlerden biri haline gelmiştir [19,20]. Bu seçimin temel nedeni, sistemlerin basit matematiksel modeller sayesinde çok hızlı sonuçlar üretebilmeleridir. Sürekli zamanlı sistemlerin en büyük avantajı, ayrık zamanlı sistemlere göre daha karmaşık matematiksel modellere sahip olmalarıdır [21]. Bu karmaşıklığın entropi kaynağının kalitesini olumlu yönde etkileyeceği düşünülmektedir. Sürekli zamanlı sistemlerin bu avantajını en etkin şekilde kullanmak için tasarım sürecinde hiper kaotik [22, 23], zaman gecikmeli [24, 25] ve kesirli sıralı sistemler [26, 27] gibi özel kaotik sistemler de kullanılmıştır.

Şekil 2.1 'de görselleştirilen genel tasarım mimarisinin bir diğer dikkat çekici unsuru dönüştürme işlevidir. Bu fonksiyonun amacı, kaotik sistem çıktılarını bir entropi kaynağına dönüştürmektir. Literatürde genellikle iki dönüşüm işlevi öne çıkmaktadır. Birincisi eşik değer fonksiyonudur. Denklem 2.2 'de belirtildiği gibi, kaotik sistem çıkışları bir eşik değeri ile karşılaştırılarak 0 veya 1 değerlerine dönüştürülür. Uygun eşik değerinin seçilmesi kritik bir tasarım problemidir. Birçok kaynakta eşik değer olarak 0,5 seçilirse başarılı sonuçların alınabileceği gösterilmiştir [28]. Diğer dönüştürme işlevi mod işlevidir. Mod fonksiyonunun tek yönlü bir fonksiyon olması ve çeşitli istatistiksel özellikleri garanti etmesi nedeniyle çeşitli avantajlara sahip olacağı çeşitli çalışmalarda değerlendirilmiştir [29]. Bu avantajlardan dolayı önerilen yöntemde mod fonksiyonu kaotik entropi kaynağını s-box yapılarına dönüştürmek için kullanılmıştır.

$$f_{threshold}(x): \begin{cases} 0 & x \leq 0.5 \\ 1 & x > 0.5 \end{cases} \quad (2.2)$$

2.3.1. S-box Performans Değerlendirme Kriterleri

Güçlü s-box ‘lar tasarlamak oldukça zor bir problemdir. Bu problemin üstesinden gelebilmek için 5 farklı değerlendirme kriteri vardır. Bunlar, eşit olası giriş-çıkış XOR dağılımı, katı çığ kriteri, bijektiflik, çıkış bitlerinden bağımsızlık kriteri ve en önemlisi doğrusal olmama kriteridir.

Giriş-çıkış XOR dağılımı:
Giriş-çıkış XOR dağılım tablosundaki dengesizliği temel alan bir S-box için diferansiyel kriptanaliz Biham ve Shamir tarafından önerilmiştir[30]. Çıkışta oluşan XOR değerleri, girişlerde oluşan XOR değerleri ile aynı olasılığa sahip olmalıdır. Başka bir ifadeyle bir s-box ‘ın giriş-çıkış olasılık dağılımına izin verilmediğinde, bu sistem diferansiyel kriptanalize karşı dirençli hale gelir.

Katı çığ kriteri (SAC):
SAC kriteri, bir giriş biti değiştirildiğinde her bir çıkış bitinin değişme olasılığını ölçmektedir [31]. Bu testin sonucu bir n×n matrisidir. Satır i ve sütun j matrisi için, giriş biti olan i değiştiğinde çıkış biti j ’nin de değişme olasılığını göstermektedir. Bu kriterde en iyi çözümün 0,5 olduğu tespit

edilmiştir. Her bir değerin SAC değeri 0,5 veya bu değer yakın bir değer olduğunda giriş ve çıkıştaki bitlerin birbirinden bağımsız olduğu söylenebilir.

Bijektiflik:

Bijektiflik temelde bir fonksiyonun birebir ve örten olması anlamına gelmektedir. Bizim önerdiğimiz s-box 0 ile 255 arasındaki değerlerin her birini bir kez kullanmaktadır.

Bitlerinden bağımsızlık kriteri (BIC):

BIC kriteri, iki bitin birbirinden bağımsız bir şekilde değişmesi gerektiği ifade etmektedir. Diğer bir deyişle, bir bitin diğerinden çıkarılmasının mümkün olmadığı bir olayın meydana gelişinin bağımsızlığını değerlendirmektedir [31]. BIC değerinin çıktısı hem yüksek oranda doğrusal olmamalı hem de SAC değerini karşılamalıdır.

Doğrusal olmama kriteri:

Bir kriptosistemin doğrusal olmayan bir saldırıya karşı dirençli olabilmesi için, kullandığı s-box 'ın yüksek doğrusal olmama değerine sahip olması gerekir [31]. Çünkü çoğu şifreleme sisteminde doğrusal olmayan tek birim s-box 'lar dır.

2.3.2. Mevcut Çalışmaların Temel Karakteristikleri

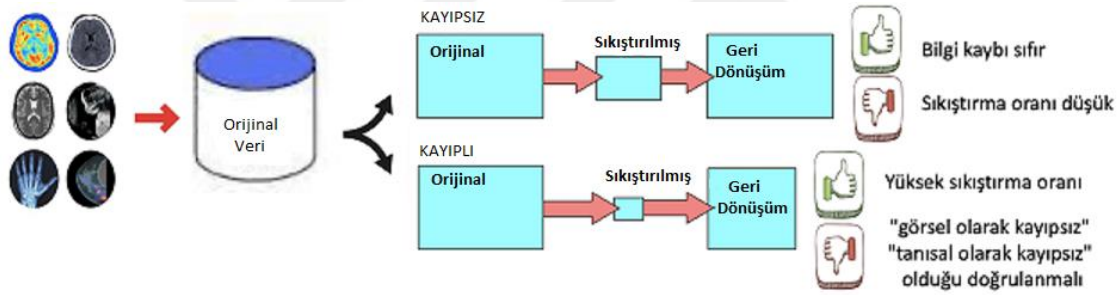
Literatüre bakıldığında s-box geliştirmek için farklı yaklaşımlar kullanılmıştır. Bu yaklaşımların başında kaos, matematiksel dönüşüm ve optimizasyon tabanlı olanlar gelmektedir. Ancak bu yöntemlerin bazı dezavantajları mevcuttur. Kaos tabanlı yöntemler rastgelelik olarak güçlüdürler, ancak düşük doğrusal olmama değerine sahip olmaları önemli bir sorundur. Bunun yanında matematiksel ve optimizasyon tabanlı yöntemlerde yüksek doğrusal olmama değerine sahip s-box 'lar üretilmektedir. Ancak bu yöntemlerde hesaplama karmaşıklığı oldukça yüksektir. Bu tez çalışmasının bir amacı kaos tabanlı s-box 'ların doğrusal olmama değerlerini olabildiğince yükselten akıllı ve güçlü algoritmalar geliştirmektir.

Son yıllarda yapılan bazı çalışmalar şöyledir: [32] 'de GF (2^8) üzerindeki projektif çizgi üzerindeki eylemi için koset grafiği yardımıyla s-box geliştirmek için yeni bir yöntem geliştirilmiştir. [33] 'de yüksek doğrusal olmama değerine sahip anahtara bağlı dinamik bir s-box yapısı önermektedir. Bu yöntem, kesirli sıralı zaman gecikmeli Hopfield sinir ağına dayalı olarak geliştirilmiş doğrusal olmayanlık için başlangıçta oluşturulan s-box evrimini içerir. [34] 'de yazarlar ayrık hiper kaos haritalama ve cebirsel grup teorisinin birleşik yapısını kullanan, kriptografik ikame kutuları üretmeye yönelik yeni bir yöntem önermektedir. [35] 'de yazarlar en çok kullanılan optimizasyon algoritmalarından biri olan genetik algoritmayı kullanarak etkili s-box 'lar üretmeyi önermektedir.

[36] ‘da yazarlar parçacık sürü optimizasyonu algoritması yardımıyla güvenlik uygulamalarında kullanılabilecek etkili s-box ‘lar geliştirilebileceğini göstermişlerdir. [37] ‘de kaotik haritalara ve kompozisyon yöntemine dayalı rastgele ikili s-box ‘lar elde oluşturmak için yeni bir yöntem önerilmiştir. [38] ‘de 8 × 8 etkili s-box ‘lar geliştirmek için ateş böceği algoritması optimizasyonu tabanlı metasezgisel bir yaklaşım kullanılmıştır. [22] ‘de yeni ve etkili bir hiperkaotik sistemin karmaşık yapısına dayanan kriptografik olarak oldukça güçlü s-box ‘lar oluşturmak için yeni bir yöntem önerilmiştir. [39] ‘da yazarlar s-box üretme problemini öncelikle gezgin satıcı problemine dönüştürmüşlerdir. Daha sonra genetik algoritma ve kaos temelli yeni bir s-box üretme şeması önermişlerdir. [40] ‘da yazarlar s-box üretme probleminin üstesinden gelebilmek için, yapay arı kolonisi algoritması temelli kaotik bir şema geliştirmişlerdir. [41] ‘de şifreleme güvenliğini artırmak için Lucas serisi temelli s-box ‘lara odaklanan yeni bir kuantum tabanlı renkli görüntü şifreleme yaklaşımı sunulmaktadır. [42] ‘de birbiri içine geçmiş lojistik harita ve bakteriyel yiyecek arama optimizasyonu temelli yenilikçi bir kaotik s-box üretme yöntemi önerilmiştir. [43] ‘de etkili bir s-box elde etmek için karınca kolonisi optimizasyonu algoritması ve kaosu temel alan yeni bir meta sezgisel yöntem önerilmiştir. [44] ‘de kaotik sistemlerin s-box üretiminde nasıl kullanılabileceğini gösteren yeni bir yöntem önerilmiştir. [45] ‘de geliştirilmiş tek boyutlu ayrık kaotik bir haritayı temel alan rastgele ikili s-box ‘lar oluşturmak için yeni bir yöntem önerilmiştir. [46] ‘da yüksek doğrusal olmama değerlerine ulaşmak için öğretme-öğrenme tabanlı yeni bir optimizasyon şeması sunulmuştur. [47] ‘de görüntü şifreleme için yeni bir kaos tabanlı hibrit şifreleme algoritması önerilmiştir. Bu algoritmayı tasarlamak için Zhongtang kaotik sistemi kullanılmıştır. Bu yöntem ile etkili ve güvenli rastgele sayı üreteci s-box üreteci elde edilmiştir. [48] ‘de kaotik sinüs haritasını temel alan yeni bir s-box üreteci için etkili bir yöntem önerilmiştir. [49] ‘da biyometrik veriler kullanılarak rastgele seçim tabanlı yeni bir s-box üreteci önerilmiştir. [50] ‘de uzay-zaman doğrusal olmayan kaotik sistem yardımıyla rastgele bir s-box üretmek için yeni bir yöntem sunulmuştur.

3. GÖRÜNTÜ SIKIŞTIRMA

Sıkıştırmanın amacı görüntüyü kodlamak için gereken hafıza miktarının mümkün olduğunca azaltılmasıdır. Yani görüntünün boyutunun mümkün olduğunca düşürülmesi işlemidir. Teknolojisinin artarak büyümesiyle, görüntü aktarımı ve depolamaya olan talep hızlı bir şekilde artmaktadır. Bilgisayar teknolojisindeki gelişmeler toplu depolama ve dijital işleme için, görüntülerin aktarımı ve depolanmasının verimliliğini artırmak için ileri veri sıkıştırma tekniklerini uygulamanın yolunu açtı. Görüntü işleme teknolojisinin önemli bir parçası olan görüntü sıkıştırma, görsel sinyal iletim ve iletişim gibi bazı alanlarda uygulanmıştır [51]. Görüntü sıkıştırma yöntemleri genel olarak kayıplı ve kayıpsız olmak üzere iki sınıfta toplanmaktadır. Kayıpsız sıkıştırmada görüntü geri dönüştürüldüğünde hiçbir veri kaybolmaz, ancak sıkıştırma oranı düşüktür. Kayıplı yöntemlerde ise bir miktar veri kaybolur, ancak sıkıştırma oranı daha yüksektir. Bu algoritmaların avantaj ve dezavantajları şekil 3.1'de görselleştirilmeye çalışılmıştır.



Şekil 3.1. Kayıplı ve kayıpsız görüntü sıkıştırma algoritmalarının avantaj ve dezavantajları

3.1. Kayıpsız Görüntü Sıkıştırma

Kayıpsız görüntü sıkıştırma yöntemlerinde kodlanan görüntü belli oranlarda sıkıştırılır. Sıkıştırılmış görüntü geri dönüştürüldüğünde orijinal görüntünün aynısı elde edilir. Yani görüntüde bir kayıp meydana gelmez. Ancak kayıplı yöntemlerle kıyaslandığında sıkıştırma oranı oldukça düşük kalmaktadır. En büyük dezavantajı budur. Bu algoritmalar genellikle medikal görüntülerde kullanılmaktadır. Kayıpsız görüntü kodlama tekniklerinin en çok bilinenleri, RLE(Run Length Encoding), Huffman kodlama ve Aritmetik kodlamadır.

3.1.1. Çalıştırma Uzunluğu Kodlaması (RLE-Run Length Encoding)

Bütün veri tipleri için kullanılabilecek bir kodlama olmasına rağmen, aynı sembolün ardışık olarak çok defa tekrar etmesi durumunda iyi bir sıkıştırma performansı elde ettiği için, genellikle görüntü

sıkıştırmada kullanılır. RLE, bir değerin ardışık olarak çok sayıda tekrar etmesi durumunda, o değeri bir defa kodlayıp, daha sonra tekrar sayısını kodlama mantığına dayanmaktadır [52]. Örneğin 1-bit renk derinliğine sahip, yani sadece siyah ve beyaz renkte olan bir görüntünün bir satırındaki 1000 pikselin renkleri sırayla; önce 350 adet beyaz, ardından 250 adet siyah ve daha sonra yine 400 adet beyaz düzeninde ise, o satır RLE ile (350, 250, 400) şeklinde kodlanabilir. Burada kod çözücünün ilk pikselin ne renk olduğunu bilmesi gerekmektedir. Ya ilk pikselin rengi kodlamanın başında belirtilir, ya da ilk pikselin her zaman beyaz olduğu kabul edilir. Bu durumda ilk 350 piksel siyah olsaydı önce 0 ardından 350 kodlanacaktı.

3.1.2. Huffman Kodlama

Bilgisayar bilimlerinde veri sıkıştırmak için kullanılan bir kodlama yöntemidir. Kayıpsız olarak veriyi sıkıştırıp tekrar açmak için kullanılır. Huffman kodlamasının en büyük avantajlarından birisi kullanılan karakterlerin frekanslarına göre bir kodlama yapması ve bu sayede sık kullanılan karakterlerin daha az, nadir kullanılan karakterlerin ise daha fazla yer kaplamasını sağlamasıdır. Şayet bütün karakterlerin dağılımı eşitse yani aynı oranda tekrarlanıyorsa, bu durumda Huffman kodlaması aslında blok sıkıştırma algoritması (örneğin ASCII kodlama) ile aynı başarıya sahiptir [53]. Ancak bu teorik durumun gerçekleşmesi neredeyse imkânsız olduğu için her zaman daha başarılı sonuçlar verir.

3.1.3. Aritmetik Kodlama

Aritmetik kodlamanın temeli, kodlanacak veri parçasını 0 ile 1 arasında gerçek sayı aralığı ile temsil etmeye dayanır [54]. Veri kümesindeki her sembol bu sayı aralığını daraltır. Veri içerisindeki sembolün kullanım sıklığı az olanlar bu aralığı hızlı şekilde daraltırken fazla olanlar aralığı daha az daraltır. Kullanım sıklığı fazla olan semboller aralığı daha az daralttığından onu temsil eden bit sayısı, Huffman algoritmasında da olduğu gibi, azdır. Veride tekrar eden semboller çoksa veri az sayıda bit ile kodlanabilir. Alfabenin küçük olduğu ve karakterlerin tekrar etme sıklığında büyük farklar olduğu durumlarda, Huffman Kodlaması etkinliğini yitirirken, Aritmetik kodlama bu durumlarda daha başarılıdır.

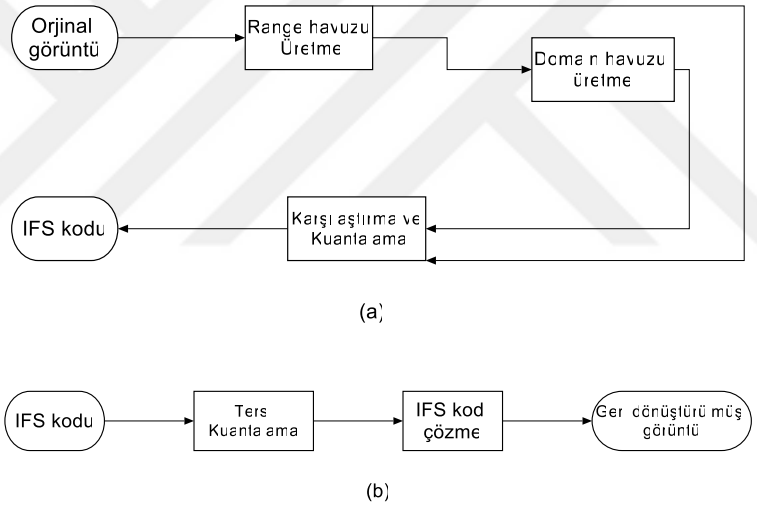
3.2. Kayıplı Görüntü Sıkıştırma

Kayıplı görüntü sıkıştırma yöntemlerinde kodlanan görüntü belli oranlarda sıkıştırılır. Sıkıştırılmış görüntü geri dönüştürüldüğünde bir miktar kayıp meydana gelmektedir. Ancak kayıpsız yöntemlerle kıyaslandığında sıkıştırma oranı oldukça yüksektir. En büyük avantajı budur. Bu algoritmalar genellikle belli kayıpların önemli olmadığı görüntülerde kullanılmaktadır. Kayıplı

görüntü kodlama tekniklerinin en çok bilinenleri, Fraktal kodlama, Ayrık dalgacık dönüşümü tabanlı(JPEG2000), Ayrık kosinüs dönüşümü tabanlı(JPEG) olarak verilebilir.

3.2.1. Fraktal Kodlama

Fraktal sıkıştırma, görüntünün benzer bölümlerini taklit etme üzerine kurulu bir yöntemdir[55]. Bu benzerlikler tekrarlı fonksiyon sistemleri yani IFS olarak adlandırılır. Tabii ki, bu özelliklerin taklit edilmesi doğal olarak sorunlu olacaktır. Bu bağlamda ele alınan amaçlar için orijinal görüntüyü doğru bir biçimde ifade etmelidir. Sıkıştırma ve analiz yöntemlerinden kaynaklanan bir başka zorluk, görüntüleri sıkıştırmak için mevcut yöntemlerin sıkıştırma oranlarının genellikle tolere edilebilir seviyeden düşük olmasıdır [56]. Bu nedenle, sorunu çözmek ve uygulamaların ihtiyacını karşılamak için yeni ve verimli sıkıştırma algoritmaları geliştirmek zorunlu hale gelmiştir. Fraktal yöntemler belirtilen problemleri doğru ve etkili bir şekilde çözme potansiyelini sağlar. Fraktal kodlama sistem modeli şekil 3.2 ‘de verilmiştir.



Şekil 3.2. Fraktal Görüntü Sıkıştırma Sistemi Modeli (a-Kodlama birimi, b- Kod çözme birimi)

Fraktal görüntü sıkıştırma algoritmasının adımları aşağıda açıklanmıştır.

Adım 1. Görüntüyü bölme ve her bölüm için dönüşümler bulma;

Adım 2. Görüntüyü kodlama (Sıkıştırma, encoding)

Adım 3. Görüntünün kodunu çözmek (Sıkıştırmayı açma, decoding).

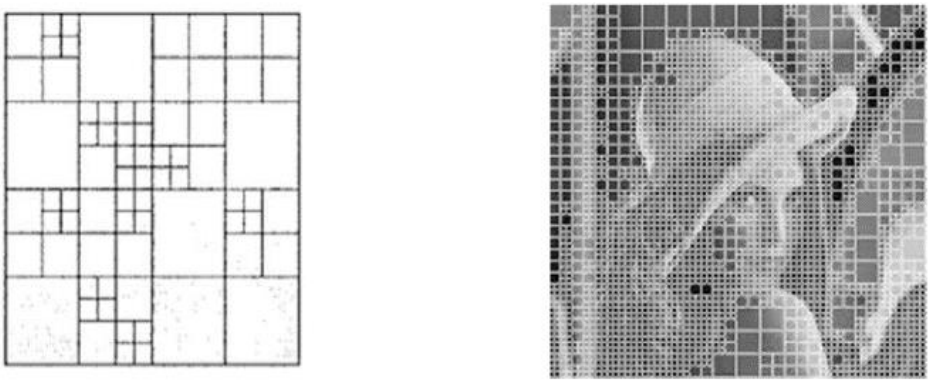
Görüntüyü Bölme:

Uygun bir görüntü veri yapısı ya da görüntü parçalamanın uygun bir yolunu seçmek çok önemlidir. Çünkü görüntüleri parçalamanın metodu konuyla ilgili geliştirilen algoritmanın adımlarıyla yakından ilişkilidir. Verilerin biçimi, verilerin alınma biçimini ve veriler üzerinde en etkin biçimde

kullanılan işleme yöntemlerini belirler. Belirli bir sayı için doğru görüntü verilerini bölümlendirme yöntemi seçilirse, sorunun çözümü basitleştirilir. Fraktal görüntü sıkıştırma sorunu için, görüntülerin düzen derecesi, basitliği ve verimliliği nedeniyle görüntülerin parçalanması için genellikle quadtree bölme tekniği kullanılmaktadır.

Quadtree Bölme Yöntemi:

Bu yöntemde parçalama işlemi belli bir eşik değerinin altına düşmediği sürece görüntü sürekli dört eşit parçaya bölünür. Bu yüzden görüntüde detayın fazla olduğu yerler daha fazla parçalanır. Yani daha küçük parçalarla ifade edilir. Detayın az olduğu yerlerde ise daha az parçalanma meydana gelir. Yani daha büyük parçalar kabul görür. Küçük parçalara range, büyük parçalara ise domain adı verilir. Parçalar ne kadar küçük olursa sıkıştırma oranı azalır ve görüntü kalitesi artar. Aynı şekilde parçalar ne kadar büyük olursa sıkıştırma oranı artar ancak görüntü kalitesi düşer. Quadtree bölme tekniği ile bölünmüş bir görüntü örneği şekil 3.3 ‘de verilmiştir.



Şekil 3.3. Quadtree parçalama örneği

Görüntüyü Kodlama:

Kodlama işleminde görüntü range ve domainlere parçalanır. Yani range havuzu ve domain havuzu elde edilir. Daha sonra her range tüm domainlerle karşılaştırılır ve en yakın olan domain bilgileri kaydedilir. Bu şekilde bütün range havuzu bu işlemlerden geçirilerek kodlama işlemi tamamlanır.

Görüntünün Kodunu Çözme:

Kod çözme algoritmasında ise önceden kaydedilmiş bilgiler kullanılarak işlemler tersten gerçekleştirilerek görüntünün kodu çözülmüş olur.

3.2.2. Ayrık Dalgacık dönüşümü Tabanlı(JPEG2000)

JPEG2000 standardı, JPEG standardının kısıtlamalarını gidermek ve yüksek kalitede görüntüler elde etmek amacıyla tasarlanmıştır [57]. JPEG2000, ayrık dalgacık dönüşümü(DWT) tabanlı görüntü sıkıştırma standardıdır. 2000 yılında, orijinal ayrık kosinüs dönüşümü tabanlı JPEG standardı [58] yerine geçmek amacıyla Birleşmiş Fotoğraf Uzmanları Grubu komitesi tarafından oluşturuldu. JPEG2000 'in JPEG 'e göre sıkıştırma performansında artış olurken, JPEG2000 'in sunduğu başlıca avantaj, kod akışının önemli esnekliğidir. JPEG2000 ile bir görüntünün sıkıştırılmasından sonra elde edilen kod akışı doğada ölçeklenebilir, birçok yolla kodu çözülebilir [59]. Örneğin, kod akışının herhangi bir noktada kesilmesiyle, görüntünün daha düşük bir çözünürlükte veya sinyal-gürültü oranında bir temsili elde edilebilir. Bununla birlikte, bu esnekliğin bir sonucu olarak, JPEG2000 karmaşık ve hesaplama gerektiren kodlayıcı ve kod çözücüleri gerektirir. Ayrıca JPEG2000' in JPEG'den üstünlükleri aşağıda maddeler halinde verilmiştir.

- Renkli görüntülerde 48-bit, gri-tonlamalı görüntülerde 16-bit renk uzayına olanak sağlar.
- Kaliteden ödün vermeden daha yüksek sıkıştırma oranı sağlar.
- JPEG' deki en büyük dezavantajlardan biri; görüntü önce 8×8'lik bloklara ayrılıp daha sonra DCT uygulandığı için, özellikle yüksek sıkıştırma oranlarında bloklar arası geçişin keskinleşmesi ve gözle fark edilir hale gelmesidir. Özellikle 1/30 'dan yüksek oranlarda sıkıştırmış görüntülerde bloklar belli olur. JPEG2000 'de böyle bir bloklama yapısı olmadığı için bu dezavantaj ortadan kalkmıştır.
- Görüntüdeki önemli parçaların daha yüksek kalitede önemsiz parçaların ise daha düşük kalitede sıkıştırılmasına olanak tanımasıdır.
- Kayıpsız sıkıştırmaya da izin verir.

JPEG2000 görüntü sıkıştırma algoritması temel olarak aşağıdaki adımlardan meydana gelmektedir.

RGB 'den YUV 'a dönüşüm veya RCT:

Burada kullanılan YUV yöntemi JPEG yöntemindeki YUV yöntemidir. RGB yöntemi ise kayıpsız sıkıştırmaya olanak tanıyan bir dönüşümdür ve bu dönüşümün formülü denklem 3.1 'de gösterilmektedir.

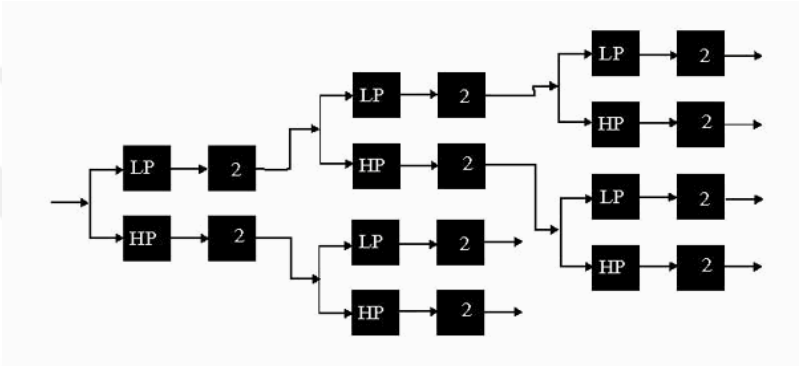
$$G = Y_r - \left\lfloor \frac{U_r + V_r - 2}{4} \right\rfloor, \quad Y_r = \left\lfloor \frac{R + 2G + B}{4} \right\rfloor$$
$$\mathrm{R} = U_r + G \qquad U_r = R - G \tag{3.1}$$
$$\mathrm{B} = V_r + G \qquad V_r = B - G$$

Görüntüyü Parçalama (Tiling):

Bu adımda görüntü bloklara ayrılır. Daha sonra her bir blok ayrı bir şekilde sıkıştırılır. Bu adım eğer istenildiğinde görüntünün tamamını değil sadece belli bölümlerini geri açabildiği için önemlidir.

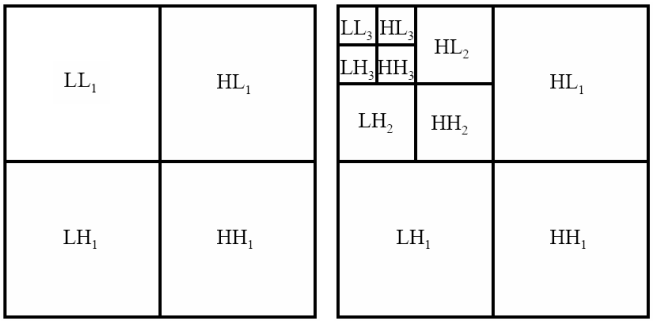
Ayrık dalgacık dönüşümü (DWT) kullanarak, piksel bilgisini uzamsal etki alanından frekans etki alanına çevirme:

Dalgacıklar veriyi farklı frekans bileşenlerine ayırmak için kullanılan matematiksel fonksiyonlardır. DWT, şekil 3.4 'de gösterildiği gibi birçok alt-geçişli (LP, low - pass) ve üst-geçişli (HP, high - pass) sayısal filtre serisi ile gerçekleştirilebilir.



Şekil 3.4. DWT geçişleri

Bir görüntünün dalgacık ayrıştırmasında, ayrıştırma önce satır satır, daha sonra sütun sütun gerçekleştirilir. Örneğin N×M boyutlarında bir görüntü için, önce her satır filtrelenir ve filtre çıkışı iki adet N×(M/2) boyutunda görüntü elde etmek için alt örneklenir. Daha sonra her sütun filtrelenir ve dört adet (N/2)×(M/2) boyutunda görüntü elde etmek için alt örneklenir. Her alt görüntü aranılan alt-bant yapısı sağlanana kadar şekil 3.5 'de gösterildiği gibi dörde bölünmeye devam eder.



Şekil 3.5. DWT ayrıştırma

ROI kodlaması (Region of Interest):

ROI kodlamasında, görüntünün belirli bölgeleri daha yüksek kalitede, diğer yerleri daha düşük kalitede kodlanır. Görüntülerin belli parçalarının daha iyi kodlanmasını istediğimiz uygulamalar için bu adım kullanışlıdır.

DWT dönüşümü sonuç değerlerini Niceleme:

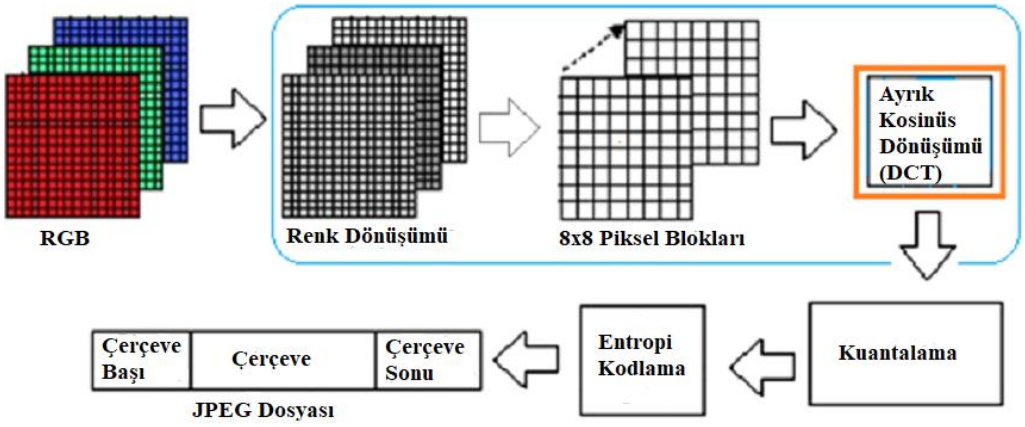
Niceleme adımı DWT' nin kademeli yapısına uygun olarak tasarlanmıştır. Bu adımda kayıplar meydana gelmektedir. Temel amaç JPEG 'de olduğu gibi yüksek katsayılı olan frekansları sıfıra indirgemektir.

Entropi Kodlama:

Kodlama işlemi algoritmanın son adımıdır. Kodlama işlemi, bir bit düzlemi kodlama tekniğidir. EBCOT algoritmasına dayanır ve her kod bloğunda bağımsız olarak gerçekleştirilir.

3.2.3. Ayrık Kosinüs Dönüşümü Tabanlı(JPEG)

JPEG [58], görüntüleri sıkıştırılmış bir biçimde saklamak için kullanılan bir görüntü sıkıştırma standardıdır. Ortak Fotoğraf Uzmanları Grubu anlamına gelir. JPEG formatı oldukça popülerdir ve dijital kameralar gibi çeşitli cihazlarda kullanılır ve ayrıca internet gibi bant genişliği kısıtlı bir ortamda büyük boyutlu görüntülerin hızlı bir şekilde aktarımı için kullanılan en yaygın standarttır. JPEG formatında kaydedilen görüntü dosyaları genellikle jpg, jpeg veya jpe gibi uzantılara sahiptir. Günümüzde pek çok JPEG görüntü sıkıştırma algoritması mevcuttur ve birçoğu hala geliştirilmeye devam edilmektedir [60]. JPEG görüntü sıkıştırma algoritmasının genel yapısı şekil 3.6 'da verilmiş ve bu adımlar aşağıda açıklanmıştır. Kod çözme işlemi ise bu adımların tersten gerçekleştirilmesidir.



Şekil 3.6. JPEG algoritmasının genel yapısı

Renk Dönüşümü:

Görüntüdeki renklerin gösterimi RGB 'den YUV renk uzayına dönüştürülür. Bu dönüşüm işlemi zorunlu değildir. Ancak daha iyi sıkıştırma oranları elde etmek için genel olarak tercih edilir. YUV renk biçimi, renkleri, parlaklık ve renklilik olarak ifade eder. Y parlaklığı, U ve V değerleri de renkliliği ifade eder. Bu dönüşüm bir doğrusal dönüşümdür ve denklem 3.2 'de gösterildiği gibi hesaplanır.

$$Y = 0.299R + 0.587G + 0.114B$$
$$U = Cb = 0.564(B-Y) = -0.169R - 0.331G + 0.500B \quad (3.2)$$
$$V = Cr = 0.713(R-Y) = 0.500R - 0.419G - 0.081B$$

Ayrık Kosinüs Dönüşümü (DCT):

Görüntü 8 × 8 piksel bloklara bölünür ve daha sonra en önemli adımlardan biri olan ayrık kosinüs dönüşümü uygulanır. Ayrık kosinüs dönüşümü uygulandıktan sonra ortaya 64 katsayı çıkar bunlardan ilkine DC, diğerlerine ise AC adı verilir. Denklem 3.3 ileriye doğru ayrık kosinüs dönüşümünü tanımlamaktadır [61].

$$F(u,v) = \frac{2}{N}\mathrm{C(u)C(v)}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad (3.3)$$

u = 0,…,N-1 ve v=0,…,N-1 $\quad C(k)=\begin{cases}\frac{1}{\sqrt{2}} & k=0\\ 1 & diğer\end{cases}$

Niceleme:

DCT dönüşümü sonrasında ortaya çıkan katsayılar genellikle ondalıklıdır. Bu değerler niceleme yöntemi ile tamsayılara dönüştürülür. Niceleme yönteminde öncelikle her katsayı 1 ile 255 arasında bir tamsayıya bölünür ve daha sonra en yakın tamsayıya yuvarlanır ve görüntüdeki kayıp bu esnada meydana gelir. Nicelemeden sonra katsayılar Zik-Zak adı verilen Şekil 4.1 'de gösterildiği gibi taranarak bit dizisi haline getirilir.

Entropi Kodlama:

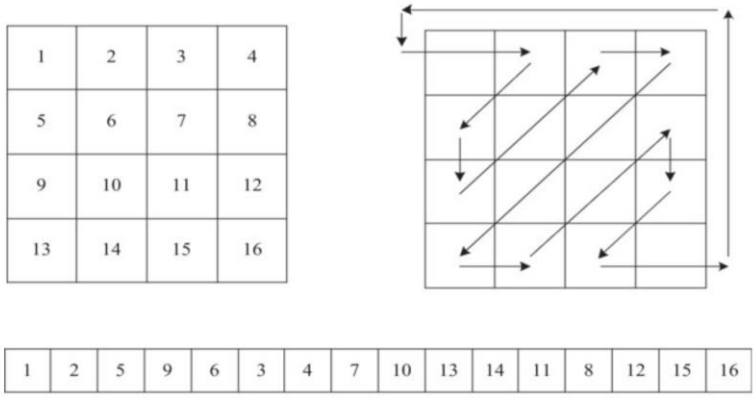
Son adım olarak entropi kodlama işlemi gerçekleştirilir ve görüntü bu adımda sıkıştırılır. Bu adım kayıpsız bir adımdır ve birçok entropi kodlama algoritması mevcuttur. Bunların en çok bilinenleri huffman kodlaması, aritmetik kodlama, çalıştırma uzunluğu kodlamasıdır.

4. KAOS TEMELLİ YER DEĞİŞTİRME KUTULARININ PERFORMANS İYİLEŞTİRMESİ İÇİN YENİ YAKLAŞIMLAR

Bu bölümde, kaos tabanlı s-box yapılarının performansını iyileştirmek için 7 farklı yöntem önerilmiştir. Önerilen yöntemlerin detayları ve performans analizleri kapsamlı bir şekilde açıklanmıştır.

4.1. Zik-zak Tarama Yöntemi Temelli Performans İyileştirme Yaklaşımı

Blok şifreleme algoritmaları dijital görüntülerin şifrelenmesinde etkisizdir. Bu sorunun en önemli nedenlerinden biri bir görüntünün piksel değerleri arasındaki yüksek korelasyondur. Genellikle görüntüler m×n boyutunda bir matris ile temsil edilir. m ve n değerleri sırasıyla satır ve sütunun değerlerini gösterir. Korelasyon problemini çözmek için önerilen yaklaşımlardan biri, Şekil 4.1 'de gösterildiği gibi zik-zak dönüştürme yöntemi kullanılarak matris hücrelerinin yeniden konumlandırılmasıdır [62].



Şekil 4.1. Zik-zak dönüşüm yaklaşımının genel yapısı

4.1.1. Algoritmanın Tarifi

AES benzeri s-box tasarımları 16x16 boyutunda bir matris olduğu için zik-zak dönüşüm yaklaşımı kolaylıkla gerçekleştirilebilir. Önerilen algoritmanın işleyişi aşağıda adım adım verilmiştir.

Adım 1. Ayrık veya sürekli zamanlı bir kaotik sistem seçilir.
Adım 2. Kaotik sistemin zengin rastgele özellikler sergileyebileceği başlangıç koşulu ve kontrol parametre değerleri belirlenir.
Adım 3. Kaotik sistemin durum değişken(ler)i hesaplanır. Tercihen, geçici tepkinin etkilerini ortadan kaldırmak için ilk 1000 değer göz ardı edilebilir.

Adım 4. Kesirli değer olan durum değişkeni değeri mod 256 uygulanarak 0-255 arasında bir ondalık değere dönüştürülür.

Adım 5. Ondalık değer s-kutusuna dahil değilse eklenir, aksi takdirde yeni bir durum değişkeni değeri hesaplanır ve tablo dolana kadar devam edilir.

Adım 6. S-box hücrelerinin konumları zik-zak dönüşüm kullanılarak karıştırılır.

4.1.2. Algoritmanın Performans Analizi

Önerilen yöntemin performans kriterleri üzerindeki etkisi bu bölümde analiz edilmiştir. Daha önce açıklandığı gibi, s-box performans analizi için beş temel kriter vardır. Bijektiflik kriteri önerilen yöntemle garanti edilmektedir. Bu nedenle bu kriter analiz tablolarında yer almamaktadır.

Tablo 4.1. Lojistik haritaya dayalı orijinal ve iyileştirilmiş s-box 'lar için performans karşılaştırmaları

	Orijinal S-box için Performans Kriterleri					İyileştirilmiş S-box için Performans Kriterleri				
S-box No	**Ort. Non.**	**BIC SAC**	**BIC Non.**	**SAC**	**XOR**	**Ort. Non.**	**BIC SAC**	**BIC Non.**	**SAC**	**XOR**
1	100.75	0.4992	102.71	0.4971	12	105	0.5009	103.64	0.5046	10
2	102.5	0.5012	104.86	0.5051	12	103	0.5004	102.93	0.5056	12
3	102.75	0.5022	103.21	0.502	12	104.5	0.4983	102.93	0.5027	12
4	103.5	0.4981	104.29	0.4985	10	104.75	0.4979	103.71	0.5049	10
5	101.75	0.4996	103.21	0.4998	10	104.5	0.5011	103.64	0.4983	12
6	103.25	0.4968	103.64	0.4976	10	103.75	0.5013	103.29	0.4973	12
7	102	0.5017	103.07	0.5051	12	104.25	0.501	103.64	0.491	12
8	101.25	0.503	103.29	0.5056	12	103.75	0.4962	103.86	0.4934	12
9	103.75	0.4997	102.64	0.5059	10	104.5	0.4978	103.86	0.4907	10
10	103	0.5023	104.71	0.5015	12	104.5	0.5018	103.5	0.498	10
11	103.5	0.4999	103.36	0.5012	10	104	0.5018	104.14	0.4998	12
12	103.25	0.4948	103.64	0.5049	10	103.5	0.4978	102.36	0.5	12
13	102.25	0.503	103.64	0.5042	12	103.25	0.4963	104.07	0.5022	10
14	102	0.4969	103.36	0.512	12	103	0.5007	102.86	0.4971	12
15	102.75	0.5001	103.86	0.5007	10	103.25	0.5005	104	0.5088	12
16	101	0.4976	103.07	0.5039	10	103.5	0.4974	102.86	0.5005	12
17	102.5	0.5	102.86	0.5134	10	103.5	0.4978	104.29	0.5056	10
18	103.5	0.4941	103.64	0.499	12	103.75	0.4957	103.64	0.5161	10
19	102.75	0.5037	102.93	0.5073	12	103.75	0.5018	102.5	0.5002	10
20	103.25	0.4951	103	0.491	10	104	0.4993	103,5	0.5042	10
21	102.5	0.4985	102.86	0.5078	10	103.75	0.5013	103.64	0.5154	14
22	102.75	0.4997	103.71	0.4966	10	103.75	0.4973	103	0.5066	12
23	102.25	0.5015	103.5	0.5012	12	103.25	0.5022	103.36	0.5044	12
24	102.5	0.4986	104.36	0.5068	12	104.25	0.5006	104.21	0.511	10
25	103.25	0.4992	103.29	0.5012	12	104.24	0.5027	104.71	0.5071	10

Kaotik sistemleri sınıflandırmak için iki ana kategori kullanılabilir. Bu kategoriler kesikli ve sürekli zamanlı kaotik sistemlerdir. Ayrık zamanlı sistemler birinci dereceden fark denklemleridir. Sürekli-zamanlı kaotik sistemler en az üçüncü mertebeden diferansiyel denklemlerdir. Her iki kaotik sistem sınıfı için üç farklı kaotik sistem kullanılarak altı farklı kaotik sistemin analizi yapılmıştır. Her kaotik sistem sınıfı için yirmi beş farklı s-box yapısı oluşturulmuştur. Ayrık zamanlı kaotik sistemler olarak lojistik harita, sinüs haritası ve daire haritası kullanılmaktadır. Orijinal ve geliştirilmiş s-box yapıları için performans karşılaştırmaları sırasıyla Tablo 4.1, 4.2 ve 4.3 'te

verilmiştir. Benzer şekilde, sürekli zamanlı Lorenz, Labyrinth Rene Thomas sistemi ve Chua sistemlerinin her biri için oluşturulan orijinal ve geliştirilmiş s-box yapıları için performans karşılaştırmaları sırasıyla Tablo 4.4, 4.5 ve 4.6 'da verilmiştir. Önerilen yöntemin başarısını göstermek için, analizde kullanılan tüm orijinal s-box yapılarının ortalama doğrusal olmama özelliğinin 103'ten küçük olmasına özen gösterilmiştir. Analiz tablolarında verilen tüm s-box yapılarında performans artışı gözlemlenmiştir.

Tablo 4.2. Sinüs haritaya dayalı orijinal ve iyileştirilmiş s-box ‘lar için performans karşılaştırmaları

	Orijinal S-box için Performans Kriterleri					**İyileştirilmiş S-box için Performans Kriterleri**				
S-box No	**Ort. Non.**	**BIC SAC**	**BIC Non.**	**SAC**	**XOR**	**Ort. Non.**	**BIC SAC**	**BIC Non.**	**SAC**	**XOR**
1	101.75	0.4985	104.07	0.5122	14	103.5	0.4911	103.64	0.4924	12
2	103	0.4964	102.86	0.5046	12	104.5	0.4977	103.64	0.5027	10
3	102.25	0.498	102.5	0.4988	12	104.25	0.5017	103.93	0.4978	12
4	103	0.5029	103.79	0.5063	12	104.5	0.5013	103.43	0.5034	12
5	103.25	0.4978	103.57	0.4973	12	104.5	0.5006	103.93	0.51	12
6	102.5	0.4967	104	0.51	12	103	0.4921	103.64	0.511	10
7	103.5	0.4991	102.79	0.501	12	103.75	0.504	103.5	0.5093	10
8	102.5	0.5005	104.07	0.5002	12	105	0.5029	103.79	0.5083	10
9	103.75	0.495	103.57	0.5002	12	104	0.4988	103	0.5103	12
10	101.5	0.4981	103.57	0.4973	10	103.25	0.499	104	0.4934	12
11	103.75	0.4999	104.29	0.4934	12	104.5	0.4952	104.5	0.5083	12
12	102	0.4963	103	0.5054	12	103	0.4963	103.43	0.5103	12
13	102.5	0.4967	104.29	0.4993	14	103.75	0.501	103	0.4971	12
14	101.5	0.501	103.64	0.5007	10	102.5	0.5003	104.14	0.5056	10
15	102	0.5003	103.71	0.499	12	102.75	0.4957	103.71	0.498	12
16	103	0.5026	104.07	0.5002	12	130.25	0.4925	103	0.5166	12
17	101.75	0.4995	102.86	0.4973	12	102	0.4998	103.43	0.4961	10
18	103	0.4972	103.07	0.5022	10	103.5	0.499	103.14	0.4988	10
19	102.75	0.4998	103.43	0.4978	10	104.75	0.5005	103.07	0.4976	12
20	103.25	0.4959	103.21	0.4973	12	104.75	0.5013	103.86	0.501	12
21	102.25	0.4978	103.21	0.4934	10	104.5	0.5029	104.14	0.4998	12
22	103.25	0.4987	102.86	0.5017	12	105	0.5017	105.07	0.5029	10
23	103	0.5014	103.57	0.5012	12	103.75	0.4997	104.36	0.5107	12
24	103	0.4994	103.71	0.5078	10	103.75	0.5007	104	0.5059	10
25	102.75	0.5009	103.14	0.5044	10	103.25	0.5021	103.29	0.5005	12

Tablo 4.3. Daire haritaya dayalı orijinal ve iyileştirilmiş s-box 'lar için performans karşılaştırmaları

	Orijinal S-box için Performans Kriterleri					İyileştirilmiş S-box için Performans Kriterleri				
S-box No	**Ort. Non.**	**SAC**	**BIC Non.**	**BIC SAC**	**XOR**	**Ort. Non.**	**SAC**	**BIC Non.**	**BIC SAC**	**XOR**
1	102.25	0.495	102.93	0.5098	12	104.25	0.5031	102.79	0.5015	10
2	103.5	0.501	103.29	0.5027	10	105.5	0.5055	103.64	0.5042	10
3	102.75	0.4902	104.14	0.5029	12	105.75	0.495	103.07	0.5005	10
4	103.5	0.4973	103.43	0.4915	10	104.25	0.4974	102.86	0.5005	10
5	102	0.4965	103.57	0.5115	12	102.5	0.501	104.07	0.5007	12
6	103.25	0.5022	102.93	0.5105	12	104.5	0.4988	103.29	0.4917	10
7	102.25	0.5024	102.93	0.498	12	104.25	0.4983	103.64	0.502	12
8	100.75	0.4961	104.07	0.4998	12	105	0.5026	103.71	0.4954	12
9	102	0.5009	103.07	0.498	12	102.75	0.4977	103.86	0.5066	10
10	103.25	0.5017	103.36	0.4978	12	103.5	0.4986	103	0.5037	14
11	103	0.5034	103	0.4946	14	104.25	0.5004	103.5	0.5007	12
12	103.5	0.5019	103.29	0.4944	12	105.25	0.4946	103.43	0.4976	10
13	103.5	0.502	102.71	0.4932	10	104	0.4957	103.36	0.5	12
14	103.25	0.4982	103.21	0.5061	10	105.5	0.4995	103.29	0.5039	10
15	102	0.5052	104.63	0.4951	10	104.25	0.5015	103.93	0.5029	10
16	102.25	0.4957	104	0.4968	10	104	0.5044	104.86	0.5037	10
17	102.75	0.5012	104.07	0.4939	10	104.5	0.4971	103.79	0.4924	12
18	102.75	0.4979	102	0.5083	10	103	0.4983	104.21	0.5015	10
19	103	0.5017	103	0.51	10	104.25	0.4976	103.71	0.4978	10
20	101.5	0.5011	103	0.5078	12	103.25	0.5025	102.5	0.5034	14
21	101.75	0.4977	102.43	0.501	10	102.25	0.4992	104	0.4993	10
22	102	0.4925	103	0.5027	10	102.25	0.5014	103.71	0.5112	10
23	103	0.5002	103.14	0.4976	10	103.75	0.4995	102.57	0.4937	14
24	102.75	0.4983	104.57	0.4917	10	103.75	0.5004	104.79	0.4956	12
25	101.75	0.5014	102.86	0.5171	12	104.75	0.4966	102.79	0.5073	10

Tablo 4.4. Lorenz haritaya dayalı orijinal ve iyileştirilmiş s-box 'lar için performans karşılaştırmaları

	Orijinal S-box için Performans Kriterleri					İyileştirilmiş S-box için Performans Kriterleri				
S-box No	**Ort. Non.**	**BIC SAC**	**BIC Non.**	**SAC**	**XOR**	**Ort. Non.**	**BIC SAC**	**BIC Non.**	**SAC**	**XOR**
1	101.5	0.4988	103.64	0.4902	10	103.75	0.5041	103.21	0.4973	12
2	103.25	0.5063	103.29	0.5044	12	105	0.4989	102.79	0.5037	12
3	101.75	0.4911	103.36	0.5063	12	103	0.4985	103	0.4998	12
4	102.75	0.5005	103.5	0.5042	12	104.25	0.5013	103.21	0.5027	10
5	103.75	0.4928	104.86	0.5095	12	104.25	0.5039	103	0.5024	12
6	103.5	0.5015	103.79	0.4944	12	105.5	0.4991	104	0.4937	10
7	102.5	0.4959	103.21	0.5027	12	106.25	0.499	104.07	0.4929	14
8	102.25	0.5002	103.14	0.4978	14	103.25	0.5029	103.21	0.4912	12
9	102.25	0.5	104.21	0.4954	12	105.5	0.4957	103.07	0.499	12
10	103.25	0.4959	103.36	0.5029	12	103.75	0.5028	103.43	0.5068	12
11	101.5	0.5018	104.07	0.5002	10	103.75	0.5036	103.07	0.4961	12
12	101.25	0.4981	103.71	0.5085	10	103	5033	103.29	0.5015	12
13	101	0.4989	103.64	0.5029	10	105	0.4993	103.21	0.5039	12
14	102.75	0.4938	103.93	0.4934	12	104.5	0.4992	103.5	0.4988	12
15	103.25	0.4996	103	0.4995	10	103.5	0.5045	103.29	0.4985	10
16	103	0.4987	103.07	0.4961	14	103.25	0.5008	104.07	0.5071	12
17	103.75	0.5015	103.57	0.5093	12	104.25	0.4958	103.86	0.4917	14
18	102.75	0.4994	103.07	0.5068	10	103.25	0.499	103.29	0.4939	12
19	101.25	0.5029	102.79	0.4998	12	103	0.5029	104.79	0.491	10
20	103.25	0.5015	102.79	0.5098	10	104.25	0.4973	103.57	0.499	10
21	103.5	0.4959	103.21	0.4973	12	103.75	0.4985	102.71	0.4971	12
22	103.25	0.4964	103.21	0.5046	12	104.24	0.4986	103.29	0.4988	12
23	102.75	0.504	103	0.5017	12	103.75	0.4991	103.86	0.5007	12
24	103.5	0.5007	103.14	0.5005	10	103.75	0.4964	102.43	0.4978	12
25	102.75	0.5003	104.14	0.5017	12	105.5	0.4993	103.71	0.4993	12

Tablo 4.5. Thomas haritaya dayalı orijinal ve iyileştirilmiş s-box 'lar için performans karşılaştırmaları

	Orijinal S-box için Performans Kriterleri					İyileştirilmiş S-box için Performans Kriterleri				
S-box No	**Ort. Non.**	**SAC**	**BIC Non.**	**BIC SAC**	**XOR**	**Ort. Non.**	**SAC**	**BIC Non.**	**BIC SAC**	**XOR**
1	101.75	0.5018	103.86	0.5046	10	103.5	0.4997	103.86	0.4966	10
2	103.25	0.4995	103.29	0.4993	10	104.5	0.4971	103.07	0.4932	12
3	102.5	0.4937	104.43	0.5039	12	104	0.5022	103.5	0.5002	12
4	103.5	0.4962	104.07	0.5132	12	104	0.4957	102.93	0.5032	12
5	102.5	0.4982	103.64	0.5037	12	104	0.5033	103.86	0.5022	14
6	103.25	0.499	103.29	0.51	12	104.25	0.4952	103.36	0.5015	10
7	103.25	0.4967	103.36	0.4944	12	104.25	0.5047	104.14	0.5034	10
8	103	0.502	102.93	0.5054	12	104.75	0.502	103.57	0.5137	12
9	103.25	0.4962	103.43	0.4893	12	105.25	0.5017	103.64	0.5088	12
10	102	0.4939	104.07	0.4963	12	105.5	0.4992	103.71	0.5095	10
11	103	0.4975	102.79	0.5071	10	104	0.496	103.29	0.502	10
12	102	0.4963	104.71	0.4976	12	103	0.5031	103.43	0.5149	12
13	102.25	0.4941	103.14	0.5037	10	103.5	0.4999	103.5	0.5083	10
14	102.75	0.5001	103.36	0.5	10	103	0.5008	103.14	0.4971	12
15	103.25	0.4978	102.29	0.5117	10	104	0.4951	104.07	0.5063	12
16	103	0.502	102.64	0.5017	10	104	0.5037	103.86	0.5105	12
17	101	0.501	103.07	0.4961	12	104.25	0.498	103.86	0.4897	10
18	102.5	0.4994	103.86	0.5056	10	103.5	0.5047	103.57	0.5078	10
19	103.5	0.5017	103.14	0.4995	10	103.75	0.4967	103.21	0.4924	14
20	103	0.4971	103.5	0.5078	10	104.5	0.5006	104.07	0.5012	12
21	103.25	0.4996	104	0.5095	12	104	0.4983	103	0.5049	10
22	103	0.5009	104.14	0.5027	10	103.75	0.5017	104.21	0.4998	10
23	102.5	0.5021	104	0.5088	12	104	0.4983	104.57	0.5056	10
24	102.5	0.4969	104.14	0.5051	12	104.5	0.498	103.5	0.4998	10
25	103.25	0.5059	102.86	0.4983	12	103.5	0.5001	103.79	0.4951	10

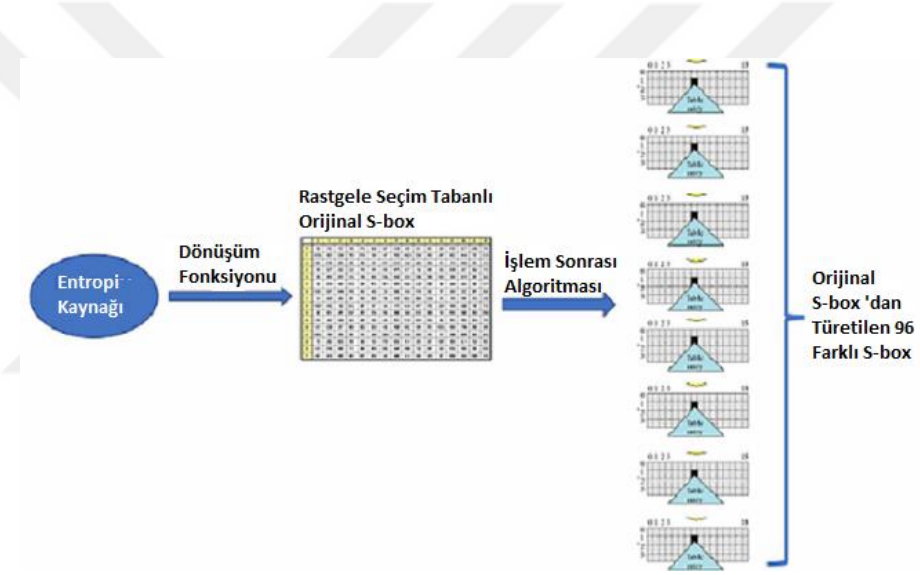
Tablo 4.6. Chua haritaya dayalı orijinal ve iyileştirilmiş s-box 'lar için performans karşılaştırmaları

	Orijinal S-box için Performans Kriterleri					İyileştirilmiş S-box için Performans Kriterleri				
S-box No	**Ort. Non.**	**BIC SAC**	**BIC Non.**	**SAC**	**XOR**	**Ort. Non.**	**BIC SAC**	**BIC Non.**	**SAC**	**XOR**
1	103.75	0.4988	103.64	0.4922	14	104.25	0.4999	103.64	0.5051	10
2	103.75	0.494	103.29	0.4995	12	104.75	0.4943	104.21	0.5078	12
3	102.25	0.506	103.79	0.4939	12	105.5	0.5001	102.86	0.5063	12
4	103.25	0.5054	104.57	0.5032	10	105	0.5046	103.21	0.51	10
5	103.5	0.5028	103	0.4954	12	103.75	0.4948	103.5	0.4956	10
6	103.5	0.502	103.29	0.5034	12	104.25	0.4973	104	0.5027	10
7	103	0.5024	103.57	0.5027	12	103.75	0.4995	103.21	0.5051	12
8	102.5	0.5015	104.29	0.5029	10	104	0.4994	103.21	0.5068	10
9	102.75	0.5011	103.29	0.5059	10	105.25	0.5009	103.5	0.5034	12
10	103	0.4958	103.43	0.4956	12	104.5	0.4986	103.57	0.5027	12
11	102.75	0.4971	103.36	0.5022	12	104.25	0.498	103.79	0.4968	12
12	103.75	0.4999	103.43	0.5039	10	104.75	0.5018	104.07	0.4976	12
13	101.75	0.4981	104.07	0.498	12	104.75	0.4993	103.57	0.4985	12
14	102	0.4994	103.64	0.5	12	103.5	0.502	104.29	0.5024	12
15	102.5	0.4994	104	0.5049	10	103.5	0.5037	103.36	0.5029	12
16	103	0.4993	103.29	0.4939	14	104.25	0.5006	102.71	0.5081	10
17	103	0.502	103.86	0.5044	12	105.5	0.4979	103.57	0.4998	12
18	103	0.5012	103.64	0.4922	12	103.5	0.4979	102.29	0.4983	12
19	102.75	0.4998	104.57	0.5034	12	104.25	0.4931	103.57	0.5	10
20	103.25	0.4992	103.79	0.5056	12	103.5	0.4976	102.5	0.4922	12
21	102.25	0.5065	103.14	0.5007	12	103.5	0.4956	103.07	0.4956	14
22	103.25	0.4985	103.36	0.4917	10	105	0.4937	103.5	0.5088	12
23	101.25	0.493	103.36	0.4995	12	103.75	0.4992	103.29	0.4915	12
24	103	0.4929	102.79	0.5103	14	104.5	0.5042	103.64	0.5007	10
25	102.75	0.4985	103.57	0.499	12	103.25	0.5013	103	0.5034	12

S-box için yapılan literatür taramasında, doğrusal olmama değeri için ortalama değerin 103 olarak ifade edilebileceği görülmüştür. Bu nedenle, analizde kullanılan tüm s-box değerlerinin ortalama doğrusal olmama değerinin 103'ün altında olmasına özen gösterilmiştir. Bu koşullar doğrultusunda 150 farklı s-box yapısı oluşturulmuştur. Üretilen s-box yapıları, iki farklı kaotik sistem sınıfından seçilen altı farklı kaotik sistemden elde edilmiştir. Farklı kaotik sistemlerin kullanılmasının nedeni, önerilen yöntemin tüm kaotik sistemler için başarılı olabileceğini göstermektir.

4.2. DES S-box Yapıları Kullanılarak Performans İyileştirme Yaklaşımı

Önerilen mimarinin çalışma mantığını temsil edem akış şeması şekil 4.2 ’de sunulmuştur. Yöntem iki aşamadan oluşmaktadır. Bu aşamalar rasgele seçim tabanlı s-box yapısının üretilmesi ve ardından önerilen yaklaşımla s-box hücrelerinin pozisyonlarının karılmasıdır [63].



Şekil 4.2. Önerilen mimariye genel bakış

En genel ifade ile s-box yapısı; m-bit uzunluklu bir girişi n-bit uzunluklu bir çıkışa haritalayan doğrusal olmayan bir fonksiyondur. Bu doğrusal olmayan yapı kriptolojik algoritmalarda diferansiyel saldırıların başarısını engellemeyi amaçlamaktadır. AES algoritmasında Nyberg tarafından önerilen algoritma diferansiyel saldırıları en iyi şekilde adresleyecek biçimde tasarlanmıştır. AES s-box yapısının bir diğer avantajı yazılımsal olarak efektif bir tasarıma sahip olmasıdır. Birçok programlama dili bayt tabanlı çalıştığı için AES s-box yapıları 8-bit uzunluklu girişleri yine 8-bit uzunluklu çıktılara dönüştürmektedir. Adil bir karşılaştırma yapabilmek için bu yüzden AES benzeri s-box yapıları rasgele bir entropi kaynağı kullanılarak üretilmiştir. Kullanılan entropi kaynağı olarak ayrık zamanlı kaotik sistemler, sürekli zamanlı kaotik sistemler ve klasik rastgelelik fonksiyonu kullanılabilir. Elde edilen çıktılara mod fonksiyonu uygulanarak rasgele

çıkışlar 0-255 arasına dönüştürülmüştür. Giriş için üretilmiş doğrusal olamama değeri 102.75 olan örnek bir s-box yapısı Tablo 4.7 ’de gösterilmiştir.

Tablo 4.7. İyileştirilmeden önceki orijinal rastgele üretilmiş S-box

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

Önerilen yöntem optimizasyon algoritmalarına göre daha basit ve daha hızlı sonuç veren bir yapıya sahiptir. Yöntemin amacı basitlik ve hızdan ödün vermeden doğrusal olmama kriterinin değerini artırabilmektir. Bu amacı gerçekleştirmek için DES s-box tabloları aracılığı ile rasgele seçim prensibine göre üretilen s-box yapılarının satır, sütun ve hem satır hem de sütunlarının karılması önerilmiştir. S-box hücrelerinin pozisyonlarının değiştirilerek performans ölçütlerinin iyileştirilebileceği yakın zamanda gösterilmiştir. Bu çalışmada önerilen son işlem tekniğinin DES s-box tabloları aracılığı ile daha da iyileştirilmesidir. Daha önce önerilen yöntemde orijinal her bir s-box yapısından son işlem tekniği ile yeni bir s-box yapısı üretilmiştir. Bu çalışmada önerilen algoritma ile her bir orijinal s-box yapısından 96 farklı s-box yapısı elde edilebileceği gösterilmiştir. Çünkü DES s-box ‘ları 4*16 boyutunda sekiz adet tablodan oluşmaktadır. Her bir satırdaki 0-15 arasında değerler DES s-box tasarımları ile karılmıştır. Toplam 32 farklı karma tablosu Tablo 4.8 ’de verilmiştir.

Tablo 4.8. DES S-box ‘ları

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
4	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
5	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
6	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
7	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
8	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
9	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
10	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
11	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
12	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
14	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
15	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
16	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
17	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
18	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
19	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
20	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
21	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
22	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
23	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
24	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
25	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
26	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
27	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
28	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
29	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
30	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
31	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Örneğin Tablo 4.8 ’in ilk satırı kullanılarak Tablo 4.7 ’de verilen s-box tablosunun satırları karılabilir. İlk değer 14 olduğu için orijinal tablonun 14. Satırı yeni tabloda 0. Satır olarak yer değişmiştir. Benzer şekilde orijinal tablonun 4. satırı yeni tablonun 1. satırı olarak yer değiştirmiştir. Tüm bu yer değişmeler sonucunda Tablo 4.9 ’daki s-box yapısı oluşmuştur.

4.2.1. Algoritmanın Tarifi

Algoritmanın çalışma mantığı aşağıda adım adım verilmiştir.

Adım 1. Ayrık veya sürekli zamanlı bir kaotik sistem seçilir.

Adım 2. Kaotik sistemin zengin rastgele özellikler sergileyebileceği başlangıç koşulu ve kontrol parametre değerleri belirlenir.

Adım 3. Kaotik sistemin durum değişken(ler)i hesaplanır. Tercihen, geçici tepkinin etkilerini ortadan kaldırmak için ilk 1000 değer göz ardı edilebilir.

Adım 4. Kesirli değer olan durum değişkeni değeri mod 256 uygulanarak 0-255 arasında bir ondalık değere dönüştürülür.

Adım 5. Ondalık değer s-kutusuna dahil değilse eklenir, aksi takdirde yeni bir durum değişkeni değeri hesaplanır ve tablo dolana kadar devam edilir.

Adım 6. S-box hücrelerinin konumları Tablo 4.8 ‘deki değerlere göre satır, sütun veya satır-sütun karıştırma işlemleri kullanılarak karıştırılır.

Tablo 4.9. Tablo 2.7 'deki s-box dan türetilen yeni s-box yapısı

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

4.2.2. Algoritmanın Performans Analizi

Tablo 4.7 ’deki s-box yapısının satırları Tablo 4.8 ’deki değerlere göre karılması sonucunda elde edilen 32 yeni s-box yapısı için s-box tasarım ölçütleri Tablo 4.10 ’da verilmiştir.

Tablo 4.10. Satır karıştırma kullanılarak orijinal s-box ‘dan türetilen s-box 'ların performans analizi

S-box No	Non.			BIC		SAC			En Yüksek I/O XOR
	Ort	Max	Min	SAC	Non.	Ort	Min	Max	
1	104.75	108	100	0.5054	103.71	0.5037	0.3906	0.625	12
2	103.75	106	98	0.4987	103.43	0.501	0.3906	0.5781	12
3	103.75	108	98	0.5015	103.71	0.502	0.3906	0.5781	10
4	103.5	106	100	0.4994	103.29	0.5051	0.3906	0.6094	10
5	102.75	106	96	0.5002	103.5	0.5044	0.3906	0.625	12
6	103.75	106	100	0.5015	103.79	0.5042	0.3906	0.5938	12
7	101	106	96	0.5037	103.29	0.5049	0.3906	0.5781	10
8	104.75	108	98	0.5029	103.07	0.5056	0.3594	0.6094	10
9	104.25	108	102	0.4969	104	0.5024	0.3906	0.6406	12
10	103.75	106	100	0.4999	104.21	0.5002	0.3906	0.5938	10
11	103.75	108	100	0.4935	103.79	0.5029	0.3594	0.5781	10
12	103.25	106	100	0.5033	103.57	0.5042	0.3594	0.625	10
13	103.5	106	100	0.5004	104.79	0.4985	0.3906	0.5781	10
14	103.25	106	100	0.5001	103.07	0.5022	0.375	0.6094	12
15	103.25	106	100	0.5032	103.07	0.502	0.3906	0.6094	12
16	101.75	108	96	0.4978	103.43	0.5024	0.3906	0.6094	12
17	104.5	108	100	0.4981	103.57	0.5015	0.3906	0.5938	10
18	103	106	100	0.4999	104.21	0.5071	0.3906	0.5938	10
19	104	108	100	0.495	103.86	0.5017	0.3906	0.5781	10
20	106	108	104	0.502	103.71	0.5015	0.3906	0.5938	12
21	103.75	108	100	0.4969	103.93	0.5037	0.3906	0.5781	12
22	101.75	108	90	0.4986	103.14	0.5066	0.3906	0.5938	12
23	103.5	108	98	0.5001	103.86	0.501	0.3906	0.5938	12
24	103.25	108	94	0.5	103.36	0.5029	0.3906	0.5781	10
25	105.5	108	102	0.4964	104.21	0.5098	0.3906	0.6094	12
26	103	108	100	0.4958	103	0.5066	0.3906	0.5938	12
27	103.25	108	92	0.4985	103.29	0.5103	0.3906	0.625	12
28	102.5	108	98	0.5033	102.71	0.499	0.3906	0.5781	12
29	104.5	108	98	0.4978	104.14	0.5017	0.3906	0.6094	12
30	102.5	108	94	0.4987	104.21	0.5044	0.3906	0.6094	10
31	104	108	98	0.5024	104.29	0.501	0.3906	0.5781	10
32	103.5	106	102	0.501	103.71	0.5024	0.3906	0.5781	10

Benzer şekilde Tablo 4.7 ’deki s-box yapısının sütunları Tablo 4.8 ’deki değerlere göre karılması sonucunda elde edilen 32 yeni s-box yapısı için s-box tasarım ölçütleri Tablo 4.11 ’de verilmiştir.

Tablo 4.11. Sütun karıştırma kullanılarak orijinal s-box ‘dan türetilen s-box 'ların performans analizi

S-box No	Non.			BIC		SAC			En Yüksek I/O XOR
	Ort	Max	Min	SAC	Non.	Ort	Min	Max	
1	103.75	106	100	0.5027	103.5	0.4998	0.4062	0.625	10
2	105.5	110	100	0.5013	103.21	0.4985	0.4062	0.5938	12
3	103.75	106	100	0.4988	104.43	0.5017	0.4062	0.6094	12
4	104.5	108	100	0.5	104.07	0.499	0.4062	0.5938	10
5	104.25	108	102	0.4979	103.29	0.5002	0.4062	0.6094	12
6	104.75	108	102	0.5056	103.36	0.5034	0.4062	0.5938	10
7	105.25	108	102	0.4982	103.21	0.499	0.4062	0.5938	10
8	103.5	108	98	0.4998	103.86	0.5017	0.4062	0.5938	12
9	104.75	108	102	0.4987	103.5	0.4976	0.4062	0.5938	12
10	104	108	102	0.4994	102.79	0.5012	0.4062	0.5938	10
11	104.25	108	100	0.4971	103.86	0.4966	0.4062	0.5938	10
12	104.5	108	98	0.4964	103.43	0.4993	0.4062	0.6094	12
13	103.5	106	98	0.4995	103.29	0.5027	0.4062	0.5938	12
14	104.5	110	102	0.4976	102.93	0.4944	0.4062	0.5938	12
15	104.5	110	102	0.504	102.93	0.4939	0.4062	0.5938	12
16	104.75	108	100	0.4996	103.5	0.501	0.4062	0.5938	10
17	102.75	106	98	0.5047	103.5	0.4978	0.4062	0.5938	10
18	104.5	108	100	0.5023	103.64	0.5015	0.4062	0.5938	10
19	103.5	106	96	0.4939	103.5	0.5037	0.4062	0.5938	12
20	104	106	100	0.4937	103.57	0.4998	0.4062	0.6562	10
21	103	106	96	0.4929	102.43	0.5002	0.4062	0.5938	10
22	103.5	106	102	0.5023	102.93	0.4954	0.4062	0.5938	12
23	102.75	110	98	0.4988	104.36	0.4995	0.4062	0.5938	10
24	105.25	106	102	0.499	103.21	0.4963	0.4062	0.5938	12
25	103.75	108	98	0.493	104	0.4998	0.4062	0.5938	10
26	104	108	100	0.5002	103.86	0.498	0.3906	0.5938	10
27	104.75	108	100	0.4956	103.93	0.5007	0.4062	0.6094	12
28	105.75	110	102	0.4986	102.86	0.5022	0.4062	0.6094	12
29	104.5	108	98	0.499	103.79	0.4983	0.3594	0.5938	10
30	102.5	106	100	0.5021	103.43	0.5032	0.4062	0.5938	14
31	103	108	98	0.4991	104.21	0.501	0.4062	0.6094	10
32	104.75	108	102	0.4987	102.93	0.5022	0.4062	0.6094	10

Benzer şekilde Tablo 4.7 ’deki s-box yapısının hem satır hem de sütunları Tablo 4.8 ’deki değerlere göre karılması sonucunda elde edilen 32 yeni s-box yapısı için s-box tasarım ölçütleri Tablo 4.12 ’de verilmiştir.

Tablo 4.12. Satır ve sütun karıştırma kullanılarak orijinal s-box ‘dan türetilen s-box 'ların performans analizi

S-box No	Non.			BIC		SAC			En Yüksek I/O XOR
	Ort	Max	Min	SAC	Non.	Ort	Min	Max	
1	103.5	110	98	0.5038	103.36	0.5056	0.4062	0.625	10
2	104.75	106	104	0.5052	103.29	0.5017	0.3906	0.5781	12
3	102.75	106	100	0.5029	103.57	0.5059	0.4219	0.6094	14
4	104.25	108	102	0.5022	104	0.5063	0.4219	0.6094	10
5	102	108	100	0.504	102.5	0.5068	0.4062	0.625	12
6	104	106	102	0.4991	103.5	0.5098	0.4062	0.5938	10
7	105	110	102	0.4978	102.64	0.5061	0.4062	0.5781	12
8	102.5	108	94	0.4971	103.79	0.5095	0.3594	0.6094	10
9	101.75	106	94	0.5032	103.71	0.5022	0.4062	0.6406	12
10	105.5	108	100	0.4976	103.36	0.5037	0.3906	0.5938	12
11	102	106	96	0.491	103.29	0.5017	0.3594	0.5781	12
12	103.5	106	98	0.5023	103.57	0.5056	0.3594	0.625	12
13	104.5	108	102	0.5033	103.57	0.5034	0.4062	0.5781	12
14	104.75	108	102	0.499	103.43	0.4988	0.375	0.6094	12
15	104.75	108	102	0.5024	103.43	0.498	0.4062	0.6094	12
16	104.25	108	100	0.4985	103.64	0.5056	0.4219	0.6094	12
17	102.75	106	98	0.501	104.43	0.5015	0.3906	0.5938	12
18	104.5	108	100	0.5061	103.86	0.5107	0.3906	0.5938	12
19	103.5	108	98	0.5043	103.29	0.5076	0.4219	0.5938	12
20	103	106	94	0.502	103.36	0.5034	0.4219	0.6562	10
21	102.5	106	98	0.4992	103.5	0.5061	0.4375	0.5781	12
22	102.75	106	98	0.4943	103.93	0.5042	0.4062	0.5938	12
23	104.25	108	100	0.5031	104.71	0.5027	0.3906	0.5938	12
24	104.25	108	102	0.4983	103.64	0.5015	0.4062	0.5625	12
25	101.75	106	94	0.4992	103.5	0.5117	0.4219	0.6094	10
26	104	106	100	0.5005	103.5	0.5068	0.3906	0.5938	10
27	103.75	106	96	0.5001	103.5	0.5132	0.4219	0.625	12
28	103.25	108	100	0.5022	101.64	0.5034	0.4219	0.6094	12
29	104	108	100	0.501	103	0.5022	0.3594	0.6094	12
30	103.25	108	100	0.5023	103.21	0.5098	0.4062	0.6094	16
31	103.5	106	100	0.5022	103.86	0.5042	0.4219	0.6094	12
32	104.5	106	102	0.5021	103.86	0.5068	0.4219	0.6094	12

Önerilen yöntem, ortalamanın altında değerlendirilebilen performans özelliklerine sahip s-box yapılarında önemli ölçüde performans iyileştirmeleri sağladığı gözlenmiştir. Üç farklı senaryo için orijinal s-box yapılarından yeni s-box yapılarının elde edilebileceği gösterilmiştir. Analiz sonuçları üretilen s-box yapılarından satır dönüşümlerinde %81.25, sütun dönüşümlerinde %91.6, satır-sütun dönüşümünde ise %75 tasarım ölçütlerinin iyileştirilebildiği gözlemlenmiştir. Bu sonuçlara

bakıldığında özellikle sütunların karıştırılması işlemi oldukça etkili olmuştur. Bu sonuçlar ilerideki çalışmalarda farklı teknik ve yöntemler kullanılarak rasgele seçim tabanlı yaklaşımların başarısının daha fazla iyileştirilebileceğine işaret etmektedir.

4.3. Rasgele Seçim Tabanlı S-box Yapılarının Performans İyileştirmesi İçin Yer Değiştirme Temelli Son İşlem Yöntemi

AES benzeri s-box yapıları 256 değer içerdiğinden üretilebilecek farklı s-box sayısı 256! 'dir. Bu kadar geniş bir alandan en iyi tasarım metriklerini (bijektif, doğrusal olmayan, SAC, BIC ve XOR) sağlayan s-box 'ı seçmek gerçekten zor bir süreçtir. Optimizasyon algoritmalarının bu zorlu süreç için iyi birer aday olmasının nedeni aslında bu seçim uzayının genişliğidir. Bu devasa seçim uzayından sonuç üretmek için etkili bir yöntem olmasına rağmen, optimizasyon algoritmalarının hesaplama zorlukları, ele alınması gereken bir problemdir. Bu uygulamada bu problem analiz edilmiş ve optimizasyon algoritmalarına göre çok daha etkili bir yöntem önerilmiştir. Önerilen yöntem, herhangi bir s-box üreteci yaklaşımının çıktısına uygulanabilir.

Önerilen algoritmanın amacı, doğrusal olmama değerini mümkün olduğunca iyileştirmektir. Her seferinde seçilen iki hücre değeri değiştirilerek yeni bir s-box tablosu elde edilir. Değiştirilen s-box 'ın doğrusal olmama değeri önceki s-box 'ın doğrusal olmama değerinden büyükse, yeni s-box yapısı kullanılarak algoritmanın adımlarına devam edilir. Değilse, iki yeni hücre seçip değerlerini değiştirerek devam edilir [64]. Optimizasyon algoritmalarında, seçim sürecinde genellikle doğal süreçler taklit edilir. Önerilen algoritmada hücreler mevcut sırayla seçilir. Bu seçim mantığı, süreci optimizasyon algoritmalarından çok daha kolay hale getirir.

4.3.1. Algoritmanın Tarifi

Algoritmanın adımları aşağıda verilmiştir.
Adım 1. Başlangıç için kaotik bir s-box tablosu seçilir.
Adım 2. Başlangıç tablosunun doğrusal olmama değeri hesaplanır.
Adım 3. Mevcut tabloda iki eleman seçilir ve yer değiştirilir.
Adım 4. Yeni tablosunun doğrusal olmama değeri hesaplanır.
Adım 5. Yeni doğrusal olmama değeri eski doğrusal olamama değerinden büyük ise tablo güncellenir.

4.3.2. Algoritmanın Performans Analizi

Önerilen algoritma, karmaşık optimizasyon süreçlerine odaklanmak yerine, doğrusal olmayan değeri 106.75 olan kaos tabanlı bir s-box yapısı ile başlamaktadır. Ardından doğrusal olmayan

değeri iyileştirir ve kısa sürede hızlı sonuçlar verir. Başlangıç için kaotik sistemlere dayalı örnek bir s-box yapısı Tablo 4.13 'de verilmiştir.

Tablo 4.13. Doğrusal olmama değeri 106.75 olan başlangıç tablosu

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

Tablo 4.14. Önerilen yeni S-box (Doğrusal olmama: 110)

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

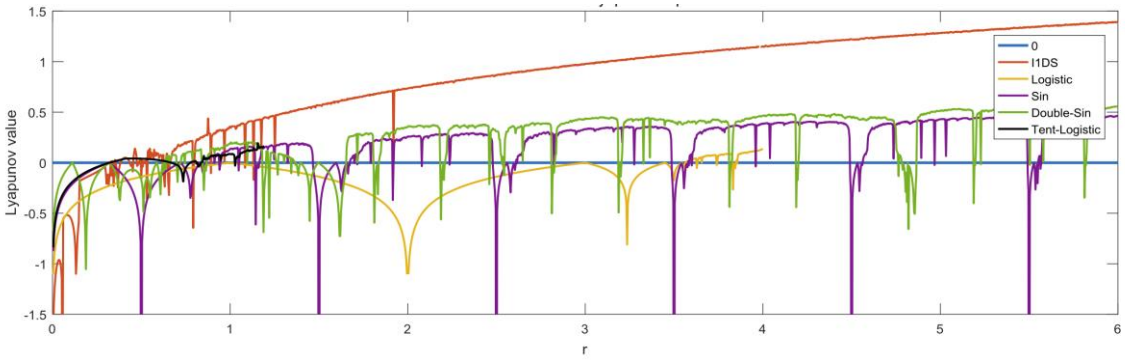
Tablo 4.13 'deki s-box, referans[65] 'deki s-box üreteci programı kullanılarak oluşturulmuştur. Daha sonra önerilen algoritma kullanılarak adım adım iki hücrenin yeri değiştirilmiştir. Analizler sonucunda toplam 12 yer değiştirmeden sonra giriş tablosunun doğrusal olmama değeri 106.75 'den 110 çıkarılmıştır. Sonuç olarak elde edilen yeni s-box yapısı Tablo 4.14 'de verilmiştir. Ayrıca başlangıç tablosunun 12 yer değiştirme sonundaki performans değişimi tablo 4.15 'de verilmiştir.

Tablo 4.15. Ara sonuçların performans karşılaştırması

S-box	Non.			BIC		SAC			XOR
	Ort	Max	Min	SAC	Non.	Ort	Min	Max	
Tablo 2.13	106.75	108	104	0.5003	104.36	0.4954	0.4062	0.625	10
Yer değiştirme 1	107.25	108	106	0.4999	103.93	0.4951	0.4062	0.625	10
Yer değiştirme 2	107.5	110	106	0.5003	103.71	0.4958	0.3906	0.625	10
Yer değiştirme 3	107.75	110	106	0.4992	103.57	0.4966	0.3906	0.625	10
Yer değiştirme 4	108	110	106	0.4992	103.64	0.4966	0.3906	0.625	10
Yer değiştirme 5	108.25	110	106	0.4987	103.43	0.4961	0.3906	0.625	10
Yer değiştirme 6	108.5	110	106	0.4932	103.43	0.4958	0.4062	0.625	10
Yer değiştirme 7	108.75	110	106	0.4979	103.5	0.4951	0.4062	0.625	10
Yer değiştirme 8	109	110	108	0.5022	103.5	0.4941	0.4062	0.6092	10
Yer değiştirme 9	109.25	110	108	0.5001	103.5	0.4954	0.4062	0.6092	10
Yer değiştirme 10	109.5	110	108	0.5021	103.21	0.4949	0.4062	0.6094	10
Yer değiştirme 11	109.75	110	108	0.5006	103.21	0.4978	0.4219	0.6094	10
Yer değiştirme 12 (Tablo 2.13)	110	112	108	0.504	103.14	0.499	0.4219	0.6094	10

4.4. Basamaklandırılmış Kaotik Haritalar Kullanılarak Performans İyileştirmesi

Kaotik sistemler birçok pratik uygulamada başarılı sonuçlar ürettikten sonra [12], yeni kaotik sistemler araştırılmıştır. Literatürde, kaotik sistemlerin kombinasyonları kullanılarak daha sağlam bir entropi kaynağının üretilebileceği gösterilmiştir [65]. Bir sistemdeki kaotik davranışı analiz etmek için çeşitli alternatifler vardır. En popüler kaos analiz araçlarından biri Lyapunov üsleridir. Rus matematikçi Aleksandr Mihayloviç Lyapunov tarafından önerilen bu kriter, doğrusal olmayan sistemlerin özdeğerleri olarak ifade edilir ve pozitif Lyapunov üstel değeri, kaotik davranışın nicel bir göstergesi olarak kullanılır [66]. Farklı kaotik sistemler için Lyapunov üsleri Şekil 4.3 'de verilmiştir. Şekil 4.3 'de de görülebileceği gibi, çadır ve sinüs haritasının birleşimi olan sistemin entropisinin Lyapunov üs değerinin daha büyük olması nedeniyle daha yüksek olduğu belirtilmektedir. Çalışmanın çıkış noktası kaotik sistemlerin bu hibrit yapısı üzerine kurulmuştur.



Şekil 4.3. Farklı kaotik sistemler için Lyapunov üslerinin karşılaştırılması

Kaotik sistemler basamaklandırılarak güçlü bir entropi kaynağı elde edilmiştir. Daha sonra bu entropi kaynağı kullanılarak 50000 farklı s-box yapısı oluşturulmuştur. Bu s-box yapıları, beş farklı s-box tasarım kriteri altında analiz edilmiştir. Üretilen s-box yapıları arasında doğrusal olmama değeri 106.75 olan iki farklı s-box yapısının olduğu gözlemlenmiştir. Bu değerler, literatüre bakıldığında yalnızca kaotik sistemler kullanılarak elde edilebilecek en yüksek doğrusal olmama değeridir. İleride yapılacak çalışmalarda bu başarılı s-box yapılarının blok şifreleme, görüntü şifreleme algoritması, anahtar üreteci ve kriptografik maske gibi farklı bilgi güvenliği uygulamalarında kullanılabileceği düşünülmektedir. Çalışmada basit matematiksel modelleri nedeniyle dört farklı ayrık zamanlı kaotik sistem kullanılmıştır. Kullanılan kaotik sistemlerin detayları denklem 4.1, 4.2, 4.3, 4.4 'da verilmiştir.

$$x_{n+1} = a * x_n * (1 - x_n) \qquad x_n \in [0,1], a \in [3.5, 4] \tag{4.1}$$

$$x_{n+1} = \begin{cases} b * x_n & x_i < 0.5 \\ b * (1 - x_n) & x_i \geq 0.5 \end{cases} \quad x_n \in [0,1], b \in [1, 2] \tag{4.2}$$

$$x_{n+1} = c * \sin(\pi x_n) \qquad x_n \in [0,1], c \in [0.85, 4] \tag{4.3}$$

$$x_{n+1} = x_n + d - \frac{e}{2\pi} \sin(2\pi x_n)\ mod\ 1 \quad x_n \in [0,1],\ d \in [0,1], e \in [0, 4\pi] \tag{4.4}$$

Seçilen kaotik sistemlerin bir diğer avantajı da optimizasyon algoritmaları ile optimum başlangıç koşullarının belirlenmesidir [67]. Önerilen mimaride, dört farklı kaotik sistem birbiri ardına basamaklandırılmış ve sağlam bir entropi kaynağı oluşturulmuştur. Bu entropi kaynağı, basit bir dönüşüm algoritması ile s-box yapılarına dönüştürülmüştür.

4.4.1. Algoritmanın Tarifi

Önerilen dönüşüm algoritmasının adımları aşağıda verilmiştir.

Adım 1. Rastgele bir değer üretilir.

Adım 2. Bu rastgele değer denklem 3 ‘e göre işleme alınır.

Adım 3. Denklem 3 ‘den gelen değer denklem 4 ‘ e göre işleme alınır.

Adım 4. Denklem 4 ‘den gelen değer denklem 5 ‘ e göre işleme alınır.

Adım 5. Denklem 5 ‘den gelen değer denklem 6 ‘ e göre işleme alınır.

Adım 4. Denklem 6 ‘dan gelen kesirli değer olan durum değişkeni değeri mod 256 uygulanarak 0-255 arasında bir ondalık değere dönüştürülür.

Adım 5. Ondalık değer s-kutusuna dahil değilse eklenir, aksi takdirde yeni bir durum değişkeni değeri hesaplanır ve tablo dolana kadar devam edilir.

4.4.2. Algoritmanın Performans Analizi

Bu algoritma ile 50000 farklı s-box tablosu oluşturulmuştur. Her bir farklı s-box yapısını oluşturmak için farklı bir başlangıç koşulu rastgele seçilir. Yalnızca kaotik sistem çıktılarının s-box değerlerine dönüştürüldüğü çalışmalarda; Ulaşılabilecek en yüksek doğrusal olmama değerinin 106,75 olduğu daha önceki çalışmalarda gösterilmiştir [28]. Bu çalışmada üretilen 50000 s-box yapıdan ikisi için bu sonuca ulaşılmıştır. Bu s-box yapılarından bir tanesi Tablo 4.16 ‘da verilmiştir. 106.75'in farklı dönüşümler veya optimizasyon algoritmaları kullanılarak iyileştirilebileceği gösterilmiştir.

Tablo 4.16. Önerilen yöntem ile üretilmiş, doğrusal olmama değeri 106.75 olan s-box

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

4.5. Yeni Bir Kaotik Sistem ve S-box Üretiminde Kullanımı

Kaotik s-box yapıları için ulaşılabilecek en yüksek doğrusal olmama değerinin 106.75 olabileceği birçok çalışmada önerilen tasarımlarda test edilmiştir[28]. Bu bölümde kaos temelli s-box yapıları için en kapsamlı çalışmalardan biri gerçekleştirilmiştir. Çalışmada yedi farklı kaotik sistemin her biri kullanılarak 10.000 s-box, toplamda 70.000 farklı s-box yapısı üretilmiştir. Bu kaotik sistemlerden altısı daha önce literatürde bilinen kaotik sistemlerdir. Yedinci kaotik sistem ise bu çalışmada ilk defa önerilmiş çalışmanın özgün bir katkısıdır. Yeni önerilen kaotik sistem kullanılarak üretilen s-box yapıları arasında doğrusal olmama değerinin bilinen en yüksek değeri geçebileceği gösterilmiş olması çalışmanın literatüre bir diğer katkısıdır. Yeni en yüksek doğrusal olmama değeri olan 107 değeri için çalışmada iki farklı s-box yapısı sunulmuştur. 70.000 s-box yapısı arasında doğrusal olmama değeri 106 ve üzeri olanlar bir açık veri seti olarak paylaşılmıştır. Veri seti 289 farklı s-box yapısını içermektedir. Blok şifreler, hash fonksiyonları ve rasgele sayı üreteçleri gibi çeşitli uygulamalarda bu veri setinin kriptologlara çeşitli avantajlar sağlayacağı düşünülmektedir.

Kaos temelli şifreleme algoritmalarının tasarımında çok farklı kaotik sistemler kullanılmıştır. Ancak yapılan çalışmalar kaotik sistemin türünden ziyade dönüşüm fonksiyonunun daha önemli olabileceğini göstermiştir. Bu yüzden çalışmada özellikle ayrık zamanlı kaotik sistemlere odaklanılmıştır. Çünkü ayrık zamanlı kaotik sistemsel basit matematiksel modelleri sayesinde diğer kaotik sistem türlerine bir avantaja sahiptir. Çalışmada literatürde yaygın biçimde çalışılmış altı farklı kaotik sistem kullanılmıştır. Bu sistemlerin matematiksel modelleri sırasıyla denklem 4.5-4.10 ’da verilmiştir.

Lojistik Harita:

$$x_{n+1} = a x_n (1 - x_n)\,, \quad x_n \in [0,1]\,, \quad a \in [3.5, 4] \tag{4.5}$$

Çadır Harita:

$$x_{n+1} = \begin{cases} a x_n & x_i < 0.5 \\ a(1 - x_n) & x_i \geq 0.5 \end{cases}, \quad x_n \in [0,1]\,, \quad a \in [1,2] \tag{4.6}$$

Sinüs Harita:

$$x_{n+1} = a \sin(\pi x_n)\,, \quad x_n \in [0,1]\,, \quad a \in [0.85,1] \tag{4.7}$$

Daire Harita:

$$x_{n+1} = x_n + a - \frac{b}{2\pi} \sin(2\pi x_n) mod 1\,, \quad x_n \in [0,1]\,, \quad a \in [0,1]\,, b \in [0,4\pi] \tag{4.8}$$

May Harita:

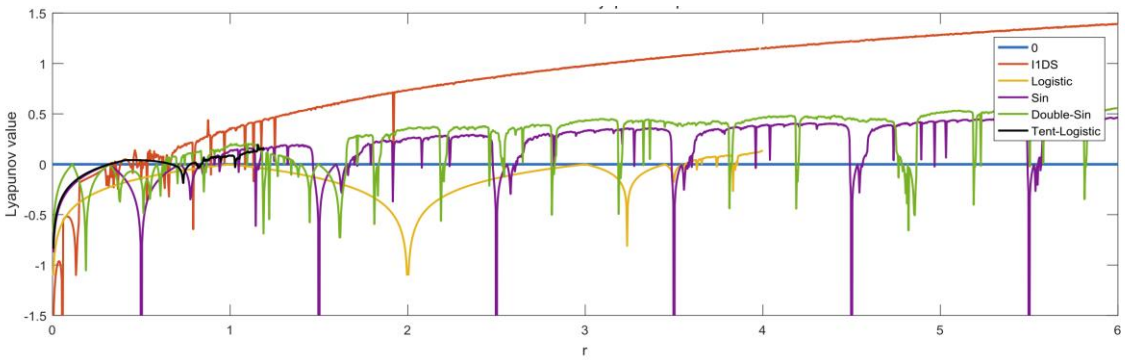
$$x_{n+1} = x_n \exp[a(1 - x_n)], \quad a \in [0,5] \tag{4.9}$$

Gauss Harita:

$$x_{n+1} = exp(-a{x_n}^2) + c, \quad a \in [4.7,17], c \in [-1,1] \tag{4.10}$$

4.5.1. Yeni Kaotik Sistem

Yeni kaotik sistemler, kaos teorisi ile ilgili çalışmalarda her zaman ilgi çekici bir konu olmuştur. Bilim ve mühendislik çalışmalarında sistem ve süreçleri en etkin şekilde modelleyebilecek matematiksel modeller ararken araştırmacılar farklı kaotik sistemlerle karşılaşmışlardır. Son zamanlarda, kaotik sistemlerin birleştirilmesiyle yeni kaotik sistemlerin elde edilebileceği gösterilmiştir. Wang ve arkadaşları birçok alanda başarılı uygulamaları olan lojistik harita ile sinüs haritasının birleştirilmesiyle yeni bir kaotik sistemin elde edilebileceğini ileri sürmüşlerdir [68]. Bu kaotik sistemin (I1DS) bilgi güvenliği uygulamalarında başarılı sonuçlar üretebildiği bir görüntü şifreleme algoritması üzerinden gösterilmiştir. Önerilen şifreleme mimarisinin başarısı, kaotik sistemin karmaşık davranışı ile ilişkilendirilmiştir. Çünkü önerilen yeni kaotik sistem, lojistik harita ve sinüs haritasından daha karmaşık bir yapıya sahiptir. Nicel bir kaos analiz aracı olan Lyapunov üsleri, yeni önerilen kaotik sistemlerin daha karmaşık bir entropi kaynağı içerdiğini göstermiştir. Örneğin Şekil 4.4 'de diğer kaotik sistemlerin Lyapunov üslerinin I1DS sistemi ile karşılaştırılması verilmiştir.



Şekil 4.4. Farklı kaotik haritalar için Lyapunov üsleri[33]

Bir sistemin pozitif Lyapunov üsteline sahip olması kaotik davranışın göstergesidir. Pozitif lyapunov üstelinin büyüklüğü ise sistemin karmaşasının (entropisinin) yüksek olması olarak yorumlanmaktadır. Yani denklem 4.5-4.10 arasındaki modeller birleştirilerek daha karmaşık bir model elde edilebilir mi? Bu kapsamda denklem 4.11'deki modelin kullanılmasının kriptolojik amaçlar için ne gibi bir katkı sunacağı bu çalışmada araştırılmıştır.

$$x_{n+1} = \frac{exp(x_n{}^2)}{\sin(2\pi x_n a)} + c, \quad a \in [1,5], c \in [-10,10] \tag{4.11}$$

4.5.2. Yeni Kaotik Sistemin Performans Analizi

Denklem 4.5-4.11 arasında matematiksel ifadesi, başlangıç koşulları ve kontrol parametreleri verilen kaotik sistemlerin her biri için 10000 olmak üzere toplamda 70000 s-box yapısı elde edilmiştir. Bu s-box yapılarından doğrusal olmama değeri 106 ve üzeri olanlar veri seti olarak kayıt edilmiştir. Tablo 4.17 'de her bir kaotik sistem için 106 ve üzeri doğrusal olmama değerine sahip s-box sayıları gösterilmiştir.

Tablo 4.17. 106 ve üzeri doğrusal olmama değerine sahip s-box sayısı

Kaotik Harita	Doğrusal Olmama Değeri					
	106	**106,25**	**106,5**	**106,75**	**107**	**Toplam**
Lojistik	18	9	1	0	0	28
Sinüs	20	14	3	1	0	38
Çadır	24	13	5	1	0	43
Daire	23	16	2	1	0	42
May	27	9	4	2	1	43
Gauss	22	15	4	2	0	43
Önerilen	27	17	5	2	1	52
Toplam	161	93	24	9	2	289

Ayrıca üretilen tüm s-box yapıları için hesaplanan doğrusal olmama değerlerinin ortalaması Tablo 4.18 'de verilmiştir.

Tablo 4.18. Üretilen tüm s-box yapıları için doğrusal olmama değerlerinin ortalaması

Lojistik Harita	**Sinüs Harita**	**Çadır Harita**	**Daire Harita**	**May Harita**	**Gauss Harita**	**Önerilen Harita**	**Tüm S-box Yapıları**
103,280725	103,52935	103,528	103,530325	103,45525	103,536825	103,527425	103.49

Tablo 4.18 'deki sonuçlar analiz edildiğinde büyük resme bakıldığında kaotik sistem türünün referans [69] 'da ifade edildiği gibi performansı çok fazla etkilemediği doğrulanmaktadır. Ancak sonuçlara daha spesifik bakıldığında doğrusal olmama değeri 107 olan iki s-box yapısının elde edildiği gözlemlenmiştir. Bu güne kadar elde edilmiş en yüksek değerin iyileştirilebileceğine işaret etmektedir. Tablo 4.19 ve Tablo 4.20 'de bu s-box yapıları ve Tablo 4.21 'de ise bu s-box 'ların tasarım kriterleri için hesaplanan analiz sonuçları verilmiştir.

Tablo 4.19. Önerilen harita kullanılarak elde edilen S-box (Doğrusal olmama: 107)

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

Tablo 4.20. May harita kullanılarak elde edilen S-box (Doğrusal olmama: 107)

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

Tablo 4.21. Doğrusal olmama değeri 107 bulunan s-box yapılarının performans ölçütleri

S-box	Non.			BIC		SAC			XOR
	Ort	Min	Max	SAC	Non.	Ort	Min	Max	
Tablo 2.18	107	104	110	0.497	103.07	0.5012	0.4062	0.6094	12
Tablo 2.19	107	104	108	0.4991	102.93	0.5037	0.4219	0.5781	12

4.6. Genetik Algoritma Temelli S-box Üretme Yöntemi

Bu yöntemde doğrusal olmayan değerler genetik algoritma ile iyileştirilmeye çalışılmıştır. Bunun için öncelikle bir başlangıç popülasyonunun elde edilmesi gerekmektedir. Kaotik sistemler başlangıç popülasyonlarının elde edilmesinde başarılı sonuçlar sağladığından[70], çalışmada kaotik sistemler kullanılarak başlangıç popülasyonları elde edilmiştir. Önerilen yöntemde ilk olarak kaotik sinüs harita kullanılarak bir s-box oluşturulmuştur. Daha sonra genetik algoritmanın çaprazlama ve mutasyon birimleri uygulanarak başlangıç tablosu optimize edilmiştir.

4.6.1. Algoritmanın Tarifi

Algoritmanın adımları aşağıda verilmiştir.

Adım 1. Başlangıç popülasyonu oluşturma: Başlangıç popülasyonu olarak kullanılacak s-box ‘ı elde etmek için kaotik sinüs harita kullanılmıştır. Bu aşamaya kadar verilen s-box elde etme, diğer bir deyişle rastgele seçimlerle s-box elde etme yaklaşımı literatürdeki çözüm önerilerinden pek farklı değildir. Bu çalışmanın orijinal yönü, genetik algoritmanın bir son işleme tekniği olarak kullanılmasını önermesidir. Çünkü çalışmanın çıkış noktası, s-box doğrusal olmayanlık değerinin çeşitli son işleme teknikleri ile iyileştirilebileceğini belirten önceki çalışmalardır [62, 63, 64].

Adım 2. Uygunluk değerinin hesaplanması: Uygunluk değeri seçilen s-box ‘ın doğrusal olmama değeridir. Bu adımda bu değer hesaplanır.

Adım 3. Çaprazlama ve mutasyon: Asıl işlemin gerçekleştiği adım burasıdır. Giriş olarak alınan kaotik s-box ‘da önce çaprazlama daha sonra mutasyon işlemi uygulanır.

- Çaprazlama: Çaprazlama işleminde s-box ‘da bulunan iki satır veya iki sütun rastgele yer değiştirilir. Çaprazlama adımından sonra yeni s-box ‘ın doğrusal olmama değeri hesaplanır. Bu değer uygunluk değerinden büyük veya eşit ise bu kromozom bir sonraki nesle aktarılır.
- Mutasyon: Çaprazlamadan gelen kromozomun iki değeri sırasıyla yer değiştirir. Yeni s-box ‘ın doğrusal olmama değeri hesaplanır. Bu değer uygunluk değerinden büyük veya eşit ise bu kromozom bir sonraki nesle aktarılır.

Önerdiğimiz yöntemin diğer yöntemlerden en önemli ve özgün farkı; çaprazlama ve mutasyon işlemlerinden sonra aynı doğrusal olmama değerine sahip kromozomların bir sonraki nesle

aktarılmasıdır. Bu sayede nesil çeşitliliği artar ve daha çok kromozom bir sonraki nesle aktarılmış olur.

4.6.2. Algoritmanın Performans Analizi

Giriş için üretilen kaotik s-box ve önerilen yöntem sonucunda çıkışta elde edilen yeni s-box ‘ın performans değerleri Tablo 4.22’de verilmiştir.

Tablo 4.22. Girişte alınan ve çıkışta elde edilen s-box ‘ların performans değerleri

S-Box	Non.			BIC		SAC			XOR
	Ort	Max	Min	SAC	Non.	Min	Max	Ort	
Giriş	100.25	106	96	0.5027	103.29	0.3594	0.5938	0.5049	12
Çıkış	111.75	112	110	0.5033	104	0.4062	0.6094	0.4968	12

Tablo 4.22 ‘ye bakıldığında önerilen yöntem ile doğrusal olmama değeri 100.25 den 111.75 e çıkarılmıştır. Buda önerilen algoritmanın ne kadar etkili çalıştığını göstermektedir. Çıkışta elde edilen s-box ise Tablo 4.23 ‘de verilmiştir.

Tablo 4.23. Çıkışta elde edilen s-box (Doğrusal olmama: 111.75)

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

4.7. Yer Değiştirme Temelli Son İşlem Tekniğinin İyileştirilmiş Versiyonu

Bu bölümde s-box ‘ların performansını iyileştirmek için iki algoritma önerilmiştir. Önerilen algoritmalar yer değiştirme tabanlı algoritmalardır. Bunlar Algoritma-1 ve Algoritma-2 olarak adlandırılmıştır.

4.7.1. Algoritmanın Tarifi

Algoritma 1 ‘de her seferinde iki elemanın yeri değiştirilerek yeni doğrusal olmama değeri hesaplanır. Yeni doğrusal olmama değeri eski doğrusal olmama değerinden büyük ise doğrusal olmama değeri güncellenir. Algoritma-1 bu şekilde tüm elemanların yerini değiştirerek optimum değere ulaşmayı hedefler. Ancak referans [64] ‘de ifade edildiği gibi bu algoritma doğrusal olmama değerini 110 ‘a kadar arttırmaktadır. Algoritma-1 ‘in adımları aşağıda verilmiştir.

Algoritma-1:

Adım 1. Başlangıç için kaotik bir s-box tablosu seçilir.
Adım 2. Başlangıç tablosunun doğrusal olmama değeri hesaplanır.
Adım 3. Mevcut tabloda iki eleman seçilir ve yer değiştirilir.
Adım 4. Yeni tablosunun doğrusal olmama değeri hesaplanır.
Adım 5. Yeni doğrusal olmama değeri eski doğrusal olamama değerinden büyük ise tablo güncellenir.

Algoritma 2 ‘de ise yine aynı şekilde her seferinde iki elemanın yeri değiştirilerek yeni doğrusal olmama değeri hesaplanır. Yeni doğrusal olmama değeri eski doğrusal olmama değerinden büyük veya eşit ise doğrusal olmama değeri güncellenir. Yani Algoritma-2 ‘nin farkı aynı doğrusal olmama değerlerine sahip durumları da kabul edip yer değiştirme işlemini gerçekleştirmesidir. Bu şekilde, algoritma-1 kullanılarak 110 değerine kadar arttırılan s-box ‘lar Algoritma-2 ‘ye giriş olarak verilir. Algoritma-2 tüm doğrusal olmama değerlerini 111 ve üstü değerlere çıkarmaktadır. Algoritma-2 ‘nin adımları aşağıda verilmektedir.

Algoritma-2:

Adım 1. Başlangıç için kaotik bir s-box tablosu seçilir.
Adım 2. Başlangıç tablosunun doğrusal olmama değeri hesaplanır.
Adım 3. Mevcut tabloda iki eleman seçilir ve yer değiştirilir.
Adım 4. Yeni tablosunun doğrusal olmama değeri hesaplanır.
Adım 5. Yeni doğrusal olmama değeri eski doğrusal olamama değerinden büyük veya eşit ise tablo güncellenir.

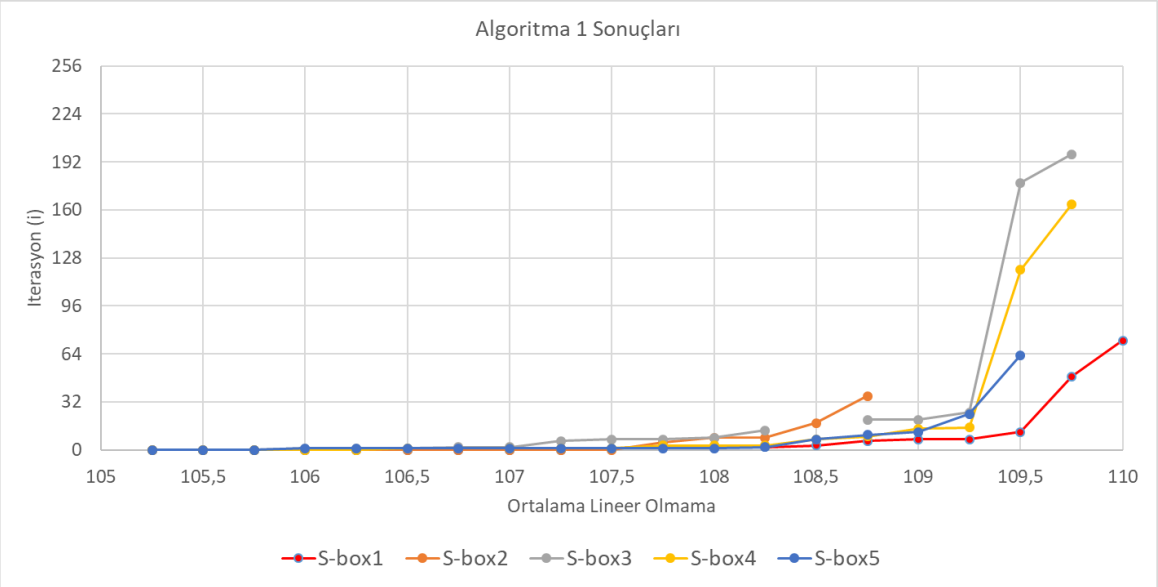
4.7.2. Algoritmanın Performans Analizi

Öncelikle kaotik gauss harita kullanılarak doğrusal olamama değeri 105 olan 5 tane s-box üretilmiştir. Bu s-box 'lar, algoritma 1 ve algoritma 2 sonucunda elde edilen s-box 'ların performans değerleri Tablo 4.24 'de verilmiştir.

Tablo 4.24. Giriş s-box 'ları, algoritma 1 ve algoritma 2 sonucunda elde edilen s-box 'ların performans değerleri

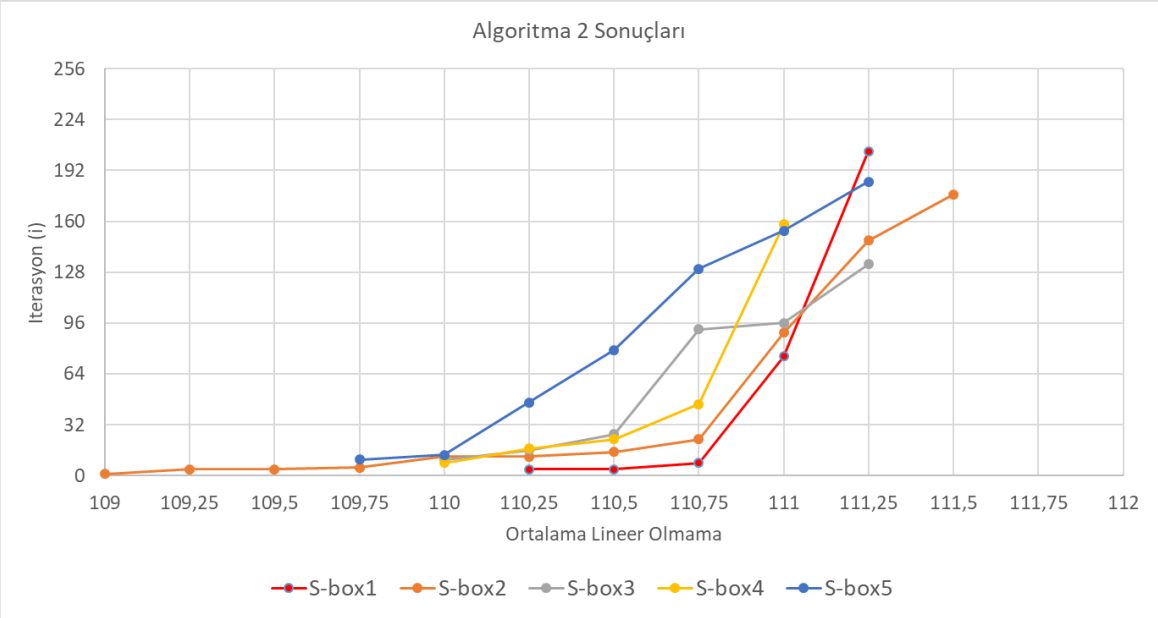
S-Box		Non.			BIC		SAC			XOR
		Ort	Min	Max	Non.	SAC	Ort	Min	Max	
Giriş	**S-box 1**	105	100	108	103.14	0.4987	0.5002	0.3906	0.5938	12
	S-box 2	105	104	106	103.29	0.4983	0.5088	0.4219	0.6094	10
	S-box 3	105	98	108	104.57	0.5013	0.502	0.3906	0.5938	12
	S-box 4	105	102	108	103.43	0.5001	0.5029	0.4062	0.6094	12
	S-box 5	105	102	108	103.93	0.4964	0.51	0.4219	0.625	12
Algoritma 1	**S-box 1**	110	108	112	103.36	0.5066	0.499	0.4219	0.5781	10
	S-box 2	108.75	108	110	103	0.4975	0.5081	0.4219	0.5938	12
	S-box 3	109.75	108	110	104.29	0.4967	0.4988	0.3906	0.6094	10
	S-box 4	109.75	108	112	103.29	0.498	0.5056	0.4062	0.5938	12
	S-box 5	109.5	108	110	103.57	0.4948	0.5056	0.4219	0.5938	10
Algoritma 2	**S-box 1**	111.25	110	112	102.57	0.4972	0.5049	0.3906	0.5781	12
	S-box 2	111.5	110	112	103.64	0.4985	0.4978	0.3906	0.5938	10
	S-box 3	111.25	110	112	103.5	0.4999	0.5085	0.4375	0.625	12
	S-box 4	111	110	112	103.71	0.501	0.5027	0.4219	0.5938	10
	S-box 5	111.25	110	112	102.57	0.4958	0.4998	0.375	0.5781	12

Algoritma-1 kullanılarak elde edilen s-box 'ların doğrusal olamama değerlerinin hangi iterasyonlarda arttığı şekil 4.5 'de verilmiştir. Şekil 4.5 'e bakıldığında sadece birinci iterasyonda bile doğrusal olamama değeri 107.5 'e kadar çıkabilmektedir. Bu değer bile literatürdeki birçok çalışmadan daha iyi bir sonuç olduğunu göstermektedir. Algoritma-1 ile optmize edilen s-box 'lara bakıldığında en yüksek değere 110 ile s-box 1, en düşük değerde ise 108.75 ile s-box 2 ulaşmıştır.



Şekil 4.5. Algoritma-1 ile doğrusal olmama değerindeki değişim

Algoritma-1 ile optimize edilmiş s-box ‘lar algoritma-2 ‘ye giriş olarak verilmektedir. Bu sayede en fazla 110 değerine kadar artan s-box ‘lar 111 ve üzeri değerlere çıkmaktadır. Bu değerler için şifreleme algoritmalarının güvenliğini önemli ölçüde arttırabilecektir. Algoritma-2 kullanılarak elde edilen s-box ‘ların doğrusal olamama değerlerinin hangi iterasyonlarda arttığı şekil 4.6 ‘da verilmiştir.



Şekil 4.6. Algoritma-2 ile doğrusal olmama değerindeki değişim

Algoritma-2 ile optmize edilen s-box ‘lara bakıldığında en yüksek değere 111.5 ile s-box 2, en düşük değere ise 111 ile s-box 4 ulaşmıştır. Bu algoritmalar sonucunda elde edilen en güçlü s-box Tablo 4.25 ‘de verilmiştir.

Tablo 4.25. Algoritma-2 ile Optimize Edilmiş S-box 2 (Doğrusal Olmama: 111,5)

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

5. JPEG ALGORİTMASI İÇİN YENİ NİCELEME TABLOSU ÜRETEÇLERİ

Dördüncü bölümde kaos temelli s-box yapılarının öneminden ve bu sahip olduğu önemden dolayı performans iyileştirmesinin literatüre nasıl kritik bir katkı yapacağından bahsedilmiştir. Önerilen yöntemlerle de s-box performans kriterlerinin iyileştirilebileceği gösterilmiştir. Tez çalışmasının bir diğer önemli katkılarından bir tanesi de s-box yapıları ile niceleme tabloları arasındaki benzerliktir. Her halükârda ikisi de n bitlik girişleri m bitlik çıkışlara dönüştüren bir dönüşüm fonksiyonudur. Buradan hareketle s-box yapılarında kullanılan rastgele üretim mekanizmasının niceleme tabloları üretiminde kullanılıp kullanılamayacağı tez çalışması kapsamında ele alınan bir diğer araştırma sorusudur. Bu bölümde iki farklı yaklaşım geliştirilerek kaotik sistemler temelli niceleme tablosu üreteçlerinin nasıl elde edilebileceği gösterilmiş olup, yöntemlerin detayları ve performans analizleri kapsamlı bir şekilde açıklanmıştır.

5.1. Kaos Temelli Niceleme Tablosu Üreteç Yaklaşımı

Birçok harika tasarım örneğinde olduğu gibi JPEG algoritmasında da matematiksel modellemenin eşsiz örneklerinden biridir. Aslında algoritmanın ilk üç adımı sayısal görüntü işleme süreçlerinde kullanılan standart aşamaları temsil etmektedir. Ayrık kosinüs dönüşümü verinin daha efektif bir şekilde temsiline hizmet etmektedir. Bir başka ifade ile algoritmanın başarısını etkileyecek aşamalar niceleme ve kodlama süreçleri olacaktır.

Niceleme aşaması ile verideki fazlalıkların atılması amaçlanmaktadır. Algoritmanın kayıplı veri sıkıştırma kategorisinde sınıflandırılmasının sebebi olan kayıplar bu aşama ile ilişkilidir. Dönüştürülmüş görüntü DCT matrisini kullanan niceleme matrisi ile bölerek nicelemeyı elde eder. Ortaya çıkan matrisin değerleri daha sonra yuvarlanır. Niceleme, daha az önemli olan yüksek frekanslı DCT katsayılarının çoğunu sıfıra indirmeyi amaçlamaktadır. Sıfırların sayısı ne kadar fazla olursa görüntünün sıkıştırma oranı o kadar yüksek olacaktır. JPEG algoritmasında sırasıyla Tablo 5.1 ve Tablo 5.2 ‘de verilen Parlaklık ve Renklilik bileşenleri için farklı niceleme tabloları kullanılmaktadır. JPEG niceleme tablolarında, genel olarak parlaklık özelliği değişir. Çünkü bu bileşendeki küçük değişiklikler normal gözlerle görülemeyeceği için kaliteye etkisi kısıtlı olur.

Tablo 5.1. JPEG parlaklık niceleme tablosu

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	16	11	10	16	24	40	51	61
1	12	12	14	19	26	58	60	55
2	14	13	16	24	40	57	69	56
3	14	17	22	29	51	87	80	62
4	18	22	37	56	68	109	103	77
5	24	35	55	64	81	104	113	92
6	49	64	78	87	103	121	120	101
7	72	92	95	98	112	100	103	99

Tablo 5.2. JPEG renklilik niceleme tablosu

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	17	18	24	47	99	99	99	99
1	18	21	26	66	99	99	99	99
2	24	26	56	99	99	99	99	99
3	47	66	99	99	99	99	99	99
4	99	99	99	99	99	99	99	99
5	99	99	99	99	99	99	99	99
6	99	99	99	99	99	99	99	99
7	99	99	99	99	99	99	99	99

JPEG ‘de kalite faktörleri(QF) sayesinde görüntünün sıkıştırma oranı ve bozulma oranı kontrol edilebilmektedir. Her bir kalite faktörü için niceleme tablosundaki değer denklem 5.1 ’de verildiği gibi hesaplanmaktadır.

$$Q_{i,j} = \frac{50+S+D_{i,j}}{100} \tag{5.1}$$

Burada $Q_{i,j}$ hesaplanmak istenen tablonun bir değerini, $D_{i,j}$ ise standanrt niceleme tablosundan gelen değerdir. Buradaki S değeri ise denklem 5.2 ‘de gösterildiği gibi hesaplanmaktadır. Q, kalite faktörüdür.

$$\begin{cases} S = 200 - 2Q\ , & Q \geq 50 \\ S = \frac{5000}{Q}\ , & Q < 50 \end{cases} \tag{5.2}$$

Ayrıca Q, 0 ’dan küçük veya eşit olduğu durumlarda 1, 100 ‘den büyük olduğu durumlarda ise 100 olarak kabul edilmektedir.

Yukarıda ifade edildiği gibi, sıkıştırma performansını etkileyebilecek iki aşamadan biri niceleme tabloları olduğu için literatürde bu konuda çeşitli çalışmalar gerçekleştirilmiştir. Bu çalışmalar üç ana kategoride listelenebilir. Bunlar, oran-bozulma, insan görsel sistemi ve optimizasyon temelli yaklaşımlardır.

5.1.1. Oran-Bozulma Yaklaşımı

Oran-bozulma yaklaşımı, görüntü ve video sıkıştırma algoritmalarının optimize edilmesinde önemli bir rol oynamıştır. Düşük bit değerleri ve yüksek bozulmaya karşılık gelen bir niceleme tablosundan başlayarak ölçüm tablosunun bir girişi güncellenir, böylece her adımda, bozulmadaki düşüşün bit oranındaki artışa oranı yaklaşık olarak en üst düzeye çıkarılır. Oran-bozulma metodunu kullanarak niceleme tablosunu oluşturmak için aşağıdaki adımlar kullanılmaktadır.

- Yüksek bozulma ve düşük bit değerine karşılık gelen bir ölçüm tablosu alınır.
- Her adımda bir niceleme tablosu girişi güncellenir. Böylece bit oranı artar ve bozulma azalır.
- Adım 2 ve 3, istenen bit oranı elde edilinceye kadar tekrar edilir.

5.1.2. İnsan Görsel Sistemi Yaklaşımı

İnsan görsel sisteminde, belirli bir bit oranı için optimum görsel kalite, jpeg algoritması için niceleme tablosunu tasarlamak bir kılavuz olarak kullanılır. Bu nedenle, niceleme tablosunun tasarımı, çeşitli Ayrık Kosinüs Dönüşümü frekanslarında meydana gelen niceleme hatalarına bağlıdır. İnsan görsel sistemi yüksek frekanslı değerlere daha az hassastır. Bu nedenle sıkıştırmanın daha çok bu yüksek frekanslı değerlere uygulanması amaçlanmaktadır. Bu şekilde insan gözünün algılayamayacağı şekilde daha yüksek sıkıştırma oranları elde edilebilir. Niceleme tablosunu oluşturmak için İnsan Görsel Sisteminde, Görüntüden Bağımsız Algısal Yaklaşım ve Görüntüye Bağlı Algısal Yaklaşım olmak üzere iki yaklaşım kullanılmaktadır.

5.1.3. Meta-Sezgisel Yaklaşımlar

JPEG temel algoritması için niceleme tablosunun oluşturulması optimizasyon problemi olarak görülmektedir. Optimizasyon problemlerinin çoğu son yıllarda meta-sezgisel yaklaşımlar uygulanarak çözülmüştür. Meta-sezgisel yaklaşımlar, optimizasyon problemine en uygun çözümü

sağlamak için doğayı taklit eder. Son yıllarda, JPEG temel algoritmasında niceleme tablosu oluşturmak için Meta-Sezgisel yaklaşımları içeren birçok çalışma bulunmaktadır.

5.1.4. Niceleme Tablolarına İlişkin Literatürdeki Gelişmeler

Yeni ve etkili niceleme tabloları oluşturmak için geçmişten günümüze pek çok çalışma yapılmıştır. Bu çalışmalardan bazıları aşağıda açıklanmıştır.

Oran bozulma yaklaşımında bit oranı yerine hesaplanmış entropi (sıkıştırma algoritması tarafından kodlanması gereken bilgi miktarı) kullanılmıştır. Nicelenen görüntünün entropisi, hesaplama karmaşıklığını azaltmak için kullanılır. Ayrıca, entropiye karşı bit oranı eğrisinin doğrusal bir ilişki sağladığı bulunmuştur. Bu yöntemi kullanmanın avantajı, belirli bir görüntü için geliştirilen optimize edilmiş tablonun benzer içeriğe sahip diğer görüntülerde kullanılabilmesidir [71]. Niceleme tablosu tasarlamak için RD-OPT yöntemi önerildi. Bu yöntemde arama stratejisinin dezavantajı, onun hesaplama karmaşıklığıdır. Tüm sıkıştırma-açma adımlarını izlemek yerine, niceleme tablolarını daha verimli bir şekilde değerlendirmektedir [72]. DCT frekansındaki gri tonlamalı görüntü üzerinde psiko-görsel bir hata eşiği araştırıldı. Yeni niceleme tablosu, belirli eşiğin psiko-görsel hataya ayarlanmasıyla oluşturulmuştur. Psiko-görsel hata eşiği kullanılarak oluşturulan sıkıştırılmış görüntünün kalitesinin, huffman kodunun daha düşük ortalama bit uzunluğunda standart JPEG niceleme tablosu kullanılarak oluşturulan sıkıştırılmış görüntünün kalitesine kıyasla daha iyi olduğu bulunmuştur [73]. JPEG sıkıştırma için niceleme tablosunu optimize etmek için algısal görüntü kalitesi değerlendirmesini kullandı. PSNR, algısal görüntü kalitesinin zayıf bir ölçüsü olarak kullanıldı. Bu nedenle, performansı değerlendirmek için Yapısal Benzerlik Endeksi (SSIM) adı verilen yeni bir yöntem kullanılmıştır. SSIM kullanılarak oluşturulan ölçüm tablosu, standart ölçüm tablosu kullanılarak oluşturulan görüntüden daha iyi kalitede sıkıştırılmış görüntü üretmiştir [74]. Tıbbi görüntüler için daha yüksek sıkıştırma performansı üreten JPEG temel algoritmasında niceleme tablosu oluşturmak için genetik algoritma (GA) kullanıldı. Amaç, bit oranı ve kod çözme kalitesi açısından daha iyi sıkıştırma verimi sağlayan ölçüm tabloları oluşturmaktır. Her yineleme sırasında, genetik algoritma uygun olmayan kromozomu elimine etmek için uygunluk fonksiyonunu kullanmıştır. Deneyler sonucunda GA temelli arama mantığı kullanılarak oluşturulan ölçüm tablosunun, JPEG 2000 ve standart JPEG temel algoritması kullanılarak üretilen ölçüm tablosuna kıyasla daha iyi kodlanmış bir görüntü ürettiği bulunmuştur [75]. Farklı görüntü sıkıştırma ve kalite değişimleri üreten en uygun niceleme tabloları ailesini oluşturmak için iki amaçlı bir evrimsel algoritma önerildi. Baskın Olmayan Sıralama Genetik Algoritması II (NSGAII) olarak adlandırılan çok amaçlı evrimsel algoritmalardan biri, JPEG temel algoritması için en uygun niceleme tablosunu oluşturmak için kullanılır. Daha iyi kalitede sıkıştırılmış görüntüler, NSGAII algoritmasının yardımı ile oluşturulan niceleme tablosu

kullanılarak üretildi ve ayrıca daha iyi sıkıştırma ve kalite değişimi sağlanmıştır [76]. Niceleme tabloları üretmek için kültürel temelli çok amaçlı parçacık sürüsü optimizasyon modeli önerildi. Bu çalışmanın temel amacı, en iyi sıkıştırma ve kalite değişimini sağlayan tabloyu oluşturmaktır. Önerilen model, görüntü sıkıştırma kalitesi değerlendirme sorununu çözdü. Bu yöntem daha iyi kalitede sıkıştırılmış görüntüler üretmiştir [77]. Farklı görüntülerle en uygun niceleme tablosunu belirlemek için ateş böceği algoritması kullanıldı. Orijinal ve sıkıştırılmış görüntü arasındaki ortalama piksel yoğunluğu mesafesi, varsayılan JPEG niceleme tablosu kullanılarak 5.9 olarak bulunurken, önerilen yöntemde piksel yoğunluğu mesafesi 5.1'e düşürüldü ve sıkıştırılmış görüntünün kalitesi diğer yöntemlere kıyasla daha iyi olduğu gösterilmiştir [78]. Optimal niceleme tablosunu bulmak için Diferansiyel Evrim Algoritması(DEA) önerildi. Genetik algoritma(GA) ve Diferansiyel Evrim Algoritması arasında kapsamlı bir performans analizi gerçekleştirildi, bunun yanında DEA 'nın GA' ya umut verici bir alternatif olduğu kanıtlandı. Yukarıdaki ifadeyi doğrulamak için istatistiksel bir hipotez testi (t-testi) yapılmıştır [79]. Genetik Algoritmada kullanılan uygunluk değerini yaklaşık olarak belirlemek için bir problem yaklaşımı vekil modeli (PASM) önerildi. Önerilen yaklaşım, GA 'nın hesaplama süresini, performansında herhangi bir kayıp olmadan azaltmıştır [80]. Tüm frekans bantları için oran bozulma maliyetlerini optimize ederek JPEG için uygun bir fark (JND) bazlı niceleme tablosu üretme yöntemi önerilmiştir. Daha iyi algısal kalite elde etmek için, DCT alanı JND tabanlı bozulma metriği, HVS tarafından algılanan basamak bozulmasını modellemek için kullanılır. Her bant için oran-bozulma maliyeti, oranın birinci dereceden ölçülmüş katsayılar entropisi ile oranı tahmin edilerek elde edilir. Daha sonra, tüm bantların toplam oran-bozulma maliyetlerini asgariye indirerek en uygun niceleme tablosu elde edilir. Önerilen yöntemle oluşturulan niceleme tablosunun, JPEG tablosundan önemli ölçüde bit oranı tasarrufları sağladığı gösterilmiştir [81]. Tek bir görüntüyü veya bir temsili görüntü koleksiyonunu optimize etmek yerine, benzetilmiş tavlama tekniği, her doku kategorisi için optimal bir niceleme tablosu aramak için doku mozaik görüntülerine uygulanır. Bu doku özelliklerini öğrenmek ve yeni görüntünün doku dağılımını tahmin etmek için önceden eğitilmiş VGG-16 CNN modelini kullanmaktadır. Ardından görüntüye özgü optimum niceleme tablosu oluşturmak için optimum doku tabloları birleştirilir. Q = 95 kalite faktörüne sahip Kodak veri kümesinde yapılan testler sonucunda, JPEG standart tablosuna göre % 23,5 'lik bir boyut azalması olduğu görülmüştür [82]. Standartlara uygun bir şekilde görüntüye uyarlanabilir bir niceleme tablosu oluşturmak için bir Evrişimli Sinir Ağı (CNN) modeli kullanılmıştır. Farklı görüntüler üzerinde yapılan testler, önerilen yöntemin son teknoloji ürünü yöntemi açıkça geride bıraktığını göstermektedir. 1.0 bpp 'lik sıkıştırma oranındaki standart tablo ile karşılaştırıldığında, regresyon ve sınıflandırma ağı, yaklaşık 1.2 ve 1.4 dB 'lik ortalama Tepe Sinyal-Gürültü Oranı (PSNR) kazancı sağladığı tespit edilmiştir [83]. Küre şeklinde koordinat sisteminde piksel üzerindeki dönüştürme hatası, yuvarlama hatası ve kesme hatasını kullanarak renkli görüntülerde yeniden sıkıştırmayı tespit etmek için etkili

bir yöntem önerilmiştir. Bu yöntemde destek vektör makinesi (SVM) yöntemi kullanılarak sınıflandırmada toplam 44 boyutlu özellik kullanılmış ve etkili sonuçlar elde edilmiştir [84]. DNN mimarisinin derin kademeli bilgi işlem mekanizması için özel olarak tasarlanmış DeepN-JPEG adlı bir görüntü sıkıştırma çerçevesi önerilmiştir. 3,5 kat daha yüksek sıkıştırma oranına ulaşabildiğini ve aynı zamanda görüntü tanıma için aynı doğruluk düzeyini koruyarak büyük potansiyelini ortaya koyduğunu göstermişlerdir [85]. Standart JPEG kodlayıcı ve kod çözücüyle tam uyumlu görüntüye özgü optimize niceleme tabloları için derin bir sinir ağı önerilmiştir. Ağın amaç işlevini ayarlayarak göreve özgü niceleme tablolarını ilkel bir şekilde öğrenme yeteneği sağlar. Bu fikrin gerçekleştirilmesindeki ana zorluk, kodlayıcıda uzunluk kodlaması ve Huffman kodlaması gibi farklılaştırılamayan bileşenlerin bulunması ve nicelenmiş görüntünün temsillerinin olasılık dağılımını tahmin etmenin kolay olmamasıdır [86].

5.1.5. Önerilen Yaklaşım

Kaos teorisi bilimsel araştırmalar için önemli bir yere sahiptir. Özellikle bilgisayar bilimlerinde birçok potansiyel uygulama alanına sahiptir. Bu potansiyelin en önemli sebeplerinden biri kaotik sistemlerin gürbüz bir entropi kaynağı olmasından kaynaklanmaktadır. Kaotik sistemlerin tahmin edilemez doğası ve doğrusal olmayan yapısı özellikle şifreleme algoritmalarının tasarımında, optimizasyon algoritmalarının parametre seçimi ve başlangıç popülasyonlarının oluşturulmasında, modelleme, zaman serilerinin kestirimi gibi birçok alanda ilerleme sağlamasına katkı sunmuştur. Buradan hareketle kaotik sistemlerin niceleme tablolarının üretilmesinde bir avantaja sahip olup olmayacağı bu tez çalışmasında araştırılmıştır.

Çalışmanın çıkış noktası kaotik sistemlerin kriptolojik yer değiştirme kutularının(s-box) tasarımı için etkili bir alternatif olmasıdır. Yer değiştirme kutuları n-bit uzunluklu bir girişi m-bit uzunluk bir çıkışa haritalayan doğrusal olmayan bir fonksiyondur. Bu yönü ile s-box yapıları ile niceleme tabloları aralında bir benzerlik vardır. Bu benzerlikten hareketle kaos temelli niceleme tabloları oluşturma fikri ilk defa bu çalışmada önerilmiştir. Önerilen algoritmanın akış şeması Şekil 5.1 ’de gösterilmiştir.

Şekil 5.1. Önerilen yönteme genel bakış

Tablo 5.3. Önerilen kaotik niceleme tablosu üretecinin sözde kodu

Girdiler: Seçilen kaotik sistemlerin başlangıç koşulu ve kontrol parametreleri
Çıktı: Niceleme tablosu

```
niceleme_tablosu←dizi[]  //dizi 64 eleman içerir
x_eski ← rastgele()
i=0
toplam=0
for i in 63
başla
    for i in 50
    başla
        x_i ← seçilen kaotik sistem için yeni durum değerini hesapla
        x_i← dönüşüm_fonksiyonu(x_i)
        toplam=toplam+x_i
    son
    x_yeni=toplam/50
    Niceleme_tablosu ← x_yeni
    x_eski ← x_yeni
son
return niceleme_tablosu
```

Şekil 5.1 ’de önerilen yöntem farklı kaotik sistemlere uygulanabilir. Literatürde çok fazla kaotik sistem bulunmaktadır. Bu kaotik sistemlerin matematiksel modellerine göre avantaj ve dezavantajları bulunmaktadır. Bazı kaotik sistemler basit matematiksel modellere sahip olması hesaplama kolaylığı sunarken; diğer kaotik sistemler karmaşık yapıları ile doğru orantılı olarak daha gürbüz bir entropi kaynağına sahiptir. Bu çalışmada basit matematiksel modellerinden dolayı dört farklı kaotik sistem kullanılarak örnek niceleme tablolarının nasıl elde edilebileceği

gösterilmiştir. Denklem 4.1-4.4 ’de bu dört farklı kaotik sistemin matematiksel modelleri verilmiştir.

Tablo 5.3, kaotik sisteme dayalı niceleme tablolarını oluşturmak için kullanılabilecek sözde kodu verir. Algoritmaya giriş parametresi olarak kaotik sistem tipi verilir. Durum değişkenleri seçilen kaotik sistem tipine göre hesaplanır. Kaotik sistemlerin durum değişkenleri kesirlidir. Bu değerler, mod işlevi aracılığıyla ondalık sayılara dönüştürülür. Bu ondalık değerler, belirtilen mantığa göre niceleme tablosu değerlerine dönüştürülür.

Lojistik harita ile elde edilen örnek bir niceleme tablosu Tablo 5.4 'de verilmiştir. Görüntüler bu tabloya ve standart JPEG tablosuna göre sıkıştırılmış ve sonuçlar karşılaştırılmıştır.

Tablo 5.4. Lojistik harita tabanlı önerilen niceleme tablosu

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	33	37	37	30	40	39	36	43
1	41	42	49	47	51	50	49	53
2	54	53	48	56	55	55	60	58
3	59	55	61	60	66	61	64	68
4	67	69	69	73	76	73	77	72
5	67	79	75	79	81	75	81	82
6	82	85	87	86	87	86	91	93
7	94	91	94	93	94	96	93	101

Önerilen algoritmadaki başlangıç koşullarını belirlemek için standart rastgele() işlevi kullanılır. Önerilen yöntemin önemli bir avantajı, gelecekteki çalışmalar için kaotik sistemlerin farklı başlangıç koşul değerleri seçilerek farklı niceleme tablolarının kolayca oluşturulabilmesidir.

5.1.6. Analiz Sonuçları ve Performans Karşılaştırmaları

Bu çalışmada, önerilen yöntemin başarısı, JPEG 'in standart parlaklık niceleme tablosu yerine Tablo 5.4 'de verilen önerilen niceleme tablosu kullanılarak analiz edilmiştir. Önerilen yöntemin performansını göstermek için farklı Piksel Başına Bit (bpp) değerlerine göre PSNR değerleri hesaplanmıştır. Ayrıca çalışmanın başarısını test etmek için Kodak veri seti ve barbara görüntüsü kullanılıştır.

Piksel Başına Bit Sayısı(Bpp - Bits Per Pixel):

Bpp, görüntü sıkıştırma performansını ölçmek için en çok kullanılan metriklerden bir tanesidir. Piksel başına düşen bit sayısını ifade eder. Bir görüntüdeki farklı renklerin sayısı, renk derinliğine veya piksel başına bit sayısına bağlıdır. Bpp değerine göre kaç farklı rengin kullanılacağı 2^{bpp} olarak hesaplanabilmektedir. Bpp değeri denklem 5.3 ‘de verildiği gibi hesaplanır.

$$Bpp = \frac{\text{Görüntü } boyutu}{Satır * Sütun} \quad (5.3)$$

Tepe Sinyal Gürültü Oranı (PSNR - Peak signal-to-noise ratio):

PSNR, orijinal görüntüdeki en yüksek sinyal gücü ile sıkıştırılmış görüntünün kalitesini etkileyen bozulma gürültüsünün gücü arasındaki oranı hesaplamak için kullanılmaktadır. İki görüntü arasındaki bu oran desibel olarak hesaplanır. PSNR, sinyallerin çok geniş bir dinamik aralığa sahip olmasından dolayı çoğunlukla desibel ölçeğinin logaritma terimi olarak hesaplanır. Denklem 5.4-5.6 'da verildiği gibi hesaplanır.

$$PSNR = 20 \log_{10} \frac{255}{RMSE} \quad (5.4)$$

$$\text{RMSE}=\sqrt{MSE} \quad (5.5)$$

$$\text{MSE}= e_{ms}^2 \approx (1/N^2) \sum_{i=1}^{N} \sum_{j=1}^{N} E(u_{i,j} - u_{i,j}^*)^2 \quad (5.6)$$

Kodak veri setinde 24 adet görüntü bulunmaktadır. Bu görüntüler, önerilen niceleme tablosu ve standart JPEG tablosun ile sıkıştırılıp sonuçların ortalaması alınmıştır. Bu sonuçların karşılaştırması Tablo 5.5 'te verilmiştir. Bu sonuçlara bakıldığında önerilen tablonun standart JPEG tablosuna göre ortalama %0.52 daha yüksek doğruluğa ulaştığı görülmüştür.

Tablo 5.5. Kodak veri seti için ortalama sıkıştırma sonuçları

	PSNR	
Bpp	**JPEG**	**Önerilen**
0,50	31,63	31,78
0,75	32,91	32,78
1,00	33,89	33,93
1,25	34,71	34,71
1,50	35,50	35,67
1,75	36,20	36,58
2,00	37,10	37,74
Ortalama	34,56	34,74
Kazanç(%)		+0,52

Sonuçların daha iyi değerlendirilebilmesi için Kodak veri setindeki kodim21 isimli görüntü sıkıştırılmış ve sonuçlar Tablo 5.6 'da verilmiştir. Bu sonuçlara bakıldığında önerilen tablonun standart JPEG tablosuna göre ortalama %1,23 daha yüksek doğruluğa ulaştığı görülmüştür.

Tablo 5.6. Kodim21 görüntüsü için sıkıştırma sonuçları

Bpp	PSNR	
	JPEG	**Önerilen**
0,50	31,45	31,72
0,75	32,74	32,61
1,00	33,64	33,58
1,25	34,22	34,45
1,50	34,88	35,54
1,75	35,60	36,51
2,00	36,34	37,38
Ortalama	34,12	34,54
Kazanç(%)		+1,23

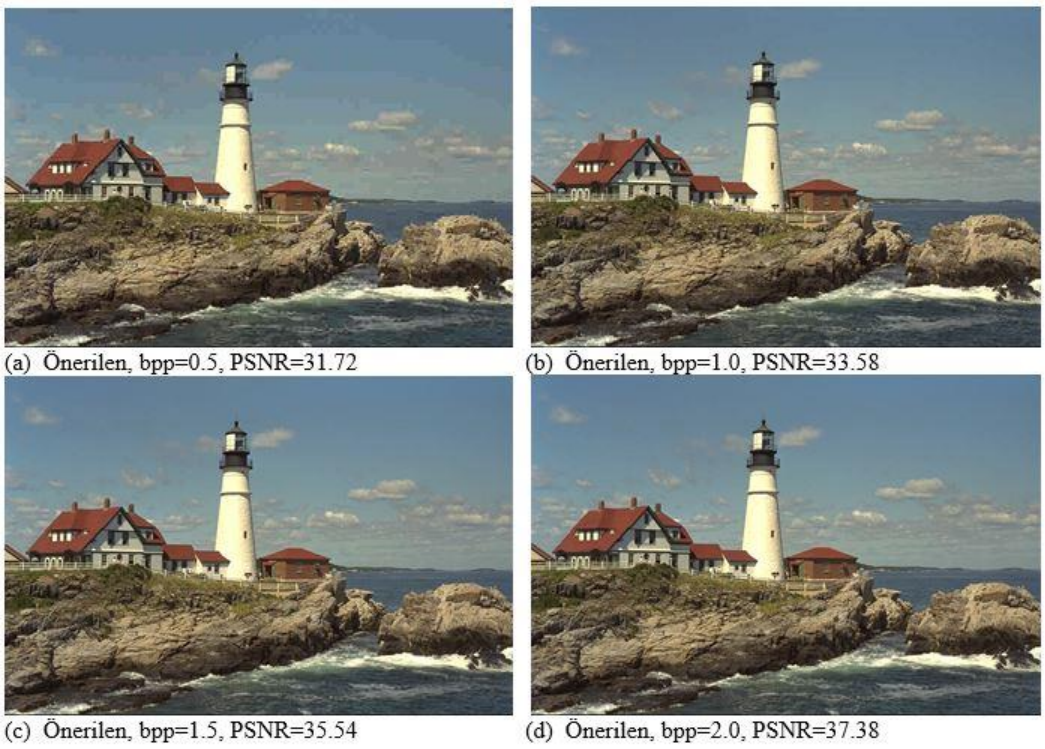
Ayrıca görüntü işleme alanında Kodak veri seti dışında en çok kullanılan görüntülerden biri olan Barbara görüntüsü her iki yöntem için de sıkıştırılmış ve sonuçlar Tablo 5.7 'de verilmiştir. Önerilen tablonun standart JPEG tablosundan ortalama %0,71 daha yüksek doğruluğa ulaştığı tespit edilmiştir.

Tablo 5.7. Barbara görüntüsü sıkıştırma sonuçları

Bpp	PSNR	
	JPEG	**Önerilen**
0,50	31,05	31,06
0,75	32,58	32,51
1,00	33,85	33,90
1,25	35,06	35,27
1,50	36,15	36,72
1,75	37,47	38,04
2,00	38,54	38,93
Ortalama	34,95	35,20
Kazanç(%)		+0,71

Kodim21 ve Barbara görüntüleri için hem önerilen yöntem hem de standart JPEG tablosu ile sıkıştırılmış görüntüler Şekil 5.2, 5.3, 5.4, 5.5 'de verilmiştir. Önerilen yöntemin neredeyse tüm bpp değerlerinde Standart JPEG tablosundan daha iyi performans gösterdiği gözlemlenmiştir.

Şekil 5.2. Standart JPEG tablosu ile Kodim21 görüntüsü sıkıştırma sonuçları



Şekil 5.3. Önerilen tablo ile Kodim21 görüntüsü sıkıştırma sonuçları

Şekil 5.4. Standart JPEG tablosu ile Barbara görüntü sıkıştırma sonuçları

Şekil 5.5. Önerilen tablo ile Barbara görüntü sıkıştırma sonuçları

5.2. Tüm Slayt Görüntülerinin Sıkıştırılması İçin Kaos Temelli Niceleme Tablosu Üreteci

Bu bölümde literatürdeki yöntemlere alternatif olabilecek yeni bir yaklaşım önerilmiştir. Kaotik sistemler kullanılarak yeni bir niceleme tablosu üretilmiştir. Niceleme tablosunun tasarım sürecinde birden fazla kaotik sistemin ardı ardına bağlanması ile elde edilmiştir. Geliştirilen niceleme tablosu kullanıldığında Tüm Slayt görüntüler(WSI) için JPEG algoritmasına kıyasla daha yüksek sıkıştırma oranlarına ulaşılabileceği gözlemlenmiştir.

5.2.1. Tüm Slayt Görüntülerin Önemi

Bilgisayar temelli teknolojilerin tıp biliminde kullanılması yeni alt disiplinler oluşturmuştur. Bu yeni disiplinlerden biri dijital patoloji olarak bilinmektedir [3]. Bu alt disiplin, sayısallaştırılmış numune slaytları tarafından oluşturulan verilere odaklanmıştır. İlk uygulamalarını 1960 'lı yıllarda telepatoloji deneylerinde gördüğümüz dijital patoloji dalı, azalan donanım (tarayıcı teknolojisi) maliyetleri ve ağ teknolojilerinin erişilebilirliği gibi gelişmelere bağlı olarak ivme kazanmıştır. Dijital patolojideki en kritik bileşenlerden biri sanal mikroskoptur [87]. Klasik cam slaytlar, bu bileşen kullanılarak dijital slaytlara kolayca sayısallaştırılabilir. Dijital slaytlar bilgisayar monitörlerinde kolaylıkla görüntülenebilir [88]. Bu özelliği sayesinde tanısal tıp uygulamalarında etkin ve daha ucuz tanıların yapılması, hastalığın seyri ile ilgili öngörülerin belirlenmesi ve yapay zekâ teknikleri kullanılarak hastalığın önceden tahmin edilmesi gibi birçok avantaj sağlamıştır [89].

Dijital slaytlar için yaygın olarak bilinen bir isim Tüm Slayt görüntüleridir(WSI). Bu görüntülerin tıptaki önemini vurgulamak için belki de en iyi açıklamalardan biri dijital patolojiyi dijital radyoloji ile karşılaştırmaktır. Radyoloji bilimi de tıpkı patoloji gibi ciddi bir dijital dönüşüm sürecinden geçmiştir. Bununla birlikte, iki disiplin arasındaki temel fark, radyolojik görüntülerin canlı hastadan elde edilirken, patolojik görüntülerin, geriye dönük çalışmalar için korunmuş ve işlenmiş numuneler gibi biyobankta saklanan çok çeşitli slaytlardan beslenmesidir [90]. Bu görüntü çeşitliliğinin en önemli sorunu, verilerin nasıl etkin bir şekilde depolanacağı, işleneceği ve iletileceğidir? Aslında bilgisayar teknolojilerinin tıpta yaygın olarak kullanılması, sorunu bilgisayar bilimcilerinin yanıtlamaya çalıştığı sıcak bir araştırma sorusu haline getirmiştir. Bu çalışmada, bu araştırma sorusunu cevaplamak için yeni bir yöntem önerilmektedir.

5.2.2. Tüm Slayt Görüntüleri ile İlgili Çalışmalar

Dijital patolojinin popülaritesine dikkat çekmek için son yıllarda bu alanda yapılan klinik çalışmaların sayısı iyi bir göstergedir. Prostat kanserinin erken teşhisi için histopatolojik görüntülerin üç boyutlu rekonstrüksiyonu [91], histoloji görüntülerini analiz etmek ve yorumlamak

için derin öğrenme yaklaşımı [92], meme kanseri tipini teşhis etmek için konvolüsyonel nöral ağlar [93], Elastik Net gibi uzun bir liste beyin kanseri teşhisi için sınıflandırıcı [94], WSI 'dan meme tümörü proliferasyon değerlendirmesi [95], malign bir karaciğer kanseri türü olan hepatoselüler karsinom lezyonlarının doğru segmentasyonu için hibrit sinir ağı [96], HookNet, WSI 'ler için semantik bir segmentasyon modeli [97], WSI 'dan tiroid malignite tahmini için çoklu anında öğrenme [98], nöroblastom hasta verilerinin farklı patolojik bileşenleri ile ilişkili görüntü bölgelerinin belirlenmesi [99], kolorektal karsinomda tümör tomurcuğu skorlaması için bir doğrulama çalışması [100], yeniden kalibre edilmiş bir multi- mide kanseri teşhisinde bilgilendirici bölgelerin nasıl seçileceğine dair örnek derin öğrenme yöntemi [101] ve odaklama işlemini yapmak için bir evrişim sinir ağı [102] çalışmalarında etkin ve etkili ocedure, son yıllarda bu klinik çalışmaların başarılı örnekleri olarak dikkat çekmektedir. PubMed kayıtlarına göre son on yılda WSI ile ilgili çalışma sayısı 2000 'den fazladır. Görüntülerin öngörülebilir modellenmesi, algı, bölütleme, öznitelik çıkarma ve doku sınıflandırma gibi birçok alanda özellikle makine öğrenmesi teknikleri kullanılarak çeşitli fırsatlar sunması, bu konuda daha fazla araştırma yapılmasına yol açmıştır. Klinik çalışmaların yanı sıra araştırma, teşhis ve eğitim amaçlı verilerin uzak yerler arasında kolayca paylaşılabilmesi bu alandaki araştırma yoğunluğunun bir başka açıklamasıdır [103].

Bununla birlikte, bu araştırma ve ilgi yoğunluğuna rağmen, başarıya ulaşmak için üstesinden gelinmesi gereken bir dizi önemli teknik ve hesaplama zorluğu vardır. Bu zorluklar dijital patolojide bilgisayar destekli görüntü analizi sorunları olarak karşımıza çıksa da klinik tanı iş akışı süreçlerinde başarı için ele alınması gereken önemli aşamalardan biridir. Dijital patoloji görüntülerinin bilgisayarlı analizinin zorluklarından biri, tüm slayt patoloji görüntülerinin çok büyük olmasıdır [103]. Bu sorun bilgisayarlı analizi verimsiz hale getirerek depolamayı, yönetimi ve iletimi zorlaştırır. Bu sorunu çözmek için çeşitli araştırmalar önerilmiştir. [104] ‘de büyük WSI veri kümelerine potansiyel bir çözüm olarak düşük çözünürlüklü girdileri kullanarak yüksek çözünürlüklü histoloji görüntülerini yeniden yapılandırmak için derin öğrenmeye dayalı bir yaklaşım önerildi. [105] 'da, WSI 'deki kaba bölgelerin çeşitliliği analiz edilmiş ve ardından görüntüyü kaplayan kiremitli bölgelerden uzamsal olarak yerelleştirilmiş şekil, renk ve doku özelliklerini kaldırarak boyutluluğu azaltmak için yapılmıştır. Başka bir çalışmada, DICOM 'un performansını iyileştirmek için yeni bir yaklaşım geliştirilmiştir. Çok seviyeli kaynak esnekliği kullanan yeni model, PS2DICOM [106] olarak adlandırılmıştır. [107] ‘de, büyük arşivlerde benzer görüntüleri aramak için dijital patoloji için özel bir arama motoru geliştirilmiştir. Bu arama motorunun tasarım sürecinde amaç, WSI 'yı kompakt bir şekilde temsil etmektir. Bu çalışmaların ortak noktası veri boyutunu küçültmek için özel çözümler geliştirmektir. Aslında WSI 'nın daha etkin işlenmesi, saklanması ve iletilmesi için kullanılabilecek genel yaklaşım veri sıkıştırma

çözümleridir. Kalinski ve arkadaşları WSI için veri sıkıştırma tekniklerinin önemini vurgulamıştır [108].

5.2.3. Tüm Slayt Görüntülerin Sıkıştırılması

Sıkıştırma sürecindeki bilgi kaybının patologların teşhisi üzerinde doğrudan bir etkisi olabileceğinden, WSI ve diğer tıbbi görüntüler için kayıplı sıkıştırmaya göre genellikle kayıpsız sıkıştırma tercih edilir [108, 109]. Ancak bazı durumlarda WSI 'lar çok büyük olduğundan kayıplı sıkıştırma kaçınılmazdır. Örneğin, 40 kat büyütmede taranan 15×15 mm 'lik bir veri, 60000×60000, 24 bit derinlikli renkli bir görüntü gerektirir, bu da 10 GB 'den fazla veri anlamına gelir. Daha düşük, daha yaygın 0,5 μm çözünürlükte bile, görüntüler 30000 × 30000 boyutlarında ve 2,5 GB sıkıştırılmamış veri elde eder [110]. Ayrıca, vaka başına yaklaşık 35 WSI üretilir. Böylece, tek bir WSI tarayıcısı tarafından her yıl yüzlerce terabayt veri üretilir [111]. Buradaki en önemli nokta, tıbbi görüntülerin kalitesini düşürmeden mümkün olduğunca sıkıştırmaktır. Bu nedenle, bu alanda kayıplı sıkıştırma yöntemlerinin kullanılabilirliği üzerinde durulmuştur. Birkaç kayıplı sıkıştırma yöntemi önerilmiştir [112-114]. Patologlar ve gerçek örnekler kayıplı sıkıştırma yöntemleriyle sıkıştırılan görüntülerin klinik ve araştırma amaçlı uygun olduğunu göstermiştir. 20:1'e kadar JPEG 2000 [115] sıkıştırma oranlarının kullanılması, geleneksel cam slaytlar kullanılarak elde edilenlerden istatistiksel olarak ayırt edilemeyen tanısal sonuçlar verir ve patologların tanıya olan güvenini etkilemez [116, 117]. Yaklaşık 13:1 'lik ortalama sıkıştırma oranları, patologların orijinal WSI 'lardan ayırt edilemez olduğuna inandıkları görüntüler üretir [118]. Temel JPEG'in [58], teşhis için kullanılabilecek sıkıştırılmış görüntüler ürettiği de gösterilmiştir [109]. JPEG için kesin sıkıştırma oranları rapor edilmemesine rağmen, üretilen sonuçlar cam slaytlar kullanılarak elde edilenlerle aynıdır [119]. Çoğu ticari WSI tarayıcısında standart JPEG 2000 veya JPEG sıkıştırması kullanılır [120].

Bu alanda yapılan bir başka çalışmada ise renk dönüşümleri, bileşenler arasındaki fazlalığı ortadan kaldırarak sıkıştırmayı iyileştirmektedir [117]. WSI 'lardaki renk bileşenleri arasındaki özellikle güçlü benzerlikler nedeniyle, yeterli dönüşümlerin uygulanması sıkıştırma performansını büyük ölçüde iyileştirebilir. WSI 'ya özgü renk dönüşümleri azdır [121, 122], ancak bileşenler arasındaki benzerliklerden yararlanmak için başka dönüşümler uygulanabilir. Renk tersine çevirme yöntemleri, WSI 'lar için CAD algoritmalarında [123] başarıyla uygulanmıştır. Bu yaklaşımlar, renk dönüşümlerini kullanarak dekonvolüsyon matrislerinin yardımıyla görüntü renklerini ayırır. Ancak, bu dönüştürmeler sıkıştırma için oluşturulmamıştır. Bu nedenle pratikte etkili sonuçlar alınamamaktadır. Tersine çevrilebilir olacak şekilde tasarlanan optimize edilmiş dönüştürmeler, tersinir renk dönüştürmelerine kıyasla sırasıyla 0,9 dB, 7,1 dB ve 0,025'e varan PSNR, HDR-VDP-2 ve çekirdek algılama doğruluğu kazanımları elde eder [124]. Dijital patolojide büyük veri görüntü

analizinin ihtiyaçlarını karşılamak için patolojik bir görüntü sıkıştırma çerçevesi önerilmiştir [4]. Bu yöntem, JPEG2000 protokolüne dayanmaktadır. Depolama ve hesaplama düğümleri arasındaki veri aktarımı miktarını en aza indirmeyi ve ayrıca sıkıştırma açmanın hesaplama taleplerini önemli ölçüde azaltmayı amaçlar. Bu çerçeve, meme biyopsisi görüntülerinden sıcak nokta saptamaya entegre edilerek veri ve hesaplama gereksinimlerinde önemli bir azalma sağlar. Özellikle histopatolojik WSI 'lar ile kullanım için, JP2-WSI adı verilen JPEG 2000 görüntü sıkıştırması için optimize edilmiş bir yöntem önerilmiştir. WSI, görüntünün arka plan kısmında çok yüksek derecede sıkıştırmaya izin verirken, görüntünün doku içeren kısmında geleneksel miktarda sıkıştırmaya izin vererek yüksek genel sıkıştırma oranlarına neden olur [125]. Başka bir çalışmada, Ölçeklenebilir Yüksek Verimli Video Kodlama (SHVC) önerilmiştir [126]. JND ‘nin altında bir sıkıştırma için sadece fark edilebilir bozulmaları (JND) haritalayan SHVC niceleme parametrelerini (QP) ve JPEG kalite seviyesini tahmin etmek için bir kullanıcı çalışmasının yanı sıra sıkıştırma oranlarının bir karşılaştırmasını içerir.

5.2.4. Önerilen Yaklaşım

Literatürde var olan yöntemlere alternatif olarak yeni bir niceleme tablosu önerilmiştir. Önerilen yöntemin avantajı, mevcut yöntemlerin dezavantajları için çeşitli alternatifler sunmasıdır. Bu çalışmanın çıkış noktası, kaos ve kriptoloji bilimi arasındaki güçlü ilişkiye dayanmaktadır. Amacımız, sağlam niceleme tabloları oluşturmak için önceki çalışmalarımızda kaotik sistemler kullanılarak yer değiştirme kutuları(s-box) tasarımında elde edilen başarıyı tekrar edip edemeyeceğimiz araştırılmıştır.

Tasarım sürecinde kaotik sistemler olarak kullanılabilecek pek çok alternatif olmasına rağmen, çalışma basit yapıları nedeniyle ayrık zamanlı kaotik sistemler üzerine kuruludur. Bu basit yapı nedeniyle önerilen niceleme tablosunun optimizasyon tabanlı tasarımlara göre avantaj sağlaması beklenmektedir. Çalışmada, niceleme tablosunun oluşturulduğu entropi kaynağını iyileştirmek için dört farklı kaotik sistem kullanılmıştır. Entropi kaynağı oluşturulurken, niceleme tablosunun değerlerinin elde edilmesinde daha etkin bir dağılım sağlamak için kaotik sistemler basamaklandırılmıştır. Kullanılan kaotik sistemler lojistik harita, çadır harita, sinüs harita ve daire harita olmak üzere 4 farklı harita kullanılmıştır. Denklem (2.7)-(2.10) ’da bu dört farklı kaotik sistemin matematiksel modelleri verilmiştir. Önerilen yöntem kullanılarak elde edilen niceleme tablosu Tablo 5.9 ‘da verilmiştir. Kaotik sistemlere dayalı niceleme tablosunun üretilmesi için önerilen yöntemin sözde kodu Tablo 5.8 'de verilmiştir.

Tablo 5.8. Önerilen niceleme tablosu üretecinin sözde kodu

```
ÖnerilenNicelemeTablosuÜreteci ()
Tablo= [0:64]
N=800, k=1
a= 1.874587458
b= 0.745874578

for (i=0 i<64 i++)
    toplam=0
    for (j=0 j<50 j++)
        r=0,7
        r=r+0.3/N
        y=rastgele(0,1)

        //Lojistik harita
        y=4*r*y*(1-y)

        //Çadır harita
        if(y<0.5)
            y=a*y
        else
            y=a*(1-y)

        //Sinüs harita
        y=a*(sin(π*y))

        //Daire harita
        y=(y+(a-((b/(2* π))*sin(2* π*y))))%1

        x= y 'nin ilk 4 değeri
        x=(1000*y)%80
        x=x+k
        toplam=toplam+x
    end for

    Tablo[i]=toplam/50
    k=k+1
    return Tablo
end for
```

Önerilen niceleme tablosunun her kalite faktörü için standart JPEG algoritmasındaki değerlerden daha büyük ve daha yakın değerlere sahip olması daha iyi sıkıştırma performansı elde etmede etkili

olmuştur. Önerilen tablodaki değerler (satır ve sütun bazında) arasındaki farkın daha az olması ve bu değerlerin daha büyük sayılardan oluşması, daha küçük kalite faktörlerinde sıkıştırmaya izin verir. Bu durumun sıkıştırma oranını arttırdığı yapılan deneyler sonucunda gözlemlenmiştir.

Tablo 5.9. Önerilen niceleme tablosu

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	22	23	26	25	27	31	30	33
1	31	32	35	36	37	39	41	45
2	41	41	45	40	44	51	44	49
3	49	51	49	50	52	56	60	55
4	58	63	60	55	59	65	60	65
5	65	72	67	64	69	70	72	70
6	76	72	74	77	78	79	82	80
7	80	85	84	82	85	85	87	89

5.2.5. Analiz Sonuçları ve Performans Karşılaştırmaları

Önerilen yöntemin performansını değerlendirmek için 1024x1204 piksel boyutunda 1000 adet WSI içeren veri seti kullanılmıştır. Önerilen yöntem temel JPEG algoritması ile karşılaştırılmış ve ortalama sonuçlar Tablo 5.10 'da verilmiştir. Bu sonuçlara bakıldığında önerilen yöntemin temel JPEG algoritmasına göre ortalama %2,43 daha yüksek doğruluğa ulaştığı görülmüştür.

Tablo 5.10. WSI veri setinin ortalama sıkıştırma sonuçları

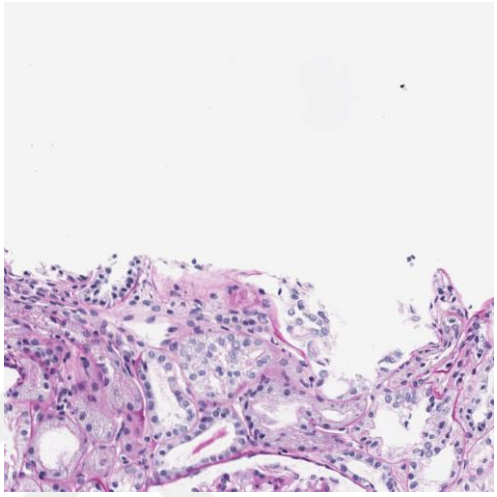
Bpp	**PSNR**	
	JPEG	**Önerilen**
0,50	35,13	36,23
0,75	38,24	37,70
1,00	40,65	40.81
1,25	41,75	42,91
1,50	44,16	46,68
1,75	48,69	50,04
2,00	50,68	52,18
Ortalama	42,75	43,79
Kazanç(%)		+2,43

Sonuçların daha iyi değerlendirilebilmesi için WSI veri setinde WSI-1, WSI-2 ve WSI-3 olarak adlandırılan görüntüler sıkıştırılmış ve sonuçlar Tablo 5.11, 5.12 ve 5.13 'de verilmiştir. Bu

sonuçlara bakıldığında, temel JPEG algoritmasına göre yaklaşık olarak sırasıyla birinci görüntü için %2,9, ikinci görüntü için %2,3 ve üçüncü görüntü için %1,88 daha yüksek doğruluk oranları elde edilmiştir.

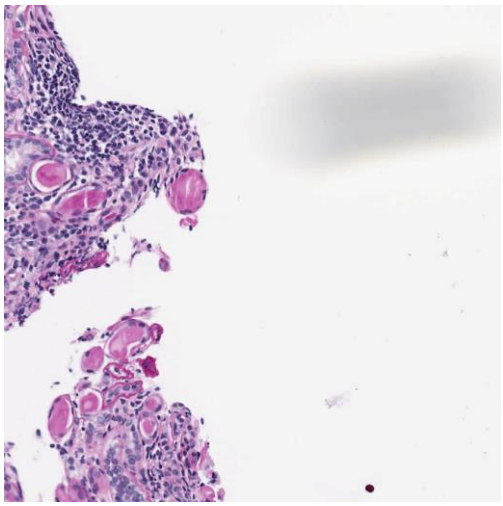
Tablo 5.11. Örnek WSI-1 sıkıştırma sonuçları

Bpp	PSNR	
	JPEG	**Önerilen**
0,50	35,12	35,39
0,75	37,98	37,87
1,00	39,94	40,24
1,25	41,81	44,65
1,50	46,55	48,48
1,75	49,10	50,60
2,00	51,20	53,26
Ortalama	43,1	44,35
Kazanç(%)		+2,9



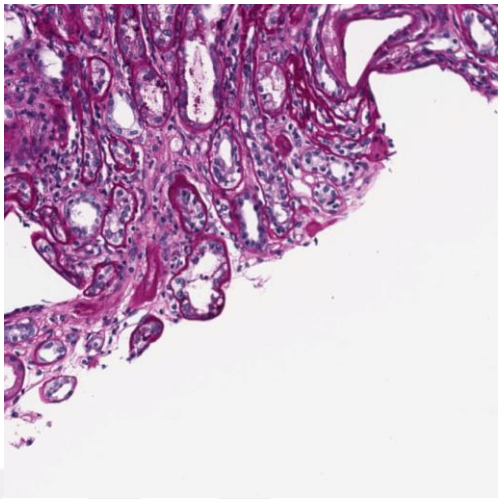
Tablo 5.12. Örnek WSI-2 sıkıştırma sonuçları

Bpp	PSNR	
	JPEG	**Önerilen**
0,50	36,86	36,67
0,75	39,11	39,40
1,00	41,52	43,62
1,25	46,15	48,50
1,50	49,11	50,62
1,75	52,54	53,26
2,00	53,60	54,15
Ortalama	45,55	46,6
Kazanç(%)		+2,3

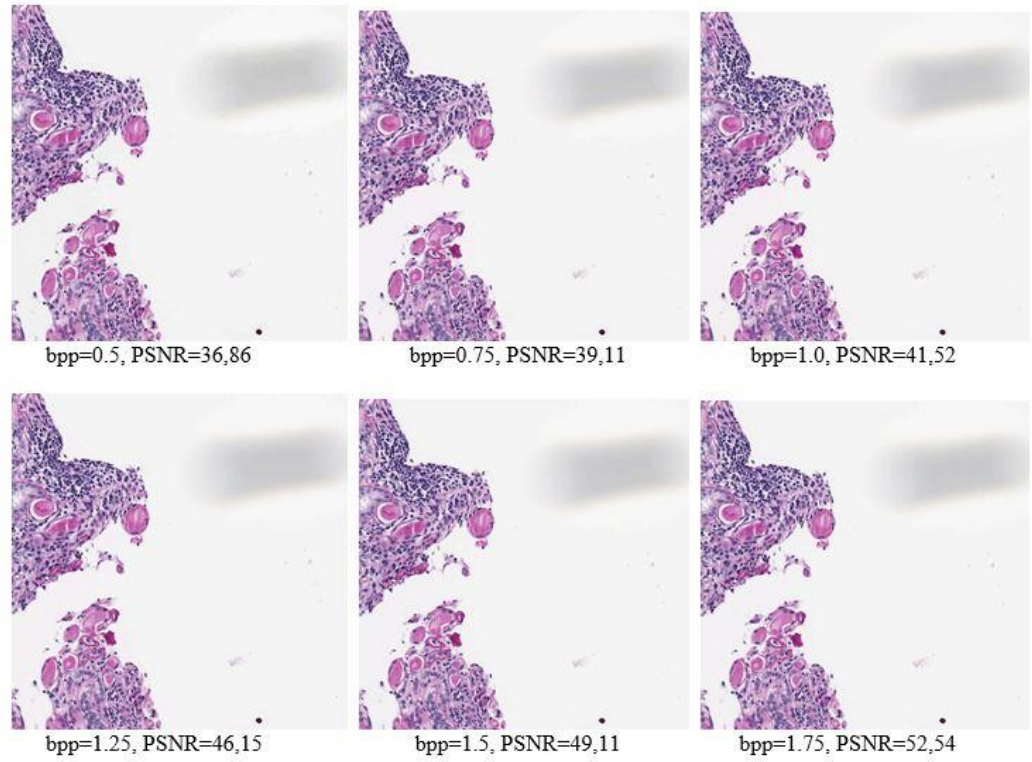


Tablo 5.13. Örnek WSI-3 sıkıştırma sonuçları

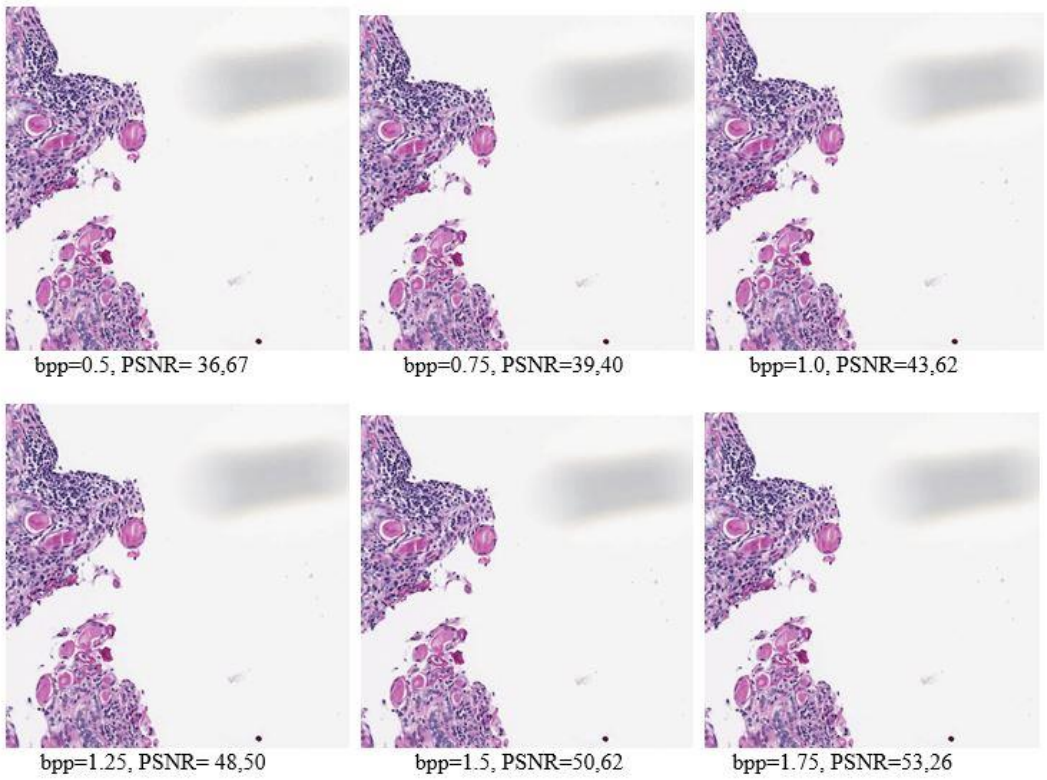
Bpp	PSNR	
	JPEG	**Önerilen**
0,50	33,20	33,35
0,75	35,70	35,34
1,00	36,96	37,45
1,25	38,60	39,07
1,50	40,28	41,16
1,75	43,08	46,17
2,00	46,54	47,00
Ortalama	39,19	39,93
Kazanç(%)		+1,88



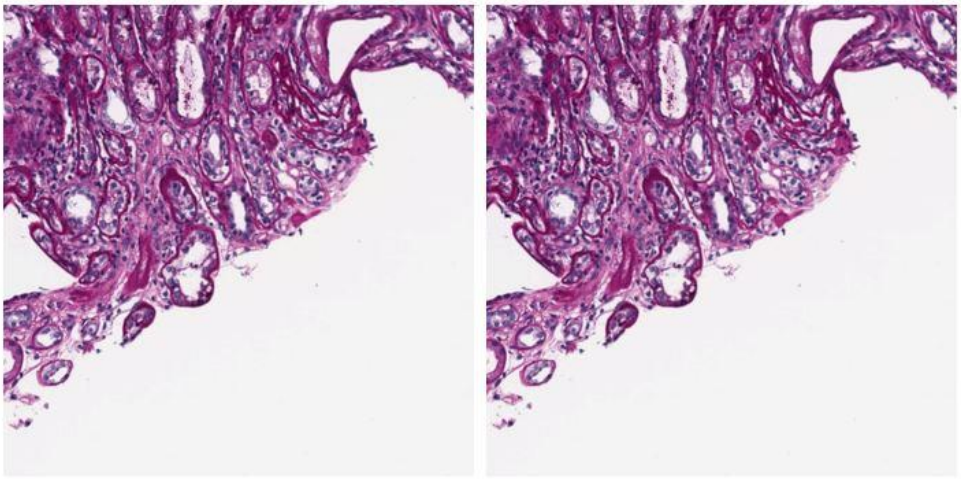
Ayrıca WSI-2 adlı görüntünün 6 farklı bpp değeri için sıkıştırma sonuçları şekil 5.6 ve şekil 5.7 'de verilmiştir. Bu sonuçlara bakıldığında önerilen yöntemin hemen hemen tüm bpp değerleri için standart JPEG yönteminden daha iyi performans gösterdiği görülmektedir. WSI-3 isimli görüntüde 1.75 bpp değeri için sıkıştırma sonuçları şekil 5.8 'de verilmiştir. Bu sonuca bakıldığında 1.75 bpp 'de önerilen yöntemin PSNR değerini 3.09 dB arttırdığı görülmektedir. WSI-1 isimli görüntüde 1.25 bpp değeri için sıkıştırma sonuçları şekil 5.9 'da verilmiştir. Bu sonuca bakıldığında önerilen yöntemin PSNR değerini 2.84 db arttırdığı görülmektedir.



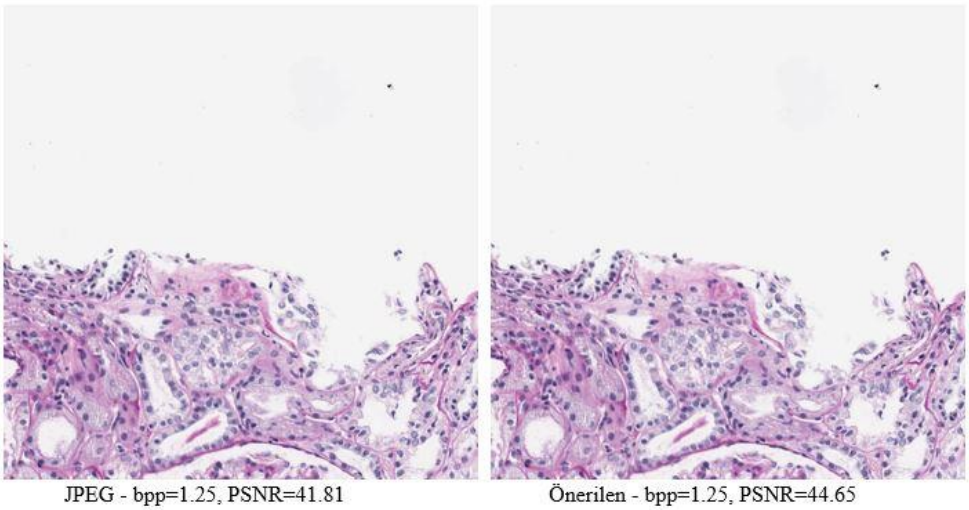
Şekil 5.6. Standart JPEG niceleme tablosu ile sıkıştırılmış WSI-2 görüntüsü sonuçları



Şekil 5.7. Önerilen niceleme tablosu ile sıkıştırılmış WSI-2 görüntüsü sonuçları



Şekil 5.8. WSI-3 görüntüsü için 1.75 bpp sıkıştırma sonuçları



Şekil 5.9. WSI-1 görüntüsü için 1.25 bpp sıkıştırma sonuçları

6. SONUÇLAR VE TARTIŞMA

Bir kriptolojik protokol tasarlanırken iki temel gereksinimin sağlanması gerekmektedir. Bunlar karıştırma ve yayılma özellikleridir. Karıştırma özelliğinin sağlanması için açık mesaj ile şifreli mesaj arasındaki ilişkinin mümkün olduğu kadar karmaşık olması gerekmektedir. Yayılma özelliğinde ise saldırganların istatistiksel çıkarımlar yapması engellenmeye çalışılmaktadır. Kaotik sistemlerin genel karakteristikleri ise tahmin edilemez bir yapıya sahip olması, başlangıç koşulları ve kontrol parametrelerine aşırı duyarlı olmasıdır. Bu çerçevede kaos ve kriptoloji bilimleri arasında güçlü bir ilişki söz konusudur. Kaotik sistemlerin tahmin edilemez yapısı, karıştırma özelliğinin sağlanmasında önemli fırsatlar yaratmaktadır. Ayrıca kaotik sistemlerin başlangıç koşulları ve kontrol parametreleri kriptolojik protokolün anahtar tasarım sürecinde kullanılması durumunda geniş bir anahtar uzayı sağlayacaktır. Çünkü her bir seçenek için farklı bir anahtar üreteceği için özellikle kaba kuvvet saldırılarına dirençli bir mimari elde etme imkânı ortaya çıkacaktır. Kaotik sistemlerin kriptojoji bilimindeki en başarılı uygulama alanlarından bir tanesi s-box yapılarının üretilmesidir. Bugüne kadar kaotik sistemler kullanılarak birçok s-box yapısı tasarlanmıştır. Ancak bu s-box yapıları matematiksel temelli s-box yapıları ile karşılaştırıldığında s-box değerlendirme metrikleri bakımından daha kötü performans sonuçları elde edildiği gözlenmiştir. Bu kötü sonuçlara rağmen kaos temelli s-box yapılarının araştırmacılar tarafından hala cezbedici olmasının en önemli sebebi ise kaos temelli s-box yapılarının son dönemde giderek popülerleşen yan kanal saldırıları gibi uygulamaya yönelik saldırılarda, matematiksel temelli s-box yapılarına göre daha dayanıklı olmasıdır. Bu avantajından dolayı kaos temelli s-box yapılarının performans kriterlerinin iyileştirilip iyileştirilemeyeceği araştırmacıların gündemini işgal eden bir araştırma sorusu olmuştur. Bu tez çalışmasının literatüre en önemli katkılarından biri çeşitli son işlem teknikleri kullanılarak s-box performans metriklerinin matematiksel temelli yaklaşımlar kadar iyileştirilebileceğinin gösterilmiş olmasıdır. Tez çalışması kapsamında işlemsel karmaşıklığı basit yöntemler kullanılarak doğrusal olmama değerinin, matematiksel temelli s-box yapıları kadar iyileştirilebileceği gösterilmiştir. Bu sayede literatürde var olan bir diğer iyileştirme yaklaşımı olan optimizasyon temelli çözüm önerilerinin hesapsal karmaşıklık problemleri de adreslenmiştir. Tez çalışması kapsamında yedi farklı yaklaşım kullanılarak ortalama seviyede bir doğrusal olmama ölçütüne sahip olan rastgele seçim prensiplerine göre üretilmiş bir s-box yapısının doğrusal olmama değerinin matematiksel temelli s-box yapıları kadar iyileştirilebileceği gösterilmiştir. Elde edilen sonuçlar maddeler halinde aşağıda özetlenmiştir.

- Son işlem teknikleri kullanılarak s-box performans kriterlerinin iyileştirilebileceği gösterilmiştir.
- Performans iyileştirmeleri için önerilen algoritmalar basit bir yapıya sahiptir.

- Hız, hesaplama karmaşıklığı ve kullanım kolaylığı, önerilen yöntemlerin dikkat çekici özellikleridir.
- Bu avantajlar göz önüne alındığında önerilen algoritmaların, literatürde daha önce kullanılan optimizasyon ve matematiksel temelli algoritmalara göre performans iyileştirmesi için daha uygun olduğu söylenebilir.
- Önerilen yöntemler, kaotik sistem tipi ve sınıfından bağımsızdır. Farklı seçenekler kullanılarak daha etkili çözümlerin elde edilmesi mümkündür.
- Çalışmanın çıktısı olarak sadece s-box üreteci düşünülmemelidir. Yan kanal saldırılarını önlemek için karşı önlem olarak kullanılabilecek yeni tasarımların geliştirilebileceği gösterilmiştir.

Tez çalışmasının bir diğer katkısı, kaos temelli s-box yapıları kullanılarak kriptoloji biliminde elde edilen başarılı sonuçların veri sıkıştırma alanına da uyarlanıp uyarlanamayacağının araştırılmasıdır. Çünkü şifreleme algoritmalarının temel bileşeni olan s-box yapıları ile sıkıştırma algoritmalarının temel bileşeni olan niceleme tabloları arasında büyük bir benzerlik söz konusudur. Her iki yapı da veriyi bir formdan başka bir forma dönüştürmektedir. S-box yapıları şifreleme algoritmalarında verinin daha fazla karılmasında kullanılırken, sıkıştırma algoritmalarında ise niceleme tabloları verinin daha düşük boyutlara sıkıştırılması amacıyla kullanılmaktadır. Burada önerilen yaklaşımlar kullanılarak s-box yapısındaki mekanizmanın niceleme tabloları için de kullanılabileceği ortaya koyulmuştur. Algoritmanın temel yaklaşımını oluşturan özgün yön ise, yine bu tasarım sürecinde de kaotik sistemlerden faydalanılmasıdır. Kaotik sistemlerin tahmin edilemez yapısı yeni niceleme tablolarının oluşturulmasında kullanılmıştır. Elde edilen sonuçlar JPEG algoritmasının performansının iyileştirilebileceğini göstermiştir. JPEG algoritması kayıplı bir sıkıştırma algoritmasıdır. Bir başka ifadeyle, seçilen kalite faktörüne göre sıkıştırma oranının derecesi değişmektedir. Önerdiğimiz yaklaşım farklı kalite faktörlerinin her biri için standart JPEG algoritmasının performansının iyileştirilebileceği gösterilmiştir.

Elde edilen sonuçlar özellikle Tam Slayt görüntülerinin (WSI) sıkıştırılmasında kullanılarak pratik uygulanabilirliği de tez kapsamında araştırılmıştır. Önerilen yeni niceleme tablosu öncelikle görüntü kalitesini ortalama 1,04 db arttırmaktadır. Bu gelişme, WSI 'lerin daha az bozulması ve tanıya engel olmaması için çok önemli bir gelişmedir. Diğer bir deyişle, standart JPEG algoritmasına göre %2,43 daha yüksek doğruluk (PSNR) değerleri elde edilmiştir. Bu katkının gelecekte dijital patoloji alanında yapılacak bilgisayar destekli tıbbi görüntü analizi çalışmalarında bir gelişme sağlayacağı düşünülmektedir. Bu şekilde tez çalışmasının bir diğer katkısı da oluşturulmuştur. Elde edilen yaklaşım aslında yeni hibrit sıkıştırma algoritmalarının geliştirilebileceğini göstermiştir. Bu tez çalışması kapsamında elde edilen sonuçlar ilerisi için de yeni motivasyonlar ve yeni araştırma konularına sebep olmuştur.

ÖNERİLER

Tez çalışmasının katkısı iki temel başlıkta gruplandırıldığı için öneriler bölümü de iki grupta sınıflandırılmıştır. Kaos temelli s-box yapıları için gelecekte yapılabilecek olası çalışmalar şunlardır.

- Performans iyileştirme için yeni son işlem algoritmaları araştırılabilir.
- Performans iyileştirmesinin kaotik sistem tipi ve sınıfından bağımsız olması, önerilen yöntemlerin farklı entropi kaynaklarında başarılı çıktılar üretebileceğini ortaya koymaktadır. Gelecekte farklı entropi kaynakları kullanılarak tasarlanacak s-box yapıları için performans iyileştirmeleri araştırılabilir.
- Kaos tabanlı s-box yapılarının bilgi güvenliği alanında pratik uygulanabilirliği araştırılabilir.
- Elde edilen çıktıların karmaşık ağlardaki genel saldırılarla başa çıkmak için W-MSR tipi esnek algoritma gibi farklı alanlardaki uygulamaları araştırılabilir.
- Tez çalışması kapsamında sadece doğrusal olmama ölçütü kullanılarak iyileştirmeler yapılmıştır. Bu alanda yapılabilecek bir diğer çalışma ise giriş/çıkış XOR dağılım tablolarının başarısının iyileştirilmesidir. Tez çalışmasında doğrusal olmama değeri neredeyse AES tablosunun doğrusal olmama değeri kadar iyileştirilmiştir. Bir sonraki belirlenen hedef, giriş/çıkış XOR dağılım tablosunun da AES tablosu kadar iyileştirilmesidir. Bu işlem olmadığı sürece tek başına kaos tabanlı s-box yapılarının bir şifreleme algoritması içerisinde kullanılması çok güvenli sonuçlar vermeyecektir.

Niceleme tabloları için ise, gelecekteki çalışmalarda kaotik sistemin türü değiştirilerek farklı niceleme tabloları oluşturulabilir. Niceleme tabloları elde etmek için kullanılabilecek başka bir seçenek ise kaotik çıktıları niceleme tablosu değerlerine dönüştürmek için farklı dönüşüm fonksiyonları kullanmaktır. Yeni oluşturulan niceleme tabloları sayesinde; sıkıştırma performansının iyileştirilmesine ek olarak, tıbbi görüntü analizi çalışmalarında iyileştirme sağlanabilir. Gelecekte yapılabilecek bir diğer çalışma ise, seçim sürecinin şifreleme anahtarı olarak kaotik sistemlerin başlangıç koşulları ve kontrol parametrelerinin kullanılması durumunda, hem sıkıştırma hem de veri şifreleme (gizleme) işlemlerinin aynı anda yapılabilmesinin mümkün olacağıdır.

KAYNAKLAR

[1] Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, 22(2), 177-183.

[2] Özkaynak, F. (2020). "Veri Güvenliği ve Risk Yönetimi, *İnönü Üniversitesi Yayınları* 88, Hasta güvenliği ve Risk Yönetimi", Editör: Prof. Dr. Nilgün Bozbuğa, Prof. Dr. Cengiz Yakıncı, ISBN 978-605-7853-50-9, 465-472

[3] Pantanowitz, L., Sharma, A., Carter, A. B., Kurc, T., Sussman, A., & Saltz, J. (2018). Twenty years of digital pathology: an overview of the road travelled, what is on the horizon, and the emergence of vendor-neutral archives. *Journal of pathology informatics*, 9.

[4] Niazi, M. K. K., Lin, Y., Liu, F., Ashok, A., Marcellin, M. W., Tozbikian, G., ... & Bilgin, A. (2019). Pathological image compression for big data image analysis: Application to hotspot detection in breast cancer. *Artificial intelligence in medicine*, 95, 82-87.

[5] https://www.greenbone.net/wp-content/uploads/Confidential-patient-data-freelyaccessible-on-the-internet_20190918.pdf.Erişim tarihi:05.03.2021

[6] https://www.hhs.gov/hipaa/index.html. Erişim tarihi: 02.03.2021

[7] Cusick, T. W., & Stanica, P. (2017). Cryptographic Boolean functions and applications. *Academic Press*.

[8] Paar, C., & Pelzl, J. (2009). Understanding cryptography: a textbook for students and practitioners. *Springer Science & Business Media*.

[9] Daemen, J., & Rijmen, V. (2002). The design of Rijndael (Vol. 2). *New York: Springer-verlag*.

[10] Standard, D. E. (1999). Data encryption standard. *Federal Information Processing Standards Publication*, 112.

[11] Alligood, K. T., Sauer, T. D., & Yorke, J. A. (1997). Chaos, *Textbooks in Mathematical Sciences*.

[12] Strogatz, S. H. (2018). Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering. *CRC press*.

[13] Kocarev, L., & Lian, S. (Eds.). (2011). Chaos-based cryptography: Theory, algorithms and applications (Vol. 354). *Springer Science & Business Media*.

[14] Zhu, C., Wang, G., & Sun, K. (2018). Cryptanalysis and improvement on an image encryption algorithm design using a novel chaos based S-box. *Symmetry*, 10(9), 399.

[15] Zhang, X., & Wang, X. (2018). Multiple-image encryption algorithm based on the 3D permutation model and chaotic system. *Symmetry*, 10(11), 660.

[16] Ding, L., Liu, C., Zhang, Y., & Ding, Q. (2019). A new lightweight stream cipher based on chaos. *Symmetry*, 11(7), 853.

[17] Demir, K., & Ergün, S. (2018). An analysis of deterministic chaos as an entropy source for random number generators. *Entropy*, 20(12), 957.

[18] Özkaynak, F. (2020) An Analysis and Generation Toolbox for Chaotic Substitution Boxes: A Case Study Based on Chaotic Labyrinth Rene Thomas System, *Iranian J. Sci. and Tech.-Trans. Elect. Eng.*, 44(1), 89-98.

[19] Hussain, I., Anees, A., Al-Maadeed, T. A., & Mustafa, M. T. (2019). Construction of S-box based on chaotic map and algebraic structures. *Symmetry*, 11(3), 351.

[20] Zhu, S., Wang, G., & Zhu, C. (2019). A secure and fast image encryption scheme based on double chaotic S-boxes. Entropy, 21(8), 790.

[21] Lai, Q., Akgul, A., Li, C., Xu, G., & Çavuşoğlu, Ü. (2017). A new chaotic system with multiple attractors: Dynamic analysis, circuit realization and S-Box design. *Entropy*, 20(1), 12.

[22] Al Solami, E., Ahmad, M., Volos, C., Doja, M. N., & Beg, M. M. S. (2018). A new hyperchaotic system-based design for efficient bijective substitution-boxes. *entropy*, 20(7), 525.

[23] Liu, G. (2017). Designing S-box based on 4D-4wing hyperchaotic system. *3D Research*, 8(1), 1-9.

[24] Özkaynak, F., & Yavuz, S. (2013). Designing chaotic S-boxes based on time-delay chaotic system. *Nonlinear Dynamics*, 74(3), 551-557.

[25] Khan, M., Shah, T., & Batool, S. I. (2016). Construction of S-box based on chaotic Boolean functions and its application in image encryption. *Neural Computing and Applications*, 27(3), 677-685.

[26] Özkaynak, F., Çelik, V., & Özer, A. B. (2017). A new S-box construction method based on the fractional-order chaotic Chen system. *Signal, Image and Video Processing*, 11(4), 659-664.

[27] Zahid, A.H.; Arshad, M.J.; Ahmad, M. (2019). A Novel Construction of Efficient Substitution-Boxes Using Cubic Fractional Transformation. *Entropy*, 21, 245.

[28] Tanyildizi, E., & Özkaynak, F. (2019). A new chaotic S-box generation method using parameter optimization of one dimensional chaotic maps. *IEEE Access*, 7, 117829-117838.

[29] Özkaynak, F. (2020). On the effect of chaotic system in performance characteristics of chaos based s-box designs. *Physica A: Statistical Mechanics and its Applications*, 550, 124072.

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

[31] Webster, A. F., & Tavares, S. E. (1985). On the design of S-boxes. *In Conference on the theory and application of cryptographic techniques* (pp. 523-534). Springer, Berlin, Heidelberg.

[32] Razaq, A., Ullah, A., Alolaiyan, H., & Yousaf, A. (2021). A novel group theoretic and graphical approach for designing cryptographically strong nonlinear components of block ciphers. *Wireless Personal Communications*, 116(4), 3165-3190.

[33] Ahmad, M., & Al-Solami, E. (2020). Evolving dynamic S-boxes using fractional-order hopfield neural network based scheme. *Entropy*, 22(7), 717.

[34] Ahmad, M., & Al-Solami, E. (2020). Improved 2D Discrete Hyperchaos Mapping with Complex Behaviour and Algebraic Structure for Strong S-Boxes Generation. *Complexity*.

[35] Wang, Y., Zhang, Z., Zhang, L. Y., Feng, J., Gao, J., & Lei, P. (2020). A genetic algorithm for constructing bijective substitution boxes with high nonlinearity. *Information Sciences*, 523, 152-166.

[36] Ahmad, M., Khaja, I. A., Baz, A., Alhakami, H., & Alhakami, W. (2020). Particle swarm optimization based highly nonlinear substitution-boxes generation for security applications. *IEEE Access*, 8, 116132-116147.

[37] Lambić, D. (2014). A novel method of S-box design based on chaotic map and composition method. *Chaos, Solitons & Fractals*, 58, 16-21.

[38] Alhadawi, H. S., Lambić, D., Zolkipli, M. F., & Ahmad, M. (2020). Globalized firefly algorithm and chaos for designing substitution box. *Journal of Information Security and Applications*, 55, 102671.

[39] Wang, Y., Wong, K. W., Li, C., & Li, Y. (2012). A novel method to design S-box based on chaotic map and genetic algorithm. *Physics Letters A*, 376(6-7), 827-833.

[40] Tian, Y., & Lu, Z. (2016). S-box: Six-dimensional compound hyperchaotic map and artificial bee colony algorithm. *Journal of Systems Engineering and Electronics*, 27(1), 232-241.

[41] Butt, K. K., Li, G., Masood, F., & Khan, S. (2020). A digital image confidentiality scheme based on pseudo-quantum chaos and lucas sequence. *Entropy*, 22(11), 1276.

[42] Tian, Y., & Lu, Z. (2017). Chaotic S-box: Intertwining logistic map and bacterial foraging optimization. *Mathematical Problems in Engineering*, 2017.

[43] Ahmad, M., Bhatia, D., & Hassan, Y. (2015). A novel ant colony optimization based scheme for substitution box design. *Procedia Computer Science*, 57, 572-580.

[44] Özkaynak, F. (2019). Construction of robust substitution boxes based on chaotic systems. *Neural Computing and Applications*, 31(8), 3317-3326.

[45] Lambić, D. (2018). S-box design method based on improved one-dimensional discrete chaotic map. *Journal of Information and Telecommunication*, 2(2), 181-191.

[46] Farah, T., Rhouma, R., & Belghith, S. (2017). A novel method for designing S-box based on chaotic map and teaching–learning-based optimization. *Nonlinear dynamics*, 88(2), 1059-1074.

[47] Çavuşoğlu, Ü., Kaçar, S., Zengin, A., & Pehlivan, I. (2018). A novel hybrid encryption algorithm based on chaos and S-AES algorithm. *Nonlinear Dynamics*, 92(4), 1745-1759.

[48] Belazi, A., & Abd El-Latif, A. A. (2017). A simple yet efficient S-box method based on chaotic sine map. *Optik*, 130, 1438-1444.

[49] Özkaynak, F. (2017). From biometric data to cryptographic primitives: A new method for generation of substitution boxes. *In Proceedings of the 2017 International Conference on Biomedical Engineering and Bioinformatics* (pp. 27-33).

[50] Liu, L., Zhang, Y., & Wang, X. (2018). A novel method for constructing the S-box based on spatiotemporal chaotic dynamics. *applied sciences*, 8(12), 2650.
[51] Salomon, D. (2004). Data compression: the complete reference. *Springer Science & Business Media*.
[52] Capon, J. (1959). A probabilistic model for run-length coding of pictures. *IRE Transactions on Information Theory*, 5(4), 157-163.
[53] Huffman, D. A. (1952). A method for the construction of minimum-redundancy codes. *Proceedings of the IRE*, 40(9), 1098-1101.
[54] Witten, I. H., Neal, R. M., & Cleary, J. G. (1987). Arithmetic coding for data compression. *Communications of the ACM*, 30(6), 520-540.
[55] Fisher, Y. (2012). Fractal image compression: theory and application. *Springer Science & Business Media*.
[56] Artuğer, F., & Özkaynak, F. (2018). Fractal image compression method for lossy data compression. In 2018 *International Conference on Artificial Intelligence and Data Processing (IDAP)* (pp. 1-6). IEEE.
[57] Taubman, D., & Marcellin, M. (2012). JPEG2000 image compression fundamentals, standards and practice: image compression fundamentals, standards and practice (Vol. 642*). Springer Science & Business Media*.
[58] Wallace, G. K. (1992). The JPEG still picture compression standard. *IEEE transactions on consumer electronics*, 38(1), xviii-xxxiv.
[59] Artuğer, F., & Özkaynak, F. (2018). Performance Comparison for Lossy Image Compression Algorithm. *International Conference on Communication and Signal Processing (ICCSP).*
[60] Artuğer, F., & Özkaynak, F. (2018). JPEG Sıkıştırma Algoritmasının Dünü Bugünü ve Geleceği. *Fırat Üniversitesi Mühendislik Bilimleri Dergisi*, 30(3), 161-167.
[61] Rao, K. R., & Yip, P. (2014). Discrete cosine transform: algorithms, advantages, applications. *Academic press*.
[62] Artuğer, F., & Özkaynak, F. (2020). A novel method for performance improvement of chaos-based substitution boxes. *Symmetry*, 12(4), 571.
[63] Artuğer, F., & Özkaynak, F. (2022). A method for generation of substitution box based on random selection. *Egyptian Informatics Journal*, 23(1), 127-135.
[64] Artuğer, F., & Özkaynak, F. (2021). An effective method to improve nonlinearity value of substitution boxes based on random selection. *Information Sciences*, 576, 577-588.
[65] Alawida, M., Samsudin, A., Teh, J. S., & Alkhawaldeh, R. S. (2019). A new hybrid digital chaotic system with applications in image encryption. *Signal Processing*, 160, 45-58.
[66] Bos, J. W., Hubain, C., Michiels, W., & Teuwen, P. (2016). Differential computation analysis: Hiding your white-box designs is not enough. *In International Conference on Cryptographic Hardware and Embedded Systems* (pp. 215-236). Springer, Berlin, Heidelberg.
[67] Açikkapi, M. Ş., & Özkaynak, F. (2020). A method to determine the most suitable initial conditions of chaotic map in statistical randomness applications. *IEEE Access*, 9, 1482-1494.
[68] Wang, X., Li, Y., & Jin, J. (2020). A new one-dimensional chaotic system with applications in image encryption. *Chaos, Solitons & Fractals*, 139, 110102.
[69] Tang, G., Liao, X., & Chen, Y. (2005). A novel method for designing S-boxes based on chaotic maps. *Chaos, Solitons & Fractals*, 23(2), 413-419.
[70] Alatas, B., Akin, E., & Ozer, A. B. (2009). Chaos embedded particle swarm optimization algorithms. *Chaos, Solitons & Fractals*, 40(4), 1715-1734.
[71] Fung, H. T., & Parker, K. J. (1995). Design of image-adaptive quantization tables for JPEG. *Journal of Electronic Imaging*, 4(2), 144-150.
[72] Ratnakar, V., & Livny, M. (2000). An efficient algorithm for optimizing DCT quantization. *IEEE Transactions on Image Processing*, 9(2), 267-270.
[73] Abu, N. A., Ernawan, F., & Suryana, N. (2013). A generic psychovisual error threshold for the quantization table generation on JPEG image compression. *In 2013 IEEE 9th International Colloquium on Signal Processing and its Applications* (pp. 39-43). IEEE.
[74] Jiang, Y., & Pattichis, M. S. (2011). JPEG image compression using quantization table optimization based on perceptual image quality assessment. *In 2011 Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)* (pp. 225-229). IEEE.

[75] Wu, Y. G. (2004). GA-based DCT quantisation table design procedure for medical images. IEE Proceedings-Vision, *Image and Signal Processing*, 151(5), 353-359.

[76] B. Lazzerini, F. Marcelloni, M. Vecchio. (2009). A multi-objective evolutionary approach to image quality/compression ratio trade-off in JPEG baseline algorithm, *Applied Soft Computing*, 10:548–561.

[77] Ma, H., & Zhang, Q. (2013). Research on cultural-based multi-objective particle swarm optimization in image compression quality assessment. *Optik*, 124(10), 957-961.

[78] Tuba, M., & Bacanin, N. (2014). JPEG quantization tables selection by the firefly algorithm. *In 2014 International Conference on Multimedia Computing and Systems (ICMCS*) (pp. 153-158). IEEE.

[79] Kumar, B. V., & Karpagam, M. (2015). Differential evolution versus genetic algorithm in optimising the quantisation table for JPEG baseline algorithm. *International Journal of Advanced Intelligence Paradigms*, 7(2), 111-135.

[80] Balasubramanian, V. K., & Manavalan, K. (2016). A problem approximation surrogate model (PASM) for fitness approximation in optimizing the quantization table for the JPEG baseline algorithm. *Turkish Journal of Electrical Engineering & Computer Sciences*, 24(6), 4623-4636.

[81] Zhang, X., Wang, S., Gu, K., Lin, W., Ma, S., & Gao, W. (2016). Just-noticeable difference-based perceptual optimization for JPEG compression. *IEEE Signal Processing Letters*, 24(1), 96-100.

[82] Huang, C. H., & Wu, J. L. (2020). JQF: Optimal JPEG Quantization Table Fusion by Simulated Annealing on Texture Images and Predicting Textures. *arXiv preprint* arXiv:2008.05672.

[83] Yan, X., Fan, Y., Chen, K., Yu, X., & Zeng, X. (2020). QNet: An Adaptive Quantization Table Generator Based on Convolutional Neural Network. *IEEE Transactions on Image Processing*, 29, 9654-9664.

[84] J. Wang, H. Wang, J. Li, X. Luo. (2020). Detecting Double JPEG Compressed Color Images with the Same Quantization Matrix in Spherical Coordinates, *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 30, NO. 8.

[85] Liu, Z., Liu, T., Wen, W., Jiang, L., Xu, J., Wang, Y., & Quan, G. (2018). DeepN-JPEG: A deep neural network favorable JPEG-based image compression framework. *In Proceedings of the 55th annual design automation conference* (pp. 1-6).

[86] Choi, J., & Han, B. (2020). Task-aware quantization network for JPEG image compression. *In European Conference on Computer Vision* (pp. 309-324). Springer, Cham.

[87] Ferreira, R., Moon, B., Humphries, J., Sussman, A., Saltz, J., Miller, R., & Demarzo, A. (1997). The virtual microscope. *In Proceedings of the AMIA Annual Fall* Symposium (p. 449). American Medical Informatics Association.

[88] Mukhopadhyay, S., Feldman, M. D., Abels, E., Ashfaq, R., Beltaifa, S., Cacciabeve, N. G., ... & Taylor, C. R. (2018). Whole slide imaging versus microscopy for primary diagnosis in surgical pathology: a multicenter blinded randomized noninferiority study of 1992 cases (pivotal study). *The American journal of surgical pathology*, 42(1), 39.

[89] Holzinger, A., Goebel, R., Mengel, M., & Müller, H. (Eds.). (2020). Artificial intelligence and machine learning for digital pathology: state-of-the-art and future challenges (Vol. 12090). Springer Nature.

[90] Hamilton, P. W., Wang, Y., & McCullough, S. J. (2012). Virtual microscopy and digital pathology in training and education. *Apmis*, 120(4), 305-315.

[91] Sood, R. R., Shao, W., Kunder, C., Teslovich, N. C., Wang, J. B., Soerensen, S. J., ... & Rusu, M. (2021). 3D registration of pre-surgical prostate MRI and histopathology images via super-resolution volume reconstruction. *Medical Image Analysis*, 69, 101957.

[92] Srinidhi, C. L., Ciga, O., & Martel, A. L. (2021). Deep neural network models for computational histopathology: A survey. *Medical Image Analysis*, 67, 101813.

[93] Aresta, G., Araújo, T., Kwok, S., Chennamsetty, S. S., Safwan, M., Alex, V., ... & Aguiar, P. (2019). Bach: Grand challenge on breast cancer histology images. *Medical image analysis*, 56, 122-139.

[94] Barker, J., Hoogi, A., Depeursinge, A., & Rubin, D. L. (2016). Automated classification of brain tumor type in whole-slide digital pathology images using local representative tiles. *Medical image analysis*, 30, 60-71.

[95] Veta, M., Heng, Y. J., Stathonikos, N., Bejnordi, B. E., Beca, F., Wollmann, T., ... & Pluim, J. P. (2019). Predicting breast tumor proliferation from whole-slide images: the TUPAC16 challenge. *Medical image analysis*, 54, 111-121.

[96] Wang, X., Fang, Y., Yang, S., Zhu, D., Wang, M., Zhang, J., ... & Han, X. (2021). A hybrid network for automatic hepatocellular carcinoma segmentation in H&E-stained whole slide images. *Medical Image Analysis*, 68, 101914.

[97] Van Rijthoven, M., Balkenhol, M., Siliņa, K., Van Der Laak, J., & Ciompi, F. (2021). HookNet: Multi-resolution convolutional neural networks for semantic segmentation in histopathology whole-slide images. *Medical Image Analysis*, 68, 101890.

[98] Dov, D., Kovalsky, S. Z., Assaad, S., Cohen, J., Range, D. E., Pendse, A. A., ... & Carin, L. (2021). Weakly supervised instance learning for thyroid malignancy prediction from whole slide cytopathology images. *Medical image analysis*, 67, 101814.

[99] Kong, J., Sertel, O., Shimada, H., Boyer, K. L., Saltz, J. H., & Gurcan, M. N. (2009). Computer-aided evaluation of neuroblastoma on whole-slide histology images: Classifying grade of neuroblastic differentiation. *Pattern Recognition*, 42(6), 1080-1092.

[100] Hacking, S., Nasim, R., Lee, L., Vitkovski, T., Thomas, R., Shaffer, E., & Nasim, M. (2020). Whole slide imaging and colorectal carcinoma: A validation study for tumor budding and stromal differentiation. *Pathology-Research and Practice*, 216(11), 153233.

[101] Wang, S., Zhu, Y., Yu, L., Chen, H., Lin, H., Wan, X., ... & Heng, P. A. (2019). RMDL: Recalibrated multi-instance deep learning for whole slide gastric image classification. *Medical image analysis*, 58, 101549.

[102] Xiang, Y., He, Z., Liu, Q., Chen, J., & Liang, Y. (2021). Autofocus of whole slide imaging based on convolution and recurrent neural networks. *Ultramicroscopy*, 220, 113146.

[103] Madabhushi, A., & Lee, G. (2016). Image analysis and machine learning in digital pathology: Challenges and opportunities. *Medical image analysis*, 33, 170-175.

[104] Li, B., Keikhosravi, A., Loeffler, A. G., & Eliceiri, K. W. (2021). Single image super-resolution for whole slide image using convolutional neural networks and self-supervised color normalization. *Medical Image Analysis*, 68, 101938.

[105] Li, B., Keikhosravi, A., Loeffler, A. G., & Eliceiri, K. W. (2021). Single image super-resolution for whole slide image using convolutional neural networks and self-supervised color normalization. *Medical Image Analysis*, 68, 101938.

[106] Rodrigues, V. F., Paim, E. P., Kunst, R., Antunes, R. S., da Costa, C. A., & da Rosa Righi, R. (2020). Exploring publish/subscribe, multilevel cloud elasticity, and data compression in telemedicine. *Computer Methods and Programs in Biomedicine*, 191, 105403.

[107] Kalra, S., Tizhoosh, H. R., Choi, C., Shah, S., Diamandis, P., Campbell, C. J., & Pantanowitz, L. (2020). Yottixel–an image search engine for large archives of histopathology whole slide images. *Medical Image Analysis*, 65, 101757.

[108] Kalinski, T., Zwönitzer, R., Grabellus, F., Sheu, S. Y., Sel, S., Hofmann, H., ... & Roessner, A. (2009). Lossy compression in diagnostic virtual 3-dimensional microscopy—where is the limit?. *Human pathology*, 40(7), 998-1005.

[109] Sharma, A., Bautista, P., & Yagi, Y. (2012). Balancing image quality and compression factor for special stains whole slide images. *Analytical Cellular Pathology*, 35(2), 101-106.

[110] Vahadane, A., Peng, T., Sethi, A., Albarqouni, S., Wang, L., Baust, M., ... & Navab, N. (2016). Structure-preserving color normalization and sparse stain separation for histological images. *IEEE transactions on medical imaging*, 35(8), 1962-1971.

[111] Snead, D. R., Tsang, Y. W., Meskiri, A., Kimani, P. K., Crossman, R., Rajpoot, N. M., ... & Cree, I. A. (2016). Validation of digital pathology imaging for primary histopathological diagnosis. *Histopathology*, 68(7), 1063-1072.

[112] González-Conejero, J., Bartrina-Rapesta, J., & Serra-Sagrista, J. (2009). JPEG2000 encoding of remote sensing multispectral images with no-data regions. *IEEE Geoscience and Remote Sensing Letters*, 7(2), 251-255.

[113] Cagnazzo, M., Parrilli, S., Poggi, G., & Verdoliva, L. (2007). Costs and advantages of object-based image coding with shape-adaptive wavelet transform. *EURASIP Journal on Image and Video Processing*, 2007, 1-13.

[114] Dong, Y., Shen, H., & Pan, W. D. (2016). An interactive tool for ROI extraction and compression on whole slide images. *In 2016 IEEE-EMBS International Conference on Biomedical and Health Informatics* (BHI) (pp. 224-227). IEEE.

[115] Taubman, D., & Marcellin, M. (2012). JPEG2000 image compression fundamentals, standards and practice: image compression fundamentals, standards and practice (Vol. 642). *Springer Science & Business Media.*

[116] Kalinski, T., Zwönitzer, R., Sel, S., Evert, M., Guenther, T., Hofmann, H., ... & Roessner, A. (2008). Virtual 3D microscopy using multiplane whole slide images in diagnostic pathology. *American journal of clinical pathology*, 130(2), 259-264.

[117] Doyle, S., Monaco, J., Madabhushi, A., Lindholm, S., Ljung, P., Ladic, L., ... & Feldman, M. (2010). Evaluation of effects of JPEG2000 compression on a computer-aided detection system for prostate cancer on digitized histopathology. *In 2010 IEEE International Symposium on Biomedical Imaging: From Nano to Macro* (pp. 1313-1316). IEEE.

[118] Johnson, J. P., Krupinski, E. A., Yan, M., Roehrig, H., Graham, A. R., & Weinstein, R. S. (2010). Using a visual discrimination model for the detection of compression artifacts in virtual pathology images. *IEEE transactions on medical imaging*, 30(2), 306-314.

[119] Barisoni, L., Troost, J. P., Nast, C., Bagnasco, S., Avila-Casado, C., Hodgin, J., ... & Hewitt, S. M. (2016). Reproducibility of the NEPTUNE descriptor-based scoring system on whole-slide images and histologic and ultrastructural digital images. *Modern Pathology*, 29(7), 671-684.

[120] Farahani, N., Parwani, A. V., & Pantanowitz, L. (2015). Whole slide imaging in pathology: advantages, limitations, and emerging perspectives. *Pathol Lab Med Int*, 7(23-33), 4321.

[121] Hernández-Cabronero, M., Sanchez, V., Auli-Llinas, F., & Serra-Sagrista, J. (2016). Fast MCT optimization for the compression of whole-slide images. *In 2016 IEEE International Conference on Image Processing* (ICIP) (pp. 2370-2374). IEEE.

[122] Zhang, L., Xiu, X., Chen, J., Karczewicz, M., He, Y., Ye, Y., ... & Kim, W. S. (2016). Adaptive color-space transform in HEVC screen content coding. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 6(4), 446-459.

[123] Niazi, M. K. K., Parwani, A. V., & Gurcan, M. N. (2016). Computer-assisted bladder cancer grading: α-shapes for color space decomposition. In Medical Imaging 2016: Digital Pathology (Vol. 9791, p. 979107). *International Society for Optics and Photonics*.

[124] Hernández-Cabronero, M., Sanchez, V., Blanes, I., Auli-Llinas, F., Marcellin, M. W., & Serra-Sagristà, J. (2018). Mosaic-based color-transform optimization for lossy and lossy-to-lossless compression of pathology whole-slide images. *IEEE Transactions on Medical Imaging*, 38(1), 21-32.

[125] Helin, H., Tolonen, T., Ylinen, O., Tolonen, P., Näpänkangas, J., & Isola, J. (2018). Optimized JPEG 2000 compression for efficient storage of histopathological whole-slide images. *Journal of pathology informatics*, 9.

[126] Bug, D., Bartsch, F., Schaadt, N. S., Wien, M., Feuerhake, F., Schüler, J., ... & Merhof, D. (2020). Scalable HEVC for Histological Whole-Slide Image Compression. *In Bildverarbeitung für die Medizin* 2020 (pp. 315-321). Springer Vieweg, Wiesbaden.

ÖZGEÇMİŞ

Fırat ARTUĞER

[redacted]

AKADEMİK FAALİYETLER

Makaleler:

1. Artuğer, F., & Özkaynak, F. (2018). JPEG Sıkıştırma Algoritmasının Dünü Bugünü ve Geleceği. Fırat Üniversitesi Mühendislik Bilimleri Dergisi, 30(3), 161-167.
2. Artuğer, F., & Özkaynak, F. (2020). A novel method for performance improvement of chaos-based substitution boxes. Symmetry, 12(4), 571.
3. Artuğer, F., & Özkaynak, F. (2021). An effective method to improve nonlinearity value of substitution boxes based on random selection. Information Sciences, 576, 577-588.
4. Artuğer, F., & Özkaynak, F. (2022). A method for generation of substitution box based on random selection. Egyptian Informatics Journal, 23(1), 127-135.
5. Artuğer, F., & Özkaynak, F. (2022). JPEG Algoritmasının Performansını İyileştirmek İçin Bir Yöntem. Fırat Üniversitesi Mühendislik Bilimleri Dergisi, 34(1), 25-32.
6. Artuğer, F., & Özkaynak, F. (2022). Görüntü Sıkıştırma Algoritmalarının Performans Analizi İçin Değerlendirme Rehberi. International Journal of Pure and Applied Sciences, 8(1), 102-110.

Bildiriler:

1. Artuğer, F., & Özkaynak, F. (2018). Performance Comparison for Lossy Image Compression Algorithm. International Conference on Communication and Signal Processing (ICCSP).

2. Artuğer, F., & Özkaynak, F. (2018). Fractal image compression method for lossy data compression. International Conference on Artificial Intelligence and Data Processing (IDAP) (pp. 1-6). IEEE.

3. Burhan, Y., Artuger, F., & Ozkaynak, F. (2019). A novel hybrid image encryption algorithm based on data compression and chaotic key planning algorithms. International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-5). IEEE.

4. Artuğer, F., & Özkaynak, F. (2022). A Substitution Box Generation Method based on Cascading Chaotic Maps. International Cumhuriyet Artificial Intelligence Applications Conference(CAIAC).