KOCAELİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

DOKTORA TEZİ

PROFILE HIDDEN MARKOV VE OLASILIKSAL GEÇİŞ TABANLI GÖRÜNTÜ ŞİFRELEME

HİKMETCAN ÖZCAN

KOCAELİ 2021

KOCAELİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ

ANABİLİM DALI

DOKTORA TEZİ

PROFILE HIDDEN MARKOV MODEL VE OLASILIKSAL GEÇİŞ TABANLI GÖRÜNTÜ ŞİFRELEME

HİKMETCAN ÖZCAN

Doç. Dr. Suhap ŞAHİN		
Danışman,	**Kocaeli Üniv.**	**.....**
Prof. Dr. Kerem KÜÇÜK		
Jüri Üyesi,	**Kocaeli Üniv.**	**.....**
Doç. Dr. Cüneyt BAYILMIŞ		
Jüri Üyesi,	**Sakarya Üniv.**	**.....**
Dr. Öğr. Üyesi Alpaslan Burak İNNER		
Jüri Üyesi,	**Kocaeli Üniv.**	**.....**
Dr. Öğr. Üyesi Oktay AYTAR		
Jüri Üyesi,	**Bolu Abant İzzet Baysal Üniv.**	**.....**

Tezin Savunulduğu Tarih: 12.04.2021

ÖNSÖZ VE TEŞEKKÜR

Bu tez çalışması, kişisel veri güvenliği kapsamında dijital görüntü şifreleme algoritmalarını incelemek ve yeni iki görüntü şifreleme algoritması geliştirmek amacıyla gerçekleştirilmiştir.

Lisans, Yüksek Lisans ve Doktora eğitimim süresince desteğini esirgemeyen, tezimin her aşamasında sorunlarımı dinleyerek, görüşleri ile çalışmalarıma katkıda bulunan ve yoğun akademik yaşamında değerli zamanını her türlü problemimi çözmeye ayıran tez danışmanım saygı değer hocam Doç. Dr. Suhap ŞAHİN'e içtenlikle teşekkür ederim.

Tez çalışmama bilgi ve tavsiyeleri ile katkıda bulunan tez ilerleme jürim Prof. Dr. Kerem KÜÇÜK'e ve Doç. Dr. Cüneyt BAYILMIŞ'a

Çalışmalarım boyunca desteğini ve yardımlarını esirgemeyen, aynı laboratuvarı paylaştığım çalışma arkadaşlarım Dr. Öğr. Üyesi Fidan KAYA GÜLAĞIZ'a, Arş. Gör. Mehmet Ali ALTUNCU'ya, Arş. Gör. Sümeyya İLKİN'e ve Gömülü ve Algılayıcı Sistem Araştırma Laboratuvarı çalışanlarına,

Tez çalışmam sırasında tecrübelerinden yararlanma fırsatı bulduğum Dr. Öğr. Üyesi Orhan AKBULUT, Öğr. Gör. Dr. Onur GÖK'e ve Mustafa MENTEŞOĞLU'na

Akademik çalışmalarım sırasında birçok aşamada beni destekleyen Bilgisayar Mühendisliği Bölümü Öğretim Üyeleri ve Araştırma Görevlilerine

Maddi ve manevi desteklerini tüm hayatı botunca esirgemeyen annem Ülkü ÖZCAN'a ve babam Birol ÖZCAN'a, tez çalışmam boyunca gösterdiği sonsuz destek ve anlayış için kayınpederim Ali OLGUN'a, eşim Arzu ÖZCAN'a ve gülücükleriyle bana güç veren sevgili kızım Defne ÖZCAN'a teşekkürü borç bilirim.

Nisan – 2021 Hikmetcan ÖZCAN

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

TABLOLAR DİZİNİ

SİMGELER VE KISALTMALAR DİZİNİ

a_{ij}	:	i durumundan j durumuna geçiş olasılığı
A	:	Geçiş olasılıkları kümesi
A_iJ	:	q_i durumundan q_j durumuna yapılan geçişlerin sayısı
B	:	Çıktı olasılıkları kümesi
C(i,j)	:	Şifresi çözülmüş görüntüdeki i. Satır ve j. Sütundaki piksel değeri
$C_{1,2}$	:	Payda dengeleyici
D	:	Profile Hidden Markov Model'de silme durumu
$e_i(x)$	:	Profile Hidden Markov Model q_i durumunda x çıktısının oluşma olasılığı
$E_i(X)$	:	Profile Hidden Markov Model q_i durumunda x çıktısının oluşma olasılığı
H	:	Yükseklik
H_t	:	t zamanındaki saat değeri
I	:	Profile Hidden Markov Model' de ekleme durumu
δ	:	En yüksek olasılıklı yol
J	:	Amaç fonksiyonu
$K_{1,2}$	:	Sabit değer
k	:	Bit değeri
L	:	Piksel değerinin dinamik aralığı
M	:	Profile Hidden Markov Model'de eşleme durumu
MAX	:	Maksimum piksel değeri
MC	:	m satır ve n sütun sayılı maksimum renk matrisi
m	:	Satır
mr_{ij}	:	Bir piksele ait maksimum renk değeri
μ	:	Ortalama
σ	:	Kovaryans
σ^2	:	Varyans
γ	:	Korelasyon katsayısı
n	:	Sütun
N	:	Durum sayısı
P	:	Olasılık
P(i,j)	:	Orijinal görüntüdeki i. satır ve j. sütundaki piksel değeri
p_{ij}	:	ProbRGB modelin'de i durumundan j durumuna geçiş olasılığı
PM	:	Piksel matrisi
r_t	:	t zamanında bulunulan durum
s_i	:	Pikseldeki renk değerinin tüm görüntü pikselleri içerisindeki kullanım olasılığı
α_{ij}	:	Piksel
q_t	:	t anındaki durum
T(n)	:	Zaman karmaşıklığı
T(i,j)	:	i. satır ve j. sütundaki iki görüntü arasındaki piksellerin birbirine eşit olup olmadığı
t	:	Zaman

V	:	Simge kümesi
W	:	Genişlik
ω	:	Başlangıç olasılığı
Q	:	Durum dizisi
X	:	Veri kümesi
X_i	:	Durum kümesi
x	:	Profile Hidden Markov Model'de oluşan çıktılar

Kısaltmalar

AES	:	Advanced Encryption Standard
B	:	Blue (Mavi)
bmp	:	Bitmap
CB	:	Chaos-based (Kaos Tabanlı)
CBC	:	Cipher Block Chaining
CC	:	Correlation Coefficent (Korelasyon Katsayısı)
DES	:	Data Encryption Standart
DNA	:	Deoksiribo Nükleik Asit
EZW	:	Embedded Zerotree Wavelet (Gömülü Sıfır Ağaç Dalgacık)
FPGA	:	Field Programmable Gate Array (Alanda Programlanabilir Kapı Dizisi)
G	:	Green (Yeşil)
IE	:	Information Entropy (Bilgi Entropisi)
IoT	:	Internet of Things (Nesnelerin İnterneti)
IV	:	Initialization Vector (Başlatma Vektörü)
JPEG	:	Joint Photographic Experts Group (Birleşik Fotoğraf Uzmanları Grubu)
KDSA	:	Knutt Durstenfeld Shuffle Algoritm
MAE	:	Mean Absolute Error (Ortalama Mutlak Hata)
MM	:	Markov Model
MSE	:	Mean Square Error (Ortalama Karesel Hata)
NPCR	:	Number of Pixel Chance Rate (Piksel Sayısı Değişim Oranı)
PHMM	:	Profile Hidden Markov Model
PSNR	:	Peak Signal-to-Noise Ratio (Tepe Sinyal Gürültü Oranı)
PV	:	Probability Vector (Olasılık Vektörü)
png	:	Portable Network Graphics (Taşınabilir Ağ Grafiği)
R	:	Red (Kırmızı)
RGB	:	Red Green Blue (Kırmızı Yeşil Mavi)
S-Box	:	Substitution-Box (Yer Değiştirme K)
SMM	:	Saklı Markov Modeli
SSIM	:	Structure Similarity (Yapısal Benzerlik)
TEA	:	Tiniy Encryption Algorithm
UACI	:	Unified Average Changing Intensity (Birleşik Ortalama Değişim Yoğunluğu)
VC	:	Visual Cryptography (Görüntü Şifreleme)
XOR	:	Exclusive OR (Özel Veya)

PROFILE HIDDEN MARKOV VE OLASILIKSAL GEÇİŞ TABANLI GÖRÜNTÜ ŞİFRELEME

ÖZET

Bu çalışmanın amacı, kişisel veri güvenliği kapsamında dijital görüntü şifreleme algoritmalarını incelemek ve yeni iki görüntü şifreleme algoritması geliştirmektir.

Bu tez çalışmasında dijital görüntüleri şifrelemek amacıyla iki farklı görüntü şifreleme yöntemi önerilmiştir. İlk yöntemde Profile Hidden Markov Model kullanılarak şifrelenecek görüntüye ait bir RGB olasılık vektörü elde edilmektedir. Rastgele değerlerden oluşturulmuş başlatma vektörü ve PHMM yöntemi üzerinden elde edilen olasılık vektörü kullanılarak görüntü pikselleri üzerinde blok şifreleme işlemi gerçekleştirilmektedir. Ayrıca şifrelenmiş piksel değerlerinin karıştırılması için S-Box'lardan yararlanılmaktadır.

İkinci yöntemde ise, olasılıksal bir renk modeli kullanılarak şifrelenecek görüntüye ait bir RGB olasılık vektörü elde edilmektedir. Ayrıca ilk yöntemde kullanılan başlatma vektörü de şifreleme için kullanılmaktadır. Son olarak birbirinden tamamen farklı iki S-Box kullanılarak hem şifreleme işlemine girmeden önce hem de şifreleme işleminden sonra piksel değerinin karıştırılması sağlamaktadır. Böylece geliştirilen her iki yeni görüntü algoritmalarındaki simetrik şifreleme ile görüntünün şifrelenmesi sağlanmaktadır. Şifreleme önerilen her iki yöntemde de renkli görüntüler için 24 bitlik, gri tonlamalı görüntüler için ise 8 bitlik bloklar halinde yapılmaktadır.

Önerilen yöntemlerin güvenlik ve performans analizleri görüntü kriptanaliz yöntemleri ile test edilmiştir. Elde edilen sonuçlar literatürde mevcut görüntü şifreleme yöntemleri ile karşılaştırılmıştır. Sonuçlara göre önerilen görüntü şifreleme algoritmalarının hem renkli hem de gri tonlamalı görüntüler için hızlı ve yüksek güvenliği sağlayabileceğini doğrulamaktadır.

Anahtar Kelimeler: Görüntü Şifreleme, Olasılık, Performans Analizi, Profile Hidden Markov Model, Viterbi Algoritması.

VISUAL CRYPTOGRAPHY BASED ON PROFILE HIDDEN MARKOV AND PROBABILITY TRANSITION

ABSTRACT

The purpose of this study is to examine visual cryptography algorithms within the scope of personal data security and to develop two new visual cryptography algorithms.

In this thesis, two different visual cryptography are proposed to encrypt digital images. In the first method, an RGB probability vector of the image to be encrypted is obtained using the Profile Hidden Markov Model method. Then, the Block encryption process is performed on the image pixels by using the initiation vector created from random values and the probability vector obtained through the PHMM method. Also, S-Box is used to mix encrypted pixel values.

In the second method, an RGB probability vector of the image to be encrypted using a probabilistic color model is obtained. In addition, an initialization vector used in the first method is used for encrypting. Finally, by using two completely different S-Boxes, the pixel value is mixed before and after the encryption process. Thus, the image is encrypted with symmetric encryption in both new visual cryptography algorithms. Encryption is done in 24-bit blocks for color images and 8-bit blocks for grayscale images in both methods.

Security and performance analysis of the proposed method was tested by visual cryptanalysis methods. The results obtained were compared with the visual cryptography methods available in the literature. According to the results obtained, it confirms that the proposed visual cryptography algorithms can provide fast and high security for both color and grayscale images.

Keywords: Visual Cryptography, Probability, Performance Analysis, Profile Hidden Markov Model, Viterbi Algorithm.

GİRİŞ

Şifreleme geçmişten günümüze kadar başkaları tarafından öğrenilmesi istenmeyen bilgilerin saklanması amacıyla yaygın olarak kullanılmaktadır. Günlük hayatta kullandığımız bankacılık işlemlerinden sosyal medya hesaplarımıza kadar şifreleme işlemlerinden yararlanmaktayız. Buna karşın, kişisel verilerin üçüncü kişilerin eline geçmesi halinde oldukça zor durumlarda kalındığı da bir gerçektir. Bu sebeple kişisel veri güvenliği için şifreleme yöntemlerine oldukça fazla ihtiyaç duyulmaktadır. Kişisel veriler sadece yazı metinlerini (banka giriş şifresi, sosyal medya şifresi vb.) içermez ayrıca görüntü verilerini de içermektedir. Dijital görüntü yakalama teknolojilerinin günümüzde yaygın olarak kullanılmasıyla kişisel görüntüleri yakalamak ve paylaşmak çok kolay ve hızlı bir hale getirmektedir. Bu durum, özel verilerin gizliliğinin sağlanmasında zorluklara ve üçüncü kişilerin bu verileri ele geçirmesi gibi risklere neden olmaktadır. Bu sebeple veri güvenliğini en etkin şekilde sağlamak için eldeki görüntü verisinin şifrelenmesi gerekmektedir.

Görüntü şifreleme, simetrik ve asimetrik şifreleme olmak üzere iki bölümden oluşmaktadır. Simetrik şifreleme tek bir anahtar ile hem şifreleme hem de şifre çözme işlemi gerçekleştirmektedir. Asimetrik şifreleme de ise bir açık ve bir gizli anahtarla şifreleme ve şifre çözme işlemini gerçekleştirmektedir. Ancak asimetrik şifreleme yöntemleri, şifreleme ve şifre çözme süreleri açısından simetrik şifreleme yöntemlerinden daha yavaş çalışır. Geçmişten günümüze kadar simetrik şifreleme temelli birçok görüntü şifreleme yöntemi geliştirilmiştir.

Güvenoğlu, yapmış olduğu çalışmada blok şifrelemede yaygın olarak kullanılan yer değiştirme kutularını(S-Box) kullanmıştır. Yer değiştirme kutusunu üretirken KDSA algoritmasından yararlanmıştır. Kayıpsız ve hızlı bir şekilde şifre çözme için ise oluşturduğu yer değiştirme kutusunu kullanarak ters yer değiştirme kutusu üretmiştir (Güvenoğlu, 2016).

Reyad ve arkadaşları, gri tonlamalı ve renkli görüntüler için iki görüntü şifreleme şeması önermişlerdir. İlk şemada, iki boyutlu görüntüyü bloklara ayırmışlardır. İkinci

şemada ise, tüm blokları sırasıyla XOR işlemine tabi tutarak şifreleme işlemini gerçekleştirmişlerdir. Çalışmada şifreli görüntülerin güvenlik analizi, hassasiyet ve sağlamlık açısından başarılı olduğu belirtilmiştir (Reyad ve diğ., 2017).

Thakur ve Kumar, DES, AES ve Blowfish algoritmalarının performans analizlerini karşılaştırmak için bir simülasyon geliştirmişlerdir. Performans karşılaştırmaları için hız, blok boyutu ve anahtar boyutu parametrelerini kullanmışlardır. Çalışmanın sonucunda Blowfish algoritmasının diğer şifreleme algoritmalarından daha iyi bir performansa sahip olduğu belirtilmiştir (Thakur ve Kumar, 2011).

Abd-El-Hafiz ve diğerleri, fraktal görüntülerden ürettikleri anahtar ile orijinal görüntüyü şifreleyerek yeni bir görüntü şifreleme sistemi geliştirmişlerdir. Şifreyi çözmek için de aynı anahtar kullanmış ve orijinal görüntünün kayıpsız olarak elde edildiğini belirtmişlerdir (Abd-El-Hafiz, 2014).

Güvenoğlu ve Esin, çalışmalarında dijital ortamdaki görüntülerin şifrelenmesi için Knutt Durstenfeld Shuffle (KDSA) algoritması kullanmışlardır. Önerilen algoritma ile elde edilen bir anahtar dizisi kullanarak görüntü piksellerinin yerlerinin değiştirilmesi amaçlanmıştır. Çalışmada farklı tip ve özellikteki görüntüler üzerinde kullanımı kolay, güçlü ve etkili bir sistem elde edildiği belirtilmiştir (Güvenoğlu ve Esin, 2009).

Naveen ve arkadaşları, tıbbi görüntülerin güvenliğinin sağlanması için iki aşamalı bir yöntem önermişlerdir. İlk aşamada görüntüyü EZW (Embedded Zerı Wavelet) görüntü sıkıştırma algoritmasını kullanarak sıkıştırmışlardır. İkinci aşamada ise görüntüyü matris haline dönüştürerek kaos tabanlı satır ve sütun tabanlı şifreleme algoritması uygulamışlardır. Yazarlar, bu aşamaların tersten uygulanmasıyla orijinal görüntüyü kayıpsız şekilde elde ettikleri belirtmişlerdir (Naveen ve diğ., 2015).

Benssalah ve diğerleri, tıbbi görüntüler üzerinde kaos temelli ve eliptik eğri tabanlı şifreleme algoritmalarını karşılaştırmışlardır. Kaos tabanlı yöntemin şifreleme süresinin çok kısa olmasına karşın pratikte uygulanmadan önce yoğun güvenlik analizi yapılması gerektiğini vurgulanmıştır. Eliptik eğri temelli yaklaşımda ise kırılması zor olan ayrık logaritma problemine karşın şifreleme süresinin uzun olduğunu belirtilmiştir (Benssalah ve diğ., 2018).

Chaudhary ve arkadaşları, akıllı şehirlerde sağlık sistemlerindeki haberleşme için kafes (lattice) tabanlı güvenli şifreleme sistemi önermişlerdir. Önerilen sistemde hastadan alınan şeker, tansiyon vb. sensör verilerinin güvenli bir şekilde doktora iletilmesi için açık bir anahtar, doktorun bu şifreyi çözebilmesi için gizli bir anahtar kullanılmıştır. Önerilen sistemin sonuçları iletişim ve hesaplama maliyeti açısından benzer çalışmalarla kıyaslandığında, sistemin daha başarılı sonuçlar verdiği belirtilmiştir (Chaudhary ve diğ., 2018).

Liu ve çalışma arkadaşları, uzaktan algılama görüntüleri (remote-sensing images) üzerinde DNA temelli olasılıksal bir şifreleme yöntemi önermişlerdir. Şifreleme aşamasında DNA kodları ve iki boyutlu lojistik DNA maskesi kullanmışlardır. Deneysel sonuçlarda, önerilen algoritmanın uzaktan algılama görüntülerine karşı mevcut çeşitli saldırı programlarına dayanabileceğini belirtmişlerdir (Liu ve diğ., 2019).

Lin ve Chung, yapmış oldukları çalışmada görüntü şifreleme şeması için olasılıksal bir model geliştirmişlerdir. Bu modelde görüntüyü temel (0 ve 1'lerden oluşan) matrise dönüştürerek n kez transparan hale getirmiş ve t adet farklı görüntü çıktısı üretmişlerdir. Ayrıca t adet görüntü çıktısından hiçbirinin tek başına bir anlam ifade etmediğini vurgulamışlardır. Orijinal görüntüyü elde edebilmenin tek yolunun t adet görüntü çıktısının hepsine sahip olunması ve üst üste birleştirilmesi olduğunu belirtmişlerdir (Lin ve Chung, 2012).

Milani ve arkadaşları yapmış oldukları çalışmada Henan kaotik sistemleri ile lojistik haritanın rastgele özelliklerinden yararlanılarak görüntü şifrelemede kullanılabilecek hızlı bir algoritma geliştirdiklerini belirtmişlerdir. Ayrıca yöntemin güvenliğini düz görüntüler ile şifrelenmiş görüntüler arasında gerçekleştirilen dönüşümler göz önünde bulundurularak analiz etmişlerdir. Önerilen yöntemin 256 elemanlı bir rastgele sayılar listesine ve bu listedeki elemanları rastgeleliğini arttırmak için Lojistik harita kullandıklarını belirtmişlerdir. Bu yol içerisinde üretilen rastgele sayıların ağırlıklı olarak başlangıç değerine bağlı olduğunu dolayısıyla kullanılan anahtar kelimenin daha hassas olduğunu belirtmişlerdir. Çalışmanın sonucunda siyah-beyaz ve renkli görüntüler üzerindeki uygulamalardan elde edilen sonuçlara göre algoritma güvenliğinin yüksek olduğunu ifade etmişlerdir (Milani ve diğ., 2011).

Maleki ve arkadaşları, güvenli bir şifreleme sistemi sunmak için kayıplı görüntü şifreleme sistemi adını verdikleri hafızalı hücresel otomata adı verilen özel tür hücresel otomata ve görüntü üzerindeki en az önemli pikseli kullanan bir şema önermişlerdir. Çalışmanın sonucunda insan gözüyle bakıldığında orijinal görüntü ve şifresi çözülmüş görüntünün ayırt edilemediğini söylemişlerdir (Maleki ve diğ., 2008).

Zhang Yun-peng ve arkadaşları, görüntü şifreleme için kaos tabanlı şifreleme ve DES şifreleme tekniklerini beraber kullanmışlardır. Görüntüyü şifrelemek için kaos rastgele dizisinden yararlanmışlardır. Rastgele diziyi elde etmek için mantıksal kaos sıralayıcıyı kullanmışlardır. Şifreleme işleminden sonra DES ile iki kez şifreleme yaparak şifreleme işlemini tamamladıklarını belirtmişlerdir. Gerçekleştirdikleri teorik analiz ve simülasyon, bu planın yüksek başlangıç değeri hassasiyetine ve yüksek güvenlik ve şifreleme hızına sahip olduğunu belirtmişlerdir. Ayrıca komşu RGB ilgisini sıfıra yakın tuttuklarını söyleyerek algoritmanın gerçek görüntü şifrelemesinde kullanılabileceğini ifade etmişlerdir (Zhang ve diğ., 2009).

Marwan ve arkadaşları, tıbbi görüntüleri bulut üzerine taşımadan önce veri güvenliğini sağlamak için bir şifreleme yöntemi önermişlerdir. Orijinal görüntüyü ikiye ayırarak her birini farklı görüntü şifreleme şeması ile şifreleyerek farklı bir bulut üzerinde saklamışlardır. Orijinal görüntüye dönmek için bulutlarda bulunan görüntüleri şifrelendikleri şema ile tekrardan çözüp birleştirmişlerdir (Marwan ve diğ., 2017).

Dalhoum ve Mahafzah çalışmalarında görüntü şifreleme için karıştırma (scrambling) tekniği kullanmışlardır. Bu teknikte dijital görüntüdeki satır ve sütunların yerleri rastgele üretilmiş dağıtıcı matrislerine göre değiştirilmektedir. Dijital görüntüyü grayscale matrisine dönüştürerek matris içerisindeki satır ve sütunlardaki değerleri dağıtıcı matrisine göre yerlerini değiştirerek şifreleme işlemini tamamlamışlardır. Şifre çözme için aynı dağıtım matrislerini kullanarak orijinal görüntüye ulaşmışlardır (Dalhoum ve Mahafzah, 2012).

Wang ve Hsu, çalışmalarında konvansiyonel matris ve olasılıksal bir model ile paylaşımlı görüntüleri üretip görüntüyü şifrelemek için kullanmışlardır. Ayrıca paylaşımlı görüntülere etiket ekleyerek ayırt edilebilirliği ve ek özellik kazandırdıklarını belirtmişlerdir. Sonuç olarak görüntülerin güvenli bir şekilde şifrelediklerini belirtmişlerdir (Wang ve Hsu, 2011).

Muhammad ve arkadaşları, IoT sistemine bağlı kameralardaki görüntüleri şifrelemek için olasılıksal bir model kullanmışlardır. Görüntüdeki pikseller arasında olasılıksal bir bağlantı yakalamış ve şifreleme işlemini buna göre yapmışlardır. Ayrıca önerdikleri sistemin benzer yöntemlere göre daha sağlam, kısa sürede çalışan ve güvenlik açısından daha iyi olduğunu belirtmişlerdir (Muhammad ve diğ., 2018).

Khan ve arkadaşları, görüntü yakalayan IoT cihazlarından alınan görüntülerin güvenli bir şekilde şifrelenmesi için bir şema önermişlerdir. Şifreleme için görüntülerden anahtar görüntü belirlemişler ve şifreleme için kullanmışlardır. Sonuç olarak benzer yöntemlere göre şifreleme şemasının daha güvenli ve efektif olduklarını vurgulamışlardır (Khan ve diğ., 2020).

Prisco ve Santis, yapmış oldukları çalışmada Naor ve Shamir'in (Naor ve Shamir, 1994) çalışmasının yanında Kafri ve Keren'in (Kafri ve Keren, 1987) görüntü şifreleme şemalarının eksik yönlerini kapatarak olasılıksal bir model ile birlikte rastgele ızgara tabanlı, deterministtik bir görüntü şifreleme şeması önermişlerdir. Sonuç olarak optimum çözümle görüntü şifreleme yaptıklarını belirtmişlerdir (Prisco ve Santis, 2014).

Li ve arkadaşları, çalışmalarında IoT cihazlarından toplanan görüntülerin güvenliğini sağlamak için kaos tabanlı bir şifreleme algoritması önermişlerdir. Algoritmanın birçok özelliğinin yanında güçlü yönünün düşük hesap karmaşıklığı olduğunu vurgulamışlardır. Simülasyonların sonucunda önerdikleri sistemin güvenlik açısından yüksek performans gösterdiğini belirtmişlerdir (Li ve diğ., 2020).

Bağbaba ve çalışma arkadaşları, JPEG standardına sahip görüntülerde lightweight algoritması olan Tiny şifreleme algoritmasını kullanarak görüntü şifreleme yöntemi geliştirmişlerdir. Geliştirilen sistem FPGA (Field Programmable Gate Array) üzerinde donanımsal olarak gerçekleyerek test edilmiştir. Sonuçlar incelendiğinde hem sıkıştırma hem de şifrelemede başarılı sonuçlar alındığını ifade etmişlerdir (Bağbaba ve diğ., 2015).

Sun, çalışmasında DNA (deoksiribonükleik asit) şifrelemesi ve kaotik bir haritalama kullanarak bir görüntü şifreleme şeması önermiştir. Şifrelemeden önce görüntünün satır ve sütunlarını inceleyerek başlangıç koşulları hesaplamıştır. Ayrıca şifreleme

güvenliğini arttırmak için şifrelemede XOR kullanmıştır. Çalışmanın sonucunda önerdiği şemanın yeterince güvenli olduğunu ve çeşitli saldırılara direnebileceğini belirtmiştir (Sun, 2017).

Chai ve arkadaşları, yapmış oldukları çalışmada DNS şifrelemesi, kaotik haritalama kullanarak bir görüntü şifreleme şeması önermişlerdir. Orijinal görüntüden SHA 256 hash değeri ile kaotik sistemin ilk değerleri hesaplanmış ve DNS şifrelemesi ile birlikte görüntüyü şifrelemeyi gerçekleştirmişlerdir. Çalışmaların sonucunda güvenlik analizlerinden başarıyla geçtiklerini belirtmişlerdir (Chai ve diğ., 2017).

Xu ve arkadaşları, çalışmalarında bir blok görüntü karıştırma şeması ve yeni bir dinamik index tabanlı difüzyon şeması içeren yeni bir kaotik görüntü şifreleme algoritması önermişlerdir. Görüntü şifreleme aşamasında, orijinal görütüyü dikey veya yatay yönlerde iki eşit bloğa bölmüşlerdir. Ardından görüntünün X ve Y koordinatlarını değiştirmek için kaos matrisinden yararlanmışlardır. Son olarak görüntü karıştırma şeması ile görüntü şifreleme işlemini tamamlamışlardır. Çalışmanın sonucunda performans analizlerinde başarılı olduğunu belirtmişlerdir (Xu ve diğ., 2017).

Hua ve arkadaşları, yapmış oldukları çalışmada Josephus problemi ve temel görüntü filtreleme tekniklerini kullanan bir görüntü şifreleme algoritması geliştirmişlerdir. Josephus problemi görüntüdeki pikselleri karıştırmak, görüntü filtrelemeyi ise şifrelemedeki difüzyonu sağlamak için kullanmışlardır. Çalışmanın sonucunda güvenlik analizlerinde son derece hassas bir gizli anahtara sahip olduğunu, çeşitli güvenlik saldırılarına direnebildiğini ve birkaç gelişmiş görüntü şifreleme algoritmasından daha iyi bir performansa sahip olduğunu belirtmişlerdir (Hua ve diğ., 2019).

Yan ve arkadaşları, görüntüyü şifrelemeye uygun hale getirmek için bir sentez yoluyla analiz sistemi önermişlerdir. Bu sistemde orijinal görüntüyü yarı tonlama işlemine tabi tutmuşlar ve olasılıksal bir model ile şifrelemeye hazır hale getirmişlerdir. Bu işlemin sonucunda görüntüyü geleneksel görüntü şifreleme algoritmaları ile kullanılabildiğini ve şifreleme güvenliğinin sağlam olduğunu vurgulamışlardır (Yan ve diğ., 2019).

Yousif ve arkadaşları, yapmış oldukları çalışmada görüntü tara tekniğini, El-Gamal açık anahtarlı şifreleme sistemini ve kaotik sistemleri entegre ederek görüntüleri güvenli hale getirmek için yeni bir yaklaşım sunmuşlardır. Permütasyonlu bir görüntü oluşturmak için ilk önce zikzak ve spiral tarama kullanmışlar sonrasında, El-Gamal şifreleme algoritması, permüte edilen görüntüyü şifrelemek için kullandığını belirtmişlerdir. Şifrelemenin son adımı olarak, Lorenz ve Rössler kaotik dizileri, karışıklık ve yayılma aşamalarındaki piksel konumlarını karıştırmak için kullanmışlardır. Çalışmanın sonucunda kriptanaliz testlerinin birçoğunda başarılı olduklarını belirtmişlerdir (Yousif ve diğ., 2020).

Ibrahim ve Alharbi, çalışmalarında görüntü şifreleme için S-Box ve eliptik eğri görüntü şifreleme tekniklerini beraber kullanan hibrit bir şema önermişlerdir. S-Box un görüntü şifreleme kalitesinin artmasında oldukça önemli olduğunu belirtmişlerdir. Çalışmanın sonucunda önerdikleri hibrit sistemin kriptanaliz sonuçlarının başarılı olduğunu söylemişlerdir (Ibrahim ve Alharbi, 2020).

Prabhat Kumar Ray ve arkadaşları yapmış oldukları çalışmada şifreli metinlerin akış şifreleme mi yoksa blok şifrelememi olduğunun tespiti için saklı markov modelden yararlanmışlardır. Bu sınıflandırma işlemi sırasında her iki şifreleme için beş tane şifreli metin kullanmışlardır. Çalışmalarının sonucunda bu algoritmaları sınıflandırmak için çeşitli özellikler ve tek değişkenli gözlem dizilerini kullandıklarını ve saklı markov modelin etkili olduğunu söylemişlerdir (Ray ve diğ., 2012).

Mark Stamp ve arkadaşları yapmış oldukları çalışmada Vigenere şifreli text metinlerin kriptanalizi için saklı markov modellerinden yararlanmışlardır. Saklı markov modelini eğiterek modelin tekniğin başarısına hangi özelliklerin katkıda bulunduğunu göstermişlerdir. Yaptıkları çalışmanın sonucunda saklı markov modelin vigenere şifreli metin mesajlarının kriptanalizi için güçlü ve etkili bir araç olduğunu belirtmişlerdir (Stamp ve diğ., 2018).

Bu tez kapsamında literatürdeki çalışmalardan farklı olarak iki farklı görüntü şifreleme yöntemi önerilmiştir. İlk yöntemde, Profile Hidden Markov Model (PHMM) kullanılarak şifrelenecek görüntüye ait bir RGB olasılık vektörü elde edilmektedir. Rastgele değerlerden oluşturulmuş başlatma vektörü (IV), PHMM üzerinden elde edilen olasılık vektörü (PV) ve şifrelenmiş piksel değerlerinin karıştırılması için S-

Box kullanılarak görüntü pikselleri üzerinde blok şifreleme işlemi gerçekleştirilmektedir. İkinci yöntemde ise, olasılıksal bir renk modeli kullanılarak şifrelenecek görüntüye ait bir RGB olasılık vektörü elde edilmektedir. Bu vektör ilk yöntemde olduğu gibi PV olarak kullanılmaktadır. Ayrıca ilk yöntemde kullanılan başlatma vektörü de şifreleme için kullanılmaktadır. Son olarak birbirinden tamamen farklı iki S-Box kullanılarak hem şifreleme işlemine girmeden önce hem de şifreleme işleminden sonra piksel değerinin karıştırılması sağlanmaktadır. Böylece geliştirilen her iki yeni görüntü algoritmalarındaki simetrik şifreleme ile görüntünün şifrelenmesi sağlanmaktadır. Şifreleme önerilen her iki yöntemde de renkli görüntüler için 24 bitlik, gri tonlamalı görüntüler için ise 8 bitlik bloklar halinde yapılmaktadır.

Gerçekleştirilen ulusal ve uluslararası literatür araştırmalarındaki görüntü şifreleme yöntemleri incelendiğinde görüntünün şifrelenmesi için PHMM yöntemini ve renklerin birbirleri arasındaki geçişlerinin olasılık modellemesini kullanan bir çalışma görülmemiştir. Bu nedenle, bu tez çalışmasının oldukça özgün bir değere sahip olduğu ve önerilen her iki yönteminde görüntü şifreleme için literatüre önemli katkılar sağlayacağı düşünülmektedir. Ayrıca tez çalışmasının katkıları sonuç bölümünde detaylı olarak incelenecektir.

Tez çalışmasının ilk bölümünde kriptoloji kavramından, tarihsel gelişiminden ve hangi alanlarda kullanıldığından bahsedilmiştir. Ayrıca görüntü şifreleme ve görüntü şifreleme algoritmaları anlatılmıştır. Son olarak görüntü şifrelemede önemli bir yere sahip olan S-Box algoritmasından bahsedilerek ilk bölüm sonlandırılmıştır. İkinci bölümde ise Markov ve Saklı markov modellerinden bahsedilmektedir. Son olarak ilk önerdiğimiz PHMMRGB yönteminde şifreleme anahtarlarından biri olan PV'nin üretilmesi için kullanılan PHMM yöntemine değinilecektir. Üçüncü bölümde ise önerilen görüntü şifreleme yöntemleri anlatılmaktadır. Bu bölümde görüntü şifreleme için gerekli tüm anahtarların üretimi, şifrelemede ve şifre çözme işlemlerinde nasıl kullanılacağı detaylı bir şekilde anlatılmaktadır. Dördüncü bölümde önerilen görüntü şifreleme yöntemleri için deneysel çalışma yapılarak performans analiz testlerine yer verilmiştir. Ayrıca bu bölümde literatürdeki diğer çalışmalarla önerdiğimiz yöntemlerin karşılaştırması yapılıp sonuçlar detaylı bir şekilde incelenmektedir. Sonuçlar ve öneriler bölümünde, yapılan çalışmalardan elde edilen sonuçların bilime

ve günümüz teknolojisine sağlayabileceği katkılar tartışılacaktır. Ayrıca ileriye dönük gerçekleştirilebilecek çalışmalar için önerilerde bulunulacaktır.

1. KRİPTOLOJİ VE GÖRÜNTÜ ŞİFRELEME

1.1. Kriptoloji Kavramı

Kriptoloji kavramını kısaca şifre bilimi şeklinde tanımlayabiliriz. Ayrıca kriptoloji, eldeki verinin belli bir sisteme göre şifrelenmesi, iletilmesi ve iletilmiş verinin deşifre edilmesi olarak tanımlanabilir. Kriptoloji, kriptografi ve kriptanaliz olmak üzere iki kısımdan oluşmaktadır. Kriptografi; verinin şifrelenmesi, kriptanaliz ise verilerin şifrelerini çözme ya da şifrelenmiş veriyi analiz etme anlamına gelmektedir. Kriptografi matematiksel yöntemleri kullanarak veriyi anlamsız hale dönüştürme yöntemlerinin tamamı olarak düşünülebilir (Massey, 1988; Bauer, 2013, Klima ve diğ, 2018).

Tarih boyunca kriptografi alanında birçok yöntemi geliştirilmiştir. Bunlardan ilkine örnek olarak Sezar şifreleme gösterilebilir. Sezar, şifreleme yöntemi olarak alfabeden yararlanmıştır. İletmek istediği mesajda A harfi yerine D harfi, B harfi yerine ise E harfi kullanmıştır. Bu da bize şifreleme işleminde her harfe karşılık alfabedeki üç harf sonrası kullanarak şifreli mesajı oluşturduğunu göstermektedir. Şifreli mesajı alan kişi üç anahtar sayısını bildiği düşünülürse mesajdaki tüm harfleri alfabetik olarak üç harf öncesine alıp mesajın şifresini çözebilmektedir. Buda kriptanaliz işlemine örnek olarak gösterilebilir. Diğer şifreleme yöntemlerinden bazılarını inceleyecek olursak 2. Dünya savaşında Japonların geliştirdiği Purple makinesi, W. F. Friedman tarafından kriptanalizi yapılmıştır. Ayrıca Almanların geliştirdiği Enigma makinesi, Alan Turing ve ekibi tarafından çözülmüştür. Diffie ve Hellman, açık anahtar sistemli şifreleme algoritmasını bulmuşlardır. R. L. Rivest, A. Shamir ve L. M. Adleman RSA algoritmasını geliştirmişlerdir. N. Koblitz ve C. S. Miller yapmış oldukları farklı çalışmalarda eliptik eğri kriptografik sistemini geliştirmişlerdir. (Diffie ve Hellman, 1976; Koblitz, 1987; Miller, 1997; Bauer, 2013; Klima ve diğ, 2018).

Şifreleme yöntemlerinin geliştirilmesinin en temel sebebi güvenliktir. Kişilerin ya da ülkelerin kendilerini korumak için geliştirdiği bu yöntemler en çok haberleşme ve veri erişimi için kullanılmaktadır (Bauer, 2013). Askeri alanlarda telsiz haberleşmesi için,

kişilerin birbiri arasındaki metin mesajları için, doktorların kendi aralarında hastalara tanı koyabilmek adına birbirleri arasında gönderdikleri hasta fotoğrafları için, ya da televizyondaki ücretli bir kanaldaki stream görüntüsü ve daha birçok ihtiyaç için şifreleme kullanılmaktadır.

Bu tez kapsamında görüntü şifrelemeden bahsedeceğiz. Bundan sonraki bölümde görüntü şifreleme detaylı olarak açıklanmaktadır.

1.2. Görüntü Şifreleme

Görüntü şifreleme (Visual Cryptography, VC), matematiksel modeller kullanılarak bir görüntünün anlamsız bir görsel görüntüye dönüştürülmesini temsil eden kriptografik bir tekniktir (Ebrahim ve diğ., 2014).

VC yöntemleri iki bölümden oluşur; simetrik ve asimetrik. Simetrik şifreleme, tek anahtarlı bir şifreleme türüdür. Verileri şifrelemek için kullanılan anahtar aynı zamanda şifresini çözmek içinde kullanılır. Asimetrik şifreleme, simetrik şifrelemeden farklı olarak açık anahtar ve gizli anahtar içermektedir. Bu iki anahtar arasında matematiksel bir bağlantı vardır. Asimetrik şifrelemede, eliptik eğri ve fraktal tabanlı şifreleme yöntemleri yaygın olarak kullanılmaktadır. Ancak bu şifreleme yöntemleri, şifreleme ve şifre çözme süreleri açısından simetrik şifreleme yöntemlerinden daha yavaş çalışır. Simetrik şifreleme de blok şifreleri ve akış şifreleri olarak ikiye ayrılır. Bir akış şifresi, düz metin bitlerinin bir özel veya (XOR) işlemi kullanılarak sözde rastgele bir şifre anahtar akışı ile birleştirildiği simetrik bir anahtar şifresidir. Akışı olmayan görüntülerin şifrelenmesinde genellikle blok şifreleme algoritmaları tercih edilir (Kumar ve diğ., 2011; Thakur ve Kumar, 2011; Wu ve Sun, 2013; Ebrahim ve diğ., 2014; Chuman ve diğ., 2019).

Blok şifreleme yöntemleri görüntünün pikselleri üzerinde matematiksel modellerden yararlanarak hızlı ve güvenli bir şekilde şifreleme ve şifre çözme işlemlerini yapabilmektedir. Blok şifreleme için birçok yöntem geliştirilmiş olup, DES (Data Encryption Standard), AES (Advanced Encryption Standard), Blowfish, TEA (Tiny Encryption Algorithm), CB (Chaos-based), S-Box, CBC (Cipher Block Chaining) bunlara örnek olarak gösterilebilir (Thakur ve Kumar, 2011; Kumar ve diğ.,2011;

Bağbaba ve diğ., 2015; Güvenoğlu, 2016; Bejinariu ve diğ., 2016; Reyad ve diğ., 2017; Preishuber ve diğ., 2018;).

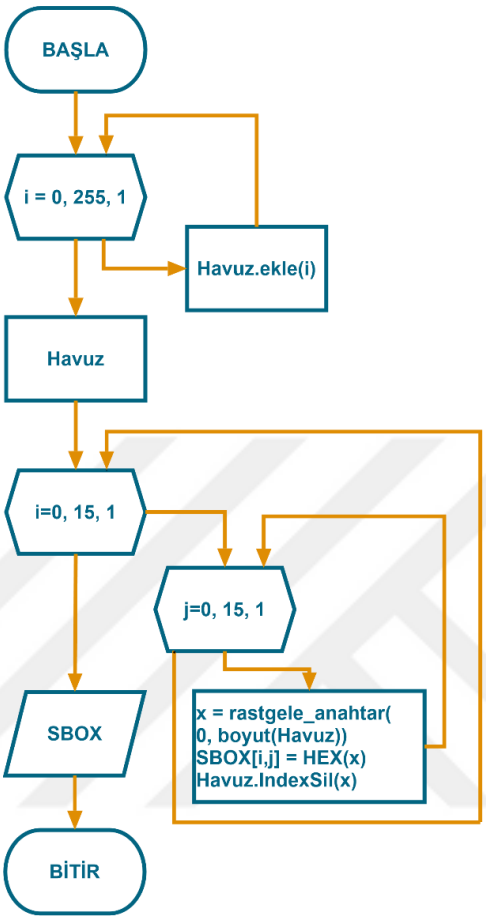
1.3. S-Box Algoritması

Yer değiştirme kutuları (Subtitution Box, S-Box), blok görüntü şifreleme algoritmalarında şifreleme güvenliğini arttıran en önemli anahtarlardan biridir. Yer değiştirme kutularını günümüzde DES (Data Encryption Standart), AES (Advanced Encrpytion Standart) vb. birçok şifreleme algoritmasında kullanılmaktadır. Yer değiştirme kutularının dinamik olarak oluşturulup şifreleme işleminde kullanılması sonucu şifreli metin ya da görüntünün anlaşılmazlığını önemli ölçüde arttırmaktadır. Bu yüzden yer değiştirme kutuları, görüntü şifreleme ve şifre çözme işlemlerinde büyük bir öneme sahiptir. S-Box'lar kullanılan şifreleme yöntemine göre boyutları değişkenlik gösterebilir. Örneğin, DES algoritmasında 4x16 boyutlarında S-Box kullanılırken, AES algoritmasında 16x16 lık bir S-Box kullanılmaktadır. Buda bize görüntü şifreleme mimarisine göre S-Box'ları kendimizin belirleyebileceğini göstermektedir (Thakur ve Kumar, 2011).

Tez kapsamında kullanılacak S-Box'ların üretilmesini sağlayan akış diyagramı Şekil 1.1'de gösterilmektedir. Buna göre, S-Box'lar 16x16 boyutunda ve 256 adet tamsayı değerinden oluşmaktadır. Görüntü piksellerindeki renk kanallarının her biri 8 bitten oluşmaktadır. Renk kanalları en fazla $2^8 - 1 = 255$ değerini alabilmektedir. Bu sebepten dolayı tam sayı değerleri [0-255] aralığındadır. Tüm bu tam sayı değerleri bir sayı havuzuna atılmaktadır. Bu havuzdan rastgele bir index değeri seçilerek tam sayı değerine ulaştırılır. Elde edilen tam sayı değeri 16'lık sayı sistemine(hexadecimal) çevrilerek kullanılmaktadır. Bunun sebebi hexadecimal karşılığının ilk değeri satır, ikinci değeri ise sütun olarak kabul edildiğinden dolayıdır. Tam sayı S-Box tablosu içerisine eklendikten sonra sayı havuzundan kaldırılmaktadır. Havuzda bulunan her bir tam sayı değeri S-Box tablosuna yerleştirildikten sonra elde edilen örnek Şekil 1.2'de gösterilmektedir (Güvenoğlu, 2016).

Ters S-Box üretimi S-Box a bağlı olarak üretilmektedir. Şekil 1.3'te Ters S-Box'ın üretilmesini sağlayan akış diyagramı gösterilmektedir. Buna göre, S-Box tablosunun ilk satır ve sütunundan başlamak üzere tüm değerler alınır. Tablonun her bir elemanı satır ve sütun olacak şekilde ayrılarak Ters S-Box'ın satır ve sütununa eklenmek için

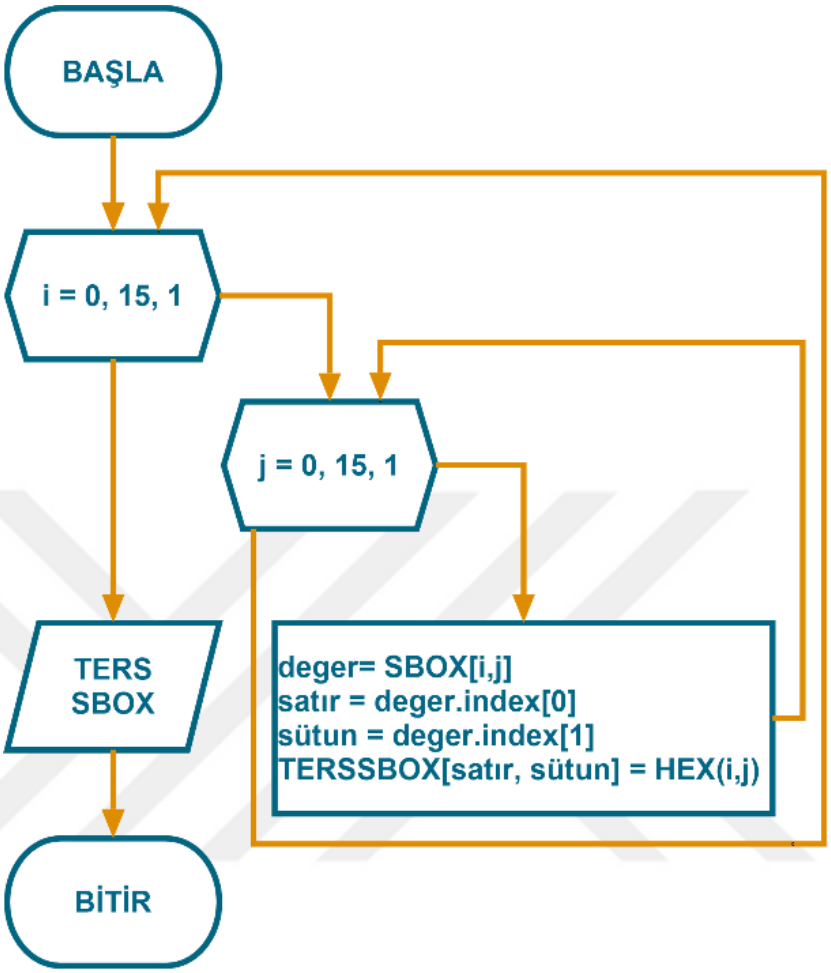
kullanılır. Tüm bu işlemlerin sonunda Şekil 1.2'teki S-Box'a göre elde edilen örnek Ters S-Box Şekil 1.4'te gösterilmektedir (Güvenoğlu, 2016).



Şekil 1.1. S-Box'ın üretilmesi

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	5	28	76	83	10	2F	A6	BE	62	E7	15	3C	6D	19	4D	79
1	6B	97	AB	AF	BB	4B	78	84	1C	70	77	E1	D8	B9	E0	74
2	41	46	38	33	B2	1	5C	4F	AD	88	68	FB	EA	B6	B1	4
3	49	53	48	C4	13	EE	44	C1	B5	F6	67	A2	BF	CB	E8	A9
4	8	9E	F9	24	DE	18	CA	64	36	5A	2	37	E4	80	98	6C
5	C7	72	95	89	6F	21	5E	55	0	86	8B	C2	9F	C0	94	E9
6	9C	C6	F4	42	BC	8A	25	2D	8D	E5	82	C3	ED	E	DA	31
7	58	FE	DF	43	2B	5D	39	EB	3B	A3	1F	5F	99	D	D1	7F
8	CE	1D	9D	23	8E	50	B4	35	4A	65	FC	91	A4	AA	6A	F5
9	A8	47	57	A1	DB	3F	BA	2E	7D	A	9	14	66	D2	A0	7C
A	16	6	F3	D4	73	BD	B3	F	4E	AE	3	D6	63	C5	45	9A
B	32	2A	CD	51	C9	29	B0	85	71	61	B7	81	40	A5	E3	8C
C	DC	7E	75	9B	D0	AC	7B	FA	A7	3A	3E	22	34	F2	E6	DD
D	D5	5B	F0	20	C	4C	D7	F7	54	69	56	11	B	26	D9	C8
E	EC	87	7	F8	2C	B8	F1	90	96	CF	92	52	EF	59	1B	6E
F	7A	E2	CC	D3	8F	3D	27	30	93	1E	17	1A	60	FD	FF	12

Şekil 1.2. S-Box örneği



Şekil 1.3. Ters S-Box'ın üretilmesi

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	58	25	4A	AA	2F	0	A1	E2	40	9A	99	DC	D4	7D	6D	A7
1	4	DB	FF	34	9B	A	A0	FA	45	D	FB	EE	18	81	F9	7A
2	D3	55	CB	83	43	66	DD	F6	1	B5	B1	74	E4	67	97	5
3	F7	6F	B0	23	CC	87	48	4B	22	76	C9	78	B	F5	CA	95
4	BC	20	63	73	36	AE	21	91	32	30	88	15	D5	E	A8	27
5	85	B3	EB	31	D8	57	DA	92	70	ED	49	D1	26	75	56	7B
6	FC	B9	8	AC	47	89	9C	3A	2A	D9	8E	10	4F	C	EF	54
7	19	B8	51	A4	1F	C2	2	1A	16	F	F0	C6	9F	98	C1	7F
8	4D	BB	6A	3	17	B7	59	E1	29	53	65	5A	BF	68	84	F4
9	E7	8B	EA	F8	5E	52	E8	11	4E	7C	AF	C3	60	82	41	5C
A	9E	93	3B	79	8C	BD	6	C8	90	3F	8D	12	C5	28	A9	13
B	B6	2E	24	A6	86	38	2D	BA	E5	1D	96	14	64	A5	7	3C
C	5D	37	5B	6B	33	AD	61	50	DF	B4	46	3D	F2	B2	80	E9
D	C4	7E	9D	F3	A3	D0	AB	D6	1C	DE	6E	94	C0	CF	44	72
E	1E	1B	F1	BE	4C	69	CE	9	3E	5F	2C	77	E0	6C	35	EC
F	D2	E6	CD	A2	62	8F	39	D7	E3	42	C7	2B	8A	FD	71	FE

Şekil 1.4. Ters S-Box örneği

Şifreleme işleminde, orijinal görüntünün her pikselinde bulunan kırmızı, yeşil ve mavi değerleri ayrı ayrı S-Box tablosundan geçirilmektedir. Her bir renk değerinin hexadecimal karşılığı alınarak işlemler yapılmaktadır. Bu işlemleri Şekil 1.2'deki S-Box ve Şekil 1.4'teki Ters S-Box a göre bir örnek üzerinden anlatalım. Şifrelenmesini istediğimiz bir pikselin renk değerleri R(kırmızı)=211, G(yeşil)=167, B(mavi)=136 ve sırasıyla hexadecimal karşılıkları R=D3, G=A7 ve B=88 olsun. S-Box tablosunda R değeri için D. satır ve 3. sütundaki değer yeni R=HexToDecimal(20)=32 değeridir. G değeri için A. satır ve 7. sütun değer yeni G=HexToDecimal(F)=15 değeridir. B değeri için 8. satır ve 8. sütundaki değer yeni B=HexToDecimal(4A)=74 değeridir. Buna göre şifrelenmiş piksel değeri sırasıyla R=32, G=15, B=74 olarak elde edilmektedir.

Şifre çözme işleminde ise şifreleme işleminde olduğu gibi tüm pikseller Ters S-Box tablosundan geçirilmektedir. Aynı örnekle devam edecek olursak şifrelenmiş R=32, G=15 ve B=74 piksel değerleri için Ters S-Box tablosuna göre işlemleri tekrarlanmaktadır. R değeri için R=DecimalToHex(32)=20, 2. satır ve 0. sütun değeri D3 ve decimal karşılığı 211'dir. G değeri için G=DecimalToHex(15)=0F, 0. satır ve F. sütun değeri A7 ve decimal karşılığı 167'dir. B değeri için B=DecimalToHex(74)=4A, 4. satır ve A. sütun değeri 88 ve decimal karşılığı 136'dır. Bu işlem sonucunda Ters S-Box tan elde edilen renk değerleri orijinal görüntüdeki renk değerleri ile aynı olduğu görülmektedir.

S-Box ve Ters S-Box örneğinde anlaşılacağı gibi [0-255] arasındaki tüm renk değerlerinin S-Box tablosunda karşılığı olması gerektiğinden dolayı 16x16 boyutlarında olması gerekmektedir. Renk değerlerini karşılamak adına 4 adet 8x8 boyutlarında ya da 16 adet 4x4 boyutunda S-Box'lar kullanılabilir ancak bu durumda her bir S-Box için Ters S-Box üretileceğinden dolayı şifreleme maliyeti de artmış olacaktı. Bu sebeple birer adet S-Box ve Ters S-Box kullanarak en uygun şifreleme maliyeti seçilmektedir.

2. MARKOV MODELLERİ

Markov modelleri (MM), graf teorisinin bir uygulaması olarak düşünülebilir. Markov model, durumları (nodes) ve bu durumlar arasında istatistiksel geçişleri modeller. Markov modellerine göre bir durum belirli bir istatiksel değere göre değişir veya değişmeden aynı kalır. Ayrıca geçmiş durumların mevcut durumlar üzerinde bir etkisi söz konusu değildir. Ancak şimdiki durum gelecek durumları etkileyebilir (Gagniuc, 2017; URL-1, 2021). Olasılıkların gösterildiği formül Denklem (2.1) deki gibi tanımlanır.

$$P[X_{t+1} = x_{t+1} \mid X_t = x_t, X_{t-1} = x_{t-1}, ..., X_1 = x_1, X_0 = x_0] = P[X_{t+1} = x_{t+1} \mid X_t = x_t] \quad (2.1)$$

X mevcut durumu, x ise bir sonraki durumu, t mevcut zamanı, $t-1$ ve $t+1$ ise sırasıyla bir önceki ve bir sonraki zamanı ifade etmektedir. Denklem (2.1) deki formülde $t+1$ zamanındaki olayların t zamanına bağlı olması söz konusudur. Hava durumu örneği (Gagniuc, 2017) üzerinden markov modelinden bahsedecek olursak; karlı, yağmurlu ve güneşli olma durumları vardır. Tablo 2.1'de durumlar arası geçiş yani bugün ve bir sonraki günün durumlarını belirtmek için olasılıksal değerler gösterilmektedir.

Tablo 2.1. Hava durumu geçiş olasılıkları

Durumlar	Karlı	Yağmurlu	Güneşli
Karlı	0,3	0,3	0,4
Yağmurlu	0,1	0,45	0,45
Güneşli	0,2	0,3	0,5

Örnek olarak bugünün yağmurlu olduğunu biliyorsak yarının güneşli olma olasılığı 0,45, karlı olma olasılığı ise 0,1'dir. Aşağıdaki maddelerde Markov modeli olasılıksal formülüne göre; karlı havadan güneşli havaya geçme olasılığı, güneşli havadan yağmurlu havaya geçme olasılığı ve yağmurlu havadan yağmurlu havaya geçme olasılıkları verilmiştir.

- P(Sonraki | Mevcut) = Olasılık Değeri

- $P(\text{Güneşli} \mid \text{Karlı}) = 0,4$
- $P(\text{Yağmurlu} \mid \text{Güneşli}) = 0,3$
- $P(\text{Yağmurlu} \mid \text{Yağmurlu}) = 0,45$

Başlangıç durumu olarak bugünkü havanın karlı, yağmurlu ve güneşli olma olasılıkları sırasıyla 0, 0,2 ve 0,8 olduğunu varsayarsak Denklem (2.2) te yarınki hava durumunun yağmurlu olma olasılığı, Denklem (2.3) te ise 100 gün içinde yağmur yağma olasılığı hesaplanabilir.

$$P = \begin{pmatrix} 0,3 & 0,3 & 0,4 \\ 0,1 & 0,45 & 0,45 \\ 0,2 & 0,3 & 0,5 \end{pmatrix}^{2} .(0,0,2,0,8)^{t} \tag{2.2}$$

$$P = \begin{pmatrix} 0,3 & 0,3 & 0,4 \\ 0,1 & 0,45 & 0,45 \\ 0,2 & 0,3 & 0,5 \end{pmatrix}^{100} .(0,0,2,0,8)^{t} \tag{2.3}$$

Bir başka örnekte (Gagniuc, 2017) iki durumlu bir Markov modeli inceleyelim. Bu modelde beyaz ve mavi olma durumları vardır. Tablo 2.2'de durumlar arası geçiş için olasılıksal değerler gösterilmektedir. Aşağıdaki maddelerde ise Markov modeli olasılıksal formülüne göre beyazdan maviye, beyazdan beyaza, maviden beyaza ve maviden maviye geçme olasılıkları verilmiştir.

Tablo 2.2. Beyaz ve mavi durumları arasındaki geçiş olasılıkları

Durumlar	Beyaz	Mavi
Beyaz	0,7	0,3
Mavi	0,6	0,4

- $P(\text{Mavi} \mid \text{Beyaz}) = 0,3$
- $P(\text{Beyaz} \mid \text{Beyaz}) = 0,3$
- $P(\text{Beyaz} \mid \text{Mavi}) = 0,6$
- $P(\text{Mavi} \mid \text{Mavi}) = 0,4$

Üç saatlik bir alışveriş sürecinin olduğunu düşünelim (Gagniuc, 2017). Her saat bir gömlek alınacak ve başlangıçta beyaz bir gömlek alacağınıza karar verdiniz. Bu nedenle mevcut durum beyaz 1 ve mavi 0'dır. Geçiş matrisinin değişmediği varsayılırsa, Denklem (2.4), Denklem (2.5) ve Denklem (2.6) için sırasıyla birinci, ikinci ve üçüncü saatlerin sonunda beyaz veya mavi gömlek alma olasılıkları hesaplanabilir. Denklem (2.4) da geçiş matrisi ile başlangıç matrislerinin çarpımı sonucunda birinci saate beyaz ya da mavi gömlek alma olasılığı, Denklem (2.5) de birinci saatin sonundaki olasılık matrisi ile başlangıç durumu matrislerinin çarpımı sonucunda ikinci saatte beyaz ya da mavi gömlek alma olasılığı, Denklem (2.6) de ise ikinci saatin sonundaki olasılık matrisi ile başlangıç durumu matrisleri çarpımı ile üçüncü saatin sonundaki beyaz ya da mavi gömlek alma olasılığı hesaplanmıştır. H_1, birinci saatin, H_2, ikinci saatin, H_3 ise üçüncü saatin sonundaki beyaz ve mavi gömlek alma olasılığı ifade etmektedir.

$$\mathrm{H}_1 = (1,0).\begin{pmatrix} 0,7 & 0,3 \\ 0,6 & 0,4 \end{pmatrix} \tag{2.4}$$

$$\mathrm{H}_2 = \mathrm{H}_1.\begin{pmatrix} 0,7 & 0,3 \\ 0,6 & 0,4 \end{pmatrix} \tag{2.5}$$

$$\mathrm{H}_3 = \mathrm{H}_2.\begin{pmatrix} 0,7 & 0,3 \\ 0,6 & 0,4 \end{pmatrix} \tag{2.6}$$

2.1. Saklı Markov Modeli

Saklı Markov Model (SMM), standart Markov modeldeki gibi durum dizisi gözlenmez. Bunun yerine durum dizisinin gözlem dizisinden elde edilmesi gerekir. Durumların gözlemlerden elde ediliyor olması, modeli saklı yapan durumdur. Bir gözlem dizisi üretmiş olan pek çok farklı durum dizisi olabilir. Ancak bu durumda dizilerinin her birinin olasılığı farklıdır (Rabiner ve Juang 1986; Fine, 1998).

SMM' de kullanılan temel örneklerden bir tanesi Alice ve Bob örneğidir (URL-2, 2021). Alice ve Bob farklı bölgelerde yaşayan iki arkadaştır. Her gün birbirlerini arayarak o gün yaptıkları aktiviteler hakkında bilgi almaktadırlar. Bob'un gün içerisinde yaptığı üç aktivite bulunmaktadır. Bunlar; parkta yürüyüş, ev temizliği ve

alışveriştir. Bunlardan hangisini yapacağı o gün havanın durumuna göre değişmektedir. Alice, Bob'un ona telefonda günlük olarak yaptığını anlattığı aktivitelere göre havanın durumunu tahmin etmeye çalışmaktadır. Havanın durumu yağmurlu ya da güneşli olarak iki farklı değer alabilmektedir. Sonuç olarak Alice, Bob'un aktivitelerini gözlemleyerek saklı olan havanın durumunu MM' de de yapıldığı gibi tahmin etmeye çalışmaktadır.

SMM i üç durumlu bir markov model örneği üzerinden anlatalım (URL-2, 2021). Evdeyiz ve havayı göremiyoruz. Hava durumları karlı, yağmurlu ve güneşli olsun. Bununla birlikte, odamızdaki sıcaklığı hissedebilir, sıcak ve soğuk olmak üzere iki olası gözlem yapabiliyoruz. Aşağıdaki maddelerde MM olasılıksal formülüne göre hava durumlarının sıcak ve soğuk olma durumlarına göre geçiş olasılıkları gösterilmiştir.

- P(Sıcak | Karlı) = 0
- P(Sıcak | Yağmurlu) = 0,2
- P(Sıcak | Güneşli) = 0,7
- P(Soğuk | Karlı) = 1
- P(Soğuk | Yağmurlu) = 0,8
- P(Soğuk | Güneşli) = 0,3

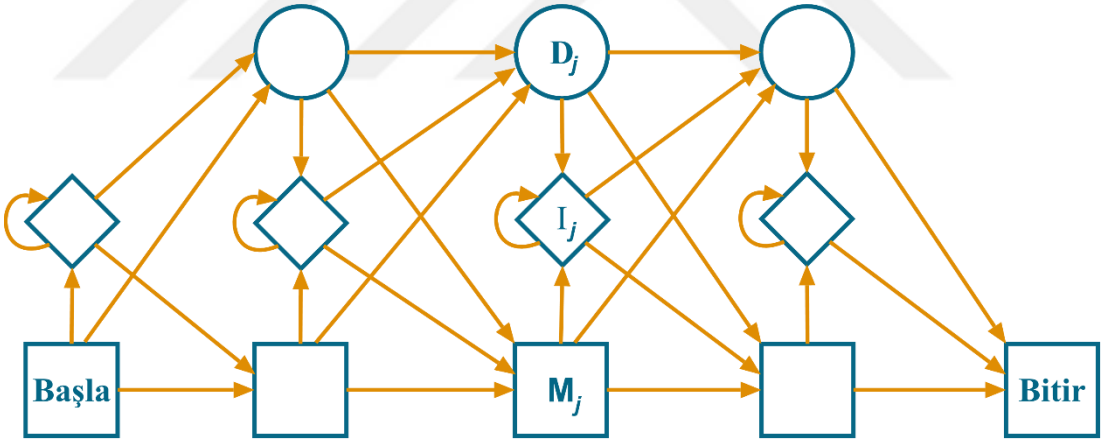
Temel bir örnek üzerinden gidecek olursak art arda iki gün odadaki havanın soğuk hissetme olasılığımızı hesaplamak için SMM uygulayalım. Bu iki günde, hava durumları için 3*3 ten 9 seçenek bulunmaktadır. Bu 9 seçenekten birinin olasılık hesaplaması Denklem (2.10)'da gösterilmiştir. Tüm seçeneklerin toplanması istenen olasılığı verecektir (URL-2, 2021).

$$P\big((Soğuk, Soğuk), (Yağmurlu, Karlı)\big) =$$
$$P\big((Soğuk, Soğuk) \mid (Yağmurlu, Karlı)\big).P(Yağmurlu, Karlı) =$$
$$P(Soğuk \mid Yağmurlu).P(Soğuk \mid Karlı).P(Karlı \mid Yağmurlu).P(Yağmurlu) =$$
$$0{,}8 * 1 * 0{,}1 * 0{,}2 = 0.016 \qquad (2.10)$$

2.2. Profile Hidden Markov Model

Profile Hidden Markov Model yöntemi Krogh ve arkadaşları (Krog ve diğ., 1993) tarafından çoklu dizi (en az üç tane, protein dizisi gibi biyolojik dizilerin) hizalaması için önerilmiştir. Proteinler pek çok aminoasidin bir araya gelmesi ile oluşan aminoasit dizileridir. PHMM'de hizalamada kullanılan dizilerin ortak bir aileye sahip olduğu düşünülür ve aralarındaki bağlantı bir model ile ortaya çıkarılmaya çalışılır (Mount, 2001; Kaya Gülağız, 2018).

PHMM'de temel olarak bir başlangıç ve bitiş durumu vardır. Bu durumlara ek olarak her bir adımda kullanılabilecek üç farklı durum (ekleme, silme ve eşleme) mevcuttur. Oluşturulan modellerde bu üç durum aynı anda bulunmak zorunda değildir. Farklı problemler için farklı durum dizilerini içeren modeller oluşturulabilir. Şekil 2.1' de PHMM'ye ait tüm durumları içeren bir model örnek olarak gösterilmiştir. Şekil 2.1'de yer alan I sembolü ekleme durumlarını, D sembolü silme durumlarını, M sembolü ile ifade edilen durumlar ise eşleme durumlarını ifade etmektedir.



Şekil 2.1. Tüm durumları içeren bir PHMM örneği (Kaya Gülağız, 2018)

PHMM matematiksel olarak 5 parametre $(Q, V, P(i), A, B)$ kullanılarak ifade edilir. Burada yer alan $Q = \{q_1, q_2, \dots, q_n\}$ durumlar kümesini, V; çıktı alfabesini, $P(i)$; t zamanında q_i durumunda bulunma olasılığını, A; geçiş olasılıkları kümesini, a_{ij}^t; t anında q_i durumundayken $t+1$ anında q_j durumunda bulunma olasılığını, B; çıktı olasılıkları kümesini ve $e_i^t(x)$; t anında q_i durumundayken x çıktısının oluşma olasılığını ifade etmektedir (Kaya Gülağız, 2018). Herhangi bir eğitim veri seti üzerinden hesaplanacak geçiş ve çıktı olasılıklarının formülü sırasıyla Denklem (2.7)

ve Denklem (2.8) de gösterilmektedir (Durbin ve diğ., 1998). Denklem (2.7)'de yer alan a_{ij} ; q_i durumundan q_j durumuna geçiş olasılığını ve A_iJ ifadesi ise q_i durumundan q_j durumuna yapılan geçişlerin sayısını ifade etmektedir. J özel bir durumu ifade etmektedir, J' ise olası tüm durumları temsil etmektedir.

$$a_{ij} = \frac{A_i J}{\sum_{j'} A_i J'} \tag{2.7}$$

$$e_i(x) = \frac{E_i(x)}{\sum_{x'} E_i(x')} \tag{2.8}$$

Denklem (2.8)'de yer alan $e_i(x)$ ifadesi q_i durumundayken x çıktısının oluşma olasılığını ve $E_i(x)$ ifadesi q_i durumundayken x çıktısının oluşma sayısını göstermektedir. Verilen veri seti üzerinden yukarıdaki Denklem (2.7) ve Denklem (2.8) kullanılarak model kurulur ve başlangıç değerleri belirlenerek iki boyutlu bir geçiş tablosu ile modelde yer alacak olasılıklar tablo üzerinden dinamik olarak hesaplanır.

PHMM bir görüntü üzerinde gerçekleyelim. Görüntü üzerindeki her bir piksel kırmızı (Red, R), yeşil (Green, G) ve mavi (Blue, B) renk değerlerinden oluşmaktadır. Görüntünün boyutlarını yükseklik m piksel ve genişlik n piksel olduğunu varsayalım. Durumlar kümesi $Q = \{M_1, M_2, \dots, M_n\}$ olarak belirlenmiştir. Görüntüye ait renk satırları PHMM modelini oluşturacak aminoasit dizilimlerine karşılık gelmektedir. Bu dizilimleri belirlemek için bir kural oluşturulmuştur. Kurala göre görüntü içerisindeki her satırda yer alan pikseller için maksimum renk değerine sahip R, G, B değerlerinden biri seçilmiştir ve bu şekilde elde edilen satırların her biri bir aminoasit dizilimi olarak düşünülmüştür. Bu kural çerçevesinde PHMM modeline geçmeden önce veri setimizi kullanılabilir hale getirmemiz gerekmektedir. Bunun için görüntü içerisindeki her bir pikselde maksimum renk değerine sahip rengin belirlenmesi ve maksimum renk matrisinin elde edilmesi gerekmektedir. Maksimum renk matrisinin el edilme aşamaları matematiksel olarak Denklem (2.9), Denklem (2.10) ve Denklem (2.11)'de ifade edilmiştir. Denklem (2.9)'da yer alan PM piksel matrisini, α_{ij} değeri bir pikseli, mr_{ij} ise bir piksele ait maksimum renk değerini ve MC ise m satır sayılı, n sütun sayılı maksimum renk matrisini ifade etmektedir.

$$m,n \in N$$
$$i = 1,2,3,\ldots m \; and \; j = 1,2,3,\ldots n$$
$$\alpha_{ij} \in RGB \, rengi$$

$$PM = \begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & \cdots & \alpha_{1,n} \\ \alpha_{2,1} & \alpha_{2,2} & & \alpha_{2,n} \\ \vdots & & \ddots & \vdots \\ \alpha_{m,1} & \alpha_{m,2} & \cdots & \alpha_{m,n} \end{bmatrix} \tag{2.9}$$

$$\begin{cases} R & eğer \;\; R > G \,\&\, B, \\ G & eğer \;\; G > R \,\&\, B, \\ B & diğer. \end{cases} , mr_{ij} \in \alpha_{ij} \tag{2.10}$$

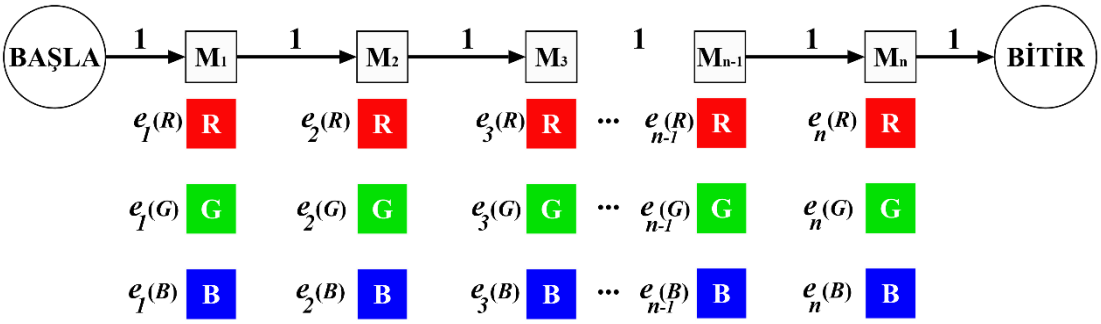
$$MC = \begin{bmatrix} mr_{1,1} & mr_{1,2} & \cdots & mr_{1,n} \\ mr_{2,1} & mr_{2,2} & & mr_{2,n} \\ \vdots & & \ddots & \vdots \\ mr_{m,1} & mr_{m,2} & \cdots & mr_{m,n} \end{bmatrix} \tag{2.11}$$

$$MC_{örnek} = \begin{bmatrix} R & G & \cdots & G \\ G & B & & B \\ \vdots & & \ddots & \vdots \\ G & R & \cdots & B \end{bmatrix}_{mxn}$$

PHMM yönteminde modeli elde etmek için amino asit sıralıları kullanılır. Örnek bir amino asit sıralısı "ACA-G-ATG" şeklinde ifade edilebilir. Çalışmamızda MC matrisinin her bir satırı (Örnek olarak: "RGBGGRRBR") PHMM yönteminde kullanılan amino asit sıralıları gibi düşünülmüştür. Her bir resmi temsil edecek en iyi çıktı vektörü yani Red, Green, Blue sıralıları PHMM ve Viterbi algoritması kullanılarak elde edilebilir. Buna göre;

Şekil 2.2'de de gösterildiği gibi model sütun sayısı kadar eşleme durumu içerecektir. MC matrisinin tüm hücrelerinde kırmızı, yeşil veya mavi değerlerinden biri bulunmaktadır. Yani kayıp değer içeren hiçbir sütun yoktur. Dolayısıyla modelde silme durumunun kullanımına gerek olmayacaktır. Silme durumunun kullanılmaması ekleme durumunun da kullanılmayacağı anlamına gelmektedir. Bu nedenle model

sütun sayısı kadar eşleme durumu içerecektir ve bir eşleme durumundayken bir sonraki eşleme durumunu mutlaka geçiş olacaktır. Bu nedenle eşleme durumları arası geçiş olasılığı da 1 olacaktır.



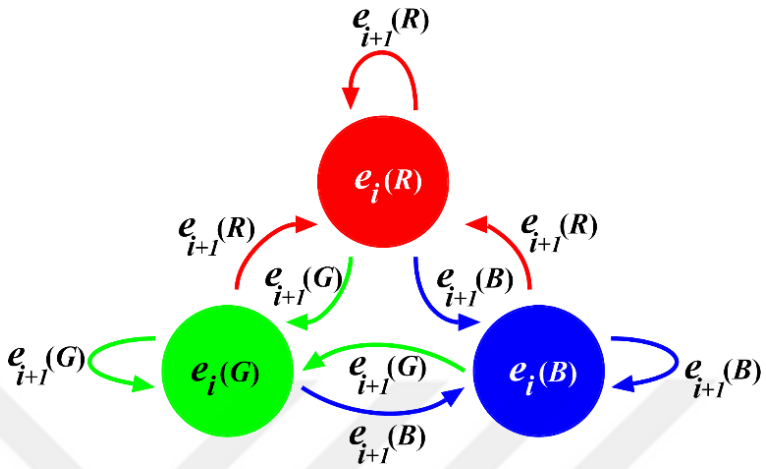
Şekil 2.2. PHMM' deki geçiş ve çıktı olasılıkları

Modeldeki durumlar belirlendikten sonra, her bir duruma ait çıktıların olasılıklarının hesaplanması gerekmektedir. Çıktı olasılıkları Denklem (2.8)'den yararlanılarak hesaplanmaktadır. Her durumda oluşabilecek üç çıktı (Kırmızı(R), Yeşil(G) ve Mavi(B)) bulunmaktadır. Çıktı olasılıkları hesaplanırken her bir duruma ait ilgili sütun göz önünde bulundurulur ve her duruma ait çıktı olasılıklarının toplamı 1 olmalıdır. Şekil 2.2'de örnek bir MC matrisi üzerinden elde edilen çıktı olasılıkları gösterilmiştir.

Model üzerinden elde edilebilecek en muhtemel durum dizisi hem de bu durum dizisinde oluşabilecek en muhtemel çıktı dizisi Viterbi algoritması kullanılarak elde edilebilir. Bu bir anlamda Viterbi algoritmasının en kısa yolu bulma mantığı ile kullanılmasıdır. Yöntemin bu şekilde kullanılabileceği daha önce yapılan çalışmalarda (Quach ve Farooq, 1994) gösterilmiştir. Denklem (2.12)'de Viterbi algoritmasının hem durum dizisi hem de bu durumlarda oluşabilecek en muhtemel çıktı dizisini bulacak şekilde düzenlenmiş hali verilmiştir. Denklem (2.12)'de yer alan $\delta_t(j)$ değeri; t anında $j$durumu ile biten en yüksek olasılıklı yolu, ifade etmektedir. $\max_j(e_j)$ değeri, j durumunda elde edilebilecek en yüksek olasılıklı çıktıyı ifade etmektedir. $\max_i\{\delta_{t-1}(i)a_{ij}\}$ ifadesi $t-1$ anındaki i durumu ile biten en yüksek olasılıklı yolu ifade etmektedir (Kaya Gülağız, 2018).

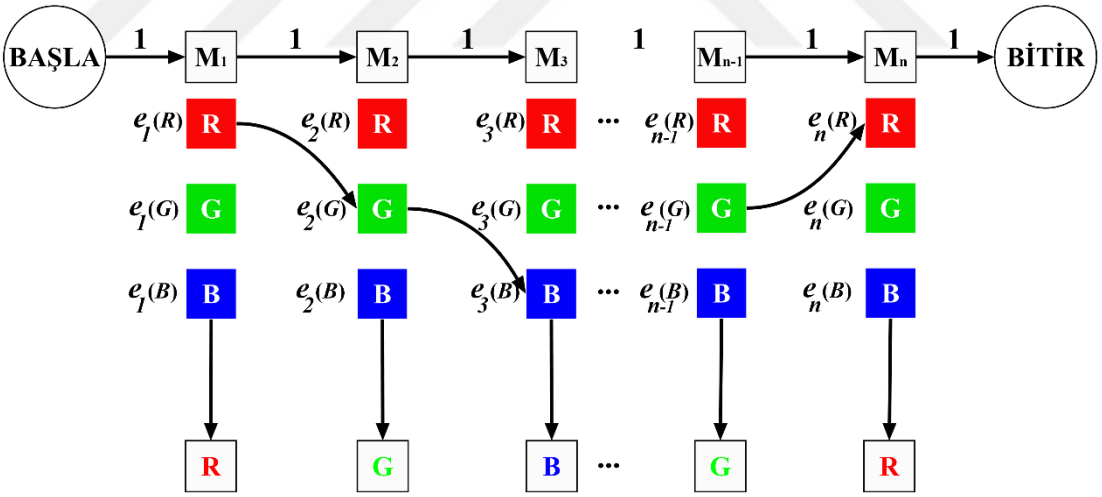
$$\delta_t(j) = \max_j\left(e_j\right)\max_i\left\{\delta_{t-1}(i)a_{ij}\right\} \tag{2.12}$$

Şekil 2.3'te i anında oluşabilecek en yüksek olasılıklı çıktı ve $i+1$ anında oluşabilecek en yüksek olasılıklı çıktıya ait olasılıkların birbiri arasındaki geçişi grafiksel olarak gösterilmektedir.



Şekil 2.3. PHMM' deki çıktıların geçiş durumları

Şekil 2.4' de Viterbi algoritması uygulandıktan sonra resme ait en yüksek olasılıklı çıktıları veren renk modeli elde edilmiştir.



Şekil 2.4. Viterbi algoritması kullanılarak en uygun yolun bulunması

Viterbi algoritması kullanılarak elde edilen çıktı dizisi PHMM temelli görüntü şifreleme algoritması için olasılık vektörü olarak kullanılmaktadır.

3. ÖNERİLEN GÖRÜNTÜ ŞİFRELEME YÖNTEMLERİ

Bölüm 2'de ele Tez kapsamında CBC şifreleme yöntemini temel alan, şifreleme ve şifre çözme işlemlerini gerçekleştiren iki yeni yöntem önerilmektedir. Bunlar PHMMRGB ve ProbRGB görüntü şifreleme yöntemleridir. Bir sonraki bölümde her iki yöntemde detaylı olarak incelenmiştir.

3.1. PHMMRGB Görüntü Şifreleme Yöntemi

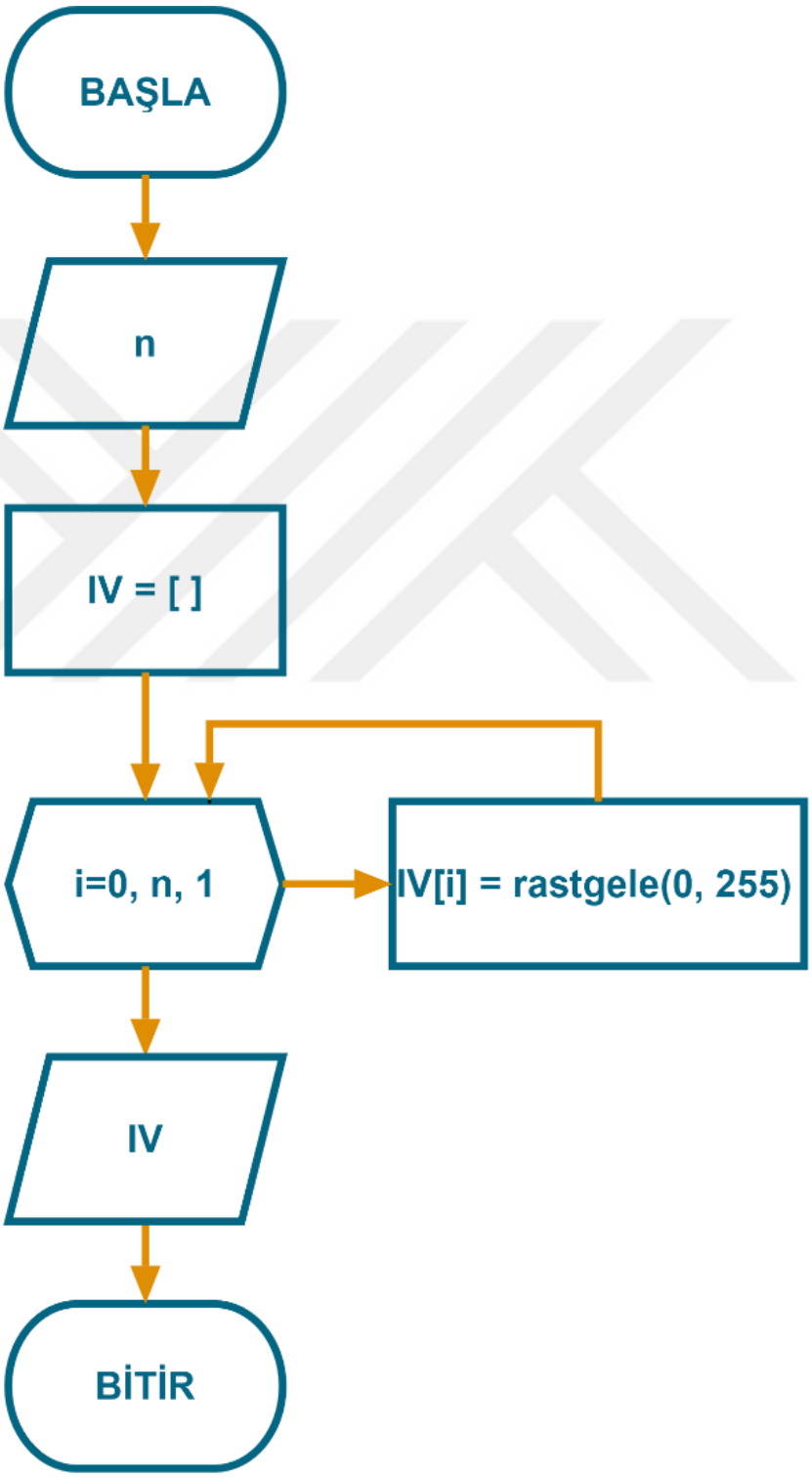
Profile Hidden Markov Model temelli görüntü şifreleme yöntemi üç anahtardan oluşmaktadır. Bunlar olasılık vektörü (Probability Vector, PV), başlatma vektörü (Initialization Vector, IV) ve yer değiştirme kutularıdır (S-Box ve Ters S-Box).

PV üç aşamada elde edilmektedir. Birincisi orijinal görüntü kullanılarak maksimum renk matrisinin elde edilmesi, ikincisi bu matris üzerinden PHMM modeli oluşturulması ve üçüncüsü Viterbi algoritmasıyla en iyi olasılıklı çıktı dizisinin elde edilmesi.

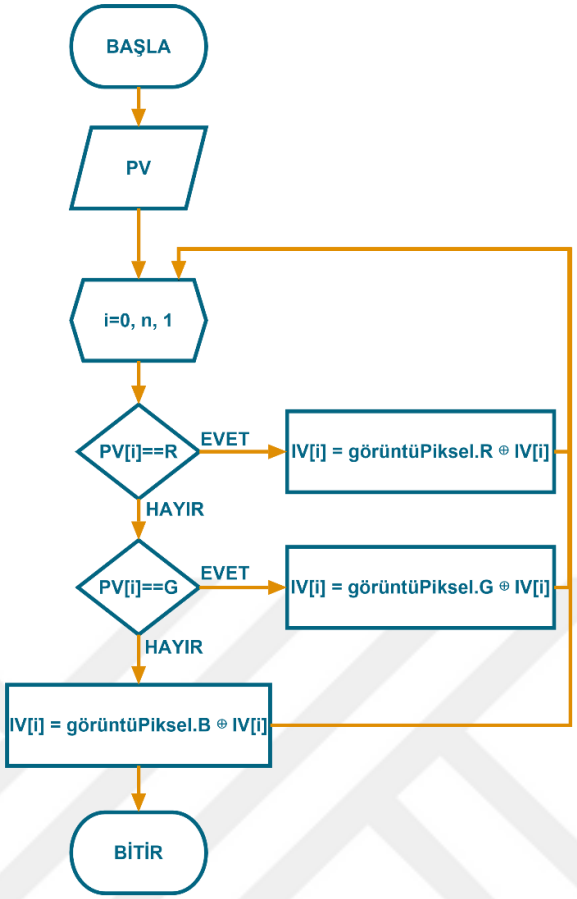
IV, şifreleme işlemlerinde rastgeleliği sağlamak ve şifre güvenliğini arttırmak için kullanılan bileşenlerden biri olarak tanımlayabiliriz. IV kullanan algoritmalara örnek olarak CBC gösterilebilir (Kumar ve diğ., 2011). IV şifrelemede kullanılacak yönteme göre boyutu ve değer aralıkları belirlenebilir (Abidi ve diğ., 2016). Tez kapsamında, renk uzayındaki 8 bitlik renkleri kullandığımızdan dolayı IV'nin her bir elemanının değer aralığı 0 ile 255 arasındadır. Boyutu ise şifrelenecek olan görüntünün genişliği kadar belirlenmektedir. Bunun sebebi kullandığımız blok şifrelemede her sütunun farklı bir başlatma değeri ile şifrelenmesini sağlamaktır. Şekil 3.1'deki akış diyagramı IV'nin şifreleme işleminden önce nasıl elde edildiğini göstermektedir.

Şifreleme güvenliğini arttırmak için her bir satır şifrelendikten sonra IV güncellenmektedir. Şekil 3.2'de güncelleme işleminin akış diyagramı gösterilmektedir. IV'nin güncelleme işlemleri PV ye göre yapılmaktadır. IV, PV'nin aynı indeksli elemanına göre güncelleme işlemini yapmaktadır. PV deki renge göre orijinal görüntüden renk değeri alınarak IV'nin mevcut değeri ile XOR işlemine tabi

tutulmaktadır. İşlem sonucunda IV yeni değerine sahip olmaktadır. Bir sonraki satırda yeni değeri ile şifreleme işlemine girmektedir. Bu sayede her bir görüntü satırı bir önceki satırdan bağımsız olarak şifrelenmiş olmaktadır. Buda bize şifreleme güvenliği açısından avantaj sağlamaktadır.



Şekil 3.1. IV oluşturma akış şeması

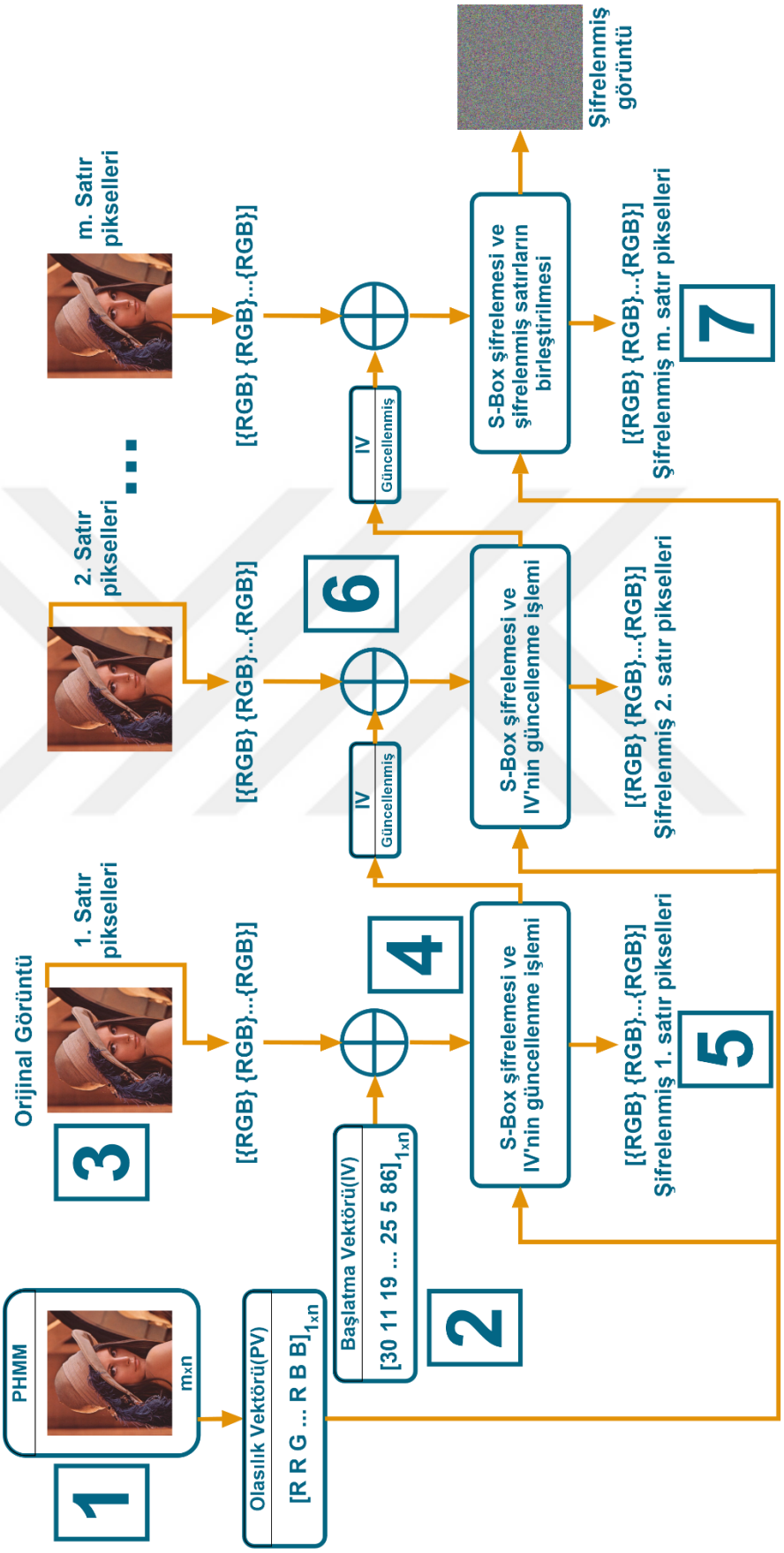


Şekil 3.2. IV'nin PV'ye göre güncellenmesi

PHMMRGB yöntemi için son anahtar S-Box ve Ters S-Box'lardır. Bu anahtarın elde edilmesi Bölüm 1.3'te anlatılmıştır.

Şekil 3.3'te PHMMRGB yöntemi şifreleme adımları modellenmiş ve aşağıda detaylı olarak listelenmiştir.

1. Orijinal görüntüden olasılık vektörünün (PV) elde edilmesi.
2. Başlatma vektörünün (IV) elde edilmesi.
3. Orijinal görüntünün ilk satırındaki piksel değerlerinin IV ile XOR işlemine tabi tutularak şifrelenmesi
4. S-Box tablosuna göre şifrelenen satırın karıştırılması
5. IV'nin PV'ye göre güncellenmesi
6. Orijinal görüntünün son satır piksellerinin şifrelenmesine kadar 3. adımdan tekrar edilmesi
7. Tüm satırların şifrelenmesinden sonra satırlar birleştirilerek şifreli görüntünün elde edilmesi



Şekil 3.3. PHMMRGB görüntü şifreleme sistem mimarisi

Önerilen blok temelli şifreleme yönteminin sonucunda PV, IV, S-BOX ve şifrelenmiş görüntü çıktı olarak elimizde bulunmaktadır. Orijinal görüntüyü kayıpsız elde etmek için bu dört bileşen kullanılmıştır. Bu bileşenlerden herhangi birinin eksik ya da yanlış olması durumunda şifre çözme işlemlerinde anlamsız veriler elde edilmektedir. Şekil 3.4'te PHMMRGB yönteminin şifre çözme adımları modellenmiştir ve aşağıda detaylı olarak listelenmiştir;

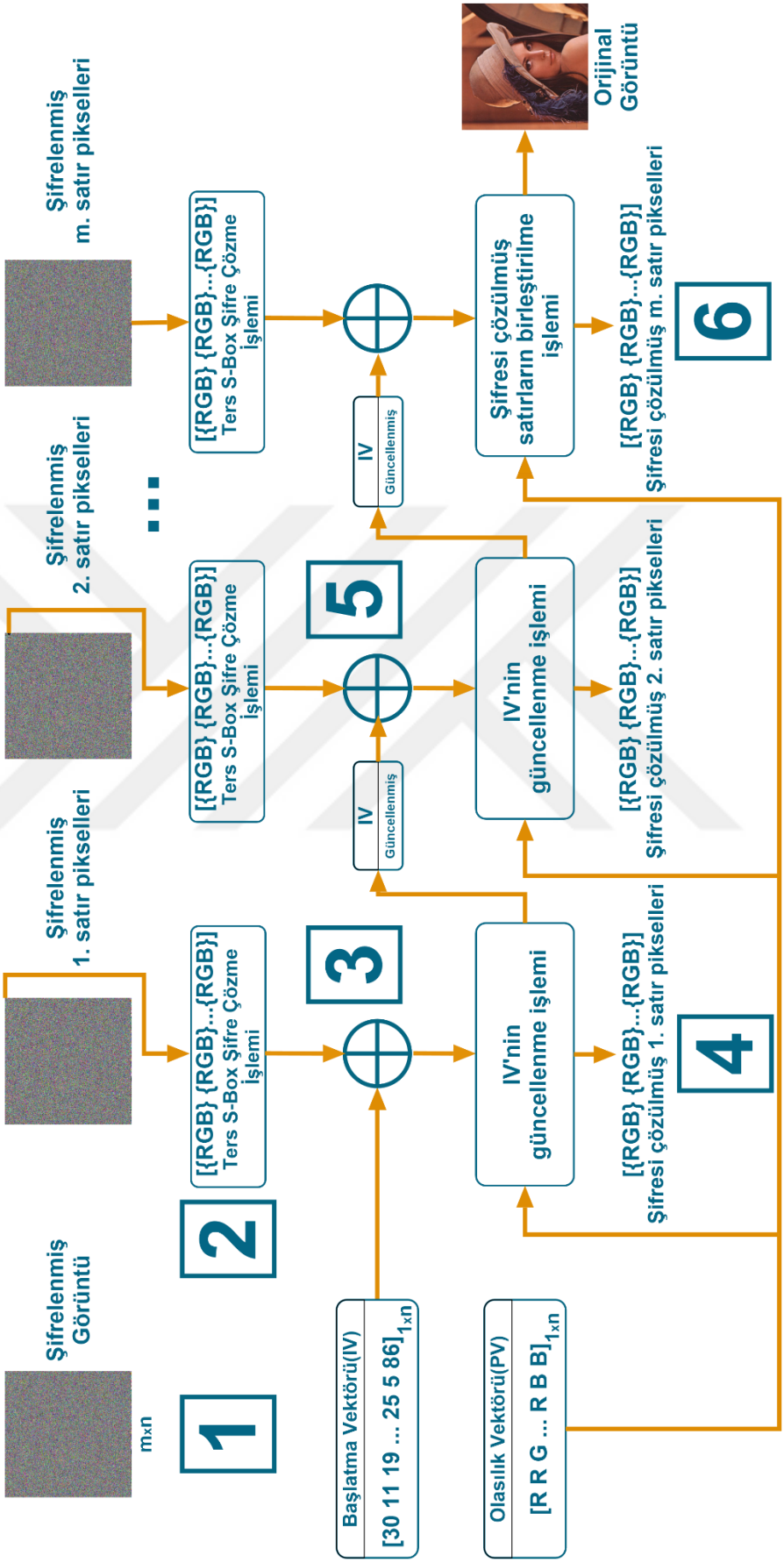
1. Önerdiğimiz PHMMRGB yönteminden elde edilen şifreli görüntü, IV, PV ve S-Box tan üretilen Ters S-Box tablosunun şifre çözme için hazır hale getirilmesi.
2. Şifreli görüntüdeki ilk satır piksellerinin Ters S-Box tablosuna göre geri dönüştürülmesi
3. Ters S-Box tan elde edilen satır piksellerinin IV ile XOR işlemine tutulup şifresinin çözülmesi
4. IV'nin PV'ye göre güncellenmesi
5. Şifreli görüntünün son satır piksellerinin şifresinin çözülmesine kadar 2. adımdan tekrar edilmesi
6. Tüm satırların şifre açma işleminden sonra satırlar birleştirilerek orijinal görüntünün elde edilmesi

3.2. ProbRGB Temelli Görüntü Şifreleme Yöntemi

ProbRGB temelli görüntü şifreleme yöntemi dört anahtardan oluşmaktadır. Bunlar PV, IV ve birbirinden tamamen farklı iki S-Box ve Ters S-Box.

PV iki aşamada elde edilmektedir. Birincisi Bölüm 3.1'de yer alan Denklem (2.9) ile Denklem (2.11) arasındaki eşitlikler kullanılarak orijinal görüntüden maksimum renk matrisinin elde edilmesi, ikincisi ise bu matris üzerinden renklerin geçiş olasılıklarına dayalı bir olasılıksal modelin oluşturularak en iyi olasılıklı çıktı dizisinin elde edilmesidir.

Olasılıksal geçiş modelini, t olarak ifade edilen bir anda, belirli bir olasılık dağılımına bağlı olarak X sembolü ile ifade edilen durumlar kümesindeki bir durumdan başka bir duruma geçiş yapılması olarak ifade edebiliriz.



Şekil 3.4. PHMMRGB görüntü şifre çözme sistem mimarisi

Kurulan bu modelde üç farklı durum olduğu kabul edilirse durum kümesi X_i: $\{X_R, X_G, X_B\}$ olarak temsil edilir. Burada X_R, kırmızı renk durumunu, X_G, yeşil renk durumunu ve X_B ise mavi renk durumunu ifade etmektedir. Bu olasılıksal modelde t değişkeni bir zamanı ya da dizideki indisi temsil edebilir ve $t = 1,2,3, \ldots \in N$ şeklinde değer alır. Burada herhangi bir t anında bulunulan durum r_t değişkeni kullanılarak temsil edilebilir. Buna göre herhangi bir t anında X_i durumunda bulunma olasılığı ise $P = (r_t = X_i)$ ile gösterilebilir. Bu tanımlamalara göre her t anında durumlar arasındaki geçiş olasılığı Denklem (3.1) ve Denklem (3.2)'de gösterildiği gibi ifade edilmektedir. Bu yöntemde kullanılan olasılıksal formüller klasik Markov Modeli (Apaydın, 2013; Kaya Gülağız, 2018) mantığı kullanılarak görüntü şifrelemeye uygun olacak şekilde yeniden düzenlenmiştir.

$$P(r_{t+1} = X_j | r_t = X_i, r_{t-1} = X_k, \ldots) \tag{3.1}$$

$$P\left(r_{t+1} = X_j \middle| r_t = X_i, r_{t-1} = X_k, \ldots\right) = P\left(r_{t+1} = X_j \middle| r_t = X_i\right) \tag{3.2}$$

Bu olasılıksal modelde bir sonraki durum sadece bir önceki duruma bağlıdır. Yani bir maksimum renk matrisini düşünecek olursak ikinci sütundaki kırmızı renkten üçüncü sütundaki mavi renge ya da ikinci sütundaki kırmızı renkten üçüncü sütundaki yeşil renge geçiş olasılığı olarak düşünülebilir. Hiçbir zaman birinci sütundaki kırmızı renkten üçüncü sütundaki mavi renge geçiş olasılık hesaplaması yapılmayacaktır. Bu durum Denklem (3.3)'te gösterildiği gibi ifade edilmektedir. Formülde verilen olasılık değeri bir durumdan başka bir duruma geçmek için hesaplanan olasılık değerini vermektedir.

$$p_{ij} = P(r_{t+1} = X_j | r_t = X_i) \tag{3.3}$$

Geçiş olasılığı bir olasılık değerini ifade ettiğinden dolayı negatif olamaz. Aynı zamanda bir durumdan yapılabilecek tüm geçişlerin olasılıklarının toplamı 1'dir. Buna göre bir renkten diğer bir renge geçiş olasılıklarının toplamı Denklem (3.4)'te gösterildiği gibi 1 olacaktır.

$$p_{ij} \geq 0 \text{ ve } \sum_{j=1}^{N} p_{ij} = 1 \tag{3.4}$$

Tasarlanan olasılıksal modelde en önemli parametrelerden biri ise her renge ait başlangıç olasılığıdır. 3 adet durum olduğuna göre 3 adet başlangıç olasılığı olacaktır. Başlangıç olasılıkları Denklem (3.5)'te gösterildiği gibi ω sembolü ile ifade edilmektedir. Bu olasılıkların toplamı da Denklem (3.6)'da gösterildiği gibi 1 olması gerekir.

$$\begin{aligned} \omega_1 &\equiv P(r_1 = X_R) \\ \omega_2 &\equiv P(r_2 = X_G) \\ \omega_3 &\equiv P(r_3 = X_B) \end{aligned} \tag{3.5}$$

$$\omega_1 + \omega_2 + \omega_3 = 1 \tag{3.6}$$

Maksimum renk matrisi elde edildiğinde yukarıda bahsedilen geçiş olasılıkları, başlangıç değeri elde edilebilir. Maksimum renk matrisinin m satır sayılı ve n sütun sayılı olması durumunda ilk sütundaki başlangıç olasılıkları Denklem (3.6) ve Denklem (3.7)' deki gibi hesaplanabilir. mc_{ij}, Denklem (2.11)'deki maksimum renk matrisindeki bir elemanı, R_T, G_T, B_T, sırasıyla ilk sütunlardaki toplam kırmızı, yeşil ve mavi renklerin toplamını ifade etmektedir. En yüksek olasılıklı rengin elde edilmesi ise Denklem (3.8)'de gösterilmektedir. Bu olasılık bize başlangıç değerini vermektedir.

$$\begin{cases} R = mc_{ij} & şartıyla \quad R_T = \sum_{i=1}^{m} mc_{i1} \\ G = mc_{ij} & şartıyla \quad G_T = \sum_{i=1}^{m} mc_{i1} \\ B = mc_{ij} & şartıyla \quad B_T = \sum_{i=1}^{m} mc_{i1} \end{cases} \tag{3.6}$$

$$\begin{aligned} \omega_1 &= \frac{\{\text{İlk Sütundaki Kırmızı Renk Sayısı}\}}{\{\text{Satır Sayısı}\}} = \frac{R_T}{m} \\ \omega_2 &= \frac{\{\text{İlk Sütundaki Yeşil Renk Sayısı}\}}{\{\text{Satır Sayısı}\}} = \frac{G_T}{m} \\ \omega_3 &= \frac{\{\text{İlk Sütundaki Mavi Renk Sayısı}\}}{\{\text{Satır Sayısı}\}} = \frac{B_T}{m} \end{aligned} \tag{3.7}$$

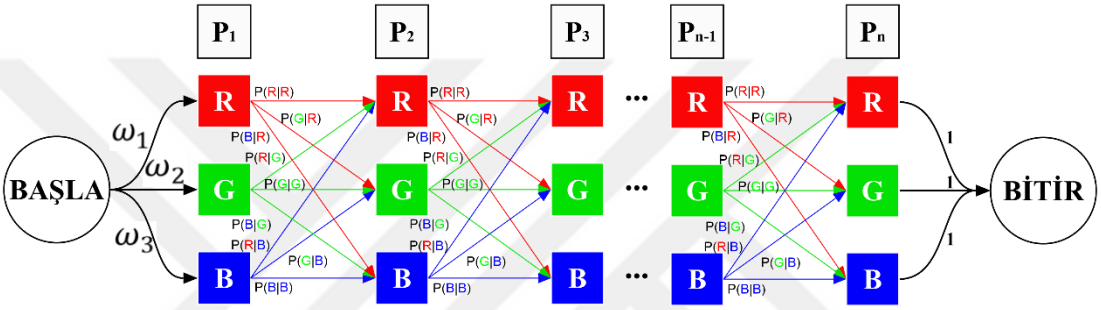
$$\omega = \underset{1 \le i \le 3}{\operatorname{argmax}}\, \omega_i \tag{3.8}$$

Başlangıç değerini yani en yüksek olasılıklı rengi belirledikten sonra bu renkten diğer renklere geçiş olasılıklarının hesaplamasına başlayabiliriz. p_{ij} olarak temsil edilen renk geçiş olasılığı; X_i durumundan X_j durumuna olan geçişlerin sayısının, X_i durumundan yapılan tüm geçişlerin sayısına bölünmesi ile elde edilir. Geçiş

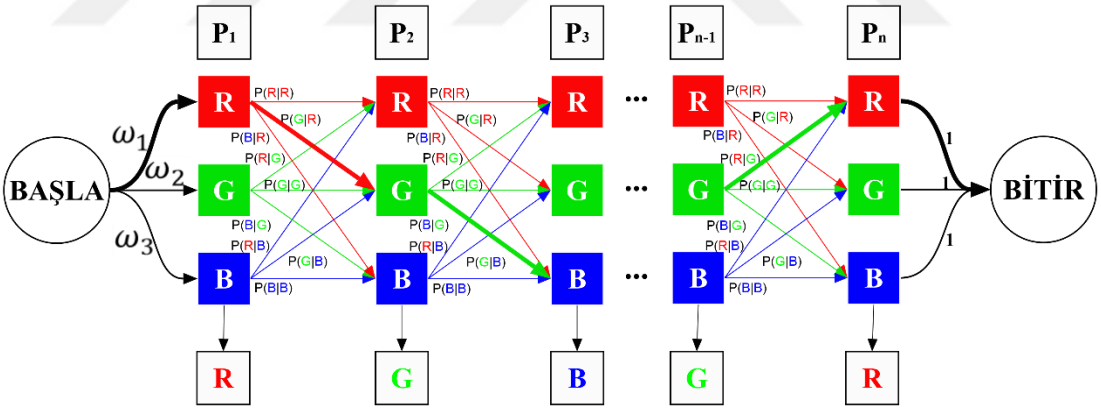
olasılıklarının matematiksek formülü Denklem (3.9)'da gösterilmektedir (Kaya Gülağız, 2018).

$$\widehat{p_{ij}} = \frac{\{X_i'\text{den } X_j'\text{ye Geçişlerin sayısı}\}}{\{X_i'\text{den Yapılan Tüm Geçişlerin Sayısı}\}} = \frac{\sum_{k=1}^{K}\sum_{t=1}^{T-1}(r_t^k = X_i \text{ ve } r_{t+1}^k = X_j)}{\sum_{k=1}^{K}\sum_{t=1}^{T-1}(r_t^k = X_i)} \quad (3.9)$$

Şekil 3.5 ve Şekil 3.6'da tasarlanan olasılıksal modele göre maksimum renk matrisinden PV'nin nasıl elde edildiğini göstermektedir. Şekillerdeki P(G|R) ve buna benzer ifadeler Markov Model de olduğu gibi R durumundan G durumuna yani kırmızıdan yeşil renge geçiş olasılığını ifade etmektedir.



Şekil 3.5. Olasılıksal modelde başlangıç değeri ve geçiş olasılıklarını belirlenmesi



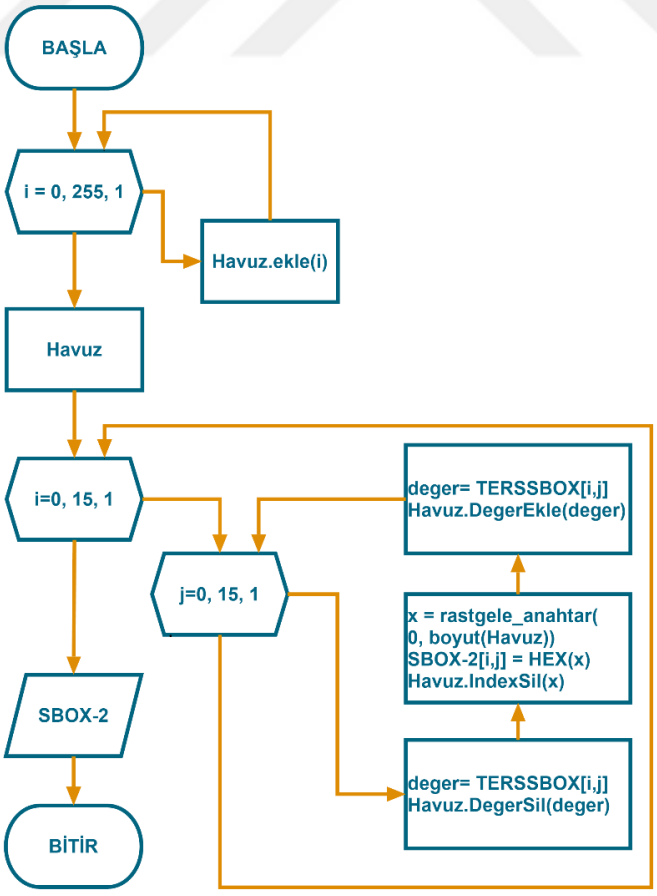
Şekil 3.6. En yüksek olasılık dizisinin elde edilmesi

Başlatma vektörü, şifre karmaşıklığını arttırmak için kullanılmaktadır ve PHMMRGB yönteminde anlatıldığı gibi üretilip güncellenmektedir.

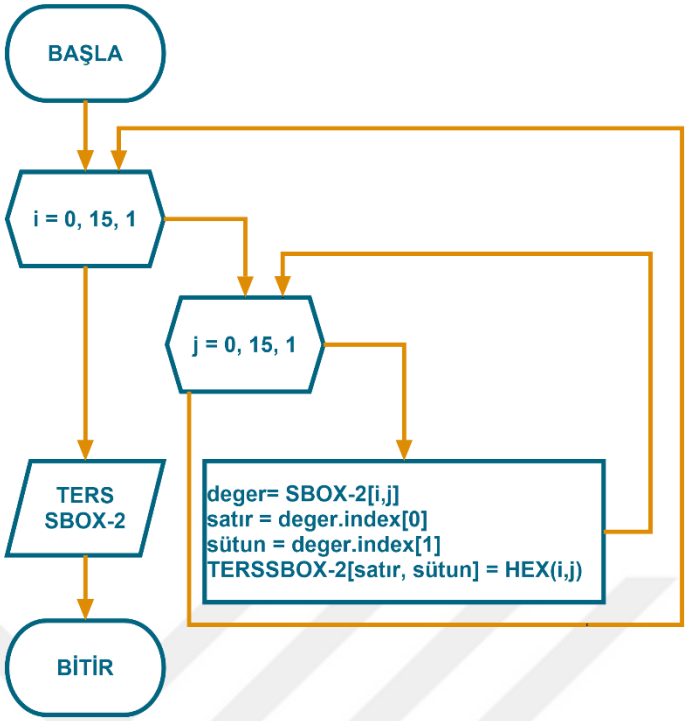
PHMMRGB yöndemindeki gibi tek bir S-Box ile şifreleme gerçekleştirdiğimizde PHMMRGB yönteminin kriptanaliz sonuçlarına çok benzediği görülmektedir. ProbRGB yöntemine şifreleme için yeni bir katman eklemek ve kriptanaliz testlerindeki başarımı arttırmak amacıyla iki adet S-Box kullanılmaktadır. Bu anahtarlar S-Box, S-Box-2, Ters S-Box ve Ters S-Box-2'dir. S-Box ve Ters S-Box

anahtarın elde edilmesi Bölüm 1.3'te anlatılmıştır. S-Box-2'nin elde edilmesi Şekil 3.7'de gösterilmektedir. S-Box ve S-Box-2 hiçbir elemanı aynı değildir. S-Box-2 oluşturulurken Ters S-Box tan yararlanılmıştır. Akış diyagramında S-Box' ı üretmek için kullanılan sayı havuzundan yararlanılmaktadır. Bu havuzdan öncelikle Ters S-Box'taki satır ve sütun değeri ile aynı değeri almaması için havuzdan çıkarılmaktadır. Sonrasında havuzda kalan diğer sayı değerleri arasından rastgele bir değer seçilip S-Box-2 tablosuna eklenmektedir. Tam sayı S-Box-2 tablosu içerisine eklendikten sonra sayı havuzundan kaldırılmaktadır. Bu işlemden önce silinen Ters S-Box'taki değer havuza yeniden eklenmektedir. Bunun nedeni S-Box ile aynı değerleri almaması içindir.

Ters S-Box-2 üretimi S-Box-2'ye bağlı olarak üretilmektedir. Şekil 3.8'de Ters S-Box-2'nin üretilmesini sağlayan akış diyagramı gösterilmektedir. Buna göre, S-Box-2 tablosunun ilk satır ve sütunundan başlamak üzere tüm değerler alınır. Tablonun her bir elemanı satır ve sütun olacak şekilde ayrılarak Ters S-Box-2'nin satır ve sütununa eklenmek için kullanılır.



Şekil 3.7. S-Box-2'nin üretilmesi

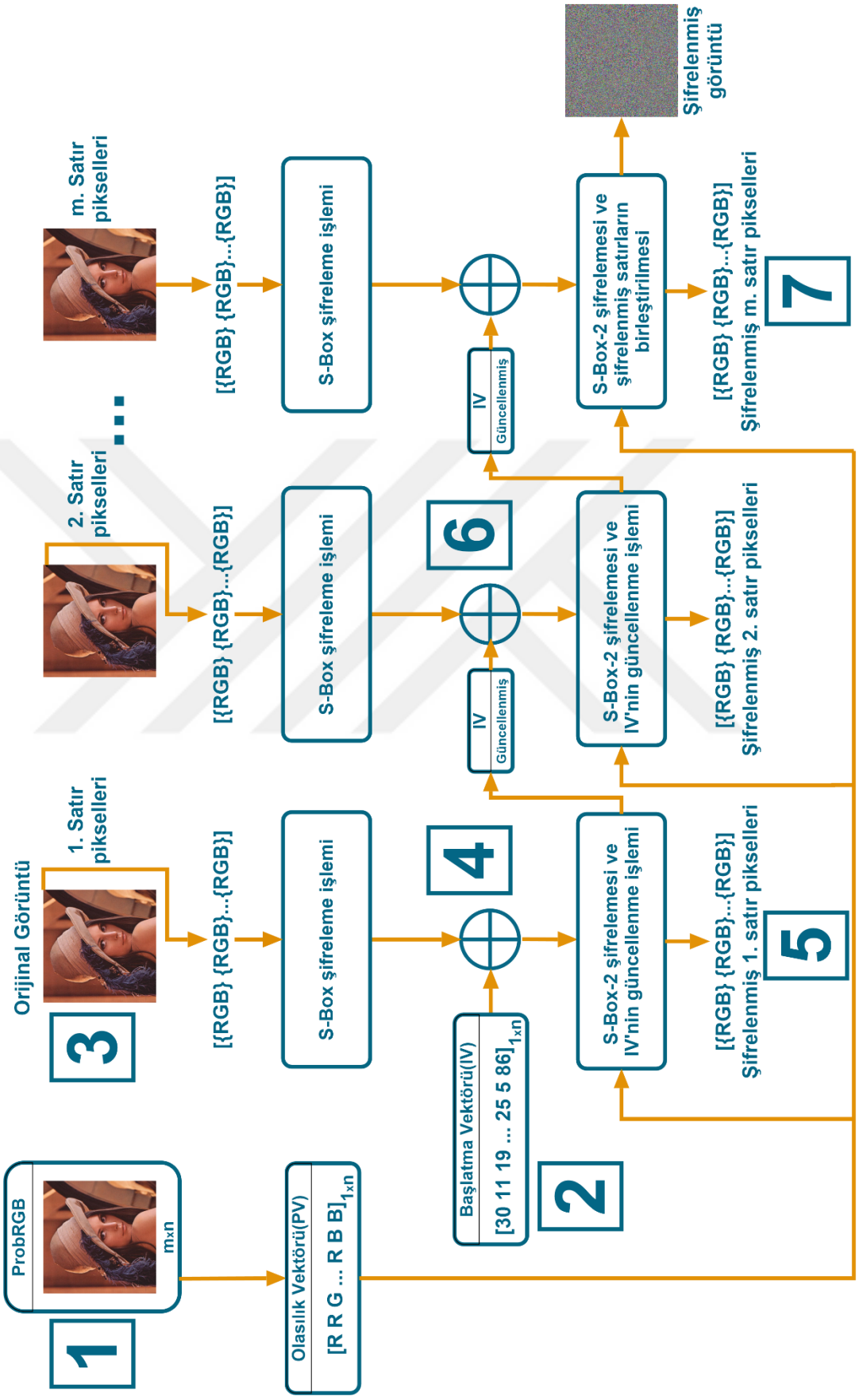


Şekil 3.8. Ters S-Box-2'nin üretilmesi

Şekil 3.9'da ProbRGB yönteminin şifreleme adımları modellenmiş ve aşağıda detaylı olarak listelenmiştir.

1- Orijinal görüntüde PV'nin üretilmesi
2- Başlatma vektörünün üretilmesi
3- Orijinal görüntünün ilk satırındaki piksel değerlerinin ilk S-Box ile karıştırılıp IV ile XOR işlemine tabi tutularak şifrelenmesi
4- S-Box-2 tablosuna göre şifrelenen satırın karıştırılması
5- IV'nin PV'ye göre güncellenmesi
6- Orijinal görüntünün son satır piksellerinin şifrelenmesine kadar 3. Adımdan tekrar edilmesi
7- Tüm satırların şifrelenmesinden sonra satırlar birleştirilerek şifrelenmiş görüntünün elde edilmesi

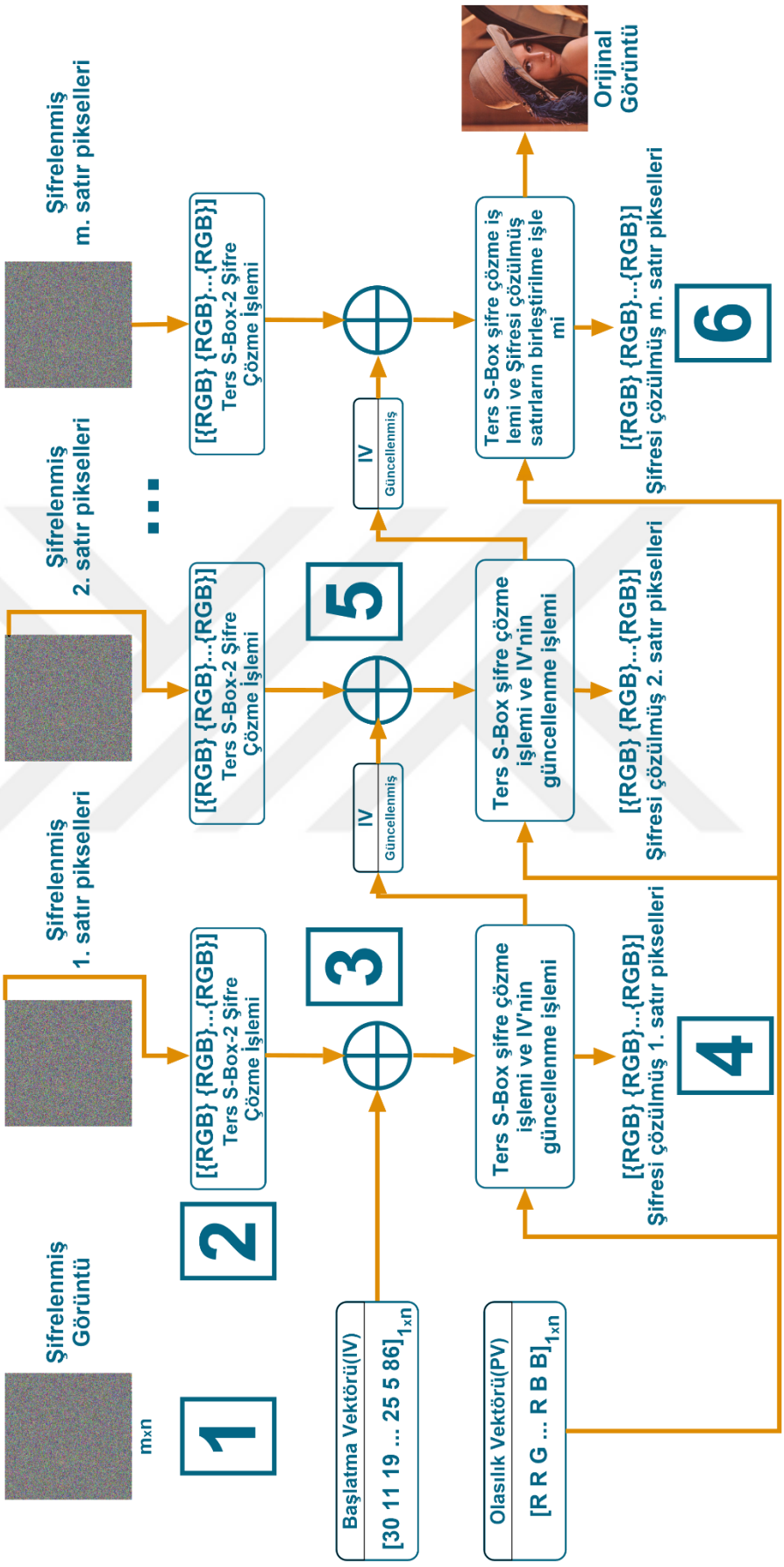
Önerilen ProbRGB temelli blok şifreleme yönteminin sonucunda PV, IV, S-Box, S-Box-2 ve şifrelenmiş görüntü çıktı olarak elimizde bulunmaktadır. Orijinal görüntüyü kayıpsız elde etmek için bu beş bileşen kullanılmıştır. Bu bileşenlerden herhangi birinin eksik ya da yanlış olması durumunda şifre çözme işlemlerinde anlamsız veriler elde edilmektedir.



Şekil 3.9. ProbRGB görüntü şifreleme sistem mimarisi

Şekil 3.10' da ProbRGB şifre çözme adımları modellenmiştir ve aşağıda detaylı olarak listelenmiştir;

1- Önerdiğimiz ProbRGB temelli görüntü şifreleme yönteminden elde edilen şifreli görüntü, IV, PV ve S-Box ve S-Box-2'den üretilen Ters S-Box ve Ters S-Box-2 tablosunun şifre çözme için hazır hale getirilmesi.
2- Şifreli görüntüdeki ilk satır piksellerinin Ters S-Box-2 tablosuna göre geri dönüştürülmesi
3- Ters S-Box-2 tan elde edilen satır piksellerinin IV ile XOR işlemine tutulduktan sonra Ters S-Box tablosuna göre şifresinin çözülmesi
4- IV'nin PV'ye göre güncellenmesi
5- Şifreli görüntünün son satır piksellerinin şifresinin çözülmesine kadar 2. adımdan tekrar edilmesi
6- Tüm satırların şifre açma işleminden sonra satırlar birleştirilerek orijinal görüntünün elde edilmesi



Şekil 3.10. ProbRGB görüntü şifre çözme sistem mimarisi

4. DENEYSEL ÇALIŞMA

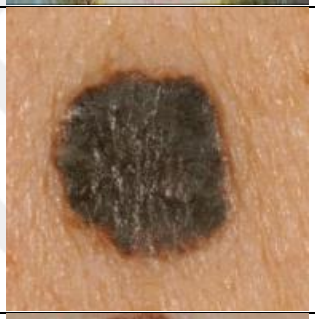
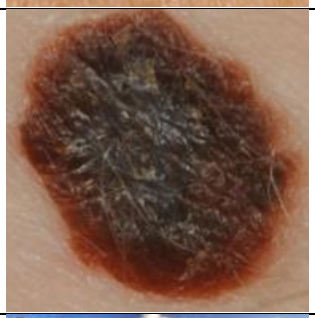
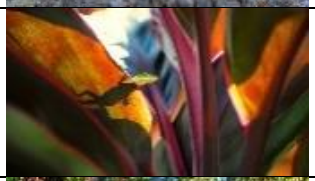
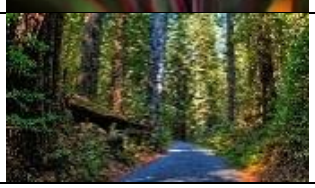
4.1. Kullanılan Veri Seti

Önerdiğimiz şifreleme yöntemlerinin test edilebilmesi için kullanılacak olan veri seti benzer birçok çalışmada ortak kullanılan Lena, Airplane, Cameraman ve Babbon görüntülerinden oluşmaktadır. Ayrıca International Skin Imaging Collaboration (ISIC) Melanoma Project kapsamında açık erişimli veri kümesinden alınan iki farklı melanoma görüntüsü de veri setine eklenmiştir (Codella ve diğ., 2019). Ek olarak yüksek çözünürlüklü görüntülerde test edebilmek için veri setine 2K, 4K ve 8K çözünürlüğe sahip üç farklı görüntü eklenmiştir. Bu görüntüler sırasıyla 2K Görüntü, 4K Görüntü ve 8K Görüntü olarak adlandırılmıştır. Benzer çalışmalarla kıyaslama yapabilmek için renkli görüntüler gri tonlamaya (grayscale) çevrilerek veri setinde kullanılmaktadır. Veri setinde kullanılan görüntüler jpeg, png ve bmp formatındadır. Veri seti ile ilgili detaylı bilgi ve görüntü görselleri Tablo 4.1'de gösterilmektedir.

Tablo 4.1. Görüntü şifreleme için kullanılacak veri seti

Görüntü Adı	Görüntü Özellikleri	Görüntü Görseli
Lena	256x256, .jpg, 12 KB, Renkli, Gray BT-709(HDTV) Metodu (0,21Kırmızı+0,72Yeşil+0,07Mavi)	
Airplane	512x512,.bmp, 192 KB, Renkli, Gray BT-709(HDTV) Metodu (0,21Kırmızı+0,72Yeşil+0,07Mavi)	

Tablo 4.1.(Devam) Görüntü şifreleme için kullanılacak veri seti

Görüntü Adı	Görüntü Özellikleri	Görüntü Görseli
Cameraman	256x256, .png, 42 KB, Gri renkli	
Baboon	512x512, .jpg, 59 KB, Renkli, Gray BT-709(HDTV) Metodu (0,21Kırmızı+0,72Yeşil+0,07Mavi)	
Melanoma 1	512x512, .jpg, 54 KB, Renkli, Gray BT-709(HDTV) Metodu (0,21Kırmızı+0,72Yeşil+0,07Mavi)	
Melanoma 2	512x512, .jpg, 53 KB, Renkli, Gray BT-709(HDTV) Metodu (0,21Kırmızı+0,72Yeşil+0,07Mavi)	
2K Görüntü	1920x1080, .jpg, 4.84 MB, Renkli, Gray BT-709(HDTV) Metodu (0,21Kırmızı+0,72Yeşil+0,07Mavi)	
4K Görüntü	3840x2160, .jpg, 17.3 MB, Renkli, Gray BT-709(HDTV) Metodu (0,21Kırmızı+0,72Yeşil+0,07Mavi)	
8K Görüntü	7680x4320, .jpg, 94.5 MB, Renkli, Gray BT-709(HDTV) Metodu (0,21Kırmızı+0,72Yeşil+0,07Mavi)	

4.2. Güvenlik ve Performans Analiz Yöntemleri

Şifreleme kalitesini değerlendirmek amacıyla orijinal ve şifreli görüntüler kriptanaliz işlemlerine tabi tutulmuştur. Bu amaçla on bir farklı analiz yöntemi kullanılmıştır. Yöntemlerin detaylı açıklaması alt bölümlerde verilmiştir.

4.2.1. Histogram analizi

Şifreli görüntü histogram analizi, görüntü şifreleme kalitesini göstermenin en basit yöntemlerinden biridir. İyi bir görüntü şifreleme yönteminde orijinal görüntüyü rastgele benzeri bir şekilde şifreleme eğilimi olduğundan, şifreli görüntü için düzgün dağılmış bir histogram olması gerekmektedir (Wu ve diğ., 2012). Şifrelenmiş piksel değerlerinin görüntü üzerinde homojen dağılması gerekmektedir. Histogram analizi görüntü şifreleme yönteminin istatistiksel saldırılara karşı dayanıklı olup olmadığını anlamamıza yardımcı olmaktadır (Güvenoğlu, 2016).

4.2.2. Ortalama mutlak hata analizi

Ortalama mutlak hata (Mean Absolute Error, MAE) analizi, orijinal görüntü ile şifresi çözülmüş görüntü arasında herhangi bir pikselde değişim olup olmadığını bilgisini vermektedir. Ortalama mutlak hata sıfırdan büyükse görüntü kalitesinde bir değişiklik olduğunu sıfır ise görüntü kalitesinde herhangi bir değişimin olmadığı bilgisini vermektedir (Jolfaei ve Mirghadri, 2010). Denklem (4.1)'de ortalama mutlak hatanın elde edilme formülü gösterilmektedir. H ve W sırasıyla görüntünün satır ve sütununu ifade etmektedir. $C(i,j)$, şifresi çözülmüş görüntüdeki i. satır ve j. sütundaki piksel değerini ifade etmektedir. $P(i,j)$, orijinal görüntüdeki i. satır ve j. sütundaki piksel değerini ifade etmektedir (Jolfaei ve Mirghadri, 2010).

$$MAE = \frac{1}{H \times W} \sum_{i=0}^{H-1} \sum_{j=0}^{W-1} \left| C(i,j) - P(i,j) \right| \tag{4.1}$$

4.2.3. Ortalama karesel hata analizi

Ortalama karesel hata, ortalama mutlak hatanın karesi alınarak hesaplanmaktadır. Orijinal görüntü ile şifresi çözülmüş görüntü arasında ortalama karesel hatanın (Mean Square Error, MSE) tespit edilerek görüntüde bozulmalara sebep olup olmadığı

gözlemlenebilmektedir. Ortalama karesel hata sıfırdan büyükse görüntüdeki piksellerde bir bozulma olduğu sıfır ise görüntünün kayıpsız olarak geri döndürülebilir olduğunu göstermektedir (Aydoğan ve Bayılmış, 2017). Denklem (4.2)'de ortalama karesel hatanın elde edilme formülü gösterilmektedir. Denklem (4.2)'de belirtilen ifadeler Denklem (4.1)'deki ifadeler ile aynı anlamı taşımaktadır (Aydoğan ve Bayılmış, 2017).

$$MSE = \frac{1}{H \times W} \sum_{i=0}^{H-1} \sum_{j=0}^{W-1} \left\| C(i,j) - P(i,j) \right\|^2 \tag{4.2}$$

4.2.4. Tepe sinyal gürültü oran analizi

Tepe sinyal gürültü oran analizi (Peak Signal-to-Noise Ratio, PSNR), benzer görüntüler üzerinde objektif görüntü kalitesi ölçümü için kullanılan yöntemlerden biridir. Tez kapsamında orijinal görüntü ve şifresi çözülmüş görüntü arasındaki görüntü kalite farkını bulmak için kullanılacaktır. Yüksek bir PSNR değeri daha yüksek görüntü kalitesi anlamına gelmektedir. Düşük PSNR değeri ise görüntüler arasındaki yüksek sayısal farkı ifade eder (Hore ve Ziou, 2010). Denklem (4.3)'te PSNR değerinin nasıl elde edildiği gösterilmektedir. MAX, kullanılan maksimum piksel değerini, MSE ise ortalama karesel hatayı temsil etmektedir (Aydoğan ve Bayılmış, 2017). PSNR değerini tespit etmek için orijinal görüntü ve şifreli görüntünün gri tonlamalı($k = 8$-bit) hale dönüştürülerek piksel değerleri üzerinden ortalama karesel hata hesaplanmıştır. Bu nedenle $MAX = 2^k - 1 = 255$ olarak seçilmiştir.

$$PSNR = 10 \log_{10} \left(\frac{MAX^2}{MSE} \right) \tag{4.3}$$

4.2.5. Yapısal benzerlik analizi

Yapısal benzerlik analizi (Structure Similarity, SSIM), karşılaştırılmak istenen iki görüntünün birbirine ne kadar oranda benzediğini göstermektedir. Sonucun sıfıra yakın olması benzerliğin düşük bire yakın olması benzerliğin çok yüksek ve bir olması durumunda görüntülerin birebir olduğunu göstermektedir (Wang ve diğ., 2004). Denklem (4.5)'ten Denklem (4.8)'e kadarki denklemlerde yapısal benzerlik testini

nasıl elde edildiği gösterilmektedir.μ_x, x değerlerinin ortalamasını, μ_y, y değerlerinin ortalamasını, σ_{xy} , x ve y değerlerinin kovaryansını, σ_x^2 ve σ_y^2 sırasıyla x ve y değerlerin varyansını, C_1 ve C_2 bölünmeyi zayıf payda ile dengelemek için kullanılan değerleri göstermektedir. K_1 ve K_2 sabit değerleri ifade etmektedir. Tez kapsamında $K_1 = 0.01$ ve $K_2 = 0.03$ olarak kullanılmaktadır. L piksel değerlerinin dinamik aralığını ifade etmektedir. Bu tez çalışmasında görüntü piksellerindeki her bir renk değeri 8 bit e karşılık geldiğinden $L = 2^8 - 1 = 255$ olarak kullanılmaktadır (Wang ve diğ., 2003).

$$C_1 = \left(K_1 L\right)^2, \quad C_2 = \left(K_2 L\right)^2. \tag{4.4}$$

$$\mu_x = \frac{1}{n}\sum_{i=1}^{n} x_i, \quad \mu_y = \frac{1}{n}\sum_{i=1}^{n} y_i. \tag{4.5}$$

$$\sigma_x = \left(\frac{1}{n-1}\sum_{i=1}^{n}\left(x_i - \mu_x\right)^2\right)^{\frac{1}{2}}, \quad \sigma_y = \left(\frac{1}{n-1}\sum_{i=1}^{n}\left(y_i - \mu_y\right)^2\right)^{\frac{1}{2}}. \tag{4.6}$$

$$\sigma_{xy} = \frac{1}{n-1}\sum_{i=1}^{n}\left(x_i - \mu_x\right)\left(y_i - \mu_y\right) \tag{4.7}$$

$$SSIM\left(x, y\right) = \frac{\left(2\mu_x\mu_y + C_1\right)\left(2\sigma_{xy} + C_2\right)}{\left(\mu_x{}^2 + \mu_y{}^2 + C_1\right)\left(\sigma_x{}^2 + \sigma_y{}^2 + C_2\right)} \tag{4.8}$$

4.2.6. Bilgi entropi analizi (Shannon Entropisi)

Bilgi entropi analizi (Shannon Information Entropy, IE), şifrelenmiş verilerdeki belirsizlik seviyesini ölçmek için kullanılan bir yöntemdir. Belirsizlik, veriler içerisinde farklılığı oluşturan ve üçüncü şahıslar açısından belirsiz olan durumdur. Şifrelenen verinin belirsizlik seviyesi arttıkça orijinal görüntüyü tahmin etmek o kadar zorlaşmaktadır. Görüntü şifreleme için kabul edilen bilgi entropi değeri 8 olarak

tanımlanmıştır (Jolfaei ve Mirghadri, 2011). Denklem (4.9)' da belirsizlik değerinin nasıl hesaplanacağı gösterilmiştir. $P(s_i)$, pikseldeki renk değerinin tüm görüntü pikselleri içerisindeki kullanım olasılığını ifade etmektedir (Shannon, 1949; Stinson, 1995; Jolfaei ve Mirghadri, 2011).

$$H(s) = -\sum_{i=0}^{2^n-1} P(s_i) \log_2 \left[P(s_i) \right] \tag{4.9}$$

4.2.7. Diferansiyel atak analizi

Diferansiyel atak analizi, sabit bir farklı ilişkili düz görüntü çiftlerini kullanmak ve dağılımlarındaki istatistiksel modeller için karşılık gelen şifre-görüntü farklını karşılaştırmak için etkili bir yöntemdir (Wu ve diğ., 2017). Şifreyi kırmak isteyen kişiler genellikle şifreleme algoritmasını kullanır ve orijinal görüntülerde bazı küçük değişiklikler yapabilir. Şifrelenmiş görüntüdeki değişiklikleri gözlemleyerek orijinal ve şifreli görüntü arasındaki ilişkiyi bulmaya çalışılır. Bu analiz, düz görüntüye duyarlılığı değerlendirmeyi amaçlamaktadır (Liu ve diğ., 2019). Piksel sayısı değişim oranı (Number of pixels change rate, NPCR) ve birleşik ortalama değişim yoğunluğu (unified average changing intensity, UACI) şifrelenmiş görüntüler arasındaki farklı ölçmek için kullanılan iki yöntemdir (Chen ve diğ., 2004; Alvarez ve Li, 2006).

Piksel sayısı değişim oranı, orijinal görüntü ve şifreli görüntüdeki piksellerin karşılaştırılması ile elde edilmektedir. 0 ile 100 arasındaki değerler ile ölçülmektedir. Sıfır değeri görüntülerin aynı olduğu 100 değeri ise piksellerin tamamen farklı olduğunu ifade etmektedir. NPCR değeri 100'e ne kadar yakın olursa şifrelenmiş görüntüden orijinal görüntü için çıkarım yapılmasının önüne geçilmiş olur (Wu ve diğ., 2011; Chen ve diğ., 2004; Alvarez ve Li, 2006). Denklem (4.10) ve Denklem (4.11)'de NPCR değerinin nasıl elde edildiği gösterilmektedir. H ve W sırasıyla görüntünün satır ve sütununu ifade etmektedir. C_1 ve C_2 iki görüntüyü ifade etmektedir. $T(i,j)$, iki görüntü arasındaki piksellerin birbirine eşit olup olmadığını göstermektedir.

$$NPCR = \frac{\sum_{i,j} T(i,j)}{H \times W} \times 100\% \tag{4.10}$$

$$T(i,j)=\begin{cases}0,\ C_1(i,j)=C_2(i,j),\\ 1,\ C_1(i,j)\neq C_2(i,j).\end{cases} \tag{4.10}$$

Birleşik ortalama değişim yoğunluğu, orijinal görüntüye karşılık gelen şifreli görüntü arasındaki ortalama yoğunluk değişikliğini ölçmektedir. Yüksek yoğunluklu UACI değeri, diferansiyel ataklara karşı güçlü bir direnç göstermektedir (Wu ve diğ., 2011; Chen ve diğ., 2004; Alvarez ve Li, 2006). Denklem (4.10)'da UACI değerinin nasıl hesaplanacağı gösterilmektedir. Denklem (4.9)'da belirtilen ifadeler Denklem (4.10)'daki ifadeler ile aynı anlamı taşımaktadır.

$$UACI=\frac{1}{H\times W}\sum_{i,j}\frac{\left|C_1(i,j)-C_2(i,j)\right|}{255}\times 100\% \tag{4.10}$$

4.2.8. Korelasyon analizi (Pearson Korelasyonu)

Şifrelenmemiş görüntülerde bitişik pikseller arasında ikili korelasyon mevcuttur. Korelasyon analizi sonucunda bitişik pikseller arasında doğrusal bir ilişki olup olmadığı ve varsa bu ilişkinin derecesi korelasyon katsayısı (Correlation Coefficent, CC) ile hesaplanır (Atalay ve diğ., 2019). Korelasyon katsayısı -1 ile +1 arasında bir değer alır. Korelasyon katsayısı -1 ise mutlak negatif doğrusal ilişki, +1 ise mutlak pozitif doğrusal ilişki, 0 ise iki değişken arasında ilişki yoktur manasına gelmektedir. Bu açıklamadan da anlaşılacağı gibi orijinal görüntüde mutlak negatif ya da mutlak pozitif doğrusal ilişki bulunuyorken şifrelenmiş görüntülerde ise doğrusal olmayan bir ilişki olması gerekmektedir. Şifreli görüntüler için korelasyon katsayısı 0 değerine ne kadar yakın olursa şifreleme kalitesi de o kadar iyi olmuş olur (Pisarchik ve Zanin, 2008; Atalay ve diğ., 2019). Şifrelenmiş görüntülerde bir doğrusallık varsa, yetkisiz kişiler tarafından görüntüyü kısmen veya tamamen geri yüklemek için kullanılabilir. Bir görüntünün bitişik pikselleri arasında yatay, dikey ve diyagonal korelasyon katsayısı (Pearson Korelasyonu (Huang ve diğ., 2018)) matematiksel olarak Denklem (4.11) ile Denklem (4.14) arasında gösterilmektedir. Burada x ve y üç yönde bitişik piksel dizisini z ise görüntüden rastgele seçilen toplam bitişik piksel sayısını temsil etmektedir. $M(x)$ ve $M(y)$ sırasıyla x ve y'nin ortalamasını, $D(x)$ ve $D(y)$ sırasıyla x ve y'nin varyansını ifade etmektedir. $Conv(x,y)$, x ve y'nin kovaryansını ifade

etmektedir. γ_{xy} ise görüntüdeki bitişik pikseller arasındaki korelasyon katsayısını göstermektedir.

$$M(x)=\frac{1}{z}\sum_{i=1}^{z}x_i,$$
$$M(y)=\frac{1}{z}\sum_{i=1}^{z}y_i, \tag{4.11}$$

$$D(x)=\frac{1}{z}\sum_{i=1}^{z}\left[x_i-M(x)\right]^2,$$
$$D(y)=\frac{1}{z}\sum_{i=1}^{z}\left[y_i-M(y)\right]^2, \tag{4.12}$$

$$Conv(x,y)=\frac{1}{z}\sum_{i=1}^{z}\left[x_i-M(x)\right]\left[y_i-M(y)\right], \tag{4.13}$$

$$\gamma_{xy}=\frac{Conv(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}. \tag{4.14}$$

4.2.9. Anahtar uzay analizi

Kabul edilebilir bir görüntü şifreleme algoritması, kaba kuvvet (Brute force) vb. saldırılara direnmek için yeterince büyük bir anahtar alanına sahip olmalıdır (Song ve diğ., 2019). Tez çalışmamız kapsamında renkli ve gri tonlamalı görüntülere uygulanabilen anahtarlar olarak PV, IV ve S-Box anahtarları kullanılmaktadır. IV ve PV'nin tek seferde bulunma olasılığı Denklem (4.15)'te gösterilmektedir. Denklem (4.15)'te kullanılan n ifadesi görüntünün sütun sayısını ifade etmektedir.

$$P(PV)=\frac{1}{3^n},$$
$$P(IV)=\frac{1}{256^n}. \tag{4.15}$$

Tez çalışması kapsamında PHMMRGB görüntü şifreleme yönteminde bir adet S-Box kutusu kullanılmıştır. Bu S-Box kutusunun tek seferde bulunma olasılığı Denklem (4.16)'da gösterilmiştir. Kullanılan S-Box 256 farklı tamsayıdan meydana gelmektedir. Bu sebeple Denklem (4.16)'da $k_{max}=256$ olarak kullanılmıştır. Tez çalışması

kapsamında önerilen diğer bir yöntem olan ProbRGB' de ise birbirinden farklı iki S-Box kullanılmıştır. Bu iki farklı S-Box kutusunun tek seferde bulunma olasılığı Denklem (4.17)'de gösterilmektedir.

$$P(S) = \frac{1}{\sum_{i=1}^{k_{\max}} (k_{\max} - i)!} \tag{4.16}$$

$$P(S_2) = \left(\frac{1}{\sum_{i=1}^{k_{\max}} (k_{\max} - i)!} \right)^2 - \left(\frac{1}{\sum_{i=1}^{k_{\max}} (k_{\max} - i)!} \right) \tag{4.17}$$

4.2.10. Hesaplama verimliliği analizi

Hesaplama verimliliği analizi, bir programın ya da fonksiyonun mevcut donanım ve yazılımsal kaynakları kullanarak işlevini tam anlamıyla yerine getirebilmesi için gerekli süreyi gösteren bir bağıntı olarak tanımlanabilir. Şifreleme işlemleri ve şifreleme hızı, şifre güvenliği için büyük önem taşır (Ishai ve diğ., 2008). Tez kapsamında şifreleme ve şifre çözme işlemleri için kullandığımız donanım, Intel Core i5 2.4 Ghz işlemci, 8 GB RAM, 512 GB HDD ve Windows 10 işletim sistemi bulunmaktadır. Bu koşullar altında, PHMMRGB görüntü şifreleme yönteminde şifreleme hızı renkli görüntüler için 0.7745Mbit/s ve gri tonlamaları görüntüler için 1.0535Mbit/s'dir. ProbRGB yönteminde ise şifreleme hızı renkli görüntüler için 0.6891Mbit/s ve gri tonlamalı görüntüler için ise 0.9853Mbit/s'dir.

4.2.11. Zaman karmaşıklık analizi

Zaman karmaşıklık analizi, bir programın ya da fonksiyonun işlevini tam anlamıyla yerine getirebilmesi için her işlemden kaç kere yapması gerektiğini gösteren bir bağıntıdır. Zaman karmaşıklığı şifreleme algoritmaları için önemlidir (Talbot ve diğ., 2006). Tez kapsamında önerilen iki görüntü şifreleme yönteminde kullanılan anahtarlardan PV, S-Box ve Ters S-Box'un üretilmesi için $\theta(N^2)$, IV'nin üretilmesi için ise $\theta(N)$'dir. Tez kapsamında önerdiğimiz PHMMRGB yöntemindeki zaman karmaşıklığı satır(m) ve sütun(n) olan görüntüler için $\theta(N^2)$ 'dir. Şekil 4.1'de

şifreleme, Şekil 4.2'de şifre çözme işlemleri için zaman karmaşıklığının hesaplanması gösterilmektedir.

PHMMRGB Yöntemi – Şifreleme Zaman Karmaşıklığı

1:**for iteration=1,2,…,n do**	$T = 2n + 2$
2: **for iteration=1,2,…,m do**	$T = n(2m + 2)$
3: Pikselin IV ile şifrelenmesi	$T = nm$
4: Şifrenmiş değerin S-Box ile karıştırılması	$T = nm$
5: IV nin PV ye göre güncellenmesi	$T = nm$
6: **end**	$T(nm) = (2n + 2) + n(2m + 2) + 3nm = 5nm + 4n + 2$
7: **end**	$T(n) = 5nn + 4n = \boldsymbol{\theta(N^2)}$

Şekil 4.1. PHMMRGB yöntemi şifreleme zaman karmaşıklığı analizi

PHMMRGB Yöntemi – Şifre Çözme Zaman Karmaşıklığı

1:**for iteration=1,2,…,n do**	$T = 2n + 2$
2: **for iteration=1,2,…,m do**	$T = n(2m + 2)$
3: Ters S-Box ile pikseli geri alma.....	$T = nm$
4: IV ile pikselin şifresini çözme.....	$T = nm$
5: IV nin PV ye göre güncellenmesi	$T = nm$
6: **end**	$T(nm) = (2n + 2) + n(2m + 2) + 3nm = 5nm + 4n + 2$
7: **end**	$T(n) = 5nn + 4n = \boldsymbol{\theta(N^2)}$

Şekil 4.2. PHMMRGB yöntemi şifre çözme zaman karmaşıklığı analizi

Tez kapsamında önerilen ikinci görüntü şifreleme algoritması olan ProbRGB yöntemindeki zaman karmaşıklığı satır (m) ve sütun (n) olan görüntüler için $\theta(N^2)$'dir. Şekil 4.3'te şifreleme ve Şekil 4.4'te şifre çözme zaman karmaşıklıkları gösterilmektedir.

ProbRGB Yöntemi – Şifreleme Zaman Karmaşıklığı	
1:**for iteration=1,2,…,n do**	$T = 2n + 2$
2: **for iteration=1,2,…,m do**	$T = n(2m + 2)$
3: Pikselin S-Box ile karıştırılması.....	$T = nm$
4: Karıştırılan değerin IV ile şifrelenmesi.....	$T = nm$
5: Şifrenmiş değerin S-Box-2 ile karıştırılması	$T = nm$
6: IV nin PV ye göre güncellenmesi	$T = nm$
7: **end**	$T(nm) = (2n + 2) + n(2m + 2) + 4nm = 6nm + 4n + 2$
8: **end**	$T(n) = 6nn + 4n = \boldsymbol{\theta(N^2)}$

Şekil 4.3. ProbRGB yöntemi şifreleme zaman karmaşıklığı analizi

ProbRGB Yöntemi – Şifre Çözme Zaman Karmaşıklığı	
1:**for iteration=1,2,…,n do**	$T = 2n + 2$
2: **for iteration=1,2,…,m do**	$T = n(2m + 2)$
3: Ters S-Box-2 ile pikseli geri alma.....	$T = nm$
4: IV ile pikselin şifresini çözme.....	$T = nm$
5: Ters S-Box ile pikseli geri alma	$T = nm$
6: IV nin PV ye göre güncellenmesi	$T = nm$
7: **end**	$T(nm) = (2n + 2) + n(2m + 2) + 4nm = 6nm + 4n + 2$
8: **end**	$T(n) = 6nn + 4n = \boldsymbol{\theta(N^2)}$

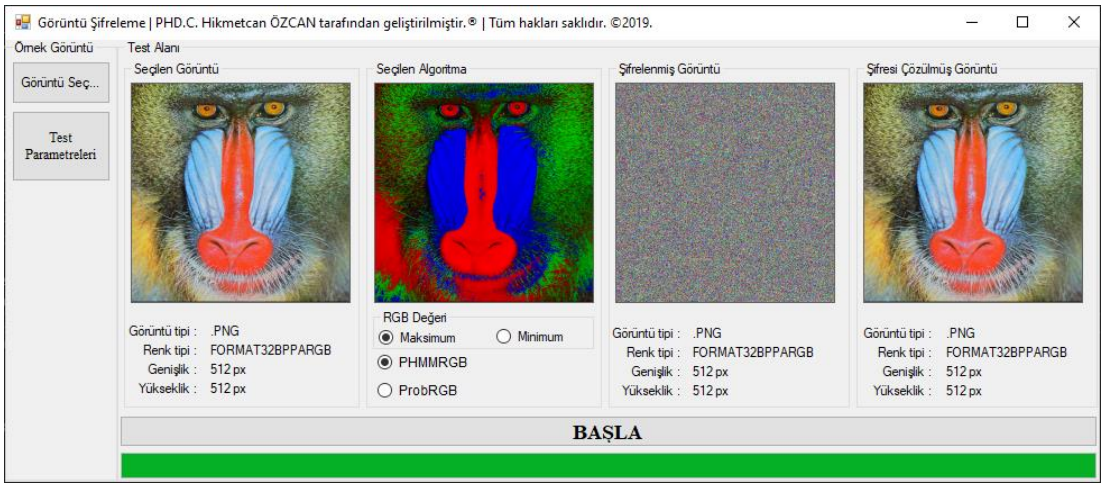
Şekil 4.4. ProbRGB yöntemi şifre çözme zaman karmaşıklığı analizi

4.3. Deneysel Sonuçlar

Tez kapsamında önerilen görüntü şifreleme yöntemlerinin uygulanması ve performans testlerinin yapılabilmesi için iki farklı uygulama geliştirilmiştir. Geliştirilen görüntü şifreleme isimli ilk uygulamanın kullanıcı arayüzü Şekil 4.5'te gösterilmiştir. Bu arayüzde kullanıcı ilk olarak şifrelemek istediği görüntüyü seçip ve ardından şifreleme yöntemini belirleyip başla butonuna basarak şifreleme işlemine başlatmaktadır.

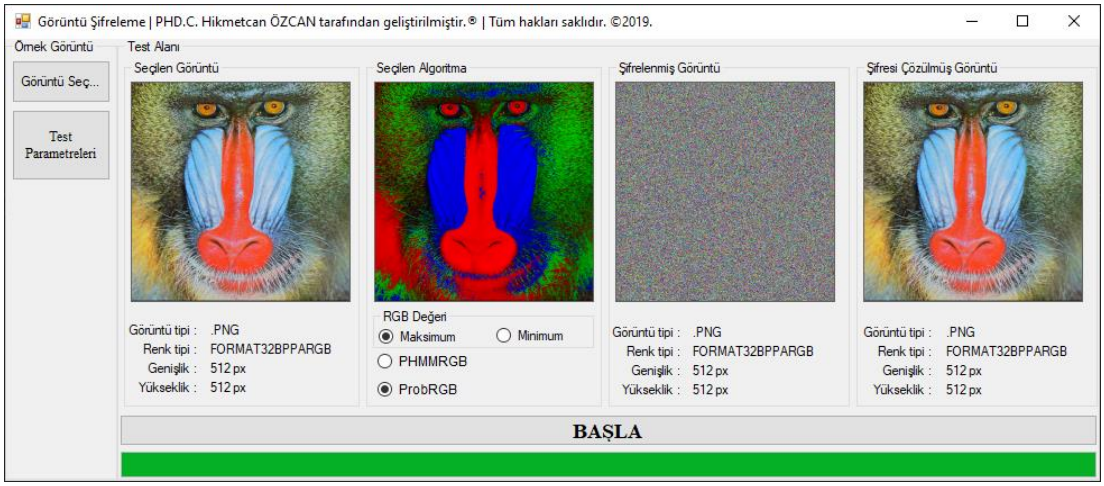
Şekil 4.5. Görüntü şifreleme uygulaması kullanıcı arayüzü

Şekil 4.6'da Baboon görüntüsünün PHMMRGB yöntemine göre şifrelenme ve şifre çözme işlemleri gösterilmektedir.



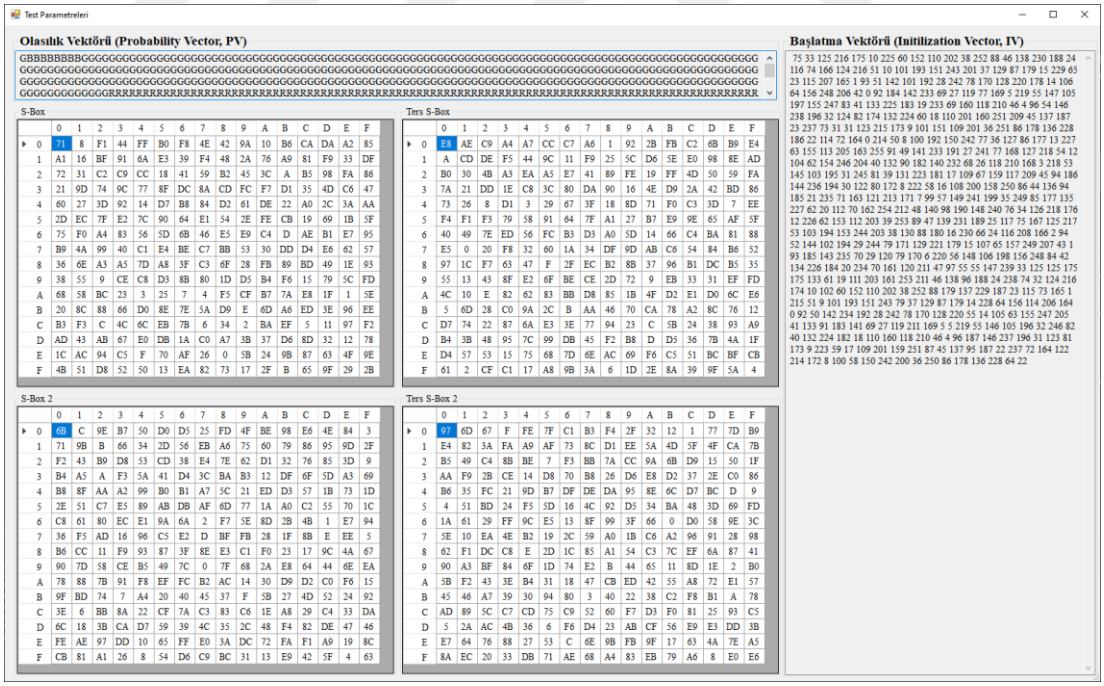
Şekil 4.6. Görüntü şifreleme uygulaması PHMMRGB yöntemi ile Baboon örneğinin çalıştırılması

Şekil 4.7'de Baboon görüntüsünün ProbRGB temelli görüntü şifreleme yöntemine göre şifrelenme ve şifre çözme işlemleri gösterilmektedir.



Şekil 4.7. Görüntü şifreleme uygulaması ProbRGB yöntemi ile Baboon örneğinin çalıştırılması

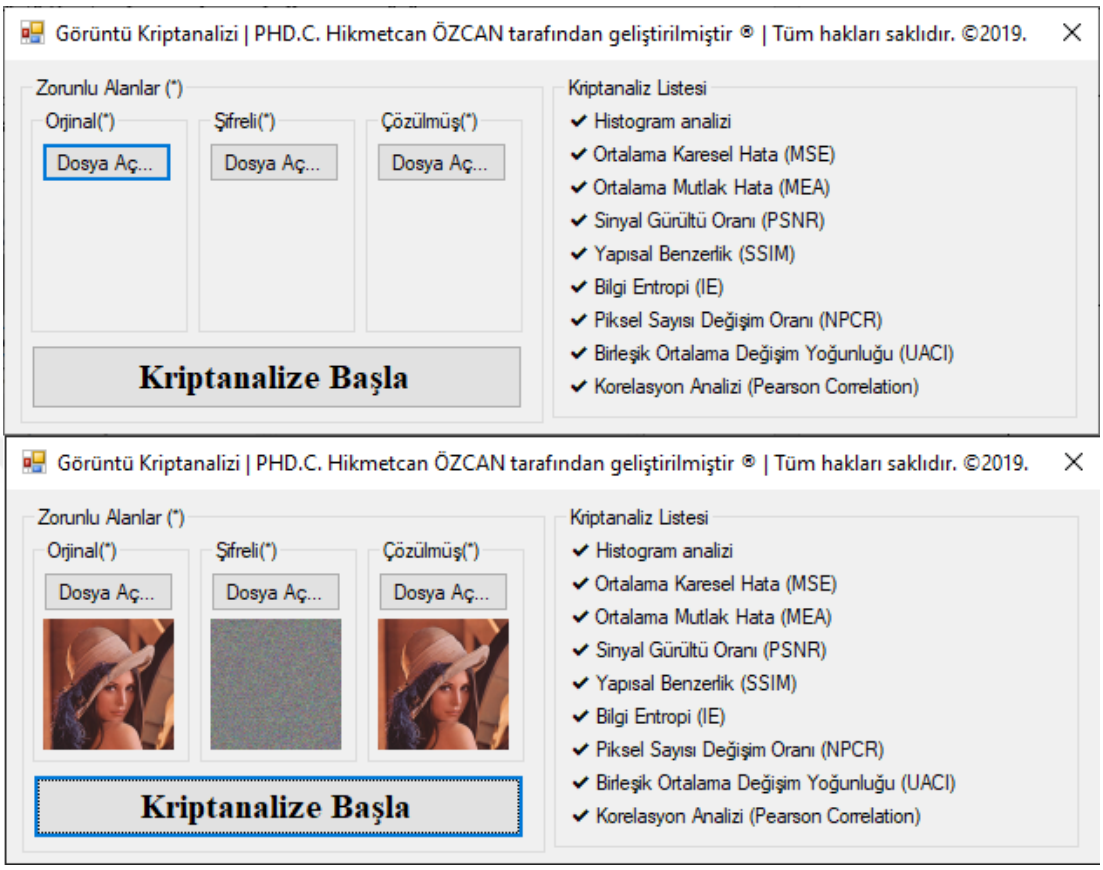
Şekil 4.8'te görüntü şifreleme uygulamasında Baboon görüntüsünün şifreleme ve şifre çözme işlemi için kullanılan olasılık vektörü, başlatma vektörü ve iki adet S-Box bilgisi gösterilmektedir. Her görüntünün şifrelenmesi ve şifre çözülmesi aşamasında bu parametreler değişmektedir.



Şekil 4.8. Görüntü şifreleme uygulamasında kullanılan parametreler

Geliştirilen görüntü kriptanalizi isimli ikinci uygulamanın kullanıcı arayüzü Şekil 4.9'da gösterilmektedir. Bu arayüzde kullanıcı sırasıyla orijinal görüntü, şifreli

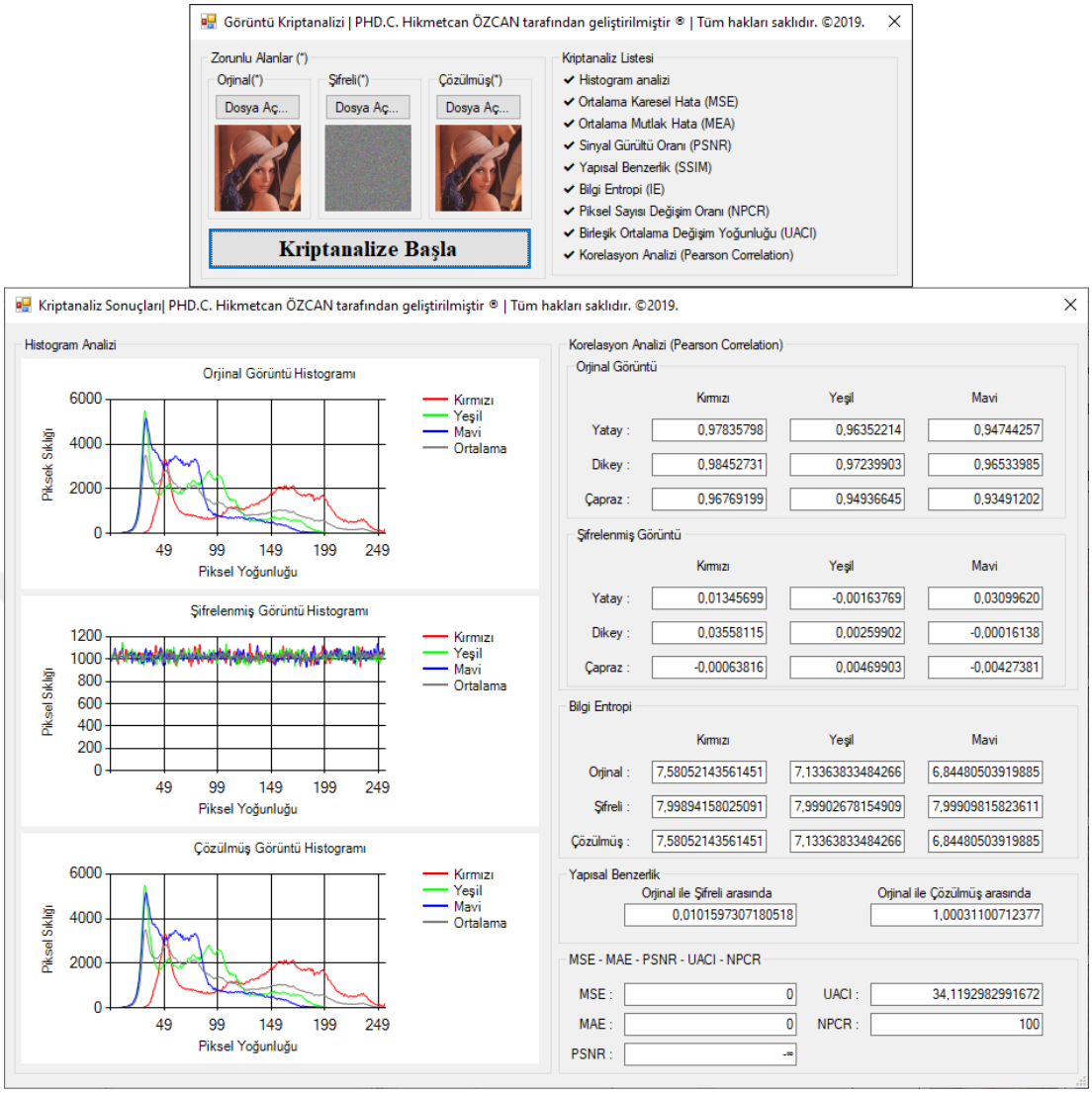
görüntü ve şifresi çözülmüş görüntü yükleyip analize başla butonuna basarak kriptanaliz işlemine başlamaktadır.



Şekil 4.9. Görüntü kriptanaliz uygulaması kullanıcı arayüzü

Şekil 4.10'da Lena görüntüsüne ait kriptanaliz analizi gösterilmektedir. Kritpanaliz sonuçlarındaki arayüzde performans analiz test sonuçları bölüm bölüm cevaplanmaktadır.

Geliştirilen bu iki uygulama veri setimizdeki tüm görüntüler için kullanılmaktadır. Görüntü şifrelemeden elde edilen şifreli ve çözülmüş görüntüler görüntü kriptanaliz uygulamasında performans analiz testine tabi tutulmaktadır. Ayrıca güvenlik ve performans analiz sonuçları literatürdeki benzer çalışmalarla karşılaştırması yapılmaktadır. PHMMRGB ve ProbRGB görüntü şifreleme yöntemlerinden elde edilen sonuçlar ilerleyen bölümlerde anlatılmıştır.

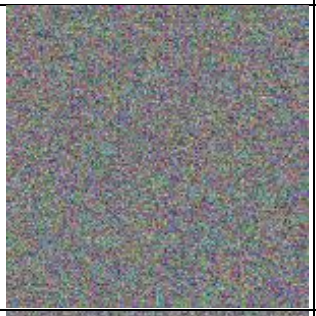
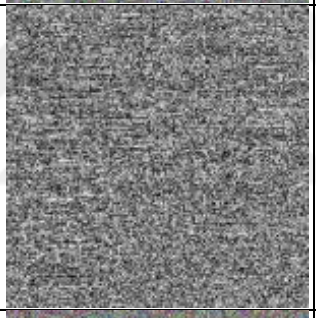
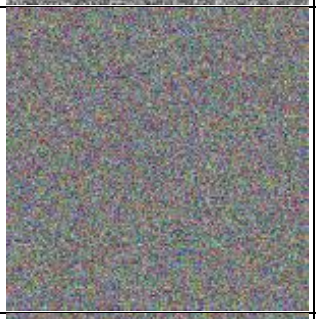
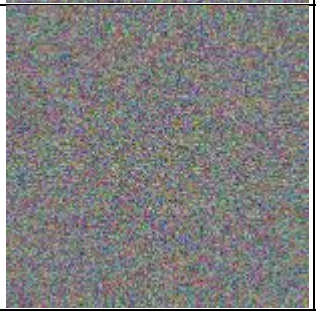


Şekil 4.10. Lena görüntüsü için kriptanaliz sonuçlarının elde edilmesi

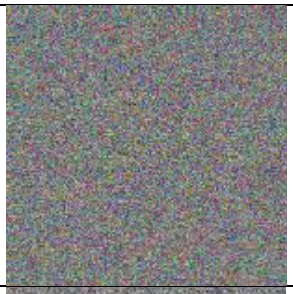
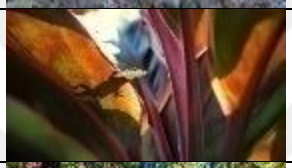
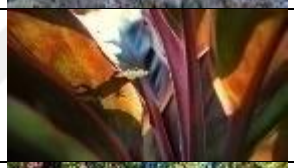
4.3.1. PHMMRGB şifreleme yöntemine ait sonuçlar

Görüntü şifreleme uygulamasında PHMMRGB görüntü şifreleme algoritması seçilerek elde edilen sonuçlar Tablo 4.2'de gösterilmektedir. Sonuçlarda, orijinal görüntü, şifreli görüntü ve şifresi çözülmüş görüntüler Görüntü Kriptanaliz uygulamasında kullanılarak histogram analizi, ortalama karesel hata analizi, ortalama mutlak hata analizi, sinyal gürültü oranı analizi, yapısal benzerlik analizi, bilgi entropi analizi, piksek sayısı değişim oranı analizi, birleşik ortalama değişim yoğunluğu analizi ve korelasyon analizleri gerçekleştirilmiş ve sonuçları değerlendirilmiştir. Ayrıca analiz sonuçları literatürdeki diğer çalışmalarla da karşılaştırılmaktadır.

Tablo 4.2. PHMMRGB görüntü şifreleme algoritmasının şifreleme ve şifre çözme sonuçları

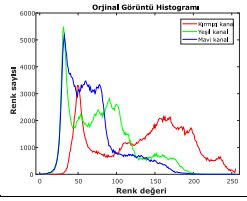
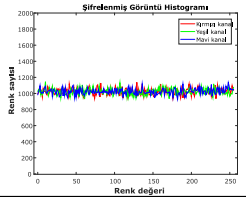
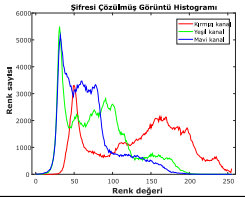
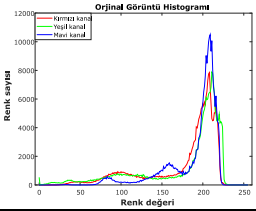
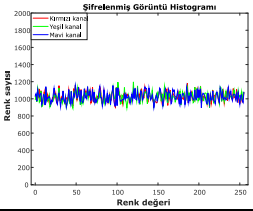
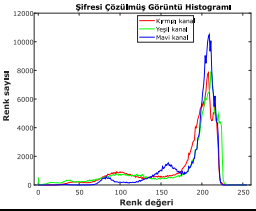
Görüntü Adı	Orijinal Görüntü	Şifreli Görüntü	Şifresi Çözülmüş Görüntü
Lena			
Airplane			
Cameraman			
Baboon			
Melanoma 1			

Tablo 4.2.(Devam) PHMMRGB görüntü şifreleme algoritmasının şifreleme ve şifre çözme sonuçları

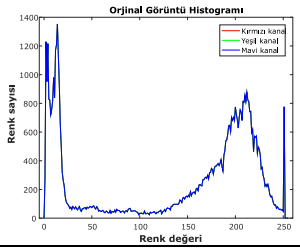
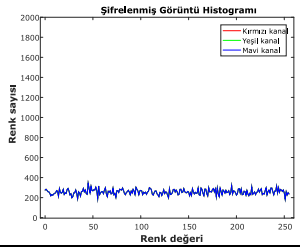
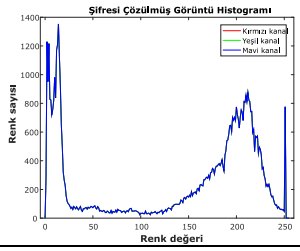
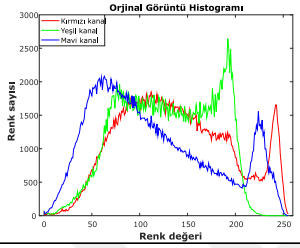
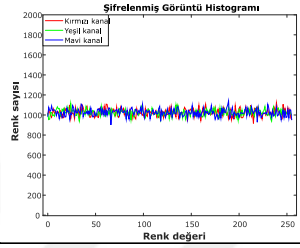
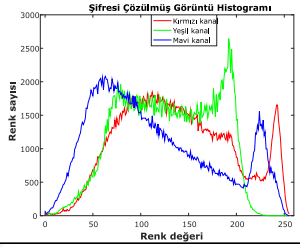
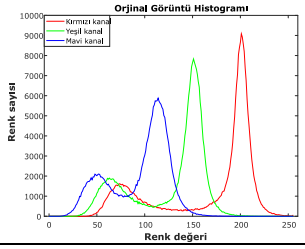
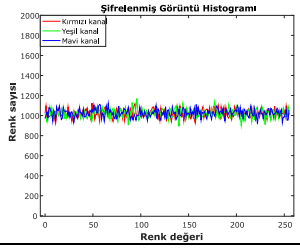
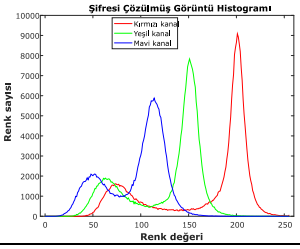
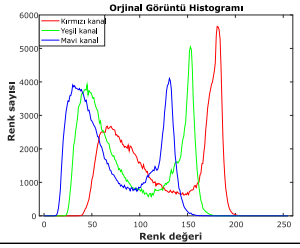
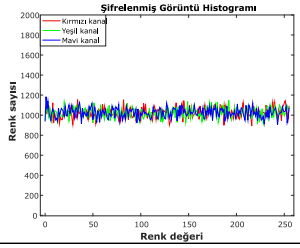
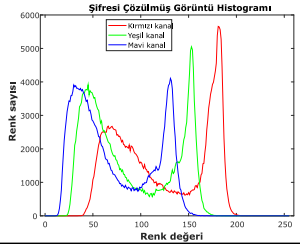
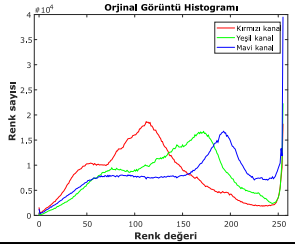
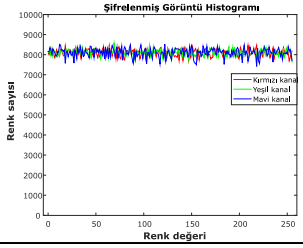
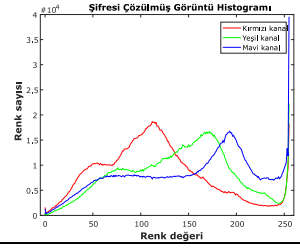
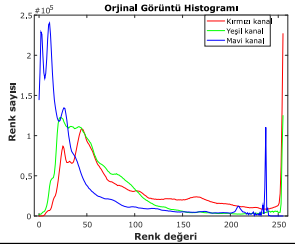
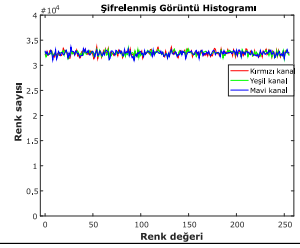
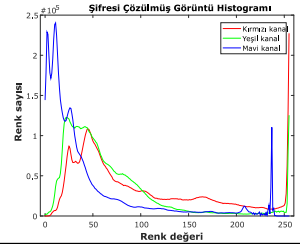
Görüntü Adı	Orijinal Görüntü	Şifreli Görüntü	Şifresi Çözülmüş Görüntü
Melanoma 2			
2K Görüntü			
4K Görüntü			
8K Görüntü			

PHMMRGB yöntemi uygulanarak şifreleme yapıldığında histogram analiz sonuçları Tablo 4.3'te gösterilmektedir. Histogram analizleri sonucunda şifrelenmiş görüntüdeki piksel değerlerinin homojen dağıldığı gözlemlenmektedir. Dolayısı ile istatistiksel saldırılara karşı dayanıklı olduğu söylenebilir.

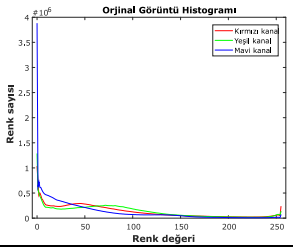
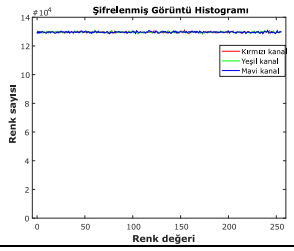
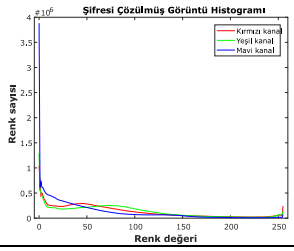
Tablo 4.3. PHMMRGB görüntü şifreleme algoritmasının histogram analiz sonuçları

Orijinal Görüntü Histogramı	Şifreli Görüntü Histogramı	Şifresi Çözülmüş Görüntü Histogramı
Lena	Lena	Lena
		
Airplane	Airplane	Airplane
		

Tablo 4.3.(Devam) PHMMRGB görüntü şifreleme algoritmasının histogram analiz sonuçları

Orijinal Görüntü Histogramı	Şifreli Görüntü Histogramı	Şifresi Çözülmüş Görüntü Histogramı
Cameraman	Cameraman	Cameraman
		
Baboon	Baboon	Baboon
		
Melanoma 1	Melanoma 1	Melanoma 1
		
Melanoma 2	Melanoma 2	Melanoma 2
		
2K Görüntü	2K Görüntü	2K Görüntü
		
4K Görüntü	4K Görüntü	4K Görüntü
		

Tablo 4.3.(Devam) PHMMRGB görüntü şifreleme algoritmasının histogram analiz sonuçları

Orijinal Görüntü Histogramı	Şifreli Görüntü Histogramı	Şifresi Çözülmüş Görüntü Histogramı
8K Görüntü	8K Görüntü	8K Görüntü
		

PHMMRGB görüntü şifreleme algoritması için MAE ve MSE sonuçları incelendiğinde tüm görüntüler için sonuç sıfırdır. Bu durum orijinal görüntü ile şifresi çözülen görüntü arasında herhangi bir bozulma olmadığını ve görüntünün kayıpsız olarak geri döndürülebildiğini göstermektedir.

Bu yöntem için PSNR analiz sonuçları analiz edildiğinde tüm görüntüler için MSE değerleri sıfır olduğundan PSNR değerleri de eksi sonsuzdur. Bu sonuç orijinal görüntüler ile şifresi çözülen görüntüler arasında kalite farkı olmadığını göstermektedir.

Tez kapsamında PHMMRGB yöntemi için orijinal görüntü ile şifrelenmiş görüntünün ve orijinal görüntü ile şifresi çözülmüş görüntünün yapısal benzerlik sonuçları Tablo 4.4'te gösterilmiştir. Yapısal benzerlik analiz sonuçları incelendiğinde orijinal görüntü ile şifreli görüntü arasındaki yapısal benzerliğin sıfıra yakın olduğu görülmektedir. Ayrıca orijinal görüntü ile şifresi çözülmüş görüntünün yapısal benzerliği bir olarak tespit edilmiştir. Bu sonuç şifrelenmiş görüntüden kayıpsız bir şekilde orijinal görüntüyü elde ettiğimizi ifade etmektedir.

Tablo 4.4. PHMMRGB görüntü şifreleme algoritmasının yapısal benzerlik analiz sonuçları

Görüntü Adı	Orijinal Görüntü ve Şifrelenmiş Görüntü arasındaki SSIM	Orijinal Görüntü ve Şifresi Çözülmüş Görüntü arasındaki SSIM
Lena	0,0101	1,0000
Airplane	0,0122	1,0000
Cameraman	0,0083	1,0000
Baboon	0,0031	1,0000

Tablo 4.4.(Devam) PHMMRGB görüntü şifreleme algoritmasının yapısal benzerlik analiz sonuçları

Görüntü Adı	Orijinal Görüntü ve Şifrelenmiş Görüntü arasındaki SSIM	Orijinal Görüntü ve Şifresi Çözülmüş Görüntü arasındaki SSIM
Melanoma 1	0,0053	1,0000
Melanoma 2	0,0066	1,0000
2K Görüntü	0,0064	1,0000
4K Görüntü	0,0061	1,0000
8K Görüntü	0,0054	1,0000

Tez kapsamında şifrelenmiş görüntünün karmaşıklığını ölçmek için kullanılan bilgi entropi testinin sonuçları Tablo 4.5'te gösterilmektedir. Sonuçlar incelendiğinde veri setimizde kullanılan görüntülerin şifreleme işleminden sonraki bilgi entropi sonuçlarının, ideal entropi değeri olan 8'e çok yakın olduğu gözükmektedir. Bu sayede şifreli görüntülerdeki rastgelelik ve düzensizliğin istenilen seviyede olduğu söylenebilir. PHMMRGB yönteminin, Tablo 4.5'te karşılaştırılan referanslarda öne sürülen yöntemlerin analiz sonuçları ile karşılaştırıldığında birçok çalışmadan daha iyi sonuçların elde edildiği açıkça görülmektedir.

Tablo 4.5. PHMMRGB görüntü şifreleme algoritmasının bilgi entropi analiz sonuçları

Görüntü Adı	Görüntü Tipi	Kırmızı	Yeşil	Mavi	Gri Tonlamalı
Lena	Orijinal	7,5805	7,1336	6.8448	7,2238
	Şifreli	7,9989	7,9990	7.9990	7,9987
	Çözülmüş	7,5805	7,1336	6.8448	7,2238
Airplane	Orijinal	6,7177	6,7989	6.2137	6,2137
	Şifreli	7,7219	7,7443	7.7032	7,9968
	Çözülmüş	6,7177	6,7989	6.2137	6,2137
Cameraman	Orijinal	7,2074	7,2074	7.2074	7,2074
	Şifreli	7,9927	7,9927	7,9927	7,9927
	Çözülmüş	7,2074	7,2074	7,2074	7,2074
Baboon	Orijinal	7,7066	7,4744	7,7522	7,3812
	Şifreli	7,9991	7,9993	7,9991	7,9992
	Çözülmüş	7,7066	7,4744	7,7522	7,3812
Melanoma 1	Orijinal	6,6979	6,6238	6,6747	6,6412
	Şifreli	7,9989	7,9988	7,9989	7,9977
	Çözülmüş	6,6979	6,6238	6,6747	6,6412

Tablo 4.5.(Devam) PHMMRGB görüntü şifreleme algoritmasının bilgi entropi analiz sonuçları

Görüntü Adı	Görüntü Tipi	Kırmızı	Yeşil	Mavi	Gri Tonlamalı
Melanoma 2	Orijinal	6,9630	6,8892	6,8347	6,8755
	Şifreli	7,9983	7,9983	7,9984	7,9974
	Çözülmüş	6,9630	6,8892	6,8347	6,8755
2K Görüntü	Orijinal	7,6989	7,7469	7,8386	7,6816
	Şifreli	7,9997	7,9997	7,9994	7,9997
	Çözülmüş	7,6989	7,7469	7,8386	7,6816
4K Görüntü	Orijinal	7,5416	7,0954	6,6616	7,4416
	Şifreli	7,9998	7,9998	7,9998	7,9998
	Çözülmüş	7,5416	7,0954	6,6616	7,4416
8K Görüntü	Orijinal	7,4595	7,4892	6,8090	7,4494
	Şifreli	7,9999	7,9999	7,9999	7,9999
	Çözülmüş	7,4595	7,4892	6,8090	7,4494
Lena (Zhu ve diğ., 2018)	Orijinal	-	-	-	-
	Şifreli	-	-	-	7,9977
	Çözülmüş	-	-	-	-
Lena (Narendra, 2012)	Orijinal	7,4451	7,4451	7,4451	7,4451
	Şifreli	7,7333	7,7333	7,7333	7,7333
	Çözülmüş	7,4451	7,4451	7,4451	7,4451
Lena Abdelfatah, 2020	Orijinal	-	-	-	-
	Şifreli	7,9999	7,9999	7,9999	7,9994
	Çözülmüş	-	-	-	-
Lena (Singh ve Singh, 2015)	Orijinal	-	-	-	-
	Şifreli	7,9998	7,9998	7,9998	-
	Çözülmüş	-	-	-	-
Baboon (Abdelfatah, 2020)	Orijinal	-	-	-	-
	Şifreli	7,9991	7,9991	7,9991	7,9994
	Çözülmüş	-	-	-	-
Baboon (Singh ve Singh, 2015)	Orijinal	-	-	-	-
	Şifreli	7,9988	7,9988	7,9988	-
	Çözülmüş	-	-	-	-

Tablo 4.5.(Devam) PHMMRGB görüntü şifreleme algoritmasının bilgi entropi analiz sonuçları

Görüntü Adı	Görüntü Tipi	Kırmızı	Yeşil	Mavi	Gri Tonlamalı
Baboon (Luo ve diğ., 2019)	Orijinal	-	-	-	-
	Şifreli	-	-	-	7,9993
	Çözülmüş	-	-	-	-
Lena (Luo ve diğ., 2019)	Orijinal	-	-	-	-
	Şifreli	-	-	-	7,9993
	Çözülmüş	-	-	-	-
Baboon (Narendra, 2012)	Orijinal	7,1839	7,1839	7,1839	7,1839
	Şifreli	7,7289	7,7289	7,7289	7,7289
	Çözülmüş	7,1839	7,1839	7,1839	7,1839
Aerial 1 (Liu ve diğ., 2019)	Orijinal	-	-	-	7,3424
	Şifreli	-	-	-	7,7289
	Çözülmüş	-	-	-	-
Aerial 3 (Liu ve diğ., 2019)	Orijinal	-	-	-	3,8595
	Şifreli	-	-	-	7,9993
	Çözülmüş	-	-	-	7,0000
Lena (Baagyere ve diğ., 2020)	Orijinal	-	-	-	-
	Şifreli	-	-	-	7,9987
	Çözülmüş	-	-	-	-
Lena (Enayatifar ve diğ., 2014)	Orijinal	-	-	-	-
	Şifreli	-	-	-	7,9997
	Çözülmüş	-	-	-	-
Lena (Wang ve diğ., 2011)	Orijinal	-	-	-	-
	Şifreli	-	-	-	7,9994
	Çözülmüş	-	-	-	-
Lena (Yousif ve diğ., 2020)	Orijinal	7,7503	7,7503	7,7503	7,4455
	Şifreli	7,9997	7,9997	7,9997	7,9993
	Çözülmüş	7,7503	7,7503	7,7503	7,4455

Tablo 4.5.(Devam) PHMMRGB görüntü şifreleme algoritmasının bilgi entropi analiz sonuçları

Görüntü Adı	Görüntü Tipi	Kırmızı	Yeşil	Mavi	Gri Tonlamalı
Baboon (Yousif ve diğ., 2020)	Orijinal	7,7624	7,7624	7,7624	7,3585
	Şifreli	7,9997	7,9997	7,9997	7,9993
	Çözülmüş	7,7624	7,7624	7,7624	7,3585

Tez kapsamında orijinal görüntü duyarlılığını ölçmek için kullanılan diferansiyel atak analizlerinden biri olan NPCR analiz sonuçları Tablo 4.6'da gösterilmektedir. NPCR analiz sonuçları incelendiğinde Lena, Baboon, Melanoma 1 ve Melanoma 2'nin %100 oranında tüm piksellerinin değiştiği, Airplane, Cameraman, 2K Görüntü, 4K Görüntü ve 8K Görüntü'nün ise 100 değerine çok yakın olduğu görülmektedir. Ayrıca veri setimizdeki tüm görüntüler referans (Wu ve diğ., 2011)'e göre (NPCR=%99.5710) testlerden başarı ile geçmiştir. Ayrıca referans (Narendra, 2012; Chai ve diğ., 2017; Khan ve diğ., 2020)'deki Lena görüntüsünün ve referans (Khan ve diğ., 2020)'deki Cameraman görüntüsünün NPCR testinden başarısız olduğu görülmektedir. PHMMRGB yönteminin, Tablo 4.6'daki referanslarda öne sürülen yöntemlerin NPCR analiz sonuçları ile karşılaştırıldığında yöntemimizin birçok çalışmadan daha iyi olduğu açıkça görülmektedir.

Tablo 4.6. PHMMRGB görüntü şifreleme algoritmasının NPCR analiz sonuçları

Görüntü Adı	NPCR [%]	Referans (Wu ve diğ., 2011)'e göre (Başarılı / Başarısız)
Lena	100,0000	Başarılı
Airplane	99,9996	Başarılı
Cameraman	99,6200	Başarılı
Baboon	100,0000	Başarılı
Melanoma 1	100,0000	Başarılı
Melanoma 2	100,0000	Başarılı
2K Görüntü	99,9974	Başarılı
4K Görüntü	99,9997	Başarılı
8K Görüntü	99,9847	Başarılı
Lena (Zhu ve diğ., 2018)	99,6323	Başarılı
Lena (Narendra, 2012)	99,1001	Başarısız

Tablo 4.6.(Devam) PHMMRGB görüntü şifreleme algoritmasının NPCR analiz sonuçları

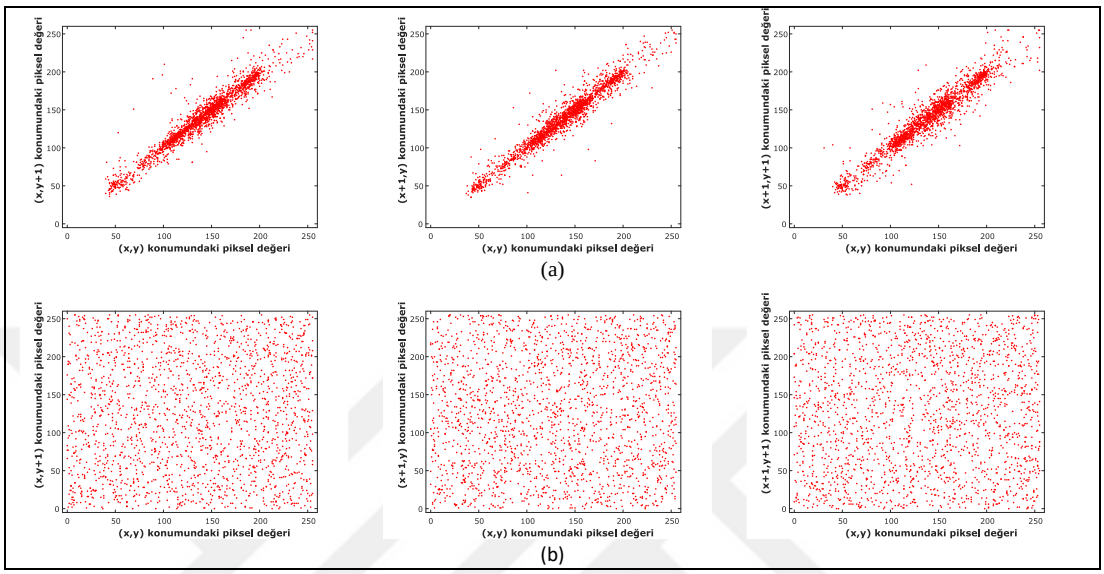
Görüntü Adı	NPCR [%]	Referans (Wu ve diğ., 2011)'e göre (Başarılı / Başarısız)
Lena (Maleki ve diğ., 2008)	99,5972	Başarılı
Baboon (Narendra, 2012)	99,4200	Başarısız
Aerial 1 (Liu ve diğ., 2019)	99,6235	Başarılı
Aerial 3 (Liu ve diğ., 2019)	99,6010	Başarılı
Lena (Singh ve Singh, 2015)	99,6204	Başarılı
Lena (Luo ve diğ., 2019)	99,6113	Başarılı
Lena (Sun, 2017)	99,6100	Başarılı
Lena (Chai ve diğ., 2017)	99,5700	Başarısız
Lena (Ye, 2014)	99,6000	Başarılı
Lena (Yong, 2018)	99,6094	Başarılı
Lena (Baagyere ve diğ., 2020)	99,8767	Başarılı
Lena (Enayatifar ve diğ., 2014)	99,9971	Başarılı
Lena (Wang ve diğ., 2011)	99,6427	Başarılı
Lena (Khan ve diğ., 2020)	90,1978	Başarısız
Cameraman (Khan ve diğ., 2020)	91,7114	Başarısız
Cameraman (Ibrahim ve Alharbi, 2020)	99,6292	Başarılı

Tablo 4.7' de diferansiyel atak analizlerinden UACI test sonuçları gösterilmektedir. UACI test sonuçları incelendiğinde veri setimizdeki tüm görüntülerin referans (Wu ve diğ., 2011)'e göre UACI (256x256 UACI=%33,2255, 512x512 UACI=%33,3445) testlerinden başarı ile geçmiştir. Bu sonuçlar doğrultusunda PHMMRGB görüntü şifreleme yönteminin diferansiyel ataklara karşı dirençli olduğu söylenebilir. Ayrıca referans (Narendra, 2012, Chai ve diğ., 2017; Baagyere ve diğ., 2020; Khan ve diğ., 2020)'deki Lena görüntüsünün, referans (Liu ve diğ., 2019)'daki Aerial 1 görüntüsünün ve (Khan ve diğ., 2020)'deki Cameraman görüntüsünün ise UACI testlerinden başarısız olduğu görülmektedir. PHMMRGB yönteminin, Tablo 4.7'de karşılaştırılan referanslarda öne sürülen yöntemlerin UACI analiz sonuçları ile karşılaştırıldığında yöntemimizin birçok çalışmadan daha iyi sonuçlar elde edildiği açıkça görülmektedir.

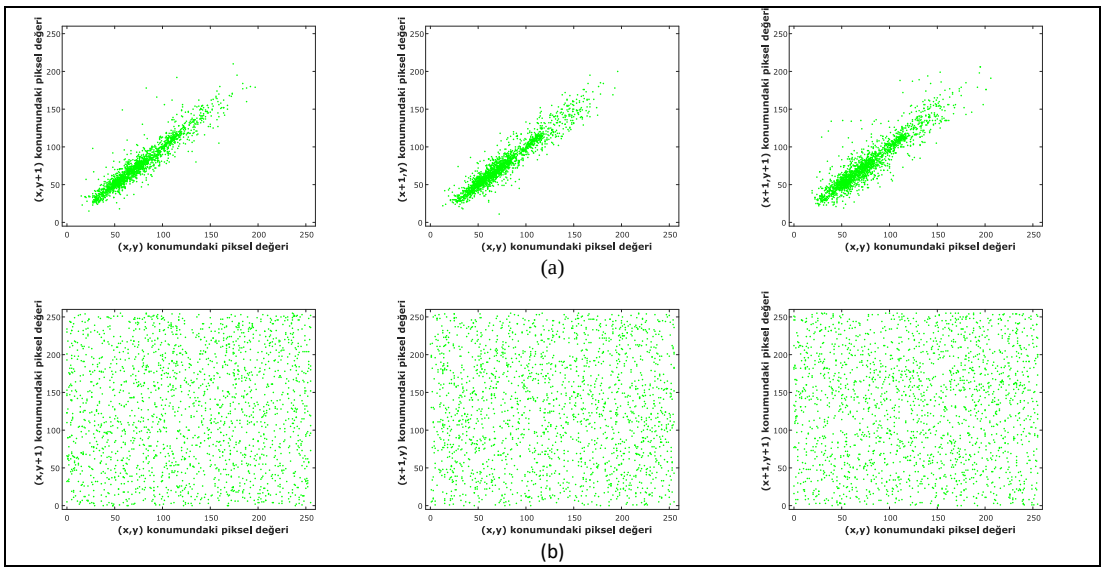
Tablo 4.7. PHMMRGB görüntü şifreleme algoritmasının UACI analiz sonuçları

Görüntü Adı	UACI [%]	Referans (Wu ve diğ., 2011)'e göre (Başarılı / Başarısız)
Lena	34,1192	Başarılı
Airplane	33,5091	Başarılı
Cameraman	36,7897	Başarılı
Baboon	33,5512	Başarılı
Melanoma 1	34,7576	Başarılı
Melanoma 2	33,7174	Başarılı
2K Görüntü	34,0016	Başarılı
4K Görüntü	33,7884	Başarılı
8K Görüntü	35,9451	Başarılı
Lena (Zhu ve diğ., 2018)	34,5960	Başarılı
Lena (Narendra, 2012)	33,2129	Başarısız
Lena (Maleki ve diğ., 2008)	33,3700	Başarılı
Baboon (Narendra, 2012)	33,2791	Başarılı
Aerial 1 (Liu ve diğ., 2019)	33,3371	Başarısız
Aerial 3 (Liu ve diğ., 2019)	33,4765	Başarılı
Lena (Singh ve Singh, 2015)	33,4898	Başarılı
Lena (Luo ve diğ., 2019)	33,4682	Başarılı
Lena (Sun, 2017)	33,3200	Başarılı
Lena (Chai ve diğ., 2017)	33,4100	Başarılı
Lena (Ye, 2014)	33,4400	Başarılı
Lena (Yong, 2018)	33,4635	Başarılı
Lena (Baagyere ve diğ., 2020)	18,1550	Başarısız
Lena (Enayatifar ve diğ., 2014)	33,6297	Başarılı
Lena (Wang ve diğ., 2011)	33,5615	Başarılı
Lena (Khan ve diğ., 2020)	30,0263	Başarısız
Cameraman (Khan ve diğ., 2020)	30,8406	Başarısız
Cameraman (Ibrahim ve Alharbi, 2020)	33,5387	Başarılı

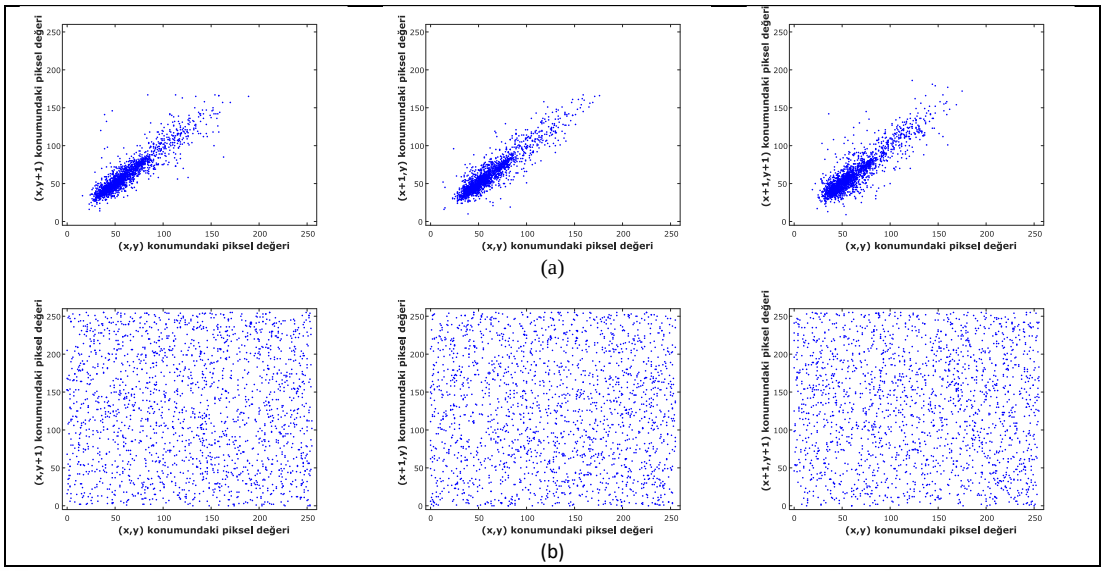
Tez kapsamında PHMMRGB görüntü şifreleme yöntemi kullanılarak Lena görüntüsüne ait 2000 adet yatay, dikey ve çapraz piksel komşulukları rastgele seçilmiş ve korelasyon analizi yapılmıştır. Korelasyon analizi kırmızı, yeşil ve mavi renk kanalı için sırasıyla Şekil 4.11, Şekil 4.12 ve Şekil 4.13'te gösterilmiştir.



Şekil 4.11. PHMMRGB yönteminde şifrelenen ve şifresi çözülen Lena görüntüsü için korelasyon katsayısının dağılımı: (a) Orijinal görüntünün bitişik piksellerinin yatay, dikey ve çapraz korelasyon katsayılarının kırmızı renk dağılımı. (b) Şifreli görüntünün bitişik piksellerinin yatay, dikey ve çapraz korelasyon katsayılarının kırmızı renk dağılımı



Şekil 4.12. PHMMRGB yönteminde şifrelenen ve şifresi çözülen Lena görüntüsü için korelasyon katsayısının dağılımı: (a) Orijinal görüntünün bitişik piksellerinin yatay, dikey ve çapraz korelasyon katsayılarının yeşil renk dağılımı. (b) Şifreli görüntünün bitişik piksellerinin yatay, dikey ve çapraz korelasyon katsayılarının yeşil renk dağılımı



Şekil 4.13. PHMMRGB yönteminde şifrelenen ve şifresi çözülen Lena görüntüsü için korelasyon katsayısının dağılımı: (a) Orijinal görüntünün bitişik piksellerinin yatay, dikey ve çapraz korelasyon katsayılarının mavi renk dağılımı. (b) Şifreli görüntünün bitişik piksellerinin yatay, dikey ve çapraz korelasyon katsayılarının kırmızı renk dağılımı

Şifre 4.11(a), Şekil 4.12(a) ve Şekil 4.13(a) görüntünün korelasyon katsayıların dağılımının doğrusal olduğu, Şifre 4.11(b), Şekil 4.12(b) ve Şekil 4.13(b)'de ise rastgele dağınık bir yapıya sahip olduğu gözlemlenmektedir. Bununla birlikte Tablo 4.8'de korelasyon katsayılarının detaylı incelendiğinde veri setimizdeki orijinal görüntülerin korelasyon katsayısının 1'e yakın, buna karşılık şifrelenmiş görüntülerin korelasyon katsayılarının da 0'a çok yakın olduğu görülmektedir. Bu sonuçlar dikkate alındığında önerilen PHMMRGB yönteminin komşu pikseller arasındaki ilişkiyi 0'a yakın hale getirdiği ve başarılı sonuçlar verdiği söylenebilir. PHMMRGB yönteminin, Tablo 4.8'de karşılaştırılan referanslarda öne sürülen yöntemlerin analiz sonuçları ile kıyaslandığında birçok çalışmadan daha iyi sonuçların elde edildiği açıkça görülmektedir.

Tablo 4.8. PHMMRGB görüntü şifreleme algoritmasının korelasyon analiz sonuçları

Ad	Tip	Yatay			Dikey			Çapraz		
		Kırmızı	Yeşil	Mavi	Kırmızı	Yeşil	Mavi	Kırmızı	Yeşil	Mavi
Lena	Orj	0,9765	0,9679	0,9487	0,9836	0,9700	0,9634	0,9680	0,9471	0,9288
	Şif	-0,0369	0,0126	0,0368	0,0401	-0,0014	-0,0145	0,0155	-0,0421	-0,0398
Airplane	Orj	0,9603	0,9687	0,9497	0,9696	0,9668	0,9421	0,9407	0,9425	0,9094
	Şif	0,0393	0,0388	0,0606	0,0489	0,0793	0,0582	0,0673	0,0767	0,0464
Cameraman	Orj	0,9403	0,9289	0,9336	0,9676	0,9616	0,9668	0,9121	0,8988	0,9158
	Şif	0,0083	0,0141	0,0012	-0,0136	0,0178	-0,0376	-0,0027	0,0064	0,0199
Baboon	Orj	0,9275	0,8472	0,9094	0,8704	0,7617	0,8784	0,8608	0,7346	0,8410
	Şif	-0,0339	0,0277	0,0087	-0,0023	0,0060	0,0127	0,0241	0,0006	-0,0083

Tablo 4.8.(Devam) PHMMRGB görüntü şifreleme algoritmasının korelasyon analiz sonuçları

Ad	Tip	Yatay			Dikey			Çapraz		
		Kırmızı	Yeşil	Mavi	Kırmızı	Yeşil	Mavi	Kırmızı	Yeşil	Mavi
Melanoma 1	Orj	0,9911	0,9831	0,9756	0,9948	0,9907	0,9847	0,9884	0,9785	0,9679
	Şif	-0,0396	0,0048	0,0188	-0,0398	0,0107	0,0056	0,0029	-0,0180	0,0194
Melanoma 2	Orj	0,9943	0,9930	0,9914	0,9951	0,9938	0,9928	0,9915	0,9904	0,9873
	Şif	-0,0110	-0,0344	0,0276	0,0165	0,0106	-0,0018	0,0362	0,0235	-0,0154
2K Image	Orj	0,9789	0,9773	0,9824	0,9743	0,9702	0,9820	0,9628	0,9602	0,9739
	Şif	-0,0198	0,0130	0,0324	0,0058	0,0050	0,0290	0,0278	-0,0342	0,0121
4K Image	Orj	0,9969	0,9977	0,9985	0,9978	0,9983	0,9990	0,9968	0,9975	0,9982
	Şif	-0,0214	-0,0269	-0,0382	-0,0191	-0,0139	0,0205	0,0475	0,0318	0,0091
8K Image	Orj	0,9574	0,9497	0,9448	0,9488	0,9496	0,9343	0,9089	0,9115	0,8929
	Şif	0,0436	-0,0231	0,0422	-0,0405	-0,0239	0,0048	-0,0150	-0,0090	0,0059
Lena (Zhu ve diğ., 2018)	Orj	0,9249	0,9249	0,9249	-	-	-	-	-	-
	Şif	0,0002	0,0002	0,0002	-	-	-	-	-	-
Lena (Narendra, 2012)	Orj	0,9608	0,9845	0,9850	-	-	-	-	-	-
	Şif	0,0489	-0,0624	-0,0666	-	-	-	-	-	-
Lena (Maleki ve diğ., 2008)	Orj	0,9677	0,9677	0,9677	0,9366	0,9366	0,9366	0,9168	0,9168	0,9168
	Şif	0,0428	0,0428	0,0428	0,0217	0,0217	0,0217	0,0005	0,0005	0,0005
Aerial 1 (Liu ve diğ., 2019)	Orj	0,9473	0,9473	0,9473	0,8963	0,8963	0,8963	0,8472	0,8472	0,8472
	Şif	0,0017	0,0017	0,0017	0,0153	0,0153	0,0153	0,0046	0,0046	0,0046
Aerial 3 (Liu ve diğ., 2019)	Orj	0,7633	0,7633	0,7633	0,6178	0,6178	0,6178	0,5698	0,5698	0,5698
	Şif	0,0107	0,0107	0,0107	0,0181	0,0181	0,0181	0,0022	0,0022	0,0022
Lena (Abdelfatah, 2020)	Orj	0,9959	0,9944	0,9876	0,9886	0,9847	0,9707	0,9931	0,9906	0,9810
	Şif	-0,0015	-0,0015	-0,0014	0,0006	-0,0007	-0,00004	-0,0009	-0,0014	-0,0001
Baboon (Abdelfatah, 2020)	Orj	0,9011	0,7957	0,8915	0,8829	0,7510	0,8510	0,9351	0,8404	0,9023
	Şif	0,0015	-0,0015	0,0038	0,0064	-0,0005	0,0014	0,0001	-0,0034	0,0030
Lena (Kumar ve diğ., 2016)	Orj	0,9326	0,9222	0,8938	0,9624	0,9546	0,9343	0,9070	0,8804	0,8634
	Şif	0,0035	-0,0097	0,0185	0,0040	0,0053	0,0106	-0,0410	-0,0085	-0,0170
Baboon (Kumar ve diğ., 2016)	Orj	0,9280	0,8625	0,9087	0,8650	0,7697	0,8859	0,8538	0,7256	0,8427
	Şif	0,0186	0,0066	0,0067	-0,0060	0,0164	0,0012	-0,0013	0,0092	0,0172
Lena (Luo ve diğ., 2019)	Orj	0,9858	-	-	0,9801	-	-	0,9669	-	-
	Şif	0,0019	-	-	-0,0024	-	-	-0,0011	-	-
Baboon (Luo ve diğ., 2019)	Orj	0,7251	-	-	0,8558	-	-	0,6920	-	-
	Şif	0,0024	-	-	0,0011	-	-	-0,0008	-	-
Lena (Liu ve diğ., 2018)	Orj	0,9325	-	-	0,9139	-	-	0,9469	-	-
	Şif	0,0074	-	-	-0,0094	-	-	-0,0054	-	-

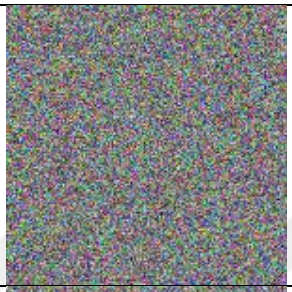
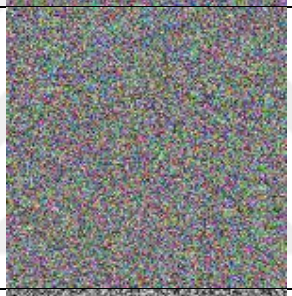
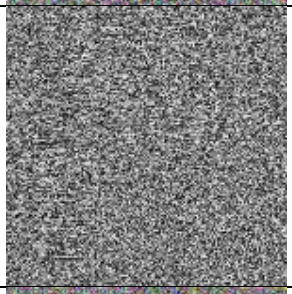
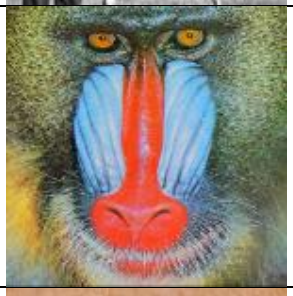
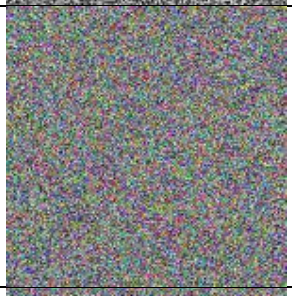
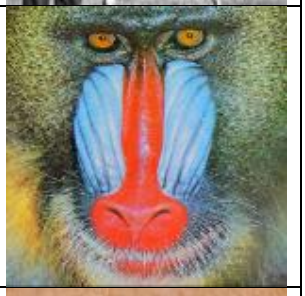
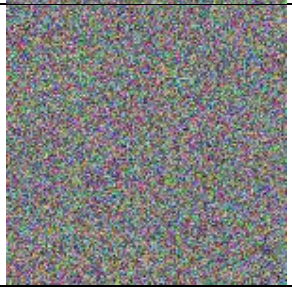
Tablo 4.8.(Devam) PHMMRGB görüntü şifreleme algoritmasının korelasyon analiz sonuçları

Ad	Tip	Yatay			Dikey			Çapraz		
		Kırmızı	Yeşil	Mavi	Kırmızı	Yeşil	Mavi	Kırmızı	Yeşil	Mavi
Lena (Ye ve diğ., 2017)	Orj	0,9771	-	-	0,9631	-	-	0,9469	-	-
	Şif	0,0925	-	-	0,0430	-	-	-0,0054	-	-
Lena (Xu ve diğ., 2017)	Orj	0,9503	-	-	0,9755	-	-	0,9275	-	-
	Şif	-0,0226	-	-	0,0041	-	-	0,0368	-	-
Baboon (Chai ve diğ., 2017)	Orj	0,7508	-	-	0,8562	-	-	0,7153	-	-
	Şif	-0,0061	-	-	0,0130	-	-	0,0017	-	-
Lena (Baagyere ve diğ.,	Orj	0,8319	-	-	0,9236	-	-	0,7814	-	-
	Şif	0,0099	-	-	0,0031	-	-	0,0002	-	-
Lena (Enayatifar ve diğ., 2014)	Orj	-	-	-	-	-	-	-	-	-
	Şif	0,0170	-	-	0,0007	-	-	0,0001	-	-
Lena (Wang ve diğ., 2011)	Orj	-	-	-	-	-	-	-	-	-
	Şif	0,0007	-	-	-0,0022	-	-	0,0149	-	-
Lena (Yousif ve diğ., 2020)	Orj	0,9818	-	-	0,9903	-	-	0,9698	-	-
	Şif	-0,0021	-	-	-0,0030	-	-	-0,0177	-	-
Baboon (Yousif ve diğ., 2020)	Orj	0,9214	-	-	0,8663	-	-	0,8510	-	-
	Şif	-0,0081	-	-	-0,0011	-	-	-0,0065	-	-
Cameraman (Yousif ve diğ., 2020)	Orj	0,9828	-	-	0,9898	-	-	0,9723	-	-
	Şif	-0,0097	-	-	-0,0021	-	-	-0,0080	-	-
Airplane (Yousif ve diğ., 2020)	Orj	0,9727	-	-	0,9517	-	-	0,9362	-	-
	Şif	-0,0206	-	-	-0,0086	-	-	-0,0099	-	-
Lena (Khan ve diğ., 2020)	Orj	0,8841	-	-	0,9463	-	-	0,8430	-	-
	Şif	-0,0041	-	-	-0,0037	-	-	-0,0065	-	-
Cameraman (Khan ve diğ., 2020)	Orj	0,8563	-	-	0,8970	-	-	0,8090	-	-
	Şif	-0,0015	-	-	-0,0143	-	-	-0,0236	-	-

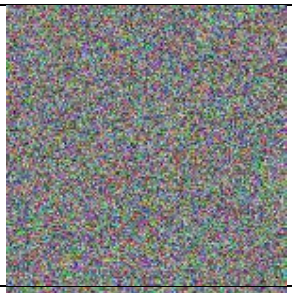
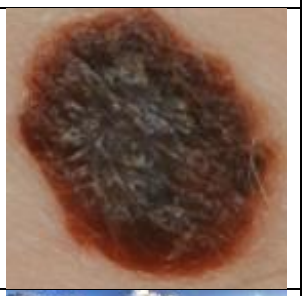
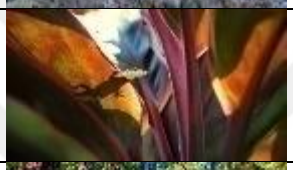
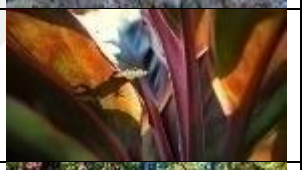
4.3.2. ProbRGB yöntemine ait sonuçlar

Görüntü şifreleme uygulamasında ProbRGB görüntü şifreleme algoritması seçilerek elde edilen sonuçlar Tablo 4.9'da gösterilmektedir.

Tablo 4.9. ProbRGB görüntü şifreleme algoritmasının şifreleme ve şifre çözme sonuçları

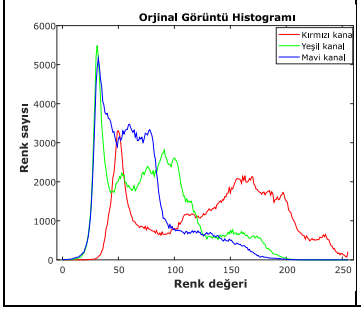
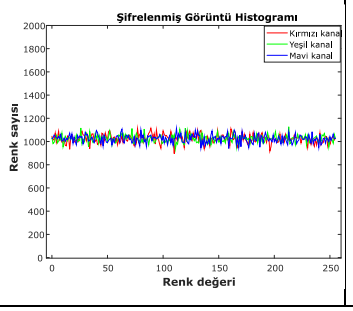
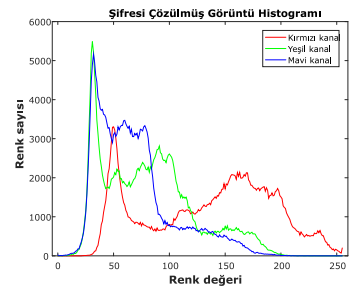
Görüntü Adı	Orijinal Görüntü	Şifreli Görüntü	Şifresi Çözülmüş Görüntü
Lena			
Airplane			
Cameraman			
Baboon			
Melanoma 1			

Tablo 4.9.(Devam) ProbRGB görüntü şifreleme algoritmasının şifreleme ve şifre çözme sonuçları

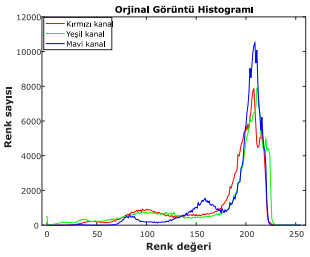
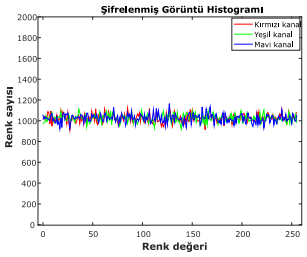
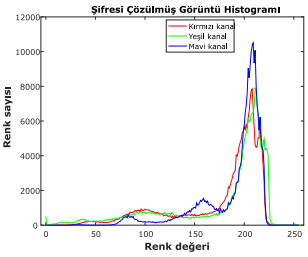
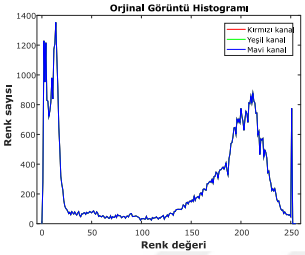
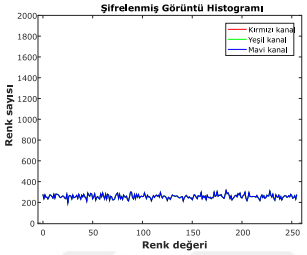
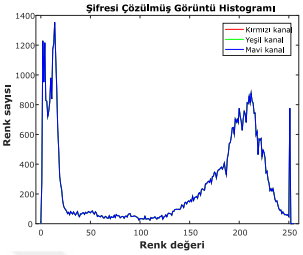
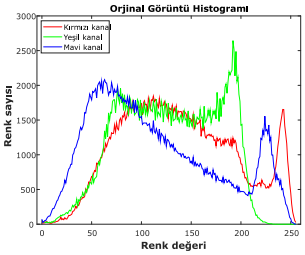
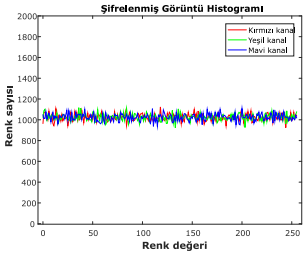
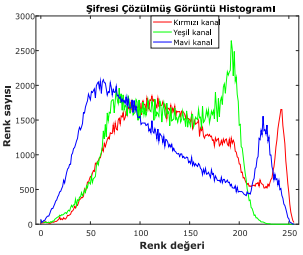
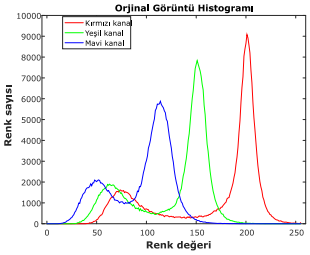
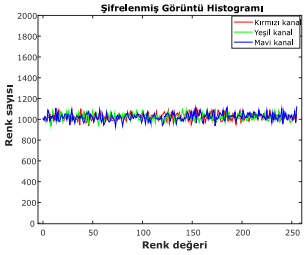
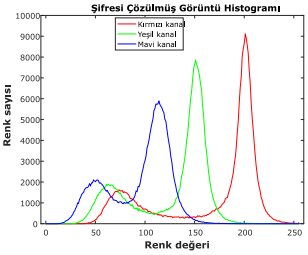
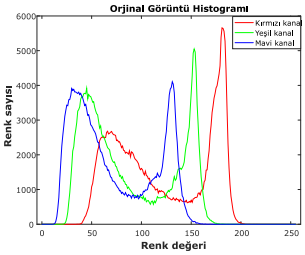
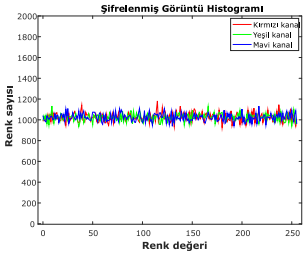
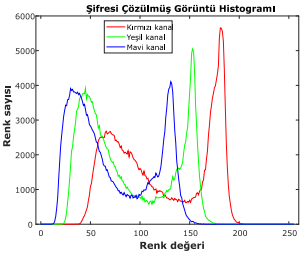
Görüntü Adı	Orijinal Görüntü	Şifreli Görüntü	Şifresi Çözülmüş Görüntü
Melanoma 2			
2K Görüntü			
4K Görüntü			
8K Görüntü			

ProbRGB görüntü şifreleme yöntemi uygulanarak şifreleme yapıldığında histogram analiz sonuçları Tablo 4.10'da gösterilmektedir. Histogram analizleri sonucunda şifrelenmiş görüntülerdeki piksel değerlerinin homojen dağıldığı gözlemlenmektedir. Dolayısı ile istatistiksel saldırılara karşı dayanaklı olduğu söylenebilir.

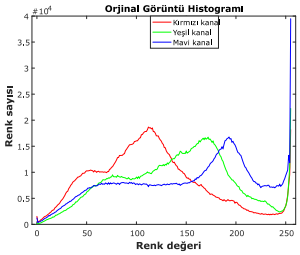
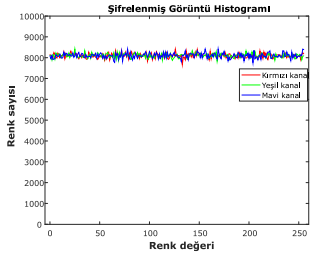
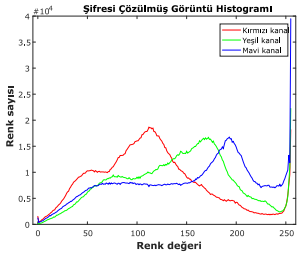
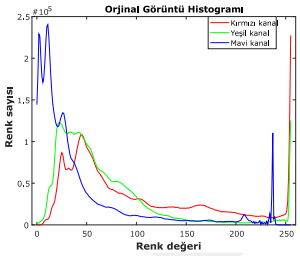
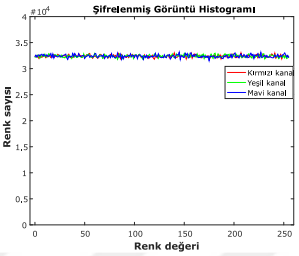
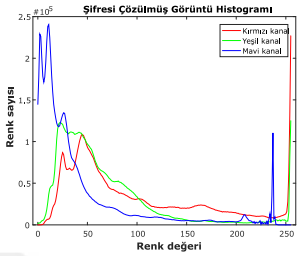
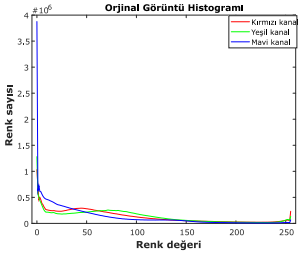
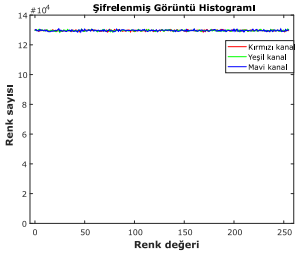
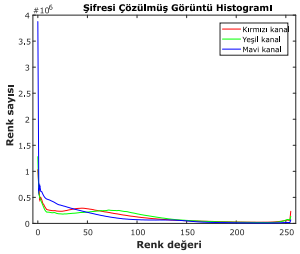
Tablo 4.10. ProbRGB görüntü şifreleme algoritmasının histogram analiz sonuçları

Orijinal Görüntü Histogramı	Şifreli Görüntü Histogramı	Şifresi Çözülmüş Görüntü Histogramı
Lena	Lena	Lena
		

Tablo 4.10.(Devam) ProbRGB görüntü şifreleme algoritmasının histogram analiz sonuçları

Orijinal Görüntü Histogramı	Şifreli Görüntü Histogramı	Şifresi Çözülmüş Görüntü Histogramı
Airplane	Airplane	Airplane
		
Cameraman	Cameraman	Cameraman
		
Baboon	Baboon	Baboon
		
Melanoma 1	Melanoma 1	Melanoma 1
		
Melanoma 2	Melanoma 2	Melanoma 2
		

Tablo 4.10. ProbRGB görüntü şifreleme algoritmasının histogram analiz sonuçları

Orijinal Görüntü Histogramı	Şifreli Görüntü Histogramı	Şifresi Çözülmüş Görüntü Histogramı
2K Görüntü	2K Görüntü	2K Görüntü
		
4K Görüntü	4K Görüntü	4K Görüntü
		
8K Görüntü	8K Görüntü	8K Görüntü
		

ProbRGB görüntü şifreleme algoritması için MAE ve MSE sonuçları incelendiğinde tüm görüntüler için sonuç sıfırdır. Bu durum orijinal görüntü ile şifresi çözülen görüntü arasında herhangi bir bozulma olmadığını ve görüntünün kayıpsız olarak geri döndürülebildiğini göstermektedir.

Bu yöntem için PSNR analiz sonuçları analiz edildiğinde tüm görüntüler için MSE değerleri sıfır olduğundan PSNR değerleri de eksi sonsuzdur. Bu sonuç orijinal görüntüler ile şifresi çözülen görüntüler arasında kalite farkı olmadığını göstermektedir.

Tez kapsamında ProbRGB yöntemi için orijinal görüntü ile şifrelenmiş görüntünün ve orijinal görüntü ile şifresi çözülmüş görüntünün yapısal benzerlik sonuçları Tablo 4.11'de gösterilmiştir. Yapısal benzerlik analiz sonuçları incelendiğinde orijinal

görüntü ile şifreli görüntü arasındaki yapısal benzerliğin sıfıra yakın olduğu görülmektedir. Ayrıca orijinal görüntü ile şifresi çözülmüş görüntünün yapısal benzerliği bir olarak tespit edilmiştir. Bu sonuç görüntünün şifrelendikten sonra kayıpsız bir şekilde orijinal görüntüyü elde ettiğimizi ifade etmektedir.

Tablo 4.11. ProbRGB görüntü şifreleme algoritmasının yapısal benzerlik analiz sonuçları

Görüntü Adı	Orijinal Görüntü ve Şifrelenmiş Görüntü arasındaki SSIM	Orijinal Görüntü ve Şifresi Çözülmüş Görüntü arasındaki SSIM
Lena	0,0060	1,0000
Airplane	0,0071	1,0000
Cameraman	0,0032	1,0000
Baboon	0,0071	1,0000
Melanoma 1	0,0098	1,0000
Melanoma 2	0,0142	1,0000
2K Görüntü	0,0070	1,0000
4K Görüntü	0,0060	1,0000
8K Görüntü	0,0051	1,0000

Tez kapsamında şifrelenmiş görüntünün karmaşıklığını ölçmek için kullanılan bilgi entropi testinin sonuçları Tablo 4.12'de gösterilmektedir. Sonuçlar incelendiğinde veri setimizde kullanılan görüntülerin şifreleme işleminden sonraki bilgi entropi sonuçlarının, ideal entropi değeri olan 8'e çok yakın olduğu gözükmektedir. Bu sayede şifreli görüntülerdeki rastgelelik ve düzensizliğin istenilen seviyede olduğu söylenebilir. ProbRGB yönteminin, Tablo 4.12'de karşılaştırılan referanslarda öne sürülen yöntemlerin analiz sonuçları ile karşılaştırıldığında birçok çalışmadan daha iyi sonuçların elde edildiği açıkça görülmektedir.

Tablo 4.12. ProbRGB görüntü şifreleme algoritmasının bilgi entropi analiz sonuçları

Görüntü Adı	Görüntü Tipi	Kırmızı	Yeşil	Mavi	Gri Tonlamalı
Lena	Orijinal	7,5805	7,1336	6,8448	7,5805
	Şifreli	7,9990	7,9992	7,9992	7,9990
	Çözülmüş	7,5805	7,1336	6,8448	7,5805

Tablo 4.12.(Devam) ProbRGB görüntü şifreleme algoritmasının bilgi entropi analiz sonuçları

Görüntü Adı	Görüntü Tipi	Kırmızı	Yeşil	Mavi	Gri Tonlamalı
Airplane	Orijinal	6,7177	6,7989	6,2137	6,2137
	Şifreli	7,9990	7,9991	7,9989	7,9989
	Çözülmüş	6,7177	6,7989	6,2137	6,2137
Cameraman	Orijinal	7,2074	7,2074	7,2074	7,2074
	Şifreli	7,9960	7,9960	7,9960	7,9960
	Çözülmüş	7,2074	7,2074	7,2074	7,2074
Baboon	Orijinal	7,7066	7,4744	7,7522	7,7066
	Şifreli	7,9992	7,9992	7,9992	7,9992
	Çözülmüş	7,7066	7,4744	7,7522	7,7066
Melanoma 1	Orijinal	6,6979	6,6238	6,6747	6,6979
	Şifreli	7,9993	7,9993	7,9991	7,9993
	Çözülmüş	6,6979	6,6238	6,6747	6,6979
Melanoma 2	Orijinal	6,9630	6,8892	6,8346	6,9692
	Şifreli	7,9989	7,9991	7,9990	7,9990
	Çözülmüş	6,9630	6,8892	6,8346	6,9692
2K Görüntü	Orijinal	7,6989	7,7469	7,8386	7,7469
	Şifreli	7,9998	7,9998	7,9998	7,9998
	Çözülmüş	7,6989	7,7469	7,8386	7,7469
4K Görüntü	Orijinal	7,5416	7,0954	6,6616	7,0954
	Şifreli	7,9999	7,9999	7,9999	7,9999
	Çözülmüş	7,5416	7,0954	6,6616	7,0954
8K Görüntü	Orijinal	7,4595	7,4892	6,8090	7,4592
	Şifreli	7,9999	7,9999	7,9999	7,9999
	Çözülmüş	7,4595	7,4892	6,8090	7,4592
Lena (Gri) (Narendra, 2012)	Orijinal	-	-	-	-
	Şifreli	-	-	-	7,9977
	Çözülmüş	-	-	-	-

Tablo 4.12.(Devam) ProbRGB görüntü şifreleme algoritmasının bilgi entropi analiz sonuçları

Görüntü Adı	Görüntü Tipi	Kırmızı	Yeşil	Mavi	Gri Tonlamalı
Lena (Narendra, 2012)	Orijinal	7,4451	7,4451	7,4451	7,4451
	Şifreli	7,7333	7,7333	7,7333	7,7333
	Çözülmüş	7,4451	7,4451	7,4451	7,4451
Baboon (Narendra, 2012)	Orijinal	7,1839	7,1839	7,1839	7,1839
	Şifreli	7,7289	7,7289	7,7289	7,7289
	Çözülmüş	7,1839	7,1839	7,1839	7,1839
Lena (Abdelfatah, 2020)	Orijinal	-	-	-	-
	Şifreli	7,9999	7,9999	7,9999	7,9994
	Çözülmüş	-	-	-	-
Lena (Singh ve Singh, 2015)	Orijinal	-	-	-	-
	Şifreli	7,9998	7,9998	7,9998	-
	Çözülmüş	-	-	-	-
Baboon (Abdelfatah, 2020)	Orijinal	-	-	-	-
	Şifreli	7,9991	7,9991	7,9991	7,9994
	Çözülmüş	-	-	-	-
Baboon (Singh ve Singh, 2015)	Orijinal	-	-	-	-
	Şifreli	7,9988	7,9988	7,9988	-
	Çözülmüş	-	-	-	-
Baboon (Gri) (Luo ve diğ., 2019)	Orijinal	-	-	-	-
	Şifreli	-	-	-	7,9993
	Çözülmüş	-	-	-	-
Lena (Gri) (Luo ve diğ., 2019)	Orijinal	-	-	-	-
	Şifreli	-	-	-	7,9993
	Çözülmüş	-	-	-	-
Aerial 1 (Liu ve diğ., 2019)	Orijinal	-	-	-	7,3424
	Şifreli	-	-	-	7,7289
	Çözülmüş	-	-	-	-

Tablo 4.12.(Devam) ProbRGB görüntü şifreleme algoritmasının bilgi entropi analiz sonuçları

Görüntü Adı	Görüntü Tipi	Kırmızı	Yeşil	Mavi	Gri Tonlamalı
Aerial 3 (Liu ve diğ., 2019)	Orijinal	-	-	-	3,8595
	Şifreli	-	-	-	7,9993
	Çözülmüş	-	-	-	7,0000
Lena (Gri) (Baagyere ve diğ., 2020)	Orijinal	-	-	-	-
	Şifreli	-	-	-	7,9987
	Çözülmüş	-	-	-	-
Lena (Gri) (Enayatifar ve diğ., 2014)	Orijinal	-	-	-	-
	Şifreli	-	-	-	7,9997
	Çözülmüş	-	-	-	-
Lena (Gri) (Wang ve diğ., 2011)	Orijinal	-	-	-	-
	Şifreli	-	-	-	7,9994
	Çözülmüş	-	-	-	-
Lena (Yousif ve diğ., 2020)	Orijinal	7,7503	7,7503	7,7503	7,4455
	Şifreli	7,9997	7,9997	7,9997	7,9993
	Çözülmüş	7,7503	7,7503	7,7503	7,4455
Baboon (Yousif ve diğ., 2020)	Orijinal	7,7624	7,7624	7,7624	7,3585
	Şifreli	7,9997	7,9997	7,9997	7,9993
	Çözülmüş	7,7624	7,7624	7,7624	7,3585

Tez kapsamında orijinal görüntü duyarlılığını ölçmek için kullanılan diferansiyel atak analizlerinden biri olan NPCR test sonuçları Tablo 4.13'te gösterilmektedir. NPCR test sonuçları incelendiğinde Lena, Baboon, Melanoma 1 ve Melanoma 2'nin %100 oranında tüm piksellerinin değiştiği, Airplane, Cameraman, 2K Görüntü, 4K Görüntü ve 8K Görüntü'nün ise 100 değerine çok yakın olduğu görülmektedir. Ayrıca veri setimizdeki tüm görüntüler referans (Wu ve diğ., 2011)'e göre (NPCR=%99,5710) testlerden başarı ile geçmiştir. Ayrıca referans (Narendra, 2012; Chai ve diğ., 2017; Khan ve diğ., 2020)'deki Lena görüntüsünün ve referans (Khan ve diğ., 2020)'deki Cameraman görüntüsünün NPCR testinden başarısız olduğu görülmektedir. PHMMRGB yönteminin, Tablo 4.13'daki referanslarda öne sürülen yöntemlerin

NPCR analiz sonuçları ile karşılaştırıldığında yöntemimizin birçok çalışmadan daha iyi olduğu açıkça görülmektedir.

Tablo 4.13. ProbRGB görüntü şifreleme algoritmasının NPCR analiz sonuçları

Görüntü Adı	NPCR [%]	Referans (Wu ve diğ., 2011)'e göre (Başarılı / Başarısız)
Lena	100,0000	Başarılı
Airplane	99,9988	Başarılı
Cameraman	99,9788	Başarılı
Baboon	100,0000	Başarılı
Melanoma 1	100,0000	Başarılı
Melanoma 2	100,0000	Başarılı
2K Görüntü	99,9981	Başarılı
4K Görüntü	99,9998	Başarılı
8K Görüntü	99,9847	Başarılı
Lena (Zhu ve diğ., 2018)	99,6323	Başarılı
Lena (Narendra, 2012)	99,1001	Başarısız
Lena (Maleki ve diğ., 2008)	99,5972	Başarılı
Baboon (Narendra, 2012)	99,4200	Başarısız
Aerial 1 (Liu ve diğ., 2019)	99,6235	Başarılı
Aerial 3 (Liu ve diğ., 2019)	99,6010	Başarılı
Lena (Abdelfatah, 2020)	99,6204	Başarılı
Lena (Luo ve diğ., 2019)	99,6113	Başarılı
Lena (Sun, 2017)	99,6100	Başarılı
Lena (Chai ve diğ., 2017)	99,5700	Başarısız
Lena (Ye, 2014)	99,6000	Başarılı
Lena (Yong, 2018)	99,6094	Başarılı
Lena (Baagyere ve diğ., 2020)	99,8767	Başarılı
Lena (Enayatifar ve diğ., 2014)	99,9971	Başarılı
Lena (Wang ve diğ., 2011)	99,6427	Başarılı
Lena (Khan ve diğ., 2020)	90,1978	Başarısız

Tablo 4.13.(Devam) ProbRGB görüntü şifreleme algoritmasının NPCR analiz sonuçları

Görüntü Adı	NPCR [%]	Referans (Wu ve diğ., 2011)'e göre (Başarılı / Başarısız)
Cameraman (Khan ve diğ., 2020)	91,7114	Başarısız
Cameraman (Ibrahim ve Alharbi, 2020)	99,6292	Başarılı

Tablo 4.14'te diferansiyel atak analizlerinden UACI test sonuçları gösterilmektedir. UACI test sonuçları incelendiğinde veri setimizdeki tüm görüntülerin referans (Wu ve diğ., 2011)'e göre (256x256 UACI=%33,2255, 512x512 UACI=%33,3445) testlerden başarı ile geçmiştir. Bu sonuçlar doğrultusunda önerdiğimiz. Ayrıca referans (Narendra, 2012, Chai ve diğ., 2017; Baagyere ve diğ., 2020; Khan ve diğ., 2020)'deki Lena görüntüsünün, referans (Liu ve diğ., 2019)'daki Aerial 1 görüntüsünün ve (Khan ve diğ., 2020)'deki Cameraman görüntüsünün ise UACI testlerinden başarısız olduğu görülmektedir. ProbRGB yönteminin, Tablo 4.14'te karşılaştırılan referanslarda öne sürülen yöntemlerin UACI analiz sonuçları ile karşılaştırıldığında yöntemimizin birçok çalışmadan daha iyi sonuçlar elde edildiği açıkça görülmektedir.

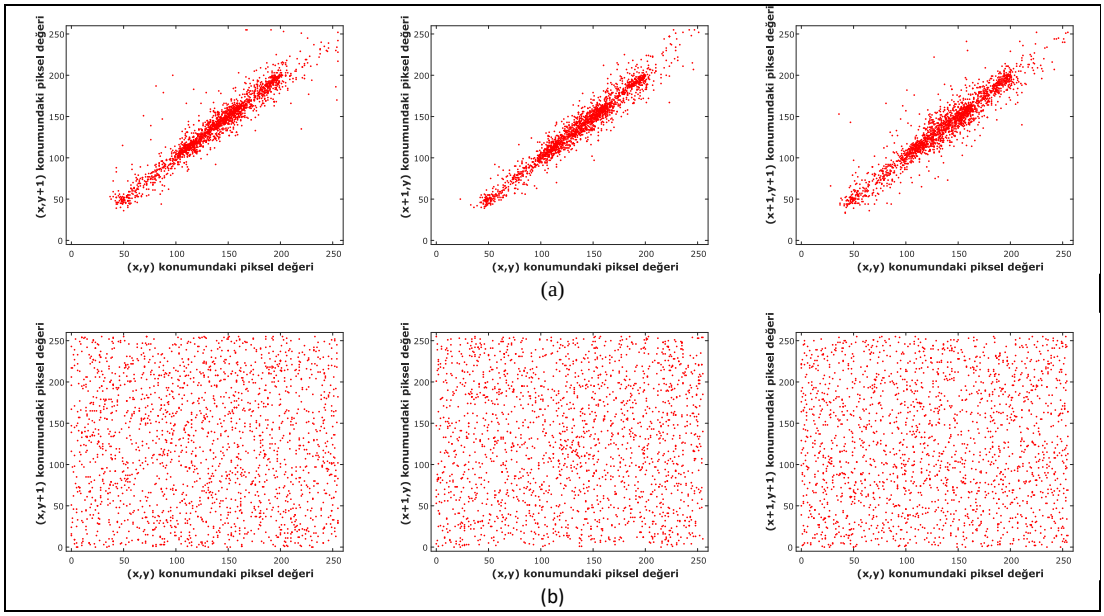
Tablo 4.14. ProbRGB görüntü şifreleme algoritmasının UACI analiz sonuçları

Görüntü Adı	UACI [%]	Referans (Wu ve diğ., 2011)'e göre (Başarılı / Başarısız)
Lena	34,1042	Başarılı
Airplane	33,9901	Başarılı
Cameraman	36,9231	Başarılı
Baboon	33,9524	Başarılı
Melanoma 1	33,6654	Başarılı
Melanoma 2	33,5459	Başarılı
2K Görüntü	34,9876	Başarılı
4K Görüntü	33,7898	Başarılı
8K Görüntü	35,9476	Başarılı
Lena (Zhu ve diğ., 2018)	34,5960	Başarılı
Lena (Narendra, 2012)	33,2129	Başarısız
Lena (Maleki ve diğ., 2008)	33,3700	Başarılı
Baboon (Narendra, 2012)	33,2791	Başarılı
Aerial 1 (Liu ve diğ., 2019)	33,3371	Başarısız
Aerial 3 (Liu ve diğ., 2019)	33,4765	Başarılı

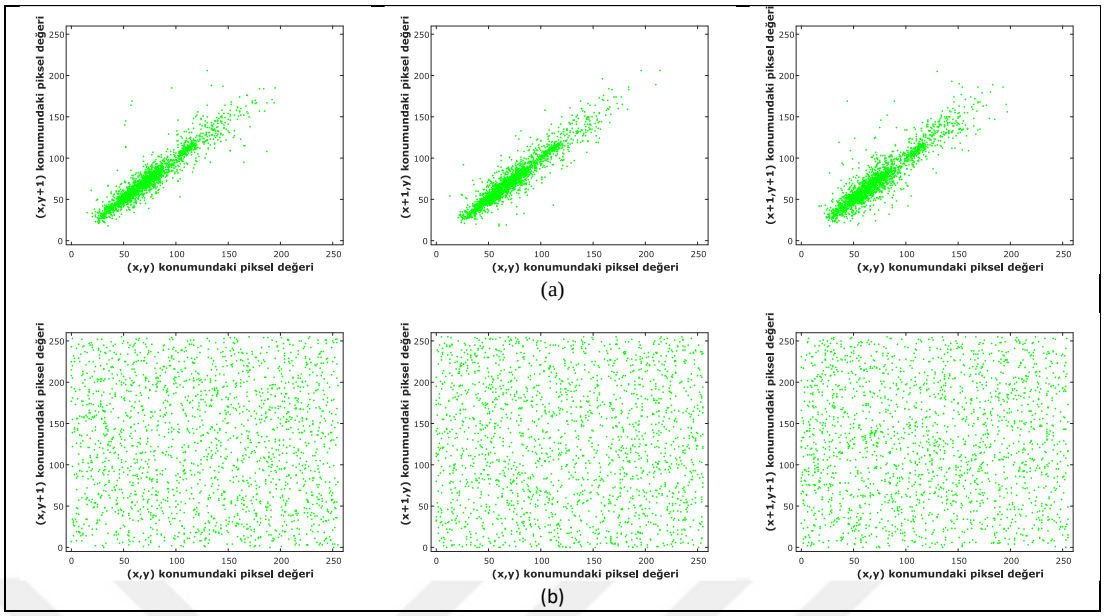
Tablo 4.14.(Devam) ProbRGB görüntü şifreleme algoritmasının UACI analiz sonuçları

Görüntü Adı	UACI [%]	Referans (Wu ve diğ., 2011)'e göre (Başarılı / Başarısız)
Lena (Abdelfatah, 2020)	33,4898	Başarılı
Lena (Luo ve diğ., 2019)	33,4682	Başarılı
Lena (Sun, 2017)	33,3200	Başarılı
Lena (Chai ve diğ., 2017)	33,4100	Başarılı
Lena (Ye, 2014)	33,4400	Başarılı
Lena (Yong, 2018)	33,4635	Başarılı
Lena (Baagyere ve diğ., 2020)	18,1550	Başarısız
Lena (Enayatifar ve diğ., 2014)	33,6297	Başarılı
Lena (Wang ve diğ., 2011)	33,5615	Başarılı
Lena (Khan ve diğ., 2020)	30,0263	Başarısız
Cameraman (Khan ve diğ., 2020)	30,8406	Başarısız
Cameraman (Ibrahim ve Alharbi, 2020)	33,5387	Başarılı

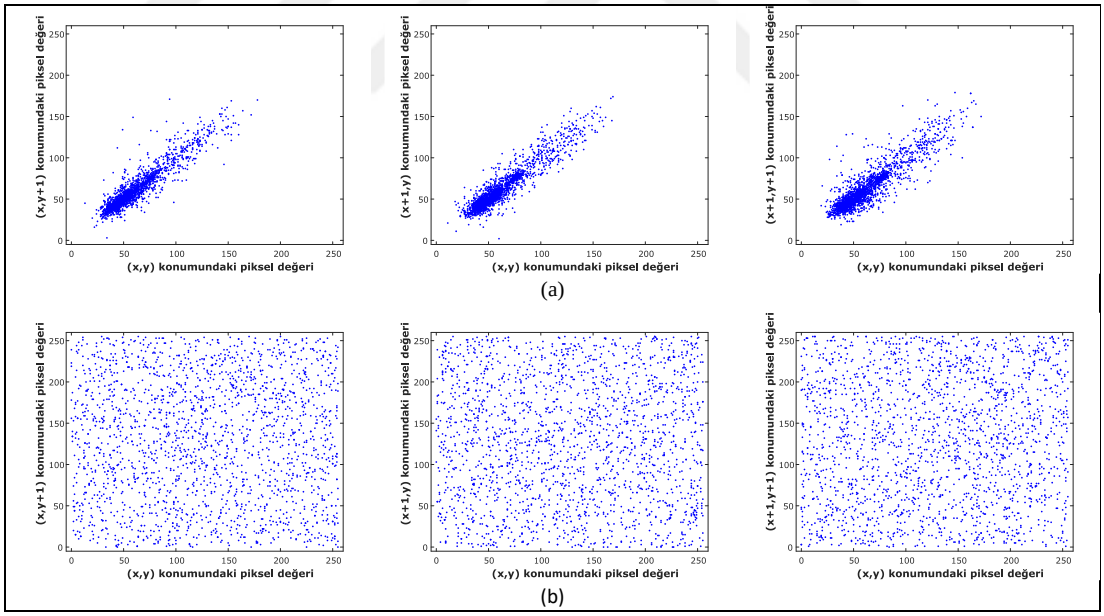
Tez kapsamında ProbRGB görüntü şifreleme yöntemi kullanılarak Lena görüntüsüne ait 2000 adet yatay, dikey ve çapraz piksel komşulukları rastgele seçilmiş ve korelasyon analizi yapılmıştır. Korelasyon analizi kırmızı, yeşil ve mavi renk kanalı için sırasıyla Şekil 4.14, Şekil 4.15 ve Şekil 4.16'da gösterilmiştir.



Şekil 4.14. ProbRGB yönteminde şifrelenen ve şifresi çözülen Lena görüntüsü için korelasyon katsayısının dağılımı: (a) Orijinal görüntünün bitişik piksellerinin yatay, dikey ve çapraz korelasyon katsayılarının kırmızı renk dağılımı. (b) Şifreli görüntünün bitişik piksellerinin yatay, dikey ve çapraz korelasyon katsayılarının kırmızı renk dağılımı



Şekil 4.15. ProbRGB yönteminde şifrelenen ve şifresi çözülen Lena görüntüsü için korelasyon katsayısının dağılımı: (a) Orijinal görüntünün bitişik piksellerinin yatay, dikey ve çapraz korelasyon katsayılarının yeşil renk dağılımı. (b) Şifreli görüntünün bitişik piksellerinin yatay, dikey ve çapraz korelasyon katsayılarının yeşil renk dağılımı



Şekil 4.16. ProbRGB yönteminde şifrelenen ve şifresi çözülen Lena görüntüsü için korelasyon katsayısının dağılımı: (a) Orijinal görüntünün bitişik piksellerinin yatay, dikey ve çapraz korelasyon katsayılarının kırmızı renk dağılımı. (b) Şifreli görüntünün bitişik piksellerinin yatay, dikey ve çapraz korelasyon katsayılarının kırmızı renk dağılımı

Şifre 4.14(a), Şekil 4.15(a) ve Şekil 4.16(a) görüntünün korelasyon katsayıların dağılımının doğrusal olduğu, Şifre 4.14(b), Şekil 4.15(b) ve Şekil 4.16(b)'de ise

rastgele dağınık bir yapıya sahip olduğu gözlemlenmektedir. Bununla birlikte Tablo 4.15'te korelasyon katsayılarının detaylı incelendiğinde veri setimizdeki orijinal görüntülerin korelasyon katsayısının 1'e yakın, buna karşılık şifrelenmiş görüntülerin korelasyon katsayılarının da 0'a çok yakın olduğu görülmektedir. Bu sonuçlar dikkate alındığında önerilen ProbRGB yönteminin komşu pikseller arasındaki ilişkiyi 0' a yakın hale getirdiği ve başarılı sonuçlar verdiği söylenebilir. Ayrıca PHMMRGB yönteminin, Tablo 4.15'te karşılaştırılan referanslarda öne sürülen yöntemlerin analiz sonuçları ile kıyaslandığında birçok çalışmadan daha iyi sonuçların elde edildiği açıkça görülmektedir.

Tablo 4.15. ProbRGB görüntü şifreleme algoritmasının korelasyon analiz sonuçları

Ad	Tip	Yatay			Dikey			Çapraz		
		Kırmızı	Yeşil	Mavi	Kırmızı	Yeşil	Mavi	Kırmızı	Yeşil	Mavi
Lena	Orj	0,9898	0,9641	0,9588	0,9871	0,9754	0,9608	0,9736	0,9556	0,9384
	Şif	0,0216	0,0274	0,0245	0,0105	-0,0392	0,0271	-0,0077	-0,0022	-0,0104
Airplane	Orj	0,9711	0,9559	0,9599	0,9224	0,9659	0,9428	0,8984	0,9335	0,9189
	Şif	0,0308	0,0093	-0,0176	-0,0181	-0,0435	-0,0081	0,0176	-0,0108	-0,0131
Cameraman	Orj	0,9285	0,9349	0,9352	0,9659	0,9640	0,9697	0,9029	0,9140	0,9116
	Şif	0,0075	-0,0093	0,0007	-0,0039	0,0044	-0,0085	-0,0008	0,0164	-0,0025
Baboon	Orj	0,9197	0,8630	0,9143	0,8523	0,7398	0,8949	0,8534	0,7215	0,8650
	Şif	0,0090	-0,0172	0,0028	0,0268	0,0062	0,0211	0,0174	-0,0166	0,0031
Melanoma	Orj	0,9921	0,9824	0,9751	0,9951	0,9901	0,9848	0,9897	0,9761	0,9658
	Şif	-0,0333	-0,0045	-0,0407	-0,0284	-0,0238	-0,0090	-0.0238	-0,0152	-0,0291
Melanoma	Orj	0,9936	0,9933	0,9918	0,9947	0,9941	0,9924	0,9918	0,9907	0,9878
	Şif	-0,0300	0,0233	0,0259	-0,0335	0,0294	-0,0104	0,0404	0,0158	-0,0356
2K Image	Orj	0,9750	0,9789	0,9852	0,9713	0,9737	0,9813	0,9573	0,9624	0,9742
	Şif	0,0225	-0,0003	0,0219	-0,0322	-0,0131	-0,0269	0,0164	-0,0161	-0,0081
4K Image	Orj	0,9977	0,9972	0,9987	0,9985	0,9983	0,9989	0,9972	0,9974	0,9982
	Şif	-0,0035	-0,0152	0,0071	0,0434	-0,0146	-0,0055	-0,0031	-0,0069	0,0086
8K Image	Orj	0,9536	0,9464	0,9470	0,9449	0,9463	0,9413	0,9123	0,9014	0,8919
	Şif	0,0017	0,0390	-0,0036	0,0295	-0,0248	-0,0172	0,0243	0,0338	-0,0423
Lena (Zhu ve diğ., 2018)	Orj	0,9249	0,9249	0,9249	-	-	-	-	-	-
	Şif	0,0002	0,0002	0,0002	-	-	-	-	-	-
Lena (Narendra, 2012)	Orj	0,9608	0,9845	0,9850	-	-	-	-	-	-
	Şif	0,0489	-0,0624	-0,0666	-	-	-	-	-	-
Lena (Maleki ve diğ., 2008)	Orj	0,9677	0,9677	0,9677	0,9366	0,9366	0,9366	0,9168	0,9168	0,9168
	Şif	0,0428	0,0428	0,0428	0,0217	0,0217	0,0217	0,0005	0,0005	0,0005
Aerial 1 (Liu ve diğ., 2019)	Orj	0,9473	0,9473	0,9473	0,8963	0,8963	0,8963	0,8472	0,8472	0,8472
	Şif	0,0017	0,0017	0,0017	0,0153	0,0153	0,0153	0,0046	0,0046	0,0046
Aerial 3 (Liu ve diğ., 2019)	Orj	0,7633	0,7633	0,7633	0,6178	0,6178	0,6178	0,5698	0,5698	0,5698
	Şif	0,0107	0,0107	0,0107	0,0181	0,0181	0,0181	0,0022	0,0022	0,0022

Tablo 4.15.(Devam) ProbRGB görüntü şifreleme algoritmasının korelasyon analiz sonuçları

Ad	Tip	Yatay			Dikey			Çapraz		
		Kırmızı	Yeşil	Mavi	Kırmızı	Yeşil	Mavi	Kırmızı	Yeşil	Mavi
Lena (Abdelfatah, 2020)	Orj	0,9959	0,9944	0,9876	0,9886	0,9847	0,9707	0,9931	0,9906	0,9810
	Şif	-0,0015	-0,0015	-0,0014	0,0006	-0,0007	-0,0004	-0,0009	-0,0014	-0,0001
Baboon (Abdelfatah, 2020)	Orj	0,9011	0,7957	0,8915	0,8829	0,7510	0,8510	0,9351	0,8404	0,9023
	Şif	0,0015	-0,0015	0,0038	0,0064	-0,0005	0,0014	0,0001	-0,0034	0,0030
Lena (Kumar ve diğ., 2016)	Orj	0,9326	0,9222	0,8938	0,9624	0,9546	0,9343	0,9070	0,8804	0,8634
	Şif	0,0035	-0,0097	0,0185	0,0040	0,0053	0,0106	-0,0410	-0,0085	-0,0170
Baboon (Kumar ve diğ., 2016)	Orj	0,9280	0,8625	0,9087	0,8650	0,7697	0,8859	0,8538	0,7256	0,8427
	Şif	0,0186	0,0066	0,0067	-0,0060	0,0164	0,0012	-0,0013	0,0092	0,0172
Lena (Luo ve diğ., 2019)	Orj	0,9858	-	-	0,9801	-	-	0,9669	-	-
	Şif	0,0019	-	-	-0,0024	-	-	-0,0011	-	-
Baboon (Luo ve diğ., 2019)	Orj	0,7251	-	-	0,8558	-	-	0,6920	-	-
	Şif	0,0024	-	-	0,0011	-	-	-0,0008	-	-
Lena (Liu ve diğ., 2018)	Orj	0,9325	-	-	0,9139	-	-	0,9469	-	-
	Şif	0,0074	-	-	-0,0094	-	-	-0,0054	-	-
Lena (Ye ve diğ., 2017)	Orj	0,9771	-	-	0,9631	-	-	0,9469	-	-
	Şif	0,0925	-	-	0,0430	-	-	-0,0054	-	-
Lena (Xu ve diğ., 2017)	Orj	0,9503	-	-	0,9755	-	-	0,9275	-	-
	Şif	-0,0226	-	-	0,0041	-	-	0,0368	-	-
Baboon (Chai ve diğ., 2017)	Orj	0,7508	-	-	0,8562	-	-	0,7153	-	-
	Şif	-0,0061	-	-	0,0130	-	-	0,0017	-	-
Lena (Baagyere ve diğ., 2020)	Orj	0,8319	-	-	0,9236	-	-	0,7814	-	-
	Şif	0,0099	-	-	0,0031	-	-	0,0002	-	-
Lena (Enayatifar ve diğ., 2014)	Orj	-	-	-	-	-	-	-	-	-
	Şif	0,017	-	-	0,0007	-	-	0,0001	-	-
Lena (Wang ve diğ., 2011)	Orj	-	-	-	-	-	-	-	-	-
	Şif	0,0007	-	-	-0,0022	-	-	0,0149	-	-
Lena (Yousif ve diğ., 2020)	Orj	0,9818	-	-	0,9903	-	-	0,9698	-	-
	Şif	-0,0021	-	-	-0,0030	-	-	-0,0177	-	-

Tablo 4.15.(Devam) ProbRGB görüntü şifreleme algoritmasının korelasyon analiz sonuçları

Ad	Tip	Yatay			Dikey			Çapraz		
		Kırmızı	Yeşil	Mavi	Kırmızı	Yeşil	Mavi	Kırmızı	Yeşil	Mavi
Baboon (Yousif ve diğ., 2020)	Orj	0,9214	-	-	0,8663	-	-	0,8510	-	-
	Şif	-0,0081	-	-	-0,0011	-	-	-0,0065	-	-
Cameraman (Yousif ve diğ., 2020)	Orj	0,9828	-	-	0,9898	-	-	0,9723	-	-
	Şif	-0,0097	-	-	-0,0021	-	-	-0,0080	-	-
Airplane (Yousif ve diğ., 2020)	Orj	0,9727	-	-	0,9517	-	-	0,9362	-	-
	Şif	-0,0206	-	-	-0,0086	-	-	-0,0099	-	-
Lena (Khan ve diğ., 2020)	Orj	0,8841	-	-	0,9463	-	-	0,8430	-	-
	Şif	-0,0041	-	-	-0,0037	-	-	-0,0065	-	-
Cameraman (Khan ve diğ., 2020)	Orj	0,8563	-	-	0,8970	-	-	0,8090	-	-
	Şif	-0,0015	-	-	-0,0143	-	-	-0,0236	-	-

4.3.3. Önerilen yöntemlerin birbirleriyle ve yaygın görüntü şifreleme algoritmaları ile karşılaştırılması

Yaygın olarak kullanılan görsel kriptografi algoritmalarının önerdiğimiz algoritma ile karşılaştırılması Tablo 4.16'da gösterilmektedir.

Karşılaştırma için kullanılan parametreler, S-Box sayısı, anahtar boyutu, blok boyutu, girdi sayısı, döngü sayısı, çıktı sayısı, şifreleme için oluşturulmuş yapı, esneklik, hesaplama verimliliği ve zaman karmaşıklığıdır. Karşılaştırma tablosundaki esneklik, şifreleme için kullanılan anahtarların sayı ve boyutlarının, şifreleme için oluşturulmuş yapının ve şifrelenecek blok boyutunun değiştirilip değiştirilemeyeceğini ifade etmektedir.

Önerilen yöntemleri DES (Kumar, 2011; Thakur ve Kumar, 2011; Gong-bin ve diğ., 2009; Stanisavljevic, 2015) algoritması ile karşılaştırdığımızda, yöntemlerimizin DES algoritmasına göre daha az S-Box, girdi, döngü verisi kullanarak daha az çıktı verisi ürettiği görülmektedir. Ayrıca anahtar boyutu DES algoritmasındaki gibi sabit değildir. Yöntemlerimizde şifrelenecek görüntünün boyutuna göre anahtarları boyutları artıp azalabilmektedir. Bunla birlikte yöntemlerimiz DES algoritmasından farklı olarak

esnektir. Bu koşullarda önerilen yöntemlerin DES algoritmasına göre esnek, hesaplama verimliliği açısından daha hızlı olduğu söylenebilir.

Yöntemlerimizi AES (Kumar, 2011; Thakur ve Kumar, 2011; Stanisavljevic, 2015; Maqsood, 2017;) algoritması ile karşılaştırırsak, piksel bazlı şifreleme yapıldığı için (8 bitten oluşan 3 renk kanalı) şifrelenen blok boyutu bakımından önerilen yöntemler AES algoritmasına göre daha düşük bloklarla işlem yapmaktadır. Ancak AES algoritmasının çıktı değeri yöntemlerimizin yaklaşık iki buçuk katıdır ve bu durum özellikle şifre çözme aşamasında AES algoritmasına ekstra maliyet getirmektedir. Ancak AES algoritmasının hesaplama verimliliği önerilen yöntemlerden yüksektir. Sonuç olarak belirtilen koşullar altında önerilen yöntemlerin AES algoritmasına göre şifreleme maliyeti açsısından daha düşük olduğu söylenebilir.

Blow-Fish (Mousa, 2005; Kumar, 2011; Thakur ve Kumar, 2011, Maqsood, 2017; Bell, 2018) algoritması önerilen yöntemler ile karşılaştırıldığında, yüksek döngü ve çıktı değerleri nedeniyle Blow-Fish algoritmasının toplam şifreleme işlemine ekstra maliyet getirdiği görülmektedir. Ayrıca hesaplama verimliliği açısından da önerilen yöntemlerin gerisinde kalmaktadır.

Yöntemlerimiz ECB (Kumar, 2011; Thakur ve Kumar, 2011; URL-3, 2021) algoritması ile karşılaştırıldığında, aynı döngü, çıktı ve zaman karmaşıklık değerlerine sahiptir. Ancak ECB yöntemi esneklik ve (URL-3, 2021) referansında belirlenen kriptanaliz testlerindeki eksikliği nedeniyle önerilen yöntemlerin güvenlik açısından gerisinde kalmıştır.

Son olarak, önerilen yöntemleri CBC (Kumar, 2011; Thakur ve Kumar, 2011; URL-3, 2021) algoritması ile karşılaştırdığımızda, benzer girdiler kullanmalarına ve benzer çıktılar üretmelerine rağmen, CBC algoritmasının (URL-3, 2021) referansında belirlenen kriptanaliz testlerindeki eksikliği nedeniyle güvenlik açısından önerilen yöntemlerin gerisinde kaldığı tespit edilmiştir.

Tablo 4.16. Yöntemlerin yaygın görüntü şifreleme algoritmaları ile karşılaştırılması

	DES	AES	Blow-Fish	ECB	CBC	**PHMMRGB**	**ProbRGB**
S-Box Sayısı	8	1	4	-	-	**1**	**2**

Tablo 4.16.(Devam) Yöntemlerin yaygın görüntü şifreleme algoritmaları ile karşılaştırılması

	DES	AES	Blow-Fish	ECB	CBC	**PHMMRGB**	**ProbRGB**
Anahtar Boyutu	64	128, 192, 256	32-448	Değişken	Değişken	**Değişken**	**Değişken**
Blok Boyutu	64	128	64	64	128	**24**	**24**
Girdi	6	8	8	2	3	**3**	**4**
Döngü	16	10, 12, 14	16	1	1	**1**	**1**
Çıktı	4	8	32	2	2	**3**	**4**
Yapı	Feistel Döngüsü	Koyma-Değiştirme Ağı	Feistel Döngüsü	Gizli Anahtar	Gizli Anahtar	**PHMMRGB, Gizli Anahtar**	**ProbRGB, Gizli Anahtar**
Esneklik	Hayır	Evet	Evet	Hayır	Evet	**Evet**	**Evet**
Hesaplama Verimliliği	0,7481 Mbit/s (Maqsood, 2017)	1,7066 Mbit/s (Maqsood, 2017))	0,6999 Mbit/s (Mousa, 2005)	Renkli (1,2171 Mbit/s) Gri Tonlamalı (1,5755 Mbit/s)	Renkli (1,1322 Mbit/s) Gri Tonlamalı (1,3719 Mbit/s)	**Renkli (0,7745 Mbit/s) Gri Tonlamalı (1,0535 Mbit/s)**	**Renkli (0,6891 Mbit/s) Gri Tonlamalı (0,9853 Mbit/s)**
Zaman Karmaşıklığı	$2^{39}-2^{41}$	2^{48}	$\theta(N)$	$\theta(N^2)$	$\theta(N^2)$	$\theta(N^2)$	$\theta(N^2)$

Tablo 4.17'de PHMMRGB ve ProbRGB yöntemlerinin kriptanaliz testlerindeki başarımlarının karşılaştırılması yapılmıştır. Histogram analizlerin de PHMMRGB ve ProbRGB yöntemlerinin çok benzer sonuçlar verdiği gözlemlenmiştir. Bununla birlikte Ortalama mutlak hata analizi, Ortalama karesel hata analizi ve Tepe sinyal gürültü oran analizlerinde de aynı sonuçlar elde edilmiştir. Yapısal benzerlik analiz sonuçlarını karşılaştırdığımızda PHMMRGB yönteminin yüksek çözünürlüklü (≥1920x1080) görüntülerde daha iyi sonuç verdiğini, ProbRGB yönteminin ise düşük çözünürlüklü (<1920x1080) görüntülerde daha iyi sonuçlar verdiğini söyleyebiliriz. Bilgi entropi analizi sonuçlarını incelediğimizde ProbRGB yönteminin daha iyi sonuçlar verdiğini görülmektedir. Diferansiyel atak analizi sonuçlarına göre gri tonlamalı görüntüler için NPCR değeri ProbRGB yönteminin daha başarılı olduğu gözlemlenmiştir. Korelasyon Analizi sonuçlarında Lena görüntüsü için tespit edilen ortalama korelasyon katsayısının ProbRGB yöntemi için daha iyi sonuç verdiği gözlemlenmiştir. Anahtar uzay analizinde ise ProbRGB yönteminde 4 anahtar kullandığından dolayı anahtarların kırılma olasılığı daha düşüktür. Hesaplama verimliliği analizi sonuçlarına göre PHMMRGB yöntemi ProbRGB yönteminden daha

hızlı çalışmaktadır. Son olarak zaman karmaşıklığı analizini incelediğimizde ise her iki yönteminde zaman karmaşıklığının aynı olduğunu söyleyebiliriz. Yapılan analizler sonucunda her iki yönteminde tüm kriptanaliz testlerinden başarılı bir şekilde geçtiği görülmektedir. Bununla birlikte ProbRGB yönteminin PHMMRGB yöntemine göre daha yavaş olduğu ancak diğer kriptanaliz testlerine göre güvenlik ve performans açısından daha iyi olduğunu söyleyebiliriz.

Tablo 4.17. PHMMRGB yöntemi ile ProbRGB yönteminin karşılaştırılması

Kriptanaliz Adı	PHMMRGB Yöntemi	ProbRGB Yöntemi
Histogram Analizi	Düzgün homojen renk dağılımı	Düzgün homojen renk dağılımı
Ortalama Mutlak Hata Analizi	Görüntü piksellerinde değişim yok	Görüntü piksellerinde değişim yok
Ortalama Karesel Hata Analizi	Görüntü piksellerinde bozulma yok	Görüntü piksellerinde bozulma yok
Tepe Sinyal Gürültü Oran Analizi	Görüntü kalitesinde herhangi bir değişiklik yok	Görüntü kalitesinde herhangi bir değişiklik yok
Yapısal Benzerlik Analizi	Yüksek çözünürlüklü (≥1920x1080) görüntülerde daha iyi	Düşük çözünürlüklü (<1920x1080) görüntülerde daha iyi
Bilgi Entropi Analizi	Renkli (7,7219+) Gri Tonlamalı (7,9927+)	Renkli (7,9989+) Gri Tonlamalı (7,9960+)
Diferansiyel Atak Analizi	NPCR Renkli (%99,9847+) NPCR Gri Tonlamalı (%99,6200+) UACI Renkli ve Gri Tonlamalı (%33,5091+)	NPCR Renkli (%99,9847+) NPCR Gri Tonlamalı (%99,9788+) UACI Renkli ve Gri Tonlamalı (%33,5459+)
Korelasyon Analizi	Korelasyon Katsayısı ortalama ≈ ±0,0266	Korelasyon Katsayısı ortalama ≈ ±0,0189
Anahtar Uzay Analizi	3 anahtar	4 anahtar
Hesaplama Verimliliği Analizi	Renkli (0,7745 Mbit/s) Gri Tonlamalı (1,0535 Mbit/s)	Renkli (0,6891 Mbit/s) Gri Tonlamalı (0,9853 Mbit/s)
Zaman Karmaşıklığı Analizi	$\theta(N^2)$	$\theta(N^2)$

5. SONUÇLAR VE ÖNERİLER

Teknolojinin gelişmesiyle birlikte dijital görüntü yakalama teknolojileri günümüzde yaygın olarak kullanılmaktadır. Bu teknolojiler, günlük yaşamda kişisel görüntüleri yakalamayı ve paylaşmayı çok kolay ve hızlı hale getirir. Bu, özel verilerin gizliliğinin sağlanmasında zorluklara ve üçüncü kişilerin bu verileri ele geçirmesi gibi risklere neden olur. Bu tip sorunların çözümü içinde görüntü şifreleme yöntemlerine ihtiyaç duyulmaktadır.

Bu tez kapsamında iki farklı görüntü şifreleme yöntemi geliştirilmiştir. Bunlardan ilki PHMMRGB olarak isimlendirilmiş yeni bir görüntü şifreleme mimarisidir. Bu mimari üç ana bileşenden oluşmaktadır. Bunlar PV, IV ve S-Box olarak listelenebilir. PV değeri PHMM modeli ile orijinal görüntüdeki maksimum değerlikli RGB modeline göre, IV değeri ise orijinal görüntünün genişliğinde ve [0,255] arasında rastgele değerlerden oluşturulmaktadır. Bir satır şifrelendiğinde IV değeri PV ye göre güncellenmektedir. Bu işlem sayesinde şifrelenecek satırın önceki satırlardan bağımsız olarak şifrelenmesi sağlanmıştır. S-Box, [0,255] değerleri arasında ve her biri bir kez kullanılmak şartıyla rastgele yerleştirilmiş 16x16'lık bir matristen oluşturulmaktadır.

Geliştirilen ikinci yöntem ise ProbRGB olarak isimlendirilmiştir. Bu yöntemin PHMMRGB mimarisinden en temel farkı elde edilen olasılık vektörünün, görüntüdeki piksellerin birbiri arasındaki olasılıksal geçişlerden elde edilmesidir. Aynı zamanda bu yöntemde birbirinden tamamen farklı iki adet S-Box kullanılmıştır.

Önerilen her iki mimarinin de diğer görüntü şifreleme mimarilerinden en temel farklı piksel bazlı şifreleme yapılmasıdır. Piksel bazlı şifreleme işlemi piksellerdeki renk kanallarının ayrı ayrı şifrelenmesini ifade etmektedir. Bununla birlikte şifreleme işlemi sırasında hiçbir pikselin yeri değiştirilmemiştir. Bu sayede şifre çözme işlemi her iki mimaride de çok hızlı olmaktadır. Bunların yanında geliştirilen yöntemlerin en önemli artılarından bir tanesi de şifrelenecek görüntünün boyutu arttıkça şifreleme güvenliğinin de doğru orantılı olarak artmasıdır. Teorik analiz ve deneysel sonuçlar, önerilen görüntü şifreleme algoritmalarının renkli ve gri tonlamalı görüntüler için

yüksek güvenlik sağlayabildiğini göstermektedir. Ek olarak, geliştirilen her iki yöntem çok yüksek çözünürlüklü görüntülerde (Örneğin 2K, 4K, 8K vb.) de test edilmiştir. Yöntemler piksel bazlı şifreleme hızı ve zaman karmaşıklığı açısından daha düşük çözünürlüklü görüntülerle aynı performansı göstermiştir. Ayrıca geliştirilen yöntemlerin literatürde yer alan benzer birçok çalışmadan daha iyi sonuçlar verdiği gerçekleştirilen performans analiz testlerinden anlaşılmaktadır.

Tez çalışmasının ana katkıları aşağıdaki gibi maddeler halinde sıralanabilir:

- PHMMRGB isimli Profile Hidden Markov Model temelli yeni bir görüntü şifreleme yöntemi tasarlanmıştır. PHMM yöntemi orijinal görüntü üzerinden RGB olasılık vektörü (PV)'nin elde edilmesi aşamasında kullanılmıştır.
- ProbRGB isimli görüntü piksellerindeki renk kanalları üzerinden hesaplanan geçiş olasılıklarına dayanan yeni bir görüntü şifreleme yöntemi tasarlanmıştır. Pikseller üzerinden hesaplanan olasılık değerleri PV'nin elde edilmesi aşamasında kullanılmıştır.
- Görüntü şifreleme işleminin rastgeleliğini arttırmak için kullanılan IV, görüntünün her bir pikselinin şifrelenmesi aşamasında kullanılmıştır.
- Şifrelemedeki güvenirlik, kalite ve karmaşıklığın arttırılması için S-Box'lar kullanılmıştır. PHMMRGB yöntemi için birer adet S-Box ve Ters S-Box, ProbRGB yöntemi için ise birbirinden tamamen farklı ikişer adet S-Box ve Ters S-Box kullanılmıştır.
- PHMMRGB ve ProbRGB yöntemlerinin istatistiksel ve diferansiyel ataklara, birçok kriptanaliz testlerine ve literatürdeki benzer çalışmalara kıyasla başarılı sonuçlar verdiği gözlemlenmiştir.
- Önerilen yöntemler temel olasılık hesaplamaları kullanılarak geliştirilmiştir. Aynı zamanda yöntemlerin ifade edilmesi aşamasında basit matematiksel açıklamalar kullanılmıştır. Bu sebeplerle geliştirilen yöntemleri pek çok kişi rahatlıkla anlayıp, uygulamaya geçirebilecektir.
- Her iki yönteminde hem renkli hem de gri tonlamalı görüntüler için şifreleme işlemini başarılı bir şekilde gerçekleştirebildiği gösterilmiştir.

- Önerilen yöntemlerin şifre çözme işlemini görüntünün boyutu ve çözünürlük gibi parametrelerden bağımsız olarak, problemsiz şekilde gerçekleştirdiği performans analiz testleri sonuçlarına dayanarak gösterilmiştir.
- Gerçekleştirilen güvenlik ve performans analiz testleri sonucunda önerilen her iki görüntü şifreleme yönteminin de mükemmel güvenlik seviyesine ulaştığı gözlemlenmiştir.

Önerilen PHMMRGB ve ProbRGB yöntemlerinin en önemli eksikliği görüntülerin boyutlarının (2K, 4K, 8K vb. çözünürlüklü) artması durumunda toplam şifreleme süresinin uzamasıdır. Ancak böyle görüntüler üzerinde dahi, performans ve analiz testleri sonuçları görüntü şifreleme kalitesinin düşmediğini aksine daha iyi sonuçlar verdiğini göstermektedir. Bu çalışmanın devamında önerilen yöntemler, 24 bitlik blok şifreleme yerine 128 bit ya da 256 bitlik bloklar halinde şifreleme yapabilecek şekilde geliştirilebilir.

KAYNAKLAR

Abd-El-Hafiz S. K., Radvan A. G., Abdel-Haleem S. H., Barakat M. L., A Fractal-Based Image Encryption System, *IET Image Processing,* 2014, **8**(12), 742-752.

Abdelfatah R. I., Secure Image Transmission Using Chaotic-Enhanced Elliptic Curve Cryptography, *in IEEE Access,* 2020, **8**, 3875-3890.

Abidi A., Wang Q., Bouallegue B., Machhout M., Guyeux C., Quantitative Evaluation of Chaotic CBC Mode of Operation, *in Proc. 2016 2nd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP),* Monastir, Tunisia, 21-23 Mar. 2016.

Alpaydın E., *Yapay Öğrenme,* 2. Baskı, Boğaziçi Üniversitesi Yayınevi, İstanbul, Türkiye, 2013.

Alvarez G., Li S. Breaking an Encryption Scheme Based on Chaotic Baker Map, *Phys Lett A,* 2006, **352**(1-2), 78-82.

Atalay N. S., Dogan S., Tuncer T., Akbal E., Image Encryption Methods and Algorithms, *Dicle University Journal of Engineering,* 2019, **10**(3), 815-831.

Aydogan T., Bayilmis C., A New Efficient Block Matching Data Hiding Method Based on Scanning Order Selection in Medical İmages, *Turkish Journal of Electrical Engineering and Computer Sciences,* 2017, **25**, 461-473.

Baagyere E. Y., Agbedemnab P. A., Qin Z., Daabo M. I., Qin Z., A Multi-layered Data Encryption and Decryption Scheme Based on Genetic Algorithm and Residual Numbers, *in IEEE Access,* 2020, **8**, 100438-100447.

Bagbaba A. C., Ors B., Kayhan O. S., Erozan A. T., JPEG İmage Encryption Via TEA Algorithm, *in Proc. 2015 23nd Signal Processing and Communications Applications Conference (SIU),* Malatya, Turkey, 16-19 May 2015.

Bauer C. P., *Secret history: The story of cryptology,* 1st ed., CRC Press, ABD, 2013.

Bejinariu S. I., Luca R., Costin H., Nature-İnspired Algorithms Based Multispectral Image Fusion, *in Proc. 9th International Conference and Exposition on Electrical and Power Engineering (EPE),* Iasi, Romania, 20-22 October 2016.

Bell N. P. S., Priya L. R., Lakshmi N. S., Secure Data Hiding Based on Most Significant Bit Error Prediction Mechanism Using Blow Fish Algorithm, *in Proc. 2018 International Conference on Smart Systems and Inventine Technology (ICSSIT),* Tirunelveli, India, 13-14 Dec. 2018.

Benssalah M., Rhaskali Y., Azzaz M. S., Medical Images Encryption Based on Elliptic Curve Cryptography and Chaos Theory, *in Proc. 2018 International Conference on Smart Communications in Network Technologies (SaCoNeT),* El Oued, Algeria, 27-31 October 2018.

Chai X., Chen Y., Broyde L., A Novel Chaos-Based Image Encryption Algorithm Using DNA Sequence Operations, *Opt. Lasers Eng.*, 2017, **88**, 197-213.

Chai X., Gan, Z., Yang K., Chen Y., Liu X., An Image Encryption Algorithm Based on The Memristive Hyperchaotic System, Cellular Automata and DNA Sequence Operations, *Signal Processing: Image Communication,* 2017, **52**, 6-19.

Chaudhary R., Jindal A., Aujla G. S., Das A. K., Saxena N., LSCSH: Lattice-based Becure Cryptosystem for Smart Healthcare in Smart Cities Environment, *IEEE Communications Magazine,* 2018, **56**, 24-32.

Chen G., Mao Y., Chui C. K., A Symmetric Encryption Scheme Based on 3D Chaotic Cat Map. *Chaos, Solitons & Fractals,* 2004, **21**, 749-761.

Chuman T., Sirichotedumrong W., Kiya H., Encryption Then Compression Systems Using Grayscale-based Image Encryption for JPEG Images," *IEEE Transactions on Information Forensics and Security,* 2019, **14**(6), 1515-1525.

Codella N. C. F., Rotemberg V., Tschandl P., Celebi M. E., Dusza S., Gutman D., Helba B., Kalloo A., Liopyris K., Marchetti M., Kittler H. Halpern A., Skin lesion analysis toward melanoma detection, *in Proc. 2018: A Challenge Hosted by the International Skin Imaging Collaboration (ISIC),* Granada, Spain, 9 February 2019.

De Prisco R., De Santis A., On the Relation of Random Grid and Deterministic Visual Cryptography, *in IEEE Transactions on Information Forensics and Security,* 2014, **9**(4), 653-665.

Diffie W., Hellman M., New Directions in Cryptography, *in IEEE Transactions on Information Theory*, 1976, **22**(6), 644-654.

Durbin R., Eddy S. R., Krogh A., Mitchison G. J., *Biological Sequence Analysis: Probabilistic Models of Proteins and Nucleic Acids,* 1st ed., Cambridge University Press, England, 1998.

Enayatifar R., Abdullah A. H., Isnin I. F., Chaos-based Image Encryption Using A Hybrid Genetic Algorithm and A DNA Sequence, *Opt. Lasers Eng.*, 2014, **56**, 83-93.

Fine S., Singer Y., Tishby N., The Hierarchical Hidden Markov Model: Analysis and Applications, *Machine Learning,* 1998, **32**, 41–62.

Gagniuc P. A., *Markov Chains: From Theory to Implementation and Experimentation,* 1st ed., John Wiley and Sons, USA, 2017.

Gong-bin Q., Quing-feng J., Shui-sheng, Q., A New Image Encrpytion Scheme Based On DES Algorithm and Chua's circuit, *in Proc. 2009 IEEE International Workshop on Imaging Systems and Techniques,* Shenzhen, China, 11-12 May 2009.

Gulagız F. K., Estimation of Synchronization Time in Content Delivery Networks with Profile Hidden Markov Model, PhD. Thesis, Kocaeli University, Computer Enginering, Turkey, 2018, 518829.

Guvenoglu E., A Dynamic S-BOX Design Method for Image Encryption, *El-Cezeri: Journal of Science and Engineering,* 2016, **3**(2), 179-191.

Guvenoglu E., Esin E. M., Image Encryption Based on Knutt / Durstenfeld Shuffle Algorithm, *Journal of Polytechnic,* 2009, **12**(3), 151-155.

Hore A., Ziou D., Image Quality Metrics: PSNR vs. SSIM, *in Proc. 2010 20th International Conference on Pattern Recognition,* Istanbul, Turkey, 23-26 August 2010.

Hua Z., Xu B., Jin F., Huang H., Image Encryption Using Josephus Problem and Filtering Diffusion, *in IEEE Access,* 2019, **7**, 8660-8674.

Huang K. T., Chiu J. H., Shen S. S., A Novel Structure With Dynamic Operation Mode for Symmetric-Key Block Ciphers, *International Journal of Network Security and Its Applications,* 2013, **5**(1), 17-36.

Huang Y., Cao L., Zhang J., Pan L., Liu Y., Exploring Feature Coupling and Model Coupling for Image Source Identification, *IEEE Transactions on Information Forensics and Security,* 2018, **13**(12), 3108-3121.

Ibrahim S., Alharbi A., Efficient Image Encryption Scheme Using Henon Map, Dynamic S-Boxes and Elliptic Curve Cryptography, *in IEEE Access,* 2020, **8**, 194289-194302.

Ishai Y., Kushilevitz E., Ostrovsky R., Sahai A, Cryptography with Constant Computational Overhead, *in Proceedings of the fortieth annual ACM symposium on Theory of computing (STOC '08),* New York, USA, 17-20 May 2008.

Jolfaei A., Mirghadri A., Image Encryption Using Chaos and Block Cipher, *Computer and Information Science,* 2010, **4**(1), 172-185.

Kafri O., Keren E., Encryption of Pictures and Shapes by Random Grids, *Opt. Lett.*,1987, **12**(6), 377-379.

Kahn J. S., Boulila W., Ahmad J., Rubaiee S., Rehman A. U., Alroobaea R., Buchanan W. J., DNA and Plaintext Dependent Chaotic Visual Selective Image Encryption, *in IEEE Access,* 2020, **8**, 159732-159744.

Khan J., Li J. P., Ahamad B., Parveen S., Haq A. U., Khan G. A., Sangaiah A. K., SMSH: Secure Surveillance Mechanism on Smart Healthcare IoT System With Probabilistic Image Encryption, *in IEEE Access,* 2020, **8**, 15747-15767.

Klima R., Klima R. E., Sigmon N., Sigmon N. P., *Cryptology: Classical and Modern,* 2nd ed., CRC Press, ABD, 2018.

Koblitz, N., Elliptic Curve Cryptosystems. Mathematics Of Computation, *Math. Comp.*, 1987, **48**(1987), 203-209.

Krogh A., Brown M., Mian I. S., Sjolander K., Haussler D, Hidden Markov Models in Computational Biology Applications to Protein Modelling, *J.Mol. Biol.*, 1994 **235**(5), 1501-1513.

Kumar M., Iqbal A., Kumar P., A New RGB Image Encryption Algorithm Based on DNA Encoding and Elliptic Curve Diffie-Hellman Cryptography, *Signal Process.*, 2016, **125**, 187-202.

Kumar Y., Munjal R., Sharma H., Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures, *International Journal of Computer Science and Management Studies*, 2011, 11, 60-63.

Li L., Wen G., Wang Z., Yang Y., Efficient and Secure Image Communication System Based on Compressed Sensing for IoT Monitoring Applications, *in IEEE Transactions on Multimedia*, 2020, **22**(1), 82-95.

Lin S., Chung W., A Probabilistic Model of (t, n) Visual Cryptography Scheme with Dynamic Group, *in IEEE Transactions on Information Forensics and Security*, 2012 **7**(1), 197-207.

Liu H., Zhao B., Huang L., A Remote-Sensing Image Encryption Scheme Using DNA Bases Probability and Two-Dimensional Logistic Map, *IEEE Access*, 2019, **7**, 65450-65459.

Liu Z., Xia T, Wang J., Image Encryption Technique Based on New Two-Dimensional Fractional-Order Discrete Chaotic Map and Menezes-Vanstone Elliptic Curve Cryptosystem, *Chin. Phys. B*, 2018, **27**(3), 1-16.

Luo Y., Ouyang X., Liu J., Cao L., An Image Encryption Method Based On Elliptic Curve Elgamal Encryption and Chaotic Systems, *IEEE Access*, 2019, **7**, 38507-38522.

Maleki F., Mohades A., Hashemi S. M., Shiri M. E., An Image Encryption System by Cellular Automata with Memory, *2008 Third International Conference on Availability, Reliability and Security*, Barcelona, Spain, 4-7 March 2008.

Mansoor E., Khan S., Khalid U. B., Symmetric Algorithm Survey: A Comparative Analysis, *International Journal of Computer Applications*, 2013, **61**(20), 12-19.

Massey J. L., An Introduction to Contemporary Cryptology, *in Proceedings of the IEEE*, 1988, **76**(5), 533-549.

Maqsood F., Ali M. M., Ahmed M., Shah M. A., Cryptography A Comparative Analysis for Modern Techniques, *International Journal of Advanced Computer Science and Applications*, 2017, **8**(6), 442-448.

Miller V. S., Elliptic Curves and Their Use in Cryptography, *in DIMACS Workshop on Unusual Applications of Number Theory*, March 1997.

Mount D. M., *Bioinformatics: Sequence and Genome Analysis,* 2nd ed., Cold Spring Harbor Laboratory Press, New York, USA, 2004.

Mousa A., Deta Encryption Performance Based On Blowfish, *in Proc. 47th International Symposium ELMAR,* Zadar, Croatia, 8-10 June 2005.

Muhammad K., Hamza R., Ahmad J., Lloret J., Wang H., Baik S. W., Secure Surveillance Framework for IoT Systems Using Probabilistic Image Encryption, *in IEEE Transactions on Industrial Informatics,* 2018, **14**(8), 3679-3689.

Naor M., Shamir A., Visual Cryptography, *in Proc. Advances in Cryptology EUROCRYPT'94,* Berlin, Germany, 9-12 May 1995.

Naor M., Shamir A., Visual cryptography, *in Advances in Cryptology,* 1994, **950**, 1-12.

Narendra P., Design and Analysis of A Novel Digital Image Encryption Scheme, *International Journal of Network Security and Its Applications,* 2012, **4**, 95-108.

Naveen C., Gupta T. V. S., Satpute V. R., Gandhi A. S., A Simple and Efficient Approach for Medical Image Security Using Chaos on EZW, *in Proc. 2015 Eighth International Conference on Advances in Pattern Recognition (ICAPR),* Kolkata, India, 4-7 January 2015.

Pisarchik A. N., Zanin M., Image Encryption with Chaotically Coupled Chaotic Maps, *Physica D,* 2008, **237**(20), 2638-2648.

Preishuber M., Hütter T., Katzenbeisser S., Uhl A., Depreciating Motivation and Empirical Security Analysis of Chaos-Based Image and Video Encryption, *IEEE Transactions On Information Forensics and Security,* 2018, **13**(9), 2137-2150.

Quach T., Farooq M., Maximum Likelihood Track Formation with The Viterbi Algorithm, *in Proc. Proceedings of 1994 33rd IEEE Conference on Decision and Control,* Lake Buena Vista, FL, USA, 14-16 December 1994.

Rabiner L., Juang B., An Introduction to Hidden Markov Models, *in IEEE ASSP Magazine,* 1986, **3**(1), 4-16.

Reyad O., Mofaddel M. A., Abd-Elhafiez W. M., Fathy M., A Novel Image Encryption Scheme Based on Different Block Sizes for Grayscale and Color İmages, *in Proc. 2017 12th International Conference on Computer Engineering and Systems (ICCES),* Cairo, Egypt, 19-20 December 2017.

Shannon C. E., Communication Theory of Secrecy Systems, *Bell Syst Tech J,* 1949, **28**(4), 656-715.

Singh L. D., Singh K. M., Image Encryption Using Elliptic Curve Cryptography, *Procedia Comput. Sci.,* 2015, **54**, 472-481.

Stanisavljevic S. Z., Data Encryption Standart Visual Representation, *in Proc. 2015 23dr Telecommunications Forum Telfor (TELFOR),* Belgrade, Serbia, 24-26 Nov. 2015.

Stinson D. R., *Cryptography: Theory and Practice,* 3rd ed., CRC Press, ABD, 1995.

Song Y., Zhu Z., Zhang W., Yu H., Zhao Y., Efficient and Secure Image Encryption Algorithm Using A Novel Key-Substitution Architecture, *IEEE Access,* 2019, **7**, 84386-84400.

Sun S., Chaotic Image Encryption Scheme Using Two-By-Two Deoxyribonucleicacid Complementary Rules, *Opt. Eng.*, 2017, **56**(11), 116117.

Talbot, J., Welsh, D., Welsh, D. J. A., *Complexity and cryptography: an introduction,* 1st ed., Cambridge University Press, England, 2006.

Thakur J., Kumar N., DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis, *International Journal of Emerging Technology and Advanced Engineering,* 2011, **1**, 6-12.

URL-1: http://bilgisayarkavramlari.com/2009/06/17/markof-modeli-markov-model/?highlight=markov (Ziyaret Tarihi: 1 Mart 2021)

URL-2: https://medium.com/@balamurali_m/markov-chain-simple-example-withpython-985 d33b14d19 (Ziyaret Tarihi: 1 Mart 2021)

URL-3: https://tr.wikipedia.org/wiki/Blok_şifre_çalışma_kipleri (Ziyaret Tarihi: 1 Mart 2021)

Wang R., Hsu S., Tagged Visual Cryptography, *in IEEE Signal Processing Letters,* 2011, **18**(11), 627-630.

Wang Y., Wong K. W., Liao X., Chen G., A New Chaos-based Fast Image Encryption Algorithm, *Appl. Soft Comput.*, 2011, **11**(1), 514-522.

Wang Z., Bovik A. C., Sheikh H. R., Simoncelli E. P., Image Quality Assessment: From Error Visibility to Structural Similarity, *IEEE Transactions on Image Processing,* 2004, **13**(4), 600-612.

Wang Z., Simoncelli E. P., Bovik A. C., Multiscale Structural Similarity for Image Quality Assessment, *in Proc. The Thrity-Seventh Asilomar Conference on Signals, Systems and Computers,* Pacific Grove, CA, USA, 9-12 November 2003.

Wolf J. K., Viterbi A. M., Dixon G. S., Finding The Best Set of K Paths Through A Trellis with Application to Multitarget Tracking, *IEEE Transactions on Aerospace and Electronic Systems,* 1989, **25**(2), 287-296.

Wu J., Liao X., Yang B., Color Image Encryption Based on Chaotic Systems and Elliptic Curve Elgamal Scheme, *Signal Processing,* 2017, **141**, 109-124.

Wu X., Sun W., Generalized Random Grid and Its Applications in Visual Cryptography, *IEEE Transactions on Information Forensics and Security*, 2013, **8**(9), 1541-1553.

Wu Y., Noonan J. P., Agaian S. S., NPCR and UACI Randomness Tests for Image Encryption, *Cyber Journals: Journal of Selected Areas in Telecommunications,* 2011, **2**, 31-38.

Wu Y., Noonan J. P., Yang G., Jin H., Image Encryption Using The Two-Dimensional Logistic Chaotic Map, *Journal of Electronic Imaging,* 2012, **21**(1), 1-16.

Xu L., Gou X., Li Z., Li J., A Novel Chaotic Image Encryption Algorithm Using Block Scrambling and Dynamic Index Based Diffusion, *Opt. Lasers Eng.*, 2017, **91**, 41-52.

Yan B., Xiang Y., Hua G., Improving The Visual Quality of Size-Invariant Visual Cryptography for Grayscale Images: An Analysis-By-Synthesis (Abs) Approach, *in IEEE Transactions on Image Processing,* 2019, **28**(2), 896-911.

Ye G., A Block Image Encryption Algorithm Based on Wave Transmission and Chaotic Systems, *Nonlinear Dyn.*, 2014, **75**(3), 417-427.

Ye G. D., Huang X. L., Zhang L. Y., Wang Z. X., A Self-Cited Pixel Summation Based Image Encryption Algorithm, *Chin. Phys. B*, 2017, **26**(1) 131-138.

Yong Z., The Unified Image Encryption Algorithm Based on Chaos and Cubic S-Box, *Inf. Sci.*, 2018, **450**, 361-377.

Yousif S. F., Abboud A. J., Radhi H. Y., Robust Image Encryption with Scanning Technology, the El-Gamal Algorithm and Chaos Theory, *in IEEE Access*, 2020, **8**, 155184-155209.

Zhu C., Wang G., Sun K., Cryptanalysis and Improvement on An Image Encryption Algorithm Design Using A Novel Chaos Based S-Box, *Symmetry,* 2018, **10**, 399-414.

KİŞİSEL YAYIN VE ESERLER

Ozcan H., Gülağız F. K., Altuncu M. A., Ilkin S. and Sahin S., A New Visual Cryptography Method based on the Profile Hidden Markov Model, *Advances in Electrical and Computer Engineering,* 2021, **21**(1), 21-36.

İlkin S., Gençtürk T. H., Kaya Gülağız F., **Özcan H.**, Altuncu M. A., Şahin S., hybSVM: Bacterial Colony Optimization Algorithm Based SVM for Malignant Melanoma Detection, *Engineering Science and Technology, an International Journal,* DOI: 10.1016/j.jestch.2021.02.002.

Çavuşlu M. A., Altuncu M., O**zcan H.**, Gülağız F. K., Sahin S., Sualtı Haberleşmede Çok Yolluluğun Bant Genişliği, Kapasite ve İletim Gücü Üzerindeki Etkisi, *Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Dergisi,* 2020, **7**(1), 404-420.

Ozcan H., Gülağız F. K., Altuncu M. A., Kaya S., Topuz G., Sahin S., A Leap Motion Based Mobile Game Design for Developing Hand and Wrist Movement in Children, *4th International Symposium on Innovative Approaches in Engineering and Natural Sciences,* Samsun, Turkey, 22-24 November 2019.

Kaya Gülağız F., **Ozcan H.**, Sahin S., Güler S. A., Şimşek T., Cantürk N. Z., Meme kanseri takip uygulaması ve kullanabilirliğinin değerlendirilmesi, *15. Ulusal Meme Hastalıkları Kongresi*, Antalya, Turkey, 17-20 October 2019.

Sahin S., **Ozcan H**., Kucuk K., Smarttag: An Indoor Positioning System Based on Smart Transmit Power Scheme Using Active Tags, *in IEEE Access,* 2018, **6**, 23500-23510.

Gülağız F., **Ozcan H.**, Sahin S., Guler S. A., Senaturk Akademisi Göğüs Sağlığı İzleme Uygulamasının Kullanılabilirlik Değerlendirmesi, *Bilge International Journal of Science and Technology Research,* 2018, **2**, 124-131.

Ozcan H., Tayfur T., İlkin S., Sahin S., Petek Topolojisi Kullanılarak Geniş Kapalı Alanlara Konum Okuyucu Yerleştirme, *Uluslararası Marmara Fen ve Sosyal Bilimler Kongresi,* Kocaeli, Turkey, 23-25 November 2018.

Ozcan H., Yıldırım D., Niyazov A., Kaya F., Sahin S., Gerçek Zamanlı RF ve GPS Tabanlı İş ve İşçi Takip Sistemi Mimarisi, *ELECO 2018,* 30 Nov–1 Dec 2018.

Altuncu M. A., Kaya F., Bir T., **Ozcan H.**, Sahin S., Imputation of Missing Data for Network Intrusion Detection, *IOSR Journal of Computer Engineering,* 2017, **19**, 8-12.

Ozcan H., Altuncu M. A., Kucuk K., Sahın S., Simulation of Indoor Positioning System Based on Radio Frequency, *IOSR Journal of Computer Engineering,* 2017, **19**, 13-18.

Ozcan H., Mutlu A., Weka Veri Madenciliği Aracı İçin Kısmı-Otomatik Arff Girdi Oluşturucu, *UMAS 2017,* 11-13 September 2017.

Kaya F., **Ozcan H.**, Sahin S., An Interactive Turkish Sign Language Learning Game Using Leap Motion Controller, *6th International Conference on Advanced Technology Sciences,* Riga, Latvia, 12-15 September 2017.

Kaya F., **Ozcan H.**, Sahin S., Gök O., Web Based Medical Archieve System Design and Implementation, *ICRES 2017,* Kuşadası, Turkey, 18-21 May 2017.

Ozcan H., Güven T., Altuncu M. A., Kır Savaş B., Sahin S., Duman O., Desıgn And Implementatıon Of A Content Delıvery Archıtecture For Museums, *ICRES 2017,* Kuşadası, Turkey, 18-21 May 2017.

Ozcan H., Güven T., Altuncu M. A., Kır Savaş B., Duman O., Sahin S., A Smart Tracking Systems for Museums, *6th World Conferance on Innovation and Computer Science,* Antalya, Turkey, 12-14 May 2016.

Ozcan H., Sahin S., Mentesoglu M., Pir F., Indoor reduction of noise in RF signal with Kalman Filter, *2015 23nd Signal Processing and Communications Applications Conference (SIU),* Malatya, Turkey, 16-19 May 2015.

Mentesoglu M., Kavak A., Yakut M., Tangel A., Sahin S., **Ozcan H.**, Design and implementation of a communication protocol for mobile device controlled smart home management system, *2015 23nd Signal Processing and Communications Applications Conference (SIU),* Malatya, Turkey, 16-19 May 2015.

ÖZGEÇMİŞ

Hikmetcan Özcan lise öğrenimini Bahçelievler Kemal Hasoğlu Lisesi'nde tamamladı. 2006 yılında girdiği Süleyman Demirel Üniversitesi Uluborlu Selahattin Karasoy Meslek Yüksek Okulun'dan 2008 yılında mezun oldu. 2010 yılında girdiği Kocaeli Üniversitesi Bilgisayar Mühendisliği Bölümü'nden 2013 yılında mezun oldu. Aynı yıl içinde Kocaeli Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı'nda yüksek lisans eğitimine başlayarak 2016 yılında mezun oldu. Yüksek lisans eğitiminde kapalı alanlarda konum tespiti konusunda çalışmaları bulunmaktadır. 2016 yılında Kocaeli Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı'nda doktora eğitimine başladı. Doktora eğitiminde görüntü şifreleme algoritmaları konusunda çalışmaları bulunmaktadır. Ayrıca 2013-2021 yılları arasında Kocaeli Üniversitesi Bilgisayar Mühendisliği'nde araştırma görevlisi olarak görev yaptı.