
GAZİ ÜNİVERSİTESİ
Gazi
1926

KAOTİK ŞİFRELEMELİ AYRICALIK TABANLI GÖRSEL GİZLİ PAYLAŞIM MODELİ GELİŞTİRİLMESİ

Aytekin YILDIZHAN

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MAYIS 2018

Aytekin YILDIZHAN tarafından hazırlanan "KAOTİK ŞİFRELEMELİ AYRICALIK TABANLI GÖRSEL GİZLİ PAYLAŞIM MODELİ GELİŞTİRİLMESİ" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Bilgisayar Mühendisliği Anabilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Doç.Dr. Nurettin TOPALOĞLU

Bilgisayar Mühendisliği Anabilim Dalı, Gazi Üniversitesi

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

Başkan: Prof.Dr. Remzi YILDIRIM

Bilgisayar Mühendisliği Anabilim Dalı, Yıldırım Beyazıt Üniversitesi

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

Üye: Prof.Dr. Recep DEMİRCİ

Bilgisayar Mühendisliği Anabilim Dalı, Gazi Üniversitesi

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

Tez Savunma Tarihi: 08/05/2018

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

……..……

Prof. Dr. Sena YAŞYERLİ

Fen Bilimleri Enstitüsü Müdürü

ETİK BEYAN

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

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

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

Aytekin YILDIZHAN

08/05/2018

KAOTİK ŞİFRELEMELİ AYRICALIK TABANLI GÖRSEL GİZLİ PAYLAŞIM MODELİ GELİŞTİRİLMESİ

(Yüksek Lisans Tezi)

Aytekin YILDIZHAN

GAZİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

Mayıs 2018

ÖZET

Sır paylaşım (SP) şeması, gizli verinin yeterli sayıda kullanıcının bir araya gelmesi sonucu ortaya çıkan bir şifreleme yöntemidir. Bu yöntem ile gizli veri bir kişide bulunmamakta ve sadece belli sayıda kişinin bir araya gelmesi ile çözülebilmektedir. Görsel sır paylaşım (GSP) şemasında ise gizlenecek veri, görüntüdür. Gizli görüntü belli sayıda pay görüntülere ayrılıp her bir kullanıcıya bir adet paylaştırılır. Gizli görüntünün ortaya çıkması için gerekli olan tüm payların üst üste getirilmesi gerekir ve tüm paylar eşit öneme sahiptir. Ayrıcalık tabanlı GSP (AT-GSP) şemasında ise her bir payın farklı ayrıcalığı olup daha yüksek ayrıcalığa sahip payın, gizli görüntüyü ortaya çıkarması için diğer paylara göre daha fazla ayrıcalığı vardır. AT-GSP şemasında en yüksek öneme sahip birkaç pay görüntü üst üste getirildiğinde, gözle görülür şekilde görüntü ortaya çıkarılabilmektedir. Bu sorunu ortadan kaldırmanın bir yolu, pay görüntülerin de ayrıca şifrelenmesidir. Bu tez çalışmasında, görüntülere ilk olarak AT-GSP şeması uygulanmış, ortaya çıkan pay görüntülere de kaos tabanlı görüntü şifreleme tekniklerinden biri olan iki boyutlu sinüs tabanlı lojistik kaos haritası (2D-STLH) uygulanmıştır. Böylelikle AT-GSP şeması ile 2D-STLH birlikte kullanılmıştır. Bu işlemde ilk olarak, gri tonlu görüntüler AT-GSP şemasıyla paylara ayrılırken ilk önce Jarvis algoritması ile ikili görüntülere çevrilmiştir. Renkli görüntüler ise ilk olarak RGB kanallarına ayrılmış, daha sonra Jarvis algoritması ile ikili görüntülere çevrilmiştir. Elde edilen ikili görüntüler, AT-GSP şeması ile paylara ayrılmış daha sonra da 2D-STLH ile şifrelenmiştir. Bu yöntem ile pay görüntüler elde edilse bile üst üste getirilerek gizli görüntü ortaya çıkarılamayacaktır. Şifrelenmiş pay görüntülere anahtar duyarlılık analizi, histogram analizi veri kaybı ve tuz-karabiber saldırıları yapılmıştır.

Bilim Kodu	:	92403
Anahtar Kelimeler	:	Görsel şifreleme, ilerleyici paylaşım şeması, ayrıcalık tabanlı görsel sır paylaşım şeması, kaotik haritalar, 2D-STLH, PSNR, SSIM, CQM
Sayfa Adedi	:	60
Danışman	:	Doç. Dr. Nurettin TOPALOĞLU

DEVELOPMENT OF CHAOTIC ENCRYPTED PRIVILEGE BASED VISUAL SECRET SHARING MODEL

(M. Sc. Thesis)

Aytekin YILDIZHAN

GAZİ UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

May 2018

ABSTRACT

The secret sharing (SS) scheme is a cryptographic method that the secret data is reconstructed when sufficient number of users come together. With this method, the secret data is not found in one person and can be solved only by a certain number of people. In the visual secret sharing (VSS) scheme, the secret data is an image. The secret image is divided into a certain number of shares and one share is distributed to each user. All the necessary shares have to be overlapped to reveal the secret image and all shares have equal importance. In the privilege-based VSS (PVSS) scheme, each share has a unique privilege and a higher-privilege share contributes more privilege to reveal the secret image. However, in the PVSS scheme, when several images with the higher priority are superimposed, the secret image can be visibly displayed. One way to remove this problem is to encrypt the share images separately. In this thesis, first PVSS scheme was applied to the images and two-dimensional Logistic-adjusted-Sine map (2D-LASM), one of the chaos-based image coding techniques, was applied to the resulting share images. Thus, PVSS scheme and 2D-LASM were used together. In this process, when grayscale images are divided into shares with the PVSS scheme, they are first converted to binary images by the Jarvis algorithm. Color images were first separated into RGB channels, then converted to binary images by the Jarvis algorithm. These binary images were divided into shares with the PVSS scheme after that, these shares were encrypted with 2D-LASM. With this method, even if the share images are obtained, it cannot be brought up to reveal the hidden image. Key sensitivity analysis, histogram analysis, data loss and salt-pepper noise attacks were performed on the encrypted share images.

Science Code : 92403

Key Words : Visual cryptography, progressive sharing scheme, privilege-based visual secret sharing scheme, chaotic maps, 2D-LASM, PSNR, SSIM, CQM

Page Number : 60

Supervisor : Assoc. Prof. Nurettin TOPALOĞLU

TEŞEKKÜR

Tezimin her aşamasında desteklerini esirgemeyen ve beni yönlendiren çok değerli danışmanım Doç. Dr. Nurettin TOPALOĞLU'na, tezimin oluşumunda büyük yardımları olan, desteğini sürekli hissettiğim değerli hocam Nurettin DOĞAN'a, iş yerindeki çalışma arkadaşlarıma ve çalışmam esnasında maddi ve manevi her türlü desteğini hissettiğim sevgili eşim Reyhan YILDIZHAN'a saygı ve teşekkürlerimi sunmayı bir borç bilirim.

İÇİNDEKİLER

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

RESİMLERİN LİSTESİ

Resim **Sayfa**

Resim **Sayfa**

SİMGELER VE KISALTMALAR

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

Simgeler	**Açıklamalar**
a	İnkâr hata sayısı
b	İhanet hata sayısı
c	Kombinasyonel hata sayısı
$\boldsymbol{C(x,y)}$	SSIM hesabında kontrast hesabı
d	Toplam hata sayısı
$\boldsymbol{L(x,y)}$	SSIM hesabında parlaklık hesabı
$\boldsymbol{n}$	Pay sayısı
$\boldsymbol{S(x,y)}$	SSIM hesabında yapı hesabı
∨	Mantıksal VEYA işlemi
$\oplus$	Mantıksal XOR işlemi

Kısaltmalar	**Açıklamalar**
2D-LASM	Two dimensional Logistic-adjusted-Sine map
2D-SIMM	Two dimensional Sine ICMIC modulation map
2D-SLMM	Two dimensional Sine Logistic modulation map
2D-STLH	İki Boyutlu Sinüs Tabanlı Lojistik Harita
AES	Advanced Encryption Standart
AP	Ayrıcalık Tabanlı Paylar
AT-GSP	Ayrıcalık Tabanlı Görsel Sır Paylaşım
CMY	Cyan Magenta Yellow
CQM	Color Image Quality Measure
ÇKT	Çinli Kalan Teoremi
dB	Desibel
DES	Data Encryption Standart
GA	Gizli Anahtar

Kısaltmalar	Açıklamalar
GSP	Görsel Sır Paylaşım
KE	Kolmogorov Entropi
LB	Lyapunov Boyutu
LSB	Least Significant Bit
LÜ	Lyapunov Üsleri
MSE	Mean Squared Error
PSNR	Peak Signal-to-Noise Ratio
RGB	Red Green Blue
RSA	Ron Shamir Adleman Şifrelemesi
SP	Sır Paylaşımı
SSIM	Structural Similarity Index
YG	Yarı Tonlu Görüntü

1. GİRİŞ

Günümüzde teknolojide yaşanan gelişmeler ışığında internet kullanımı oldukça yaygınlaşmıştır. Bunun başlıca sebebi, bilgiye ulaşma ve paylaşma isteğinin oldukça fazla olmasıdır. İnternetin halka açık olması, her ne kadar bilgilerin çok çabuk bir şekilde yayılmasına olanak sağlasa da birtakım güvenlik sorunlarını da beraberinde getirmiş ve özellikle mahrem olması gereken verilerin üçüncü şahıslar tarafından elde edilmesine zemin hazırlamıştır.

Bilgi güvenliği, her türlü verinin yetkisiz bir şekilde gözlenmesini, kullanılmasını, erişilmesini, değiştirilmesini ve hasar verilmesini önlemek olarak tanımlanmaktadır. Bu amaçla kullanılan yöntemlerden birisi şifrelemedir. Özellikle güvenilmeyen bir ortam olan internet ortamında ağ ve haberleşme güvenliği için şifreleme önemli bir araçtır [1]. Uygulanan şifreleme teknikleri, verinin türüne ve hangi amaca hizmet ettiğine göre değişiklik gösterebilmektedir.

Kriptoloji (şifreleme), çeşitli yazılı veya görsel verilerin belli bir sisteme göre şifrelenmesi, bu verilerin bir mesaj kanalında, alıcıya iletilmesi ve iletilmiş verilerin tekrar çözülmesi işlemidir [2]. Dolayısıyla kriptoloji işlemi, kriptografi ve kriptoanalizin bir birleşimidir. Şifre bilimi olan kriptolojinin bir alt çalışma alanı olan kriptografinin tam olarak Türkçe karşılığı şifre yazımıdır. Kriptografi genel olarak 4 ana madde ile ilgilenmektedir:

- Gizlilik: Gizlenmek istenen veri, yetkisiz kişiler tarafından anlaşılmamalıdır.
- Bütünlük: Gizlenmek istenen verinin bütünlüğü, ağ ortamında iletimi veya saklanması esnasında farkına varılmadan değiştirilmediği bilinmelidir.
- Reddedilemezlik: Gizlenmek istenen verinin, o veriyi oluşturan ya da gönderen kişi tarafından daha sonra kendisinin oluşturduğunu ya da gönderdiğini inkâr edememelidir.
- Kimlik belirleme: Gizli veriyi gönderen ve alan kişiler birbirlerini doğrulayabilmelidir [3].

Şifreleme işlemiyle düz metin, bir anahtar ile şifreli metne dönüştürülür. Böylelikle bu veri, üçüncü şahısların anlayamayacağı bir hale getirilmiş olur. Şifre çözme işlemiyle de şifreli metin, şifrelendiği anahtar ile işleme sokularak gizli metin elde edilir. Bu genel şifreleme mantığına dayanan Sezar, affine, permütasyon ve vigenere gibi geleneksel

şifreleme yöntemleri eskiden beri kullanılmaktadır. Çok eski çağlardan günümüze kadar gelişmekte olan kriptoloji teknikleri, teknolojide yaşanan gelişmeler ışığında dijital veriler ile daha farklı bir anlam kazanmıştır. Dijital veriler olarak adlandırdığımız ses, görüntü ve video gibi veri türlerinin gelişmesi ile birlikte, bu türlerin şifrelenmesinde kullanılan kriptoloji teknikleri de bu gelişime bağlı olarak gelişmiştir.

Metin şifrelemesinde Data Encryption Standart (DES), Advanced Encryption Standart (AES) ve Ron Shamir Adleman Şifrelemesi (RSA) [4-6] gibi şifrelemeler kullanırken, dijital verilerden olan görüntü şifrelenmesinde bu tip şifreleme tekniklerinin kullanılması zor olabilmektedir. Bunun sebebi, görüntüler metinlere göre daha çok yer kapladığı için şifreleme yapılırken daha uzun süre harcanır. Üstelik şifresi çözülen metin ile orijinal metnin bire bir aynı olması gerekirken görüntüler için böyle bir zorunluluk yoktur [7]. Özellikle askeri, istihbarat ve tıbbi görüntüler gibi önem derecesi yüksek olan verilerin geleneksel şifreleme yöntemleri ile şifrelenmesi, oldukça zor ve maliyetli olacaktır. Ayrıca sayısal damgalama ve görüntü gizleme yöntemlerinde görüntü şifrelendikten sonra tek bir haberleşme kanalından gönderime uygun olması güvenlik sorununu ortaya çıkarmaktadır [8]. Görüntü şifrelemede, geleneksel ve tek haberleşme kanalından gönderime uygun olan şifreleme yöntemlerinden farklı olarak önerilen çözümlerden birisi sır paylaşım (SP) şemasıdır.

SP şeması, ilk kez birbirinden bağımsız olarak Blakley ve Shamir tarafından önerilmiştir [9, 10]. Bu yöntemde gizli veri tek bir kullanıcıda bulunmayıp istenilen sayıdaki kullanıcıya paylaştırılır. Paylaştırılan kullanıcılar bir araya geldiklerinde gizli veri ortaya çıkarılır. SP şeması yöntemlerinden birisi olan, Naor ile Shamir tarafından önerilen [11] Görsel Sır Paylaşım (GSP) şemasında görüntü, hiçbir bilgi taşımayan n adet görüntülere dönüştürülür ve bu görüntüler her bir kullanıcıya yalnızca birer adet paylaştırılır. “Pay” adı verilen bu görüntülerden en az r adedinin üst üste bindirilmeleri ile hiçbir geleneksel şifreleme yöntemi kullanmadan gizli görüntü elde edilir. $r-1$ adet pay görüntü elde edildiğinde bile üst üste bindirildiğinde gizli görüntü hiçbir şekilde açığa çıkmayacaktır. Bu sisteme (r,n)-GSP şeması adı verilmiştir.

Gizli görüntünün ortaya çıkmasını zorlaştırmak adına pay görüntü sayısı artırılabilir, fakat bu yöntem maliyeti artırmaktadır. Eğer pay görüntü sayısı çok fazla olursa, gizli görüntüyü oluşturmak giderek zorlaşacaktır. Maliyet problemini çözmek ve pay görüntülerin daha

kolay yönetilebilmesini sağlamak adına birçok çalışma yapılmıştır. Aşağıda bu çalışmalardan bazılarına ait kullanılan yöntemlere değinilmiştir.

Fang ve Lin, ikili görüntüler üzerinde ilerleyici GSP şemasını tanımlamışlardır [12]. Geleneksel GSP şeması, gizli görüntünün ortaya çıkması için gerekli olan tüm pay görüntülere ihtiyaç duyan bir eşik mekanizmasına sahiptir. İlerleyici GSP şemasında ise her bir pay görüntü eklendikçe, gizli görüntü de yavaş yavaş ortaya çıkmaktadır. Yani gizli görüntünün ortaya çıkması için bütün pay görüntülere ihtiyaç duyulmamaktadır. Bu çalışmada gizli görüntüdeki her bir pikseli 2×2'lik bloklara dönüştürülmüştür. Eğer siyah piksel şifrelenecekse, 2×2'lik bloğun hepsi siyah olmalı, beyaz piksel şifrelenecekse, 2×2'lik bloğun rastgele seçilmiş 2 pikseli beyaz olmalıdır. Fakat piksel genişlemesi yüzünden daha fazla bellek ve zaman gerekmiştir.

Hou ve Quan yaptıkları çalışmada, Fang ve Lin'in [12] çalışmasının piksel genişlemesine sahip olduğunu ve bundan dolayı gereksiz depolama alanı ile transfer zamanı kullanıldığını, aynı zamanda birleştirilen pay görüntülerin düşük görsel kaliteye sahip olduklarını belirtmişlerdir. Hou ve Quan yaptıkları çalışmada bu dezavantajları giderdiklerini ifade etmişlerdir [13].

Jin ve diğerleri ilerleyici GSP şemasını renkli görüntülere uygulamışlardır [14]. Fang yaptığı çalışmada ilerleyici GSP şemasında pay görüntüleri ile stego görüntüleri beraber kullanmıştır [15]. Bir görüntüye bir metin gömüldüğü zaman o görüntüye stego görüntüsü adı verilmiştir [16]. Böylelikle Fang, pay görüntülerin daha kolay yönetilebilmesini sağlamıştır. Bu çalışmalarda her bir pay görüntü üst üste geldikçe gizli görüntü, kademeli olarak görülmeye başlanmaktadır. Ancak, görüntü geri elde edilirken kullanılan metotlardan dolayı piksel genişlemesi meydana gelmiş ve elde edilen görüntü orijinal görüntünün boyutunun 4 katına çıkmıştır [12, 14, 15].

Wang ve diğerleri önerdikleri metotla pay görüntülerinden geri elde ettikleri görüntüyü kayıpsız ve aynı boyutta elde etmişlerdir [17]. Üstelik de pay görüntülerinin küçük boyutta kalmasını sağlamışlardır.

Gizli görüntünün ortaya çıkarılması esnasında, askeri kurumlar, kamu kuruluşları ve kurumsal olarak hiyerarşik şekilde çalışan şirketlerde olduğu gibi, paylar arasında da

ayrıcalık sırası olması beklenebilir. Dolayısıyla bu tür kurumlarda çalışan kişilere, bulundukları konumlara göre, gizli görüntüyü ortaya çıkarmak için daha yüksek önceliğe sahip olan pay görüntülerinin paylaştırılması gerekebilir. Fakat yapılan çalışmaların çoğunda, bu durum dikkate alınmamıştır [9-15, 17]. Bu ihtiyacı gidermek için ayrıcalık tabanlı bir paylaşım modeli kullanılması gereği ortaya çıkmıştır. Buradaki ayrıcalığın anlamı, pay görüntünün gizli görüntüyü ortaya çıkarma kapasitesidir.

Hou yaptığı çalışmada, paylar arasında önem sırasını ortaya koyan bir yaklaşım önermiştir [18]. Hou çalışmasında, renkli görüntülerin paylarını oluşturmak için rastgele belirlediği bir maske ile üç ana rengi temsil eden CMY'yi (Cyan, Magenta, Yellow) kullanmıştır. Böylelikle dört adet pay üretilmiştir. Maske üst üste getirilen paylarda istenilmeyen renkleri kapatmak için oluşturulurken üç ana renk ise renkli pay görüntüleri temsil etmektedir. Her ne kadar paylar arasında ayrıcalık olmasa da maskeye göre üstü üste getirilen paylar değişmektedir. Bu durumda maske pay görüntüsü, diğer pay görüntülere göre daha ayrıcalıklı olmaktadır. Fakat bu yöntemde gizli görüntünün boyutu 4 katına çıkmış ve şifreleme sadece dört adet pay görüntüsü ile sınırlı kalmıştır.

Chen ve diğerleri, grup tabanlı ağırlıklı GSP şemasını önermişlerdir [19]. Payları birbirinden farklı gruplara bölmüşler ve grup içerisinde de paylara birer ağırlık vermişlerdir. Chen'in çalışmasında pay görüntüler katmanlara ayrılmış, aynı katmanda bulunan payların boyutları aynı olacak şekilde ayrılmışlardır. Payların boyutu küçük olunca daha aşağıdaki katmana yerleştiğinden, bu yöntem katmanların ortaya çıkmasına sebebiyet vermiştir.

Lin ve diğerleri ağırlıklarına göre payların boyutlarını belirlemişlerdir [20]. Payın boyutu büyük olması demek ağırlığının da büyük olması anlamına gelmektedir. Bu da payın önem sırasını ortaya çıkarabilmektedir. Payların önem sırası belli olursa daha önemli pay görüntüsünün ele geçirilme olasılığı artmaktadır.

Li ve diğerleri payların kendi aralarında önem sırasını belirleyen bir çalışma yapmışladır [21]. İlerleyici GSP şemasındaki pay görüntüleri zorunlu olarak yüksek öneme sahip ve zorunlu olmayan düşük öneme sahip olarak iki gruba ayırmışladır. Daha sonra bu gruplara önemli ve önemsiz olarak ara pay görüntüleri de eklenmiştir. Fakat bu çalışmada payların

yönetilmesi zorlaşmıştır. Ayrıca önemli olmayan paylar, önemli olan paylardan daha büyük boyutlu olmuştur. Boyutların farklı olması payların önem sırasını açığa çıkarmıştır.

Pay görüntülerinin önem sıralamasını Hou ve diğerleri yaptıkları çalışmada göstermişlerdir [22]. Pay görüntüler ayrıcalık seviyesi en düşükten en yükseğe göre sıralanmıştır. Böylelikle her bir pay, eşsiz bir ayrıcalık düzeyine sahip olmuştur. Payların ayrıcalık düzeyi, ilgili pay görüntüde bulunan siyah pikselin oranı ile ayarlanmıştır. Yani, pay görüntüde ne kadar siyah piksel varsa önem sırası o kadar yüksek olacaktır. Çünkü insan görme sisteminin ikili görüntülerde siyah pikseli beyaza nazaran daha kolay seçebilmesidir. Bu yöntemin avantajları, her bir payın orijinal görüntü ile aynı boyutta kalması, her bir payın kendi önemine göre gizli bilgiyi ortaya çıkarmak için uygun kapasiteye sahip olması ve geleneksel GSP yöntemlerine göre birleştirilen görüntünün daha iyi kontrasta sahip olmasıdır. Bu çalışmaya ayrıcalık tabanlı görsel sır paylaşım şeması (AT-GSP) adı verilmiştir.

AT-GSP şemasında gizli görüntü paylara ayrıldıktan sonra, en yüksek ayrıcalığa sahip birkaç pay görüntünün üst üste getirilmesiyle gözle görülür seviyede gizli görüntü ortaya çıkması, bir güvenlik sorunu yaratmıştır. Bu tez çalışmasında ilk olarak, AT-GSP şemasında oluşan güvenlik probleminin gözle görülür bir seviyede olduğu ortaya konmuş ve matematiksel olarak ifade edilmiştir. Daha sonra AT-GSP şemasından doğan bu probleme, her bir pay görüntüye kaos tabanlı görüntü şifrelemesi uygulanarak bir çözüm getirilmiştir.

Yazılı metinlerin aksine, görüntülerdeki komşu pikseller arasında güçlü derecede korelasyon ve yüksek tutarlılık olması ile görüntünün çok yer kaplamasından dolayı geleneksel şifreleme teknikleri (DES, AES, RSA ve benzeri) uygun olmamaktadır [23]. Bu tez çalışmasında özel olarak pay görüntülerinin, kaos haritaları kullanarak şifrelenmesi ile sağlanacaktır. Çünkü kontrol parametre ve anahtar duyarlılığı, sistemin başlangıç durumu, tahmin edilemezliği, ergodikliği (geçmiş bilgilerden yararlanarak geleceğe dair bilgi üretme), esnekliği ve hızı sayesinde kaos haritaları daha uygun olacaktır [24, 25]. Ayrıca, kaosun dinamik özelliklerinden olan başlangıç durumu hassasiyeti ve kontrol parametre hassasiyetinin, kriptografinin permütasyon ve difüzyon aşamaları arasında benzerlik göstermesi, kaotik sistemlerinin kriptografiye uygulanmasını daha popüler kılmıştır [26].

Dijital görüntülerin korunmasında ve aktarılmasında kaos tabanlı görüntü şifreleme yöntemleri üzerine literatürde birçok çalışma vardır. Kaos tabanlı şifrelemede güvenlik düzeyi, kullanılan kaos haritasının performansına bağlı olarak değişir [25]. Kaos haritaları bir boyutlu ve çok boyutlu haritalar olmak üzere iki sınıfta ayrılır. Lojistik, Gauss, Sinüs ve Çadır haritaları gibi bir boyutlu kaos haritalarının başlangıç durumları ve kaotik yörüngeleri yapılan çalışmalar ile tahmin edilebilmektedir [26].

Arroyo ve diğerleri yaptıkları çalışmada, bir boyutlu kaos haritaya uygulanan kontrol parametre tahmini ve zamanlama saldırıları sonucunda, gizli anahtar bilinmeden bu kaotik algoritmanın doğrusallığı üzerine zayıflıklar ortaya koymuşladır [24].

Tang ve Guan yaptıkları çalışmada, zaman gecikmeli Lojistik ve Mackey-Glass haritalarında kontrol parametrelerini genetik algoritma mantığını kullanarak tahmin edebilmişlerdir [27]. Dolayısıyla bu tür zayıflıklar, bir boyutlu kaos haritalarında güvenlik zafiyetine sebebiyet vermiştir [23, 24, 26].

Çok boyutlu kaos haritalarında ise sistemin daha çok karmaşık olması, daha çok değişken ile parametre kullanılmasından dolayı tahmin edilemezliği daha fazladır [24, 26-28]. Dolayısıyla pay görüntülerini çok boyutlu kaos haritası ile şifrelemek daha uygun olacaktır. Fakat çok boyutlu kaos haritasında parametre sayısı fazla olduğu için sistem ihtiyaçları daha pahalı ve hesaplama karmaşıklığı fazla olabilmektedir [23, 25]. Aynı zamanda birden fazla kaos haritası kullanmak, hesaplama süresini artırabilmektedir [29]. Bu yüzden çok boyutlu kaos haritasının düşük hesaplama süresi ve yüksek derecede kaos özelliği göstermesi önemlidir [30]. İki boyutlu sinüs tabanlı lojistik kaos haritası (2D-STLH), bu özellikleri sağlayan çok boyutlu bir kaotik şifreleme yöntemidir [25].

Bu tez çalışmasında, yukarıda açıklanan çalışmalardan farklı olarak, bir GSP şeması ile bir kaotik görüntü şifreleme yöntemi bir arada kullanılmıştır. Böylelikle, AT-GSP şeması ile 2D-STLH birleştirilerek daha güvenilir bir yöntem oluşturulmuştur. Bu yöntemde şifreleme aşamasında, AT-GSP aşamasında belirtilmeyen ara işlem olarak Jarvis algoritması kullanılmıştır [31]. Şifre çözme aşamasında ise renkli görüntüleri geri elde ederken, RGB (Red, Green, Blue) kanallarında bulunan 1 piksel değerinin 255 olarak değiştirilmiştir. Böylelikle sekiz adet renk geri elde edilmiştir. Bu işleme kaotik şifrelemeli

AT-GSP şeması adı verilmiş olup [32] ikili (siyah beyaz), gri tonlu ve renkli görüntülere başarıyla uygulanmıştır.

Bu çalışmada, gizlenecek görüntü ilk olarak AT-GSP şemasında anlamsız pay görüntülere ayrılmış ve daha sonra bu pay görüntüler 2D-STLH ile şifrelenmiştir. Böylelikle AT-GSP şeması ile oluşan güvenlik açığına bir çözüm önerilmiştir.

Başlangıçta, AT-GSP şeması için görüntüler ikili görüntü olmak zorundadır. Dolayısıyla ikili görüntüler sistemde doğrudan şifrelenirken gri tonlu görüntüler Jarvis algoritması ile ikili görüntülere çevrilmiştir. Gri tonlu görüntüler ikili görüntüye çevrildikten sonra oluşan paylara, ikinci aşamada 2D-STLH şifrelemesi uygulanmıştır.

Renkli görüntülerde şifreleme yaparken görüntü ilk olarak RGB kanallarına ayrılmış, daha sonra Jarvis algoritması ile renk kanalları ikili görüntüye çevrilmiştir. Her bir kanal için yukarıda bahsedilen AT-GSP ve 2D-STLH işlemleri sırasıyla uygulanmıştır.

Şifre çözme aşamasında ilk olarak gizli görüntü, ikili veya gri tonlu ise, şifreli pay görüntülere 2D-STLH'ın işlem basamakları sırasıyla ve ters yönde uygulanmış, paylar üst üste bindirilmiş ve gizli görüntü elde edilmiştir. Renkli görüntülerde ise, 2D-STLH ile şifrelenen her bir kanalın pay görüntüleri çözüldükten sonra pay görüntüler üst üste bindirilmiş ve tekrar oluşturulan RGB kanalları birleştirilmiştir. Birleştirilen RGB kanallarından renkli görüntüyü elde etmek için 1 olan piksel değerleri 255 olarak değiştirilmiş ve gizli görüntü geri elde edilmiştir.

Tezin son aşamasında ise ortaya konan bu yöntemin işlerliğini (doğruluğunu) ölçmek için, histogram analizi, anahtar duyarlılık analizi, veri kaybı saldırıları ve tuz-karabiber gürültü saldırıları yapılmıştır. Ortaya çıkan deney sonuçları hem görsel hem de matematiksel olarak açıklanmış ve yöntemin güvenilir olduğu görülmüştür.

Tez çalışmasının bundan sonraki bölümleri, sırasıyla aşağıda belirtilen ana başlıklar üzerinde durulmuştur. Bölüm 2'de sır paylaşım şeması hakkında genel bilgiler verilmiştir. Bölüm 3'te tezde yararlanılan yöntemler ve araçlar açıklanmıştır. Bu bölümde AT-GSP şeması ve 2D-STLH hakkında bilgiler verilmiştir. Bölüm 4'te bu iki şifrelemenin birleştirilmesi ile oluşan yeni yöntemin ikili, gri tonlu ve renkli görüntülerdeki uygulaması

ile bu yönteme uygulanan analizler ve saldırı sonuçları belirtilmiştir. Bölüm 5'te ise ilgili çalışmadan çıkarılan sonuçlar ve önerilerden bahsedilerek sonuçlar yorumlanmıştır.

2. SIR PAYLAŞIM ŞEMASI

Kullanılan şifreleme yöntemlerinde ilk yöntem anahtarın kopyalanmasıdır. Şifrelemede anahtar kavramı, matematiksel yöntemler kullanılarak verinin anlaşılmaz hale gelmesi ve ancak doğru kişiler tarafından açılması için bir araç demektir. Eğer anahtar kaybolsa veya zarar görse bile kopyalanan anahtar ile sistem çalışmaya devam edebilir. Diğer bir yöntem ise anahtarın parçalara ayrılmasıdır. Bu sistemde anahtar eğer n adet parçaya ayrılırsa, sistemin çalışması için de n adet parçanın bir araya gelmesi gerekir [33]. Fakat bu yöntemlerde güvenlik zafiyetinin çok olması ve ele alınan yöntemlerin kullanışsız olması sebebiyle, Shamir yaptığı çalışmada [10] anahtarı parçalayıp kullanıcılara dağıtmış ve parçaladığı bu anahtarların daha azı ile tekrar oluşturulabileceğini göstermiştir. Bu sistemde, verinin (D) n adet parçaya ayrılıp en az r adedi bir araya getirildiğinde, verinin ortaya çıkacağını, fakat $r-1$ ve daha azı bilinse bile D'yi elde edilemediği anlatılmıştır. Ayrıca hiçbir kullanıcı da elindeki bilgiyi diğeri ile paylaşmayacaktır [34]. Bu sisteme (r,n) eşik şeması adını vermiştir. Bu teknikle şifreleme güvenliğinin artırılması hedeflenmiştir.

Blakley de [9] Shamir'den bağımsız olarak bu problemi çözmeye çalışmıştır. Shamir bu problemi interpolasyon ile çözerken, Blakley uzayda vektörlerle ve hiper düzlemlerle açıklamıştır. Blakley çalışmasında şifre çözümünde yapılan hataları inkâr (abnegation), ihanet (betrayal) ve ikisini de içeren kombinasyonel (combination) hata olarak üçe ayırmış ve bu hatalara sayısal değer vermiştir. Olayların sayımı üzerine iki adet temel prensipten bahseden Blakley, ilk prensipte Boole içerme-dışlama kuralına göre inkâr hatalarına a, ihanet hatalarına b ve kombinasyonel hatalara c diyerek toplam hata sayısını $d=a+b-c$ olarak belirtmiştir. İkinci sayma prensibine göre ise bu iki ayrı olayın aynı anda olması çok nadir olacağı için kombinasyonel hatayı 0 (sıfır) olarak alınabildiğini söylemektedir. Dolayısıyla elimizde eğer en az $a+b+1$ sayıda bir koruma durumumuz olursa, güvenliğimizi sağlayabileceğimizi vurgulamıştır [9].

Blakley'in önermiş olduğu eşik şemasına göre gizli bilgi r boyutlu uzayda bir noktadır. Bir noktada kesişen hiper düzlem denklemleri, kullanıcılara gönderilecek olan bilgileri oluşturur. n adet kullanıcının her biri kesişen düzlem denklemlerinden birine sahiptir. Kullanıcılardan herhangi r adedinin bir araya gelmesi, geometrik olarak düzlem

denklemlerinin kesiştirilmesi anlamına gelir. Düzlemlerin kesişimi ise r boyutlu uzaydaki noktayı yani gizli bilgiyi tanımlar. $(2, 2)$ eşik seması için örnek verilecek olursa, $r = 2$ olduğu için gizli bilgi iki boyutlu uzayda bir noktadır. Kullanıcılara gönderilecek olan bilgiler ise iki boyutlu uzayda bu noktada kesişen doğrulardır. n farklı doğrudan $n = 2$ olduğu için herhangi iki adedinin bir araya gelmesi sonucu, doğruların kesişimi olan gizli bilgi yeniden ortaya çıkmış olacaktır.

McEliece ve Sarwate'nin çalışmasında [35], Reed-Solomon kodları kullanılarak Shamir'in geliştirmiş olduğu yönteme genişletme ve genelleme sağlamışlardır. Reed-Solomon kodları ile yetkisi olmayan kişilerden ve sistem kusurlarından doğan hatalara karşı koruma getirmişlerdir. Reed-Solomon kodları ile anahtara veri sıkıştırma uygulanmış olsa da bunun güvenli olmadığı görülmüştür.

Mignotte ve Asmuth ile Bloom, Shamir'in yapmış olduğu (r, n) eşik şemasını Çinli Kalan Teoremi (ÇKT) ile çözmeye çalışmışlardır [36, 37]. ÇKT'de seçilecek sayılar aralarında asal olmalıdır. ÇKT'ye göre yapılan çözüm, tek ve biricik bir çözüm olduğu için (r, n) şemasına göre uygun bir çözüm bulunmuştur. Shamir'in interpolasyonu [10] $O(k \times \log_2 k)$ karmaşıklığına sahipken Asmuth ve Bloom'un ÇKT ile yapmış olduğu şema, $O(k)$ karmaşıklığında çözülebilmektedir [38].

2.1. Görsel Sır Paylaşım Şeması

Matematik üzerine yapılan SP şeması çalışmalardan sonra [9, 10, 35-37], ilk kez Naor ve Shamir, görüntüler üzerinde uygulanabilecek yeni bir şifreleme yöntemi geliştirmişlerdir [11]. Yapılan bu çalışma ile, Shamir'in ortaya koymuş olduğu (r, n) eşik şeması [10], ikili görüntüler üzerine uygulanmıştır.

Şifrelenecek olan görüntü, el yazısı notu veya yazıcı çıktısı gibi siyah beyaz piksellerden oluşan görüntüler olabilir. Geleneksel hiçbir şifreleme yöntemi kullanılmadan sadece insanın görme sistemi ile gizlenen görüntü ortaya çıkabilmektedir. GSP şeması olarak literatüre geçen bu sistemde görüntü, n adet anlamsız görüntüye çevrilir ve bu görüntüler her bir kullanıcıya birer adet gönderilir. Oluşturulan bu anlamsız görüntülerin her birine 'pay' denir. Bu paylardan en az r adedi üst üste bindirilmeleri suretiyle gizli veri ortaya

çıkacaktır. Eğer $r-1$ veya daha az pay görüntüsü üst üste getirilirse gizli görüntü elde edilemeyecektir. Bu da aslında Shamir'in yapmış olduğu interpolasyon yönteminin uygulamaya dönüştürülmüş halidir [11].

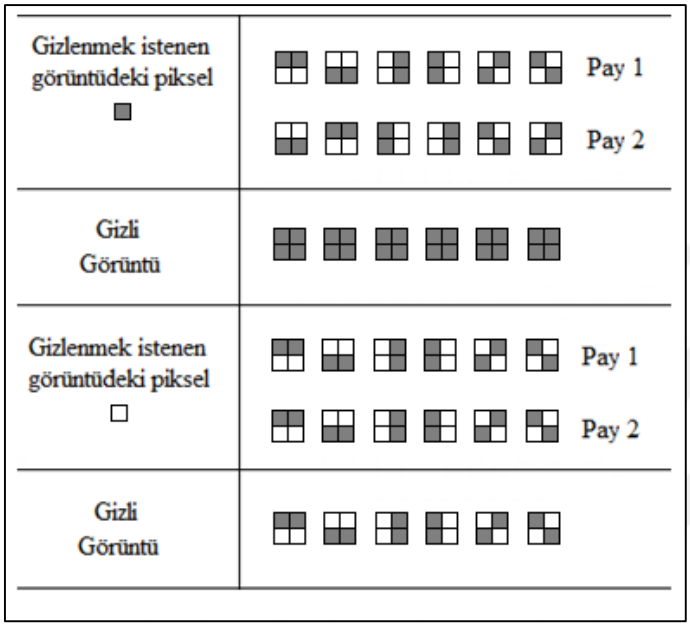
Yapılan bu çalışmada, (r,n) eşik şemasının belli kurallar çerçevesinde tanımı yapılmıştır. En uygun şekilde seçilebilecek r ve n değerleri üzerine araştırmalar yapılmış, genel olarak (r,r) ve (n,n) eşik şemaları üzerine tanımlamalar ve ispatlar yapılmıştır [38-43]. GSP şeması için 3 önemli parametre tanımlanmıştır [11]:

1. Gizlenmek istenen görüntüdeki her bir piksel, m adet alt piksele bölünmüştür. Bu rakam, orijinal resmin kaybettiği çözünürlüğü temsil etmektedir ve olabildiğince küçük bir değer olmalıdır.
2. Ortaya çıkan yeni görüntüdeki beyaz piksel ile siyah piksel ağırlıklarının farkına göreceli fark (relative difference - α) adı verilmiştir ve olabildiğince büyük bir değer olması gerekmektedir.
3. Oluşturulacak olan payların C_0 ve C_1 adı verilen matrislerden seçilirken, bu matrislerin boyutları olan s'nin belirlenmesidir. Bu matrislerin boyutlarının aynı olmasına gerek yoktur fakat bu çalışmada [11] aynı boyutlarda alınmıştır. $\log_2 s$ işlemi bir payın üretilmesi esnasında gerekli olan rastgele bit sayısını temsil etmektedir.

Önerilen şemanın en büyük avantajı, hiçbir şifreleme hesabı olmadan insanın görme sistemine dayalı bir çözüm üretilmiş olmasıdır. Bunun yanında elde edilen gizli görüntüde piksel genişlemesi ve kontrast kaybı yaşanmaktadır. Bundan sonraki yapılan çalışmalarda Naor ve Shamir'in ortaya koymuş olduğu şema örnek alınmış, optimum çözümler üzerine çalışılmış [39], gri tonlu görüntülere [42, 44] ve renkli görüntülere uygulanmış [18, 43, 45], tek bir gizli görüntü yerine birden fazla gizli görüntü kullanılmış [24, 46, 47], piksel genişlemesini ve kontrast kaybını önlemek üzere araştırmalar yapılmıştır [48, 49]. Gürültüye benzeyen pay görüntülerinin de anlamlı birer resme dönüşmesi ile [50] GSP şemasının araştırılma konuları bir hayli genişletilmiştir.

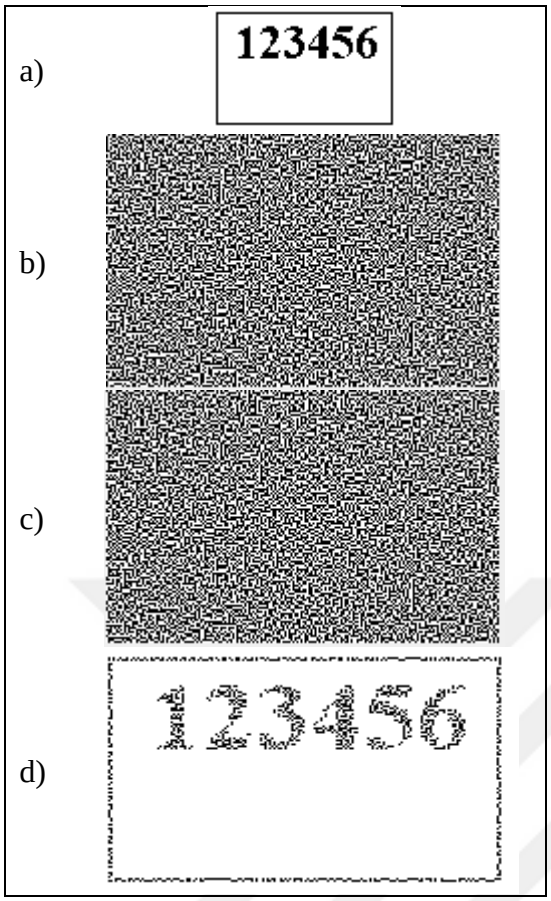
Gizli görüntünün 2 pay görüntüye ayrıldığı bir GSP şemasında siyah ve beyaz pikseller belirli bir kurala göre paylaştırılır. Naor ve Shamir'in çalışmasında örnek olarak verdikleri $(2,2)$-GSP şemasında, gizli görüntüdeki bir piksel, pay görüntülerde dört piksel olacak şekilde paylaştırılmıştır [11]. Bunun sebebi pay görüntüdeki büyüme, her ne kadar gizli

görüntünün dört katı olsa da en-boy oranının aynı kalmasını sağlamıştır. Şekil 2.1.'de verilen şemada, gizlenecek olan siyah ve beyaz pikseller için altı adet bloktan rastgele birisi seçilirken, diğer pay görüntü için de ilk seçilen bloğa uygun olan blok seçilmiştir. Siyah piksel 1 (bir), beyaz piksel de 0 (sıfır) olacak şekilde bu seçilen bloklar, mantıksal VEYA ($\vee$) işlemine sokulmuş ve gizli görüntü elde edilmiştir.



Şekil 2.1. $(2, 2)$-GSP şeması [51]

İkili bir görüntünün $(2, 2)$-GSP şeması ile şifrelenmiş hali ve gizli görüntünün elde edilirken genişlemiş hali Şekil 2.2.'de gösterilmiştir.



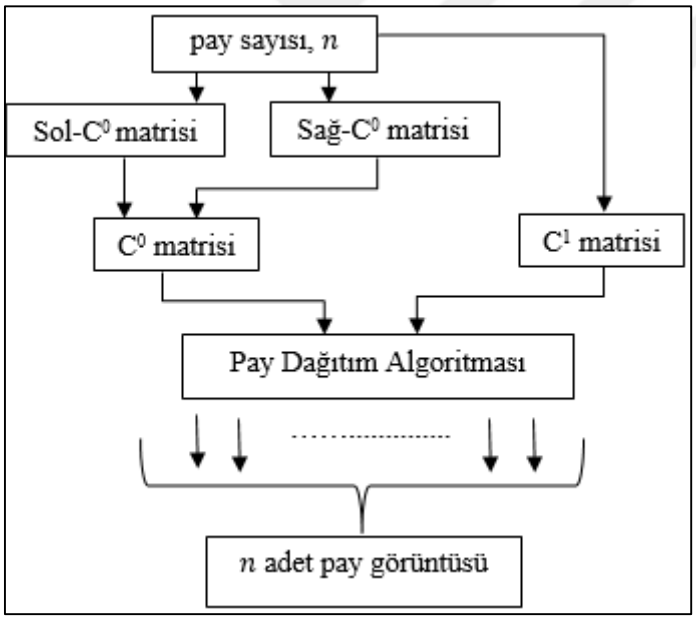
Şekil 2.2. Görsel şifreleme, (a) Gizlenecek görüntü, (b) Pay 1, (c) Pay 2, (d) Elde edilen görüntü

3. KAOTİK ŞİFRELEMELİ AT-GSP MODELİ

Bu bölümde, kaotik şifrelemeli AT-GSP modeli için kullanılan yöntemler anlatılmıştır. İlk olarak AT-GSP şeması, daha sonra 2D-STLH hakkında bilgi verilmiştir.

3.1. Ayrıcalık Tabanlı Görsel Sır Paylaşım Şeması

Bu bölümde, tez çalışmasının ilk aşamasını oluşturan AT-GSP şeması anlatılmıştır. Hou ve diğerlerinin yaptığı AT-GSP şemasında, ilk olarak pay sayısı yani "n" belirlenir. 0 (sıfır) beyaz pikseli, 1 (bir) de siyah pikseli temsil edecek şekilde, gizlenecek görüntüde beyaz ve siyah pikselleri paylaştırmak için $n \times m$'lik boyutlarında C^0 ve C^1 pay matrisleri oluşturulur. Beyaz piksel için C^0, siyah piksel için de C^1 pay matrisi kullanılmıştır [19]. AT-GSP şemasının akış diyagramı Şekil 3.1.'de gösterilmiştir.



Şekil 3.1. AT-GSP şeması akış diyagramı

3.1.1 Pay matrislerinin belirlenmesi

AT-GSP şemasında ilk olarak C^0 ve C^1 matrisleri şu kurallara göre belirlenir:

C^0 pay matrisinin belirlenmesi: C^0 matrisi sol-C^0 ve sağ-C^0 olarak iki parçadan oluşur. n pay sayısı ve satır sayısını ifade etmek üzere, sol-C^0 matrisinin sütun sayısı Eş. 3.1'e göre oluşturulur.

$$m_1 = n(n-1)/2 \tag{3.1}$$

Sol-C^0 matrisi $n \times m_1$ boyutunda olur. Sol-C^0 matrisinin $i'nci$ satırında $n - i$ adet beyaz (0) piksel olmalı ve farklı sütunlarda olmalıdır. Kalan boşluklar ise siyah (1) olmalıdır. Eğer bir görüntüyü 4 kişiye paylaştırmak istiyorsak $n = 4$ için, Eş. 3.1 kullanılır. Çıkan sonuç Eş. 3.2'deki gibidir.

$$m_1 = 4(4-1)/2 = 6 \tag{3.2}$$

Dolayısıyla sol-C^0 matrisinin 6 adet sütunu olmalıdır. Sol-C^0 matrisi $4\ x\ 6$ boyutunda bir matris olur. Sonra $i'nci$ satırında $4 - i$ tane beyaz (0)'lar, farklı sütunlarda olacak şekilde rastgele yerleştirilir (Bkz. Şekil 3.2. (a)). Diğer boş olan elemanlar da siyah (1) olarak doldurulur (Bkz. Şekil 3.2. (b)). 0'ların yerine göre birçok sol-C^0 matrisi elde edilebilir.

a)
$$\begin{bmatrix} 0 & 0 & & 0 & & \\ & & 0 & & 0 & \\ & & & & & 0 \\ & & & & & \\ & & & & & \end{bmatrix}_{4x6}$$

b)
$$\begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}_{4x6}$$

Şekil 3.2. 4×6'lık sol-C^0 matrisi, (a) 0'ların rastgele farklı sütunlara yerleşimi, (b) Kalan yerlerin 1 ile doldurulması

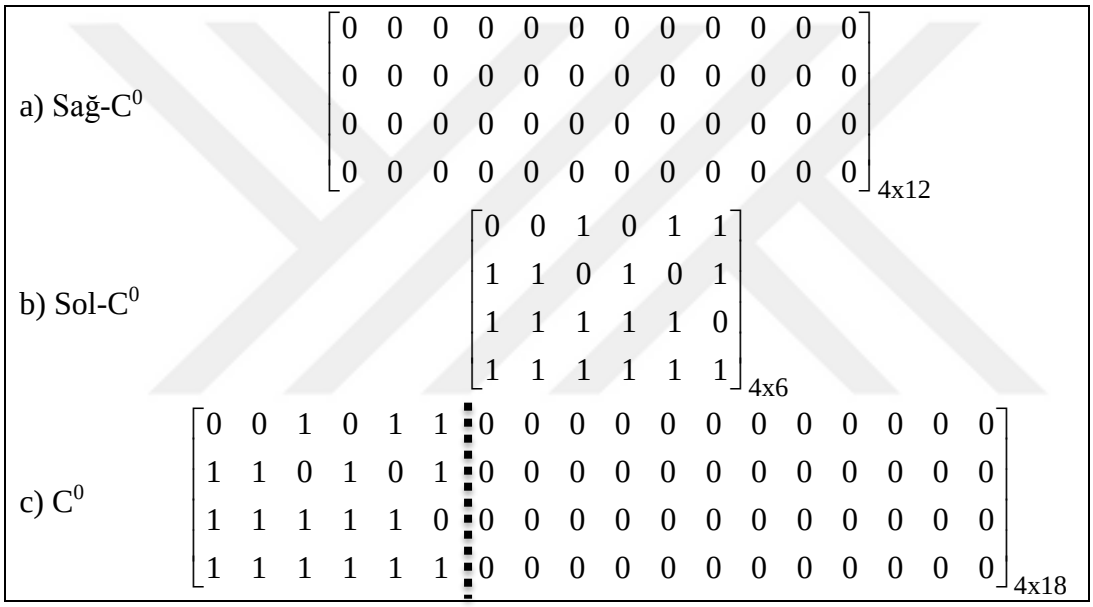
Sağ-C^0 matrisi ise sol-C^0 matrisi ile aynı satır sayısına sahiptir. Sütun sayısı ise Eş. 3.3'e göre hesaplanır.

$$m_2 = n(n-1)(n-2)/2 \tag{3.3}$$

Sağ-C^0 matrisinin tüm elemanları beyaz (0) olarak atanır. Bu işlemden sonra sol-C^0 ile sağ-C^0 matrisi yan yana getirilerek C^0 matrisini oluşturmuş olur. Görüntüyü 4 kişi paylaştığına göre, sağ-C^0 matrisinin sütun sayısı Eş. 3.4'e göre bulunur.

$$m_2 = 4(4-1)(4-2)/2 = 12 \tag{3.4}$$

Sonuç olarak sağ-C^0 matrisinin boyutu 4×12 olur (Bkz. Şekil 3.3. (a)). Tüm elemanları 0 olacak şekilde oluşturulur. Son olarak da sol-C^0 ile sağ-C^0 matrisi yan yana getirilerek C^0 matrisini oluşturur (Bkz. Şekil 3.3. (c)). C^0 matrisinin boyutu 4×18 olur.



Şekil 3.3. 4×12'lık sağ-C^0 matrisi, (a) Sağ-C^0 matrisinin tüm elemanların 0 olarak yerleştirilmesi, (b) 4×6'lık sol-C^0 matrisi, (c) Sol-C^0 ile sağ-C^0 matrisinin yan yana gelerek C^0 matrisini oluşturması

C^1 pay matrisinin belirlenmesi: C^1 matrisi de C^0 matrisi ile aynı satır ve sütun sayısına sahip olmalıdır. C^1 matrisinin sütun sayısı Eş. 3.5'e göre hesaplanır.

$$m = n(n-1)(n-1)/2 \tag{3.5}$$

Güvenliğin sağlanabilmesi için, C^1 matrisinin $i'nci$ satırındaki 1'lerin sayısı, sol-C^0 matrisinin $i'nci$ satırındaki 1'lerin sayısı ile eşit olmalıdır. $i'nci$ satırdaki 1'lerin sayısı Eş. 3.6'a göre bulunur.

$$A_i = (n^2 - 3n + 2i)/2 \tag{3.6}$$

Buna göre C^1 matrisinde 1'ler farklı sütunlarda olacak şekilde rastgele yerleştirilir (Bkz. Şekil 3.4. (a)). Geriye kalan yerler 0 ile doldurulur (Bkz. Şekil 3.4. (b)). C^1'nin boyutu da $n \times m$ olarak bulunur. Örneğimizde $n = 4$ idi. Bu durumda C^1 matrisinin sütun sayısı Eş. 3.7'ye hesaplanır.

$$m = 4(4-1)(4-1)/2 = 18 \tag{3.7}$$

Ayrıca Eş. 3.8'deki hesaplama ile de C^0 ile C^1'in sütun sayılarının da eşit olduğu görülmüş olur.

$$m = m_1 + m_2 = 6 + 12 = 18 \tag{3.8}$$

1'lerin yerlerine göre birbirinden farklı C^1 matrisi elde edilebilir.

a)
$$\begin{bmatrix} & & & & & & & & & & & & & & & 1 & 1 & 1 \\ & & & & & & & & & & 1 & 1 & 1 & 1 & & & & \\ & & & & & & 1 & 1 & 1 & 1 & 1 & & & & & & & \\ 1 & 1 & 1 & 1 & 1 & 1 & & & & & & & & & & & & \end{bmatrix}_{4x18}$$

b)
$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}_{4x18}$$

Şekil 3.4. 4×18'lik C^1 matrisi, (a) 1'lerin rastgele farklı sütunlara yerleşimi, (b) Kalan yerlerin 0 ile doldurulması

Ayrıcalık tabanlı pay görüntüleri AP olarak gösterilirse 1. pay görüntüden başlayarak AP_1, AP_2, AP_3, … AP_n olarak belirlenir. $i'nci$ pay görüntü AP_i ise, AP_i'de bulunan 0'ların oranı $(16-i)/18$, 1'lerin oranı ise $(2+i)/18$ olmaktadır. Bu oranlar, C^0 ile C^1 pay matrislerinin içeriği ne olursa olsun, pay görüntüler için içerdikleri beyaz ve siyah piksel oranları aynı olacaktır. Bu da katılımcılar için pay görüntülerinden herhangi bir şekilde bilgi çıkarımı yapamayacakları manasına gelmiş olur. Ayrıca satır sayısı arttıkça 1'lerin (siyah) sayısı da arttığı için, oluşturulan bir sonraki pay görüntüsü daha ayrıcalıklı

olacaktır. AT-GSP şemasında ayrıcalık düzeyini belirleyen, pay görüntülerde bulunan siyah piksellerin yoğunluğudur. Bunun temel sebebi insanın görme sistemi, ikili görüntülerde siyah piksele daha fazla odaklanmasıdır [22].

3.1.2 Pay dağıtım algoritması

C^0 ve C^1 pay matrislerinin oluşmasından sonra, pay görüntülerinin oluşması için pay dağıtım algoritması kullanılır. Ayrıcalık tabanlı pay görüntüleri AP olarak gösterilirse 1. pay görüntüden başlayarak AP_1, AP_2, AP_3, … AP_n olarak n'ye kadar giderek artan pay görüntüleri bu algoritmayla belirlenir. İlk olarak, 1 ile m arasından bir t sayısı rastgele seçilir. Eğer gizlenmek istenen piksel beyaz (0) ise, C^0 matrisinin $t'nci$ sütunu seçilir. Bu sütunun ilk elemanı 1. pay görüntüye, 2. elemanı 2. pay görüntüye, 3. elemanı 3. pay görüntüye… şeklinde dağıtılır. Aynı şekilde piksel siyah (1) ise bu sefer C^1 matrisinin $t'nci$ sütunu seçilir ve paylara dağıtılır. Pay dağıtım algoritması Şekil 3.5.'de verilmiştir.

Pay Dağıtım Algoritması:
Girdiler: Yarı Tonlu Görüntü YG ($\boldsymbol{En} \times \boldsymbol{boy}$), pay sayısı $\boldsymbol{n}$, C^0 ve C^1 pay matrisleri
Çıktı: Ayrıcalık Tabanlı Paylar AP_x, $\mathbf{x} = \mathbf{1}, \mathbf{2}, \mathbf{3}, \ldots, \boldsymbol{n}$
İşlem:

```
1  for i ← 1:En
2    for j ← 1:Boy
3      t ← Rastgele Sayı (1 ≤ t ≤ m)
4      if YG (i, j) siyah
5        for x ← 1:n
6          APx (i, j) = C1x,t
7      else
8        for x ← 1:n
9          APx (i, j) = C0x,t
```

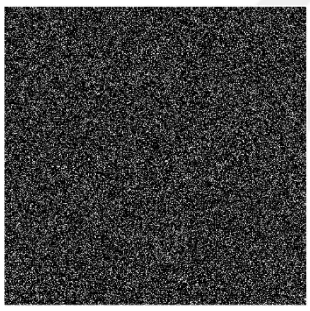
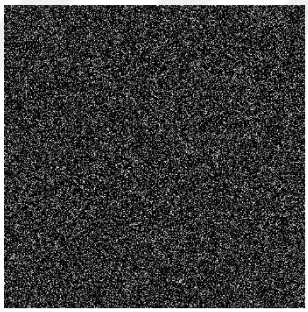
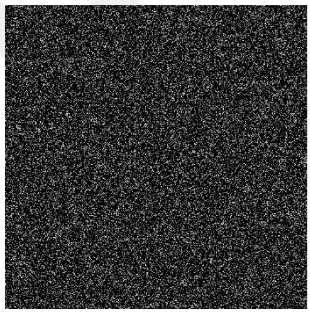
Şekil 3.5. Pay dağıtım algoritması

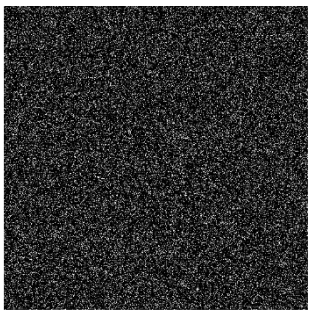
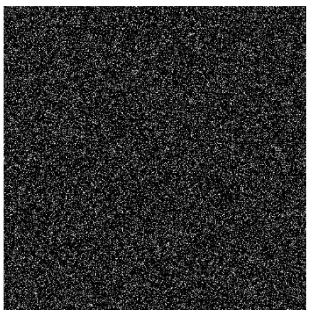
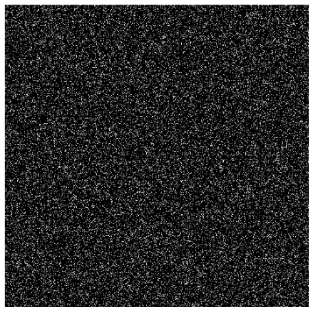
Yapılan bu çalışma gri tonlu görüntülere uygulanabilmesi için öncelikle ikili görüntülere çevrilmesi gereklidir. Bunun için gri tonlu görüntüler Jarvis algoritması ile ikili görüntülere çevrilmiştir. Elde edilen ikili görüntü AT-GSP şemasıyla paylara ayrılmaya uygun hale getirilmiştir.

AT-GSP şeması için örnek olarak kullanılan ve pay sayısı 6 olacak şekilde 512×512'lik gri tonlu görüntü, Resim 3.1.'de verilmiştir. Gri tonlu görüntü, AT-GSP şemasında ikili görüntü olarak kullanılacağı için Jarvis algoritması ile ikili görüntüye dönüştürülmüştür (Bkz. Resim 3.1. (b)). Resim 3.2.'de ise 6 adet anlamsız pay görüntüleri, artan bir ayrıcalık sırası ile verilmiştir.

a)  b) 

Resim 3.1. Deney görüntüsü (a) Gri tonlu görüntü, (b) Jarvis algoritması ile ikili görüntüye çevrilmiş görüntü

a)  b)  c) 

d)  e)  f) 

Resim 3.2. Deney görüntüsünün artan ayrıcalık sırasına göre oluşan 6 adet pay görüntüsü, (a) Pay 1, (b) Pay 2, (c) Pay 3, (d) Pay 4, (e) Pay 5, (f) Pay 6

3.2. Görüntü Şifrelemede İki Boyutlu Kaos Haritaları

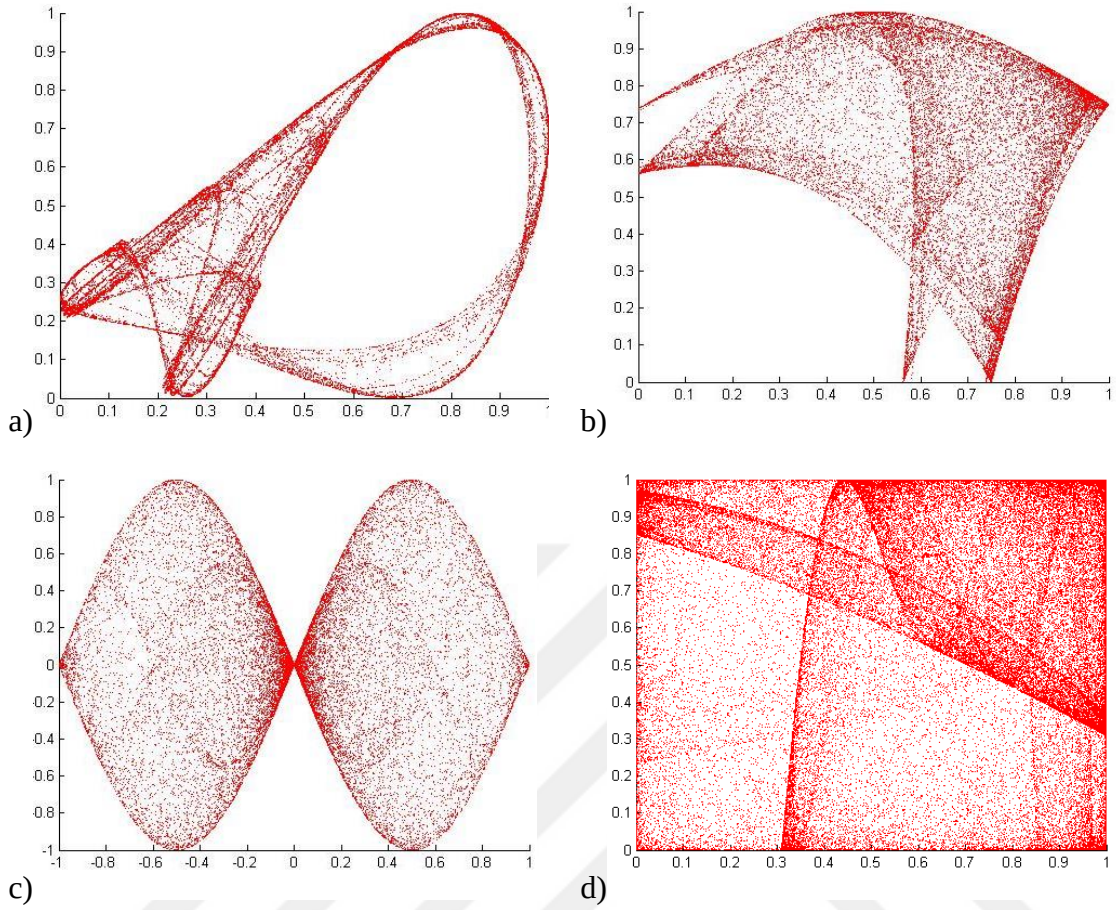
Literatürde kaos kavramı tahmin edilemezlik ve başlangıç değerlerine hassasiyet olarak yer almaktadır. Bir sigara dumanının havada yaptığı şekiller tamamen düzensiz ve rastgele görülebilir. Fakat aslında sigara dumanının yaptığı şekiller, ortamın basıncına, rüzgara,

hava akımına, sıcaklığa, neme gibi sayamayacağımız parametrelere bağlıdır. Aynı zamanda bu parametreler de birbirine bağlı olabilirler. Dolayısıyla bu parametreler o kadar değişkendir ki, incelemek ve net bir sonuca varmak imkânsıza yakın olmaktadır. Kaotik sistemlerin ekonomi, nüfus dağılımı, matematik, fizik, kimya, üç boyutlu modelleme, bulanık mantık, tıp, bilişim ve mekatronik gibi birçok alanda kullanım alanı bulunmaktadır.

Geleneksel şifreleme yöntemlerinden farklı olarak parametrelerin basitliği, fazlalığı, esnekliği, alacakları ilk değerlere göre değişkenliği, tahmin edilemezliği ve ergodikliği sayesinde kaos haritaları dijital görüntülerin saklanmasında ve iletilmesinde kullanılmaya başlanan yöntemlerden birisidir [23]. Kaos haritaları, ürettikleri birbirinden farklı ve rastgele sayı dizileri ile şifreleme konusunda iyi bir tercih sebebi olmuştur [30].

Günümüzde oldukça yaygın kullanılmaya başlanan kaos haritaları, bir boyutlu ve çok boyutlu olarak sınıflandırılmaktadır. Tek boyutlu kaos haritaları tek bir değişkene, az sayıda parametreye ve uzayda oluşturacakları basit yörüngelere sahiptirler. Bundan dolayı tahmin edilmeleri ve çözülmeleri kaotik sinyal tahmin teknolojisi ile mümkün olmaktadır. Çok boyutlu kaos haritaları tek boyutlulara göre daha karmaşık yapıya ve daha iyi performansa sahiptir. Görüntü şifrelemede kaos haritalarında çok boyutlu kullanmak daha iyi bir seçim olacaktır. Ancak çok boyutlu kaos haritası kullanırken, yüksek hesaplama zamanına ve maliyetine dikkat edilmelidir [25, 29, 30, 52, 53].

Tez çalışmasının bu kısmında çok boyutlu kaos haritalarından olan iki boyutlu kaos haritaları 2D Lojistik Harita, Two dimensional Sine Logistic modulation map (2D-SLMM), Two dimensional Sine ICMIC modulation map (2D-SIMM) ve 2D-STLH hakkında kısaca bilgi verilmiştir. Bu kaos haritalarının yörüngeleri Resim 3.3.'te verilmiştir.



Resim 3.3. İki boyutlu kaos harita yörüngeleri (a) 2D Lojistik, (b) 2D-SLMM, (c) 2D-SIMM, (d) 2D-STLH

2D Lojistik harita şu şekilde ifade edilmektedir (Bkz. Resim 3.3. (a)) [28]:

$$\begin{cases} x_{i+1} = r(3y_i + 1)x_i(1 - x_i) \\ y_{i+1} = r(3x_{i+1} + 1)y_i(1 - y_i) \end{cases} \tag{3.9}$$

Eş. 3.9'da r kontrol değişkenidir ve değeri 1,19'dur. 2D-SLMM şu şekilde ifade edilmiştir (Bkz. Resim 3.3. (b)) [30]:

$$\begin{cases} x_{i+1} = \alpha\,(\sin(\pi y_i) + \beta)\,x_i(1 - x_i) \\ y_{i+1} = \alpha\,(\sin(\pi x_{i+1}) + \beta)\,y_i(1 - y_i) \end{cases} \tag{3.10}$$

Eş. 3.10'da $\alpha \in [0, 1]$ ve β genelde 3 olarak alınır. 2D-SIMM şu şekilde ifade edilmiştir (Bkz. Resim 3.3. (c)) [52]:

$$\begin{cases} x_{i+1} = a\sin(\pi y_i)\sin\left({}^{b}/_{x_i}\right) \\ y_{i+1} = \alpha\sin(\pi x_{i+1})\sin\left({}^{b}/_{y_i}\right) \end{cases} \quad (3.11)$$

Eş. 3.11'de $\alpha, b \in (0, +\infty)$ alınır. Son olarak da 2D-STLH şu şekilde tanımlanmıştır (Bkz. Resim 3.3. (d)) [25]:

$$\begin{cases} x_{i+1} = \sin(\pi\rho(y_i + 3)\, x_i(1 - x_i)) \\ y_{i+1} = \sin(\pi\rho(x_{i+1} + 3)\, y_i(1 - y_i)) \end{cases} \quad (3.12)$$

Eş. 3.12'de $\rho = 0{,}9$ olarak alınmıştır.

Resim 3.3.'te gösterilen kaos haritalarının ilk değerleri ($x = 0{,}1$ ve $y = 0{,}2$) olarak belirlenmiştir. Resim 3.3.'teki yörüngelere göre, 2D-STLH tüm alana ve daha fazla yayılmıştır. Bundan dolayı da 2D-STLH kaos haritasının çıktılarının daha fazla rastgele olduğunu ve tahmin edilmesinin daha zor olduğu anlaşılmaktadır.

Kaos haritalarının performansının ölçülmesinde Lyapunov üsleri (LÜ), Lyapunov boyutu (LB) ve Kolmogorov entropi (KE) değerlerine bakılır. Dinamik bir sistemin kaotikliği LÜ ve LB ile ölçülmektedir. Dinamik bir sistem, pozitif bir LÜ sahip ise kaotiktir. Çok boyutlu kaos haritalarında en az iki adet LÜ değeri vardır. LB ise sistemin karmaşıklığını ölçmektedir. Kolmogorov entropi bir sinyalin rastgeleliğinin nicel açıklamasını verir ve bir dinamik bir sistemin yörüngesini tahmin etmek için gerekli olan ekstra bilginin ne kadar olduğunu ölçmek için kullanılır [25, 30].

Kolmogorov entropinin matematiksel tanımı Eş. 3.13'teki gibidir [25]:

$$KE = \lim_{\tau\to 0}\tau^{-1}\lim_{\varepsilon\to 0}\lim_{m\to 0} K_{m,\tau}(\varepsilon) \quad (3.13)$$

Eş. 3.13'te m gömme boyutudur.

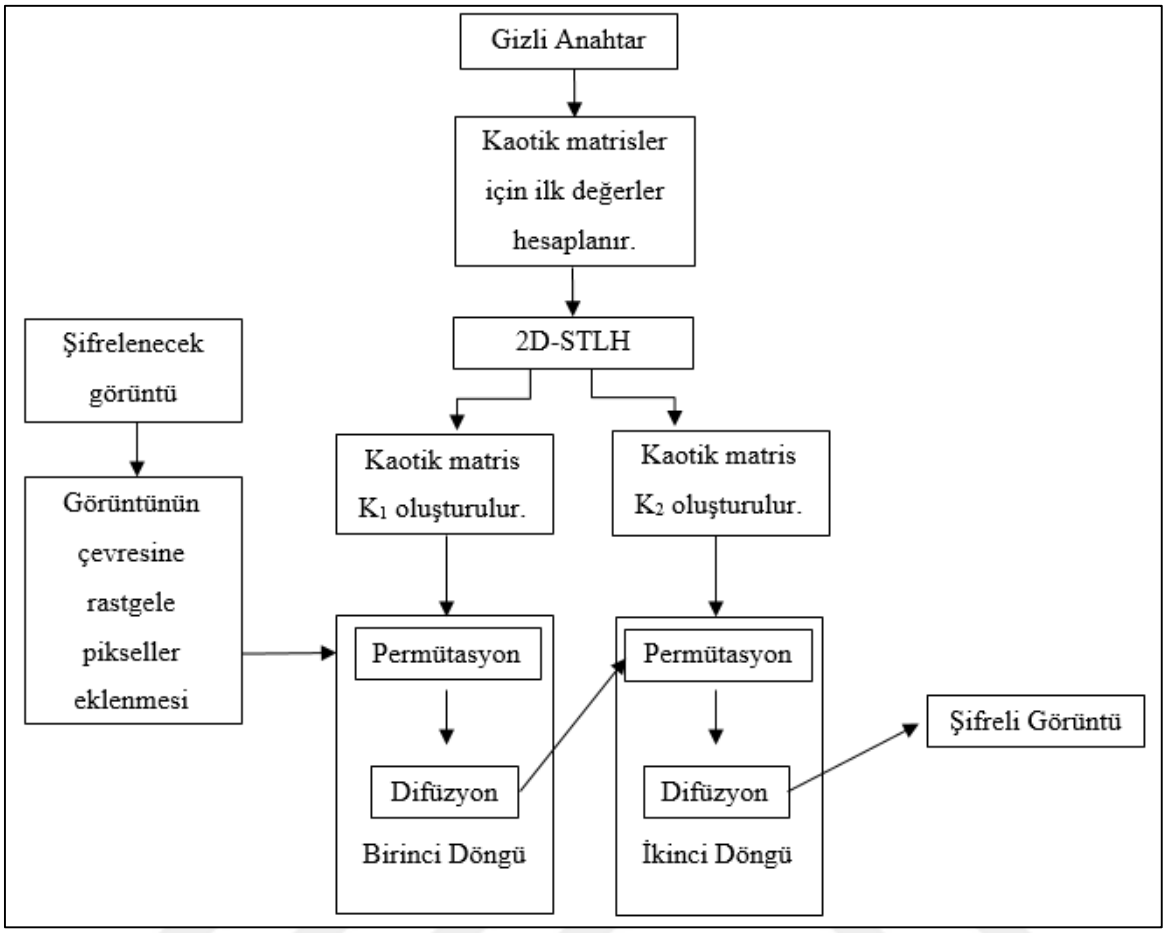
$$K_{m,\tau}(\varepsilon) = -\sum_{i_1,i_2,\ldots,i_m \le n(\varepsilon)} p(i_1, i_2, \ldots, i_m)\log p(i_1, i_2, \ldots, i_m) \quad (3.14)$$

Eş. 3.14'te $p(i_1, i_2, \dots, i_m)$ τ zamanında ϕ_{i_1} parçacığında, 2τ zamanında ϕ_{i_2} parçacığında, ..., $m\tau$ zamanında ϕ_{i_m} parçacığında yörüngeyi doğru tahmin etmenin ortak olasılığını temsil eder ve $\phi_{i_1}, \phi_{i_2}, \dots, \phi_{i_m}$ faz düzlemindeki m adet örtüşmeyen parçacıktır [25].

Eğer KE değeri pozitif ise sistem kaotiktir ve KE değerinin daha büyük olması demek ise sistemin daha fazla tahmin edilemediği manasına gelmektedir. 2D-STLH'da $\mu \in [0{,}37;\ 0{,}038] \cup [0{,}4;\ 0{,}42] \cup [0{,}44;\ 0{,}93]$ için LÜ değerleri pozitiftir ve sistem kaotik davranış göstermektedir. Ayrıca $\mu \in [0{,}44;\ 0{,}93]$ için ise iki farklı LÜ değeri aynı anda pozitif olduğu için yüksek kaotik özelliği gösterir. KE için ise 2D-STLH, daha geniş kaotik aralığa sahiptir. Bu ölçümlerden dolayı Hua ve Zhou tarafından yapılan 2D-STLH, diğer dinamik sistemlere göre daha fazla tahmin edilemezdir [25, 30].

3.2.1. İki boyutlu sinüs tabanlı lojistik kaos haritası

Bu bölümde, tezin ikinci kısmını oluşturan 2D-STLH şifreleme yapısı anlatılmıştır. 2D-STLH ile görüntü şifrelemesinin ana yapısı Şekil 3.6.'da verilmiştir.



Şekil 3.6. 2D-STLH şifreleme yapısı

Gizli anahtar oluşturma

2D-STLH'ta 232 bitlik bir gizli anahtar belirlenir. Bu gizli anahtar kullanılarak Şekil 3.7.'deki algoritmaya göre 2D-STLH için gerekli olan ilk parametreler bulunur. Bulunan (x_0^1, y_0^1, ρ_1) ve (x_0^2, y_0^2, ρ_2) değerleri ile Eş. 3.12'te verilen 2D-STLH'ın formülüne göre K_1 ve K_2 kaotik matrisin elemanları oluşturulur. Çıkan değerler 0-255 arasında olacak şekilde dönüştürülür.

Kaotik Matrislerin İlk Durumlarının Belirlenme Algoritması

Girdi: 232 bitlik gizli anahtar, GA

Çıktı: Kaotik matrislerin ilk durum değerleri (x_0^1, y_0^1, ρ_1) ve (x_0^2, y_0^2, ρ_2)

İşlem:

$x_0 = (\sum_{i=1}^{52} GA[i] \times 2^{i-1})/2^{52}$;

$y_0 = (\sum_{i=53}^{104} GA[i] \times 2^{i-53})/2^{52}$;

$\rho = (\sum_{i=105}^{156} GA[i] \times 2^{i-105})/2^{52}$;

$\varepsilon = (\sum_{i=157}^{208} GA[i] \times 2^{i-157})/2^{52}$;

$\sigma_1 = (\sum_{i=209}^{220} GA[i] \times 2^{i-209})$;

$\sigma_2 = (\sum_{i=221}^{232} GA[i] \times 2^{i-221})$;

for $\boldsymbol{i} \leftarrow \mathbf{1}:\mathbf{2}$

  $x_0^i = (x_0 + \varepsilon \times \sigma_i)\ mod\ 1$;

  $y_0^i = (y_0 + \varepsilon \times \sigma_i)\ mod\ 1$;

  $\rho_i = \big((\rho + \varepsilon \times \sigma_i)\ mod\ 0.4\big) + 0.5$;

  if $x_0^i == 0$

    $x_0^i = 0.4$;

  if $y_0^i == 0$

    $y_0^i = 0.4$;

end for

Şekil 3.7. Kaotik matrislerin ilk durum parametrelerinin belirlenmesi

Gizli anahtar GA, örnek olarak 16'lık tabanda Eş. 3.15'deki gibi belirlenir.

$$GA = CBDF65E7EDA08BB1721E318AFA2F771DCE63D87A1774897558D887D196 \quad (3.15)$$

Şekil 3.7.'deki algoritmaya göre, gizli anahtarı 2'lik tabana çevrildikten sonra algoritmanın ilk çıktıları sırasıyla Eş. 3.16, 3.17 ve 3.18'deki gibi olur.

$$(x_0, y_0, \rho) = (0{,}06389608;\ 0{,}37233808;\ 0{,}88178105) \quad (3.16)$$

$$\varepsilon = 0{,}10587588 \quad (3.17)$$

$$(\sigma_1, \sigma_2) = (3041;\ 1688) \quad (3.18)$$

Bu değerler kaotik matrislerin orijinal değerleridir. Bu orijinal değerler kullanılarak iki tane kaotik matris oluşturacak ilk değerler Eş. 3.19 ve 3.20'deki gibi bulunur.

$$(x_0^1, y_0^1, \rho_1) = (0{,}03245789;\ 0{,}34089988;\ 0{,}55034286) \tag{3.19}$$

$$(x_0^2, y_0^2, \rho_2) = (0{,}78238748;\ 0{,}09082947;\ 0{,}50027244) \tag{3.20}$$

Eş. 3.19 kaotik matrislerin, yani K_1'in ilk değerleri, Eş. 3.20 ise K_2'in ilk değerleri olup, her iki kaotik matris 2D-STLH'ın formülü olan Eş. 3.12 ile oluşturulur. Ancak kaotik matristeki değerler 0 ile 1 arasında ve ondalık halinde olduğu için, 0 ile 255 arasında olacak şekilde (mod 256 işlemi ile) yeniden düzenlenir. Çünkü şifrelenecek görüntüler ile aynı formatta yani tam sayı formatında olmalıdır.

Gizli görüntünün çevresine piksel ekleme

Kaotik matrislerin belirlenmesinden sonra gizlenmek istenen görüntünün etrafını bir kere çevreleyecek şekilde rastgele 0-255 arasında piksel değerleri eklenir. Bunun amacı, aynı görüntü aynı gizli anahtar ile şifrelense bile eklenen bu rastgele piksel değerleri sayesinde gizli görüntünün her zaman farklı olmasını sağlayacaktır. Şifrelenmek istenen görüntünün boyutu $n \times m$ ise, rastgele birer satır ve sütun eklenirse görüntünün yeni boyutu $(n+2) \times (m+2)$ şeklinde olacaktır. Şekil 3.8.'de örnek olarak verilen bir gizli görüntü piksellerine rastgele eklenen satır ve sütunlar kalın ve altı çizili olarak gösterilmiştir.

a)

222	235	254	…	12	34	52
234	143	190	…	87	90	43
52	178	190	…	99	76	213
…	…	…	…	…	**...**	…
39	59	71	…	137	167	0
128	40	71	…	124	255	11
178	123	229	…	33	176	223

b)

14	**65**	**31**	**33**	**…**	**0**	**200**	**240**	**21**
213	222	235	254	…	12	34	52	**123**
34	234	143	190	…	87	90	43	**45**
8	52	178	190	…	99	76	213	**45**
9	…	…	…	…	…	**...**	…	**255**
123	39	59	71	…	137	167	0	**1**
42	128	40	71	…	124	255	11	**100**
99	178	123	229	…	33	176	223	**96**
100	**123**	**32**	**45**	**…**	**55**	**66**	**77**	**54**

Şekil 3.8. Gizlenecek görüntüye rastgele eklenen 0 ile 255 arasında olan pikseller (a) Gizlenmek istenen görüntü, G, (b) Elde edilen yeni görüntü, G”

Permütasyon işlemi

Genel olarak kaotik görüntü şifrelemede permütasyon-difüzyon işlemleri sırası ile uygulanır [25]. Permütasyon işlemi etrafına rastgele pikseller eklenen gizli görüntüye uygulanır. Permütasyon işlemi piksellerin yerlerini değiştirmek için kullanılırken piksel değerleri bu işlemde değişmeyecektir [26]. Permütasyon işlemi için kullanılan algoritma Şekil 3.9.’da verilmiştir.

Permütasyon Algoritması

Girdi: Çevresine Rastgele Pikseller Eklenmiş Görüntü G ve Kaotik Matris K,
Boyutları $(n+2) \times (m+2)$ ve 'p' bit olarak temsil edilirler. (Gri tonlu görüntü için p = 8 bit)

Çıktı: Piksellerin Yerinin Değişmesi Sonucu Oluşan Yeni Görüntü, P

İşlem:

1 $(n+2) \times (m+2)$ boyutlarında bir D matrisi belirlenir.

2 q $= \lceil \log_2(n+2)(m+2) \rceil$;

3 for $\boldsymbol{i} \leftarrow 1$: $(\boldsymbol{n+2})$

4 for $\boldsymbol{j} \leftarrow 1$: $(\boldsymbol{m+2})$

5 $t = (i-1)(m+2)+j$; {t sayısı 1'den başlayarak $(n+2)(m+2)$ sayısına kadar gider}

6 $indeks\_elemanı = donustur(t, q)$; {t sayısı, q adet basamaklı ikilik tabana çevrilir}

7 $\boldsymbol{D_{i,j} = birlestir(K_{i,j}, indeks\_elemanı, G_{i,j})}$; {3 tane ikili sayıyı birleştirip tek bir ikili sayı elde edilir}

8 end for

9 end for

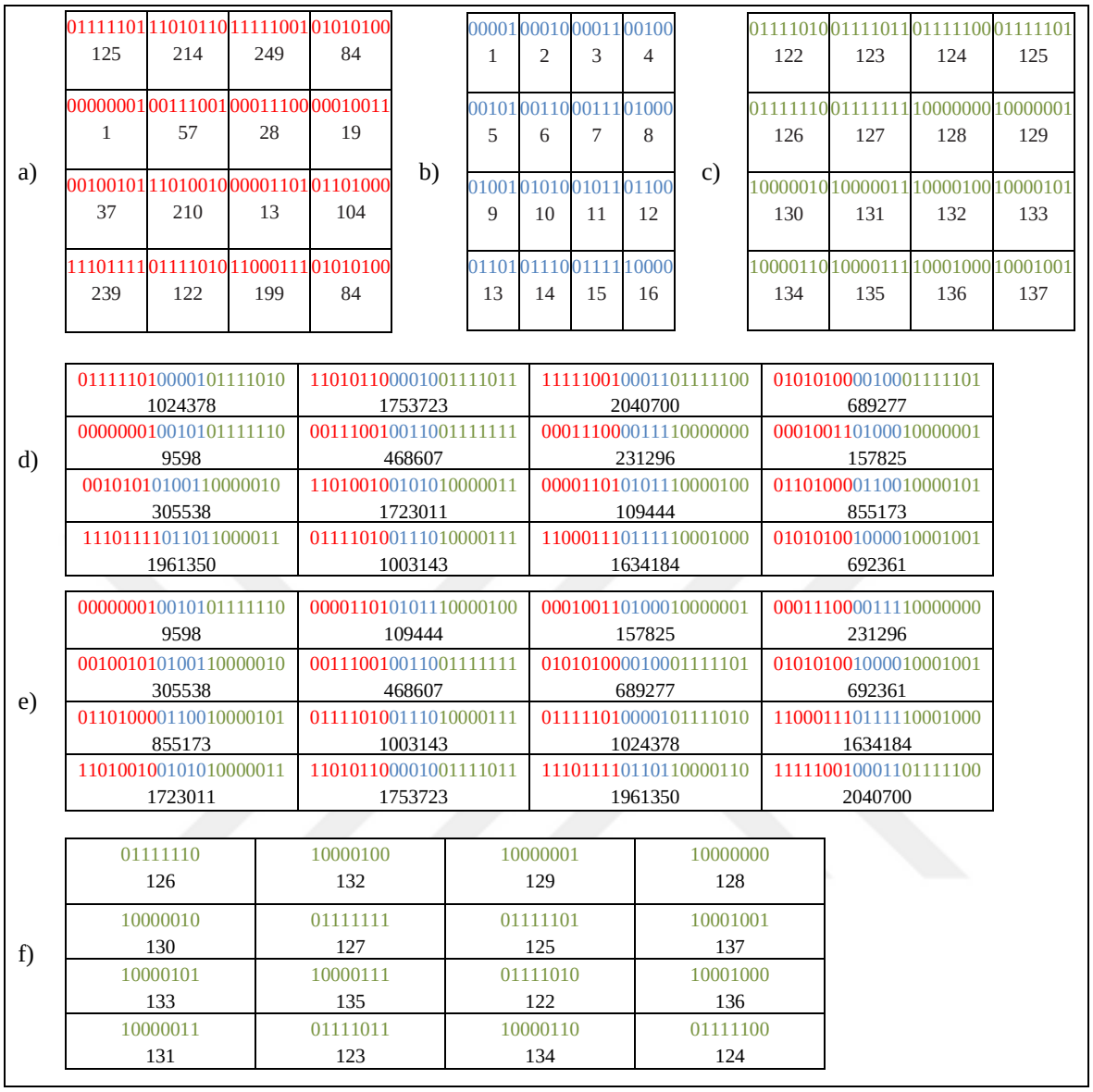
10 $D = yatay\_yönde\_kucukten\_buyuge\_sirala(D)$;

11 $D = dikey\_yönde\_kucukten\_buyuge\_sirala(D)$;

12 $P = ayarla(D, p)$; {D matrisinin elemanlarının son p biti alınır ve işlem tamamlanır.}

Şekil 3.9. Permütasyon algoritması

Permütasyon işlemine G gizli görüntü ile K kaotik matrisi işleme sokulur. Bunlara ek olarak indeks elemanı da kullanılır. İndeks elemanı 1'den başlayarak $(n+2)(m+2)$ sayısına kadar gider. İndeks elemanları indeks matrisi adı verilen matriste tutulabilir. Dolayısıyla indeks matrisindeki sayılar 1'den başlayarak $(n+2)(m+2)$ sayısına kadar giden tüm sayılardır. Gizli görüntü, kaotik matris ve indeks matrisi aynı boyutlarda olup p bitlik pikseller ile ifade edilir. Örnek olarak $p = 8$ alınıp 8 bitlik bir görüntü için açıklanırsa; bu 3 tane matrisin içindeki sayılar, ikilik sayıya çevrilir. İlk 8 bit kaotik matristen, sonraki 8 bit indeks matrisinden ve son 8 bit ise gizlenecek görüntüdeki bitler olacak şekilde birleştirilip her bir elemanı 24 bitlik bir sayıdan oluşan bir matris elde edilir. Bu matristeki sayılar sırasıyla yatay daha sonra da dikey olarak küçükten büyüğe doğru sıralanır. Sonra bu 24 bitlik sayıların son 8 biti seçilip ilk 16 biti ayrılır. Çünkü bu 3 matrisin en son 8 biti, gizlenecek görüntünün pikselleridir ve gizlenecek piksellerin yeri bu şekilde yer değiştirilmiş olur. Şekil 3.10.'da sayısal örnek üzerinden permütasyon algoritması gösterilmiştir.



Şekil 3.10. Permütasyon aşamasında sayısal bir örnek**,** (a) Örnek olarak verilen kaotik matris pikselleri, (b) Örnek olarak verilen indeks matrisi pikselleri, (c) Örnek olarak verilen görüntü pikselleri**,** (d) 3 matrisin ikili rakama çevrilip birleştirilmesi, (e) Birleştirilen ikili rakamların küçükten büyüğe sıralanması**,** (f) Birleştirilen matrisin son 8 rakamının alınması ve görüntünün şifreli hali

Difüzyon işlemi

Permütasyon aşamasından sonra yeri değişen pikseller, difüzyon aşaması ile değerleri değişecektir. P matrisi permütasyon sonucu gelen matris, K kaotik matris ve Q matrisi de difüzyon işlemi sonucu olmak üzere, difüzyon algoritması ve difüzyon çözme algoritması Şekil 3.11.'de verilmiştir. Şekil 3.11.'deki $\oplus$ işlemi XOR işlemidir. Difüzyon algoritması şifreleme aşamasında uygulanırken, difüzyon çözme algoritması ise şifreli görüntüleri çözme aşamasında kullanılır. Bir permütasyon-difüzyon işlemine bir döngü dersek ikinci

döngü işlemi, birinci döngüde elde edilen matrisi kullanır. Birinci döngüde K_1 kaotik matrisi kullanılırken, ikinci döngüde K_2 kaotik matrisi kullanır. İki döngü sonucunda tamamen rastgele piksellerden oluşmuş şifreli görüntü elde edilir.

Difüzyon Algoritması	**Difüzyon Çözme Algoritması**
Girdi: P, K matrisleri $(N \times M)$ boyutunda	**Girdi:** Q, K matrisleri $(N \times M)$ boyutunda
Çıktı: Q matrisi $(N \times M)$ boyutunda	**Çıktı:** P matrisi $(N \times M)$ boyutunda
İşlem:	**İşlem:**
for $\boldsymbol{i} \leftarrow 1$: $\boldsymbol{N}$	for $\boldsymbol{i} \leftarrow 1$: $\boldsymbol{N}$
for $\boldsymbol{j} \leftarrow 1$: $\boldsymbol{M}$	for $\boldsymbol{j} \leftarrow 1$: $\boldsymbol{M}$
$Q_{i,j} = \begin{cases} P_{i,j} \oplus P_{N,M} \oplus K_{i,j} \ \ if\ i == 1, j == 1 \\ P_{i,j} \oplus Q_{i-1,M} \oplus K_{i,j} \ \ if\ i \neq 1, j == 1 \\ P_{i,j} \oplus Q_{i,j-1} \oplus K_{i,j}\ if\ j \neq 1 \end{cases}$	$P_{i,j} = \begin{cases} Q_{i,j} \oplus P_{N,M} \oplus K_{i,j} \ \ if\ i == 1, j == 1 \\ Q_{i,j} \oplus Q_{i-1,M} \oplus K_{i,j} \ \ if\ i \neq 1, j == 1 \\ Q_{i,j} \oplus Q_{i,j-1} \oplus K_{i,j}\ if\ j \neq 1 \end{cases}$
end for	end for
end for	end for

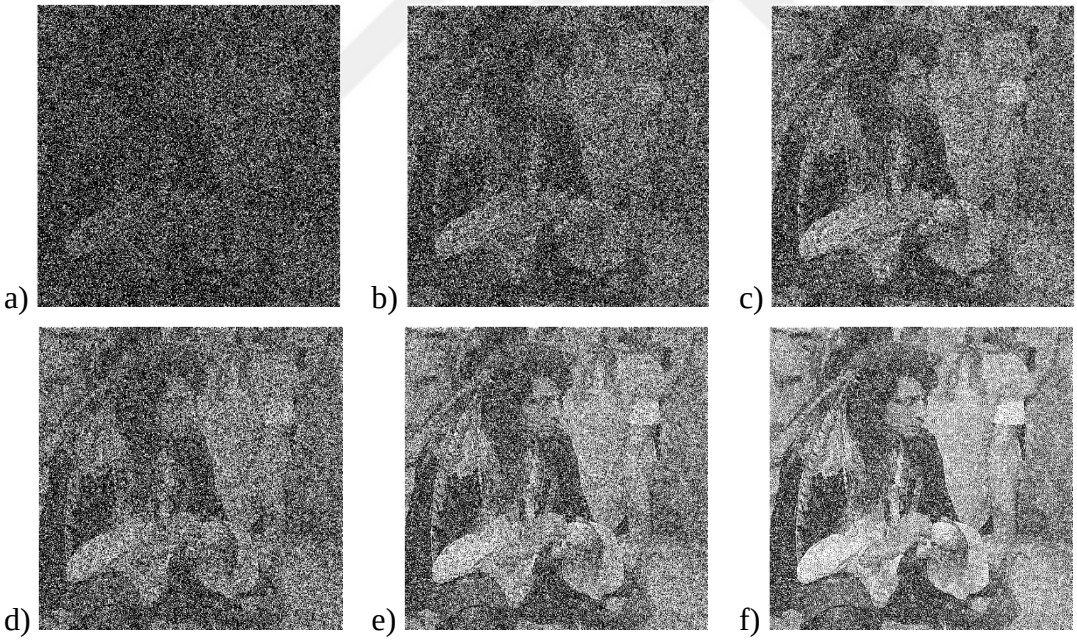
Şekil 3.11. Difüzyon algoritması ve difüzyon çözme algoritması

4. DENEYSEL SONUÇLAR VE YORUMLAR

Bu bölümde, AT-GSP ve 2D-STLH şifreleme yapısının birleştirilmesi, bu yapıya uygulanan saldırılar ve saldırıların sonuçları açıklanmıştır.

4.1. AT-GSP Şemasındaki Güvenlik Problemi

AT-GSP şeması, paylar arasında önem sırasını belirleyen bir çalışmadır. Ancak Şekil 4.1.'de AT-GSP şeması kullanıldığında en yüksek önceliğe sahip pay görüntüleri birleştirildiğinde gizlenen görüntünün görsel olarak büyük bir ölçüde ortaya çıktığı görülmektedir. Dolayısıyla gizli görüntüyü elde etmek için tüm paylara ihtiyaç kalmamıştır. Pay görüntüleri elde geçirmek isteyen üçüncü şahıslar, yüksek ayrıcalığa sahip birkaç payı elde ederse gizli görüntüyü ele geçirmiş olacaktır. Bu da güvenlik sorununu ortaya çıkarmıştır.



Resim 4.1. Pay görüntülerin üst üste getirilmesi ile gizli görüntünün ortaya çıkması (a) Pay 1 ∨ Pay 2, (b) Pay 1 ∨ Pay 2 ∨ Pay 3, (c) Pay 1 ∨ Pay 2 ∨ Pay 3 ∨ Pay 4 (d) Pay 1 ∨ Pay 2 ∨ Pay 4 ∨ Pay 5, (e) Pay 1 ∨ Pay 2 ∨ Pay 3 ∨ Pay 4 ∨ Pay 5, (f) Pay 1 ∨ Pay 2 ∨ Pay 3 ∨ Pay 4 ∨ Pay 5 ∨ Pay 6

Şekil 4.1.'deki görüntülerin orijinal görüntüyle olan benzerlik oranını hesaplayabilmek için PSNR (Peak Signal-to-Noise Ratio) ve SSIM (Structural Similarity Index) adı verilen metrikler kullanılmıştır.

Görüntülerin birbirleri ile olan benzerliklerini karşılaştırmak için PSNR kullanılır. PSNR değeri bir görüntü için ne kadar yüksek olursa o görüntünün çözünürlüğünün daha az bozulduğu manasına gelmektedir. PSNR değeri sonsuz ise, görüntü üzerinde hiçbir gürültü yok demektir. Yani iki görüntü de aynıdır. $n \times m$ boyutunda bir görüntünün PSNR değeri Eş. 4.1'de verilmiştir [54].

$$PSNR = 10\log_{10}\frac{255^2}{MSE}\ (dB) \tag{4.1}$$

$$MSE = \frac{1}{n\times m}\sum_{i=0}^{n-1}\sum_{j=0}^{m-1}(X_{ij} - X'_{ij})^2 \tag{4.2}$$

Eş. 4.2.'deki X_{ij} ve X'_{ij} olarak gösterilen ifadeler, gizli görüntü ile geri elde edilen görüntünün piksel değerlerini göstermektedir. Eş. 4.2'de verilen MSE (Mean Squared Error) ise gizli görüntü ile geri elde edilen görüntünün ne kadar değiştiğini ölçmek için kullanılan bir ölçümdür. PSNR hesaplanırken, bulunan MSE değeri Eş. 4.1'de yerine konularak bulunmuştur.

SSIM iki görüntünün birbirine ne kadar benzediğinin ölçümüdür. Eğer sonuç 1 ise iki görüntü birbirinin aynısıdır. SSIM hesabında üç adet parametre bulunmaktadır. Bunlar parlaklık $L(x,y)$, kontrast $C(x,y)$ ve yapıdır $S(x,y)$. SSIM hesabı Eş. 4.3'te açıklanmıştır [55].

$$SSIM(x,y) = (L(x,y)^{\alpha} \times C(x,y)^{\beta} \times S(x,y)^{\gamma}) \tag{4.3}$$

$L(x,y)$, $C(x,y)$ ve $S(x,y)$ değerleri sırasıyla Eş. 4.4, 4.6 ve 4.8'de verilmiştir.

$$L(x,y) = \frac{2\mu_x\mu_y + C1}{\mu_x^2 + \mu_y^2 + C1} \tag{4.4}$$

Eş. 4.4'teki μ_x ve μ_y, x ile y görüntülerinin ortalama değerleridir. $C1$ Eş. 4.5'de açıklanmıştır.

$$C1 = (K_1 L)^2,\ L = \text{maksimum yoğunluk değeri},\ K_1 \leq 1 \tag{4.5}$$

$$C(x,y) = \frac{2\sigma_x\sigma_y+C2}{\sigma_x^2+\sigma_y^2+C2} \quad (4.6)$$

Eş. 4.6'daki σ_x ve σ_y, x ile y görüntülerinin varyans değerleridir. $C2$ Eş. 4.7'de açıklanmıştır.

$$C2 = (K_2L)^2,\ L = \text{maksimum yoğunluk değeri},\ K_2 \leq 1 \quad (4.7)$$

$$S(x,y) = \frac{\sigma_{xy}+C3}{\sigma_x+\sigma_y+C3} \quad (4.8)$$

Eş. 4.8'de verilen σ_{xy} değeri, x ile y görüntülerinin kovaryansıdır. $C3$ Eş. 4.9'da açıklanmıştır.

$$C3 = \frac{C2}{2} \quad (4.9)$$

Bu hesaplamalardan sonra α, β ve γ değerleri 1 olarak alınmış ve SSIM bu şekilde hesaplanmıştır. Çizelge 4.1.'de, Resim 4.1.'deki görüntülerin her birinin Resim 3.1.(b)'deki deney görüntüsü ile benzerlik oranları, PSNR ve SSIM ile hesaplanmıştır.

Çizelge 4.1. Resim 4.1'deki görüntüler ile Resim 3.1.(b)'deki deney görüntüsünün PSNR ve SSIM değerleri

	(a)	(b)	(c)	(d)	(e)	(f)
PSNR	52,3784	53,3662	54,5234	54,3006	55,9546	57,7802
SSIM	0,9868	0,9915	0,9944	0,9940	0,9958	0,9961

Çizelge 4.1.'de görüldüğü gibi, pay görüntülerin birleştirilmesi sonucu elde edilen görüntü ile Jarvis algoritmasıyla siyah beyaz görüntüye çevrilmiş kameraman görüntüsü arasında yüksek benzerlik çıktığı görülmüştür. Ayrıcalık kullanımı bir avantaj getirirken aynı zamanda en yüksek önceliğe sahip olan görüntülerin ele geçirilmiş olma tehlikesine karşı zayıf duruma düşmüş olmaktadır.

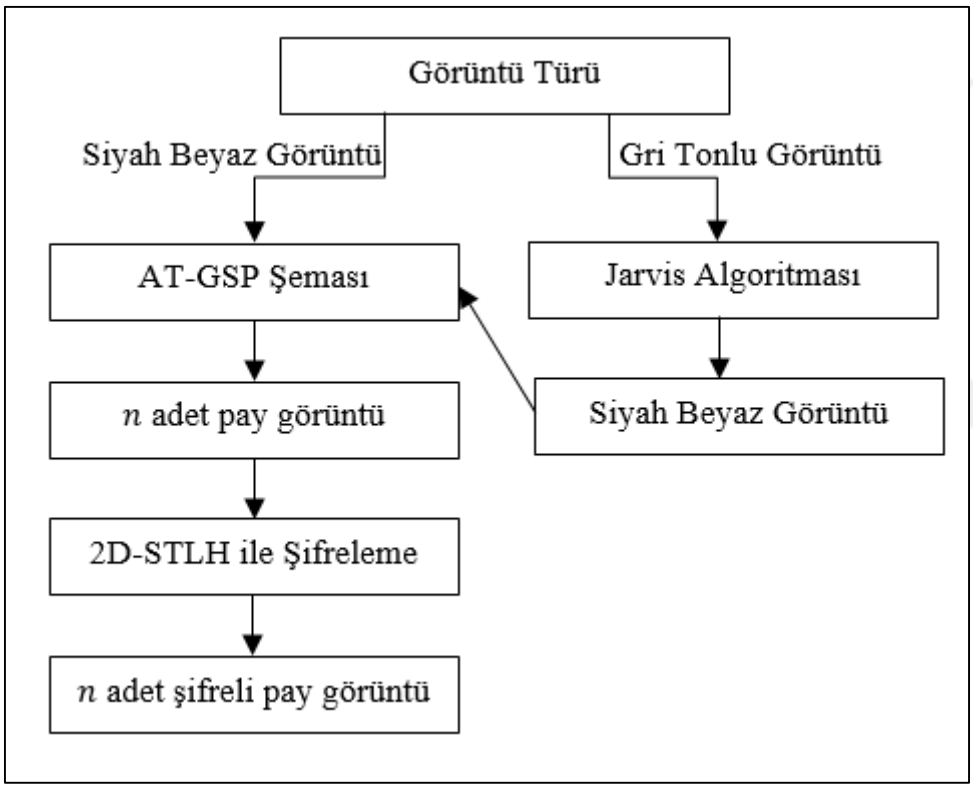
4.2. Kaotik Şifrelemeli AT-GSP Şeması

Bölüm 4.1.'de anlatılan AT-GSP şemasının zayıflığını giderebilmek için pay görüntülerinin de şifrelenmesi uygun bir yol olarak benimsenmiştir. Görüntü şifrelemede

kullanılan birçok yöntem olmasına rağmen, bölüm 3.2.1'de bahsedilen, güncel ve güvenirliği daha fazla olan 2D-STLH şifreleme yöntemi kullanılmıştır. Bu tez çalışmasında GSP şeması ile kaos haritaları birlikte kullanılarak AT-GSP şemasında meydana gelen güvenlik problemine bir çözüm önerisi getirilmiştir.

4.2.1. İkili ve gri tonlu görüntülerde kaotik şifrelemeli AT-GSP şeması ve uygulaması

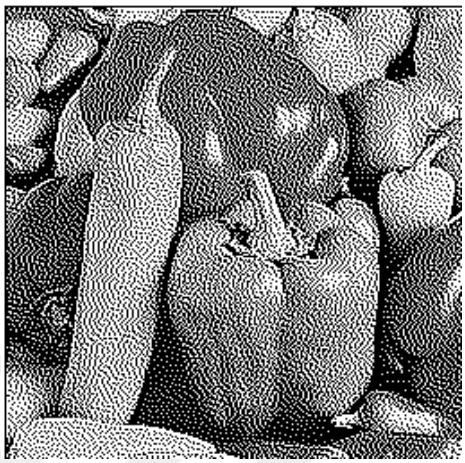
İkili ve gri tonlu görüntüler için uygulanan akış diyagramı, Şekil 4.1.'de verilmiştir.



Şekil 4.1. İkili ve gri tonlu görüntülerde kaotik şifrelemeli AT-GSP şemasının akış diyagramı

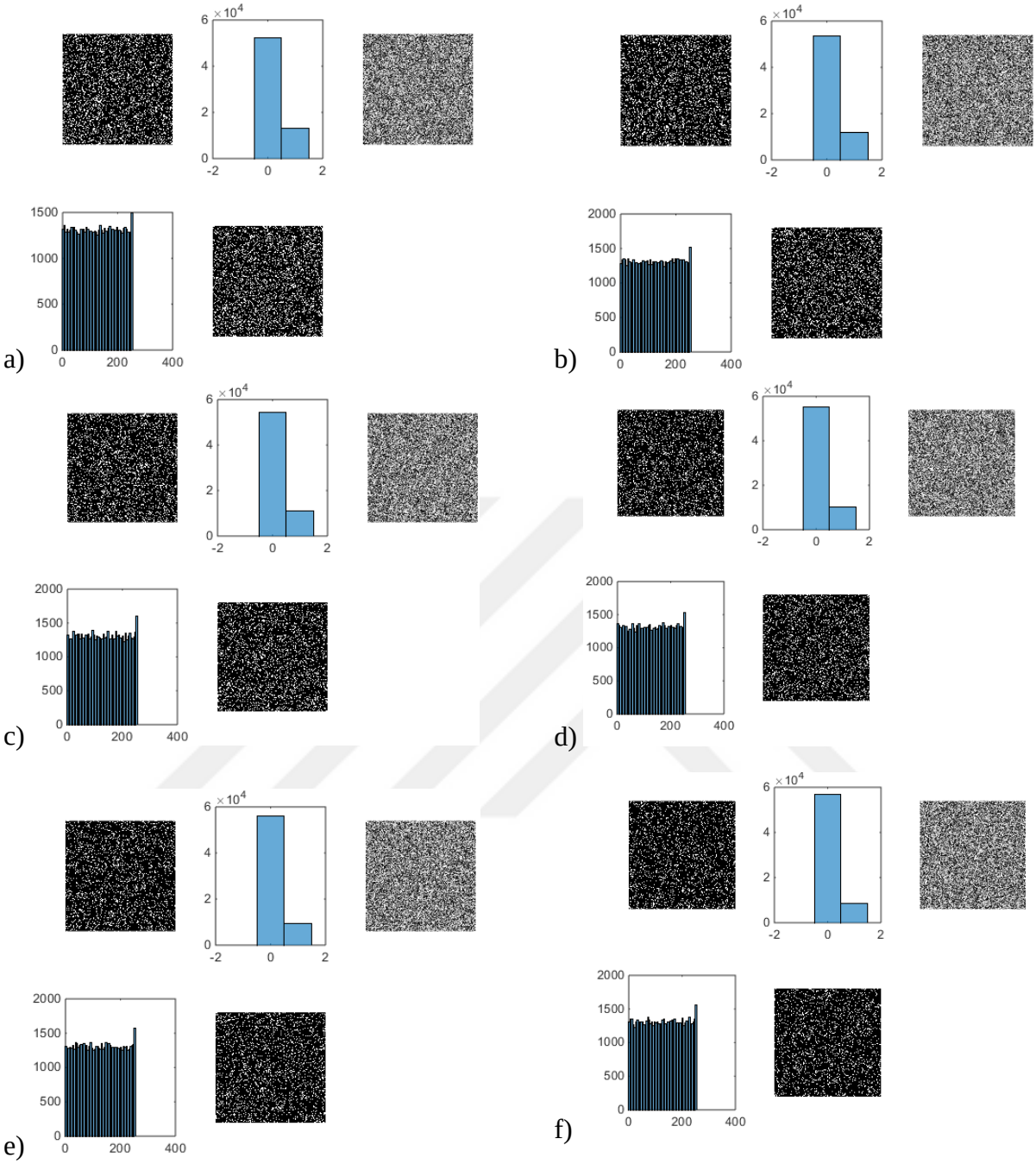
Şekil 4.1'de görüldüğü gibi, görüntü eğer ikili bir görüntü ise doğrudan AT-GSP şemasına gri tonlu görüntüler ise ilk olarak Jarvis algoritması ile ikili görüntüye çevrildikten sonra AT-GSP şemasına sokulmuştur. Daha sonra, oluşturulan n adet pay görüntüsünün her birine 2D-STLH şifrelemesi uygulanır. Elde edilen n adet şifreli pay görüntüsü, n adet kullanıcının her birine paylaştırılmıştır. Böylelikle n adet şifreli pay görüntüsü, ele geçirilip üst üste getirilse bile hiçbir şekilde gizli görüntüye ait bilgi elde edilememiştir.

Yukarıdaki işlemlerin gri tonlu görüntüler için uygulamasında, dizüstü bir bilgisayar ve MATLAB 2014b yazılımı kullanılmıştır. Deney görüntüsü olarak Resim 4.2.(a)'daki 256×256 boyutlarında gri tonlu görüntüsü kullanılmıştır.

a)  b) 

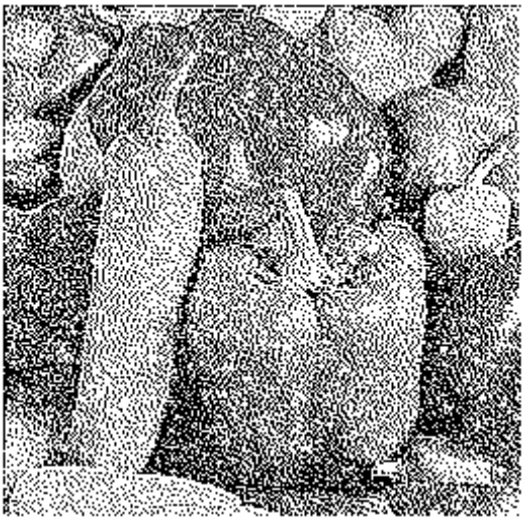
Resim 4.2. Deney görüntüsü (a) Gri tonlu görüntü, (b) Jarvis algoritması ile siyah beyaz görüntüye çevrilmiş görüntü

Uygulamada öncelikle gri tonlu görüntü, Jarvis algoritması ile siyah beyaz görüntüye çevrilmiş, sonra AT-GSP şeması ile 6 adet pay görüntüye ayrılmış ve 2D-STLH şifrelemesi uygulanmıştır. Resim 4.3.'de, pay görüntüsü, payın histogramı, payın şifreli görüntüsü, şifreli görüntünün histogramı ve şifresi çözülen pay görüntüsü sıralanmıştır.



Resim 4.3. AT-GSP şeması ile 6 adet pay görüntüye ayrılan deney görüntüsünün 2D-STLH ile şifrelenmiş hali (a) Pay 1, (b) Pay 2, (c) Pay 3, (d) Pay 4, (e) Pay 5, (f) Pay 6

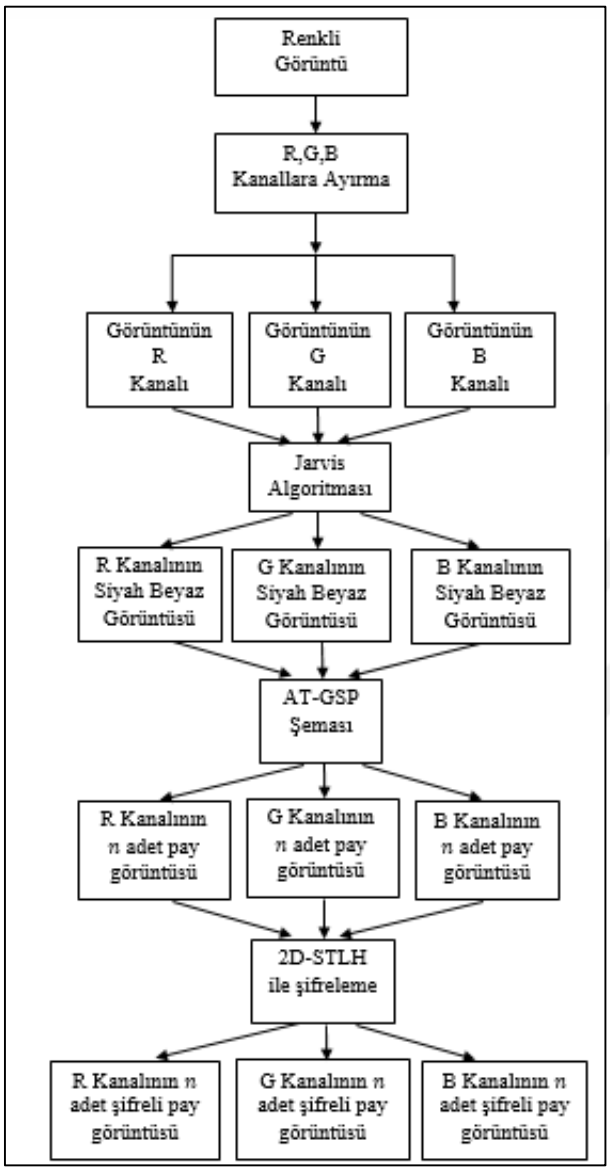
Resim 4.3.’ten anlaşılacağı gibi, pay görüntülere başarılı bir şekilde 2D-STLH uygulanmıştır. Paylar elde edilip üst üste bindirilse bile gizli görüntü ortaya çıkarılamamıştır. Şifreli pay görüntülerin histogramları dengeli dağılıma sahiptir. Pay görüntüsü ile şifresi çözülen pay görüntüleri arasındaki PSNR ölçümünde sonuçlar sonsuzdur, yani aynı görüntüdür. Bu da şifreli görüntülerin tekrar sorunsuz bir şekilde elde edilebildiğini göstermektedir. Şifresi çözülen ve üst üste getirilip elde edilen görüntü Resim 4.4.’te verilmiştir.



Resim 4.4. Şifresi çözülen gri tonlu deney görüntüsü

4.2.2. Renkli görüntülerde kaotik şifrelemeli AT-GSP şeması ve uygulaması

Renkli görüntüler için uygulanan akış diyagramı, Şekil 4.2.'de verilmiştir.



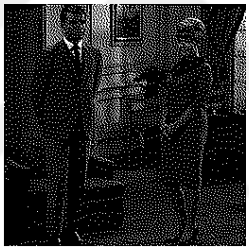
Şekil 4.2. Renkli görüntülerde kaotik şifrelemeli AT-GSP şemasının akış diyagramı

AT-GSP şemasının renkli görüntülere uygulanabilmesi için öncelikle siyah beyaz görüntülere çevrilmesi gereklidir. Bu yüzden renkli görüntüler ilk olarak RGB kanallarına ayrılmış ve bu renk kanalları Jarvis algoritması ile siyah beyaz görüntülere çevrilmiştir. Siyah beyaz renk kanalları AT-GSP şeması ile pay görüntülerine ayrılmıştır. Pay görüntüler oluşturulduktan sonra, her bir paya 2D-STLH uygulanmıştır. Bu şekilde her bir renk kanalının pay görüntüleri şifrelenmiştir.

Tez çalışmasının renkli tonlu görüntüler için uygulamasında da aynı bilgisayar ve yazılım kullanılmıştır. Deney görüntüsü olarak Resim 4.5. (a)'daki 256×256'lık renkli deney görüntüsü kullanılmıştır. İlk olarak renkli deney görüntüsü RGB kanallarına ayrılmıştır. Daha sonra bu ayrılan renk kanalları, Jarvis algoritması kullanılarak siyah beyaz resme dönüştürülmüştür (Bkz. Resim 4.6).

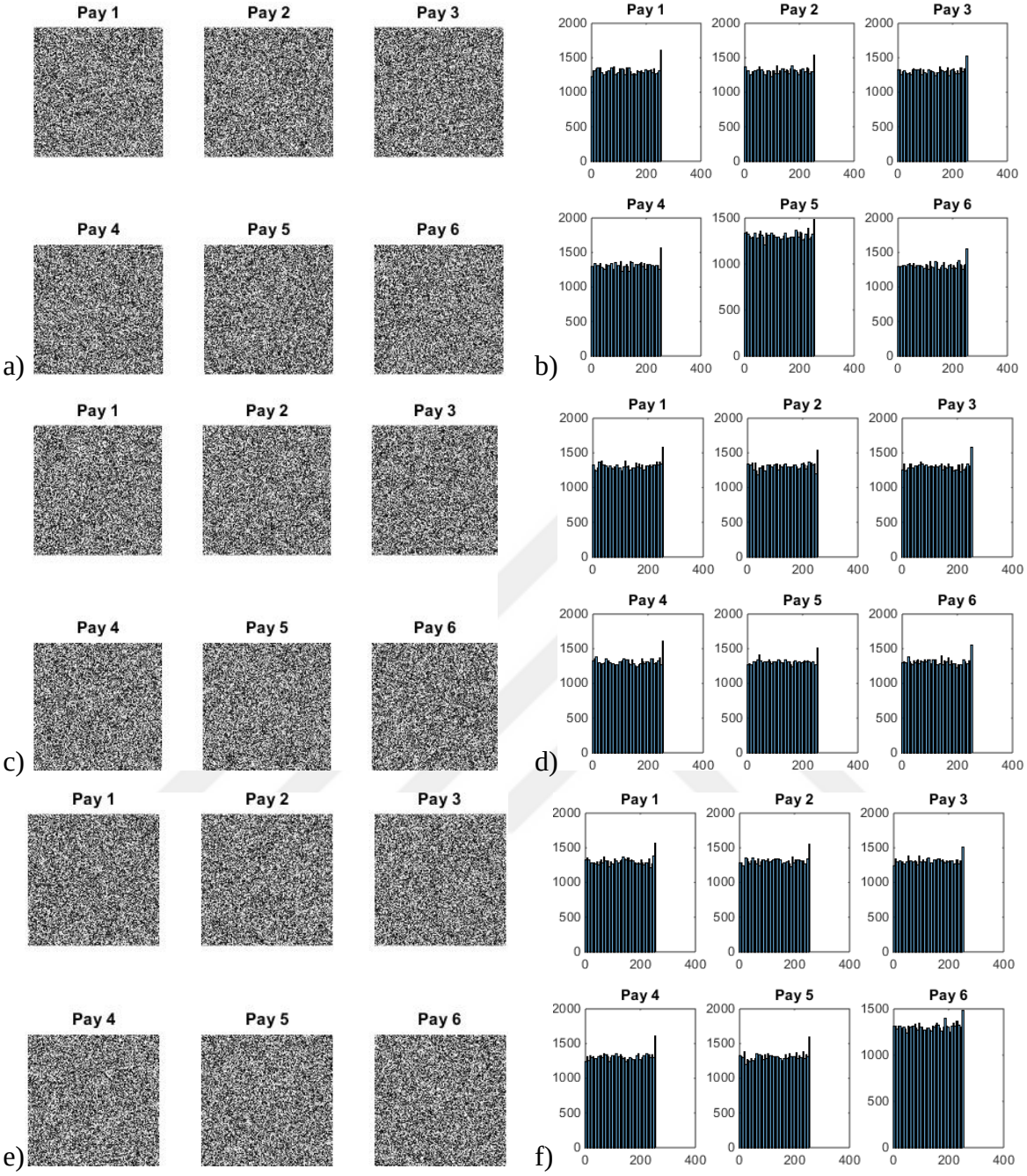
a)  b)  c)  d) 

Resim 4.5. Renkli deney görüntüsü ve RGB bileşenleri (a) Orijinal deney görüntüsü, (b) R bileşeni, (c) G bileşeni, (d) B bileşeni

a)  b)  c) 

Resim 4.6. RGB kanallarının Jarvis algoritması ile siyah beyaz görüntüye dönüştürülmesi (a) R bileşeni, (b) G bileşeni, (c) B bileşeni

AT-GSP şeması ile siyah beyaz RGB kanalları 6′şar adet pay görüntüye ayrılmıştır ve ayrılan 6'şar adet pay görüntüsüne 2D-STLH uygulanmıştır. Resim 4.7.'de RGB kanallarının paylarının şifrelenmiş hali ve histogramları verilmiştir.



Resim 4.7. Kaotik şifrelemeli AT-GSP şemasının renkli görüntülerde uygulanması (a) R kanalının paylarının şifrelenmiş hali, (b) R kanalının şifreli paylarının histogramları, (c) G kanalının paylarının şifrelenmiş hali, (d) G kanalının şifreli paylarının histogramları, (e) B kanalının paylarının şifrelenmiş hali, (f) B kanalının şifreli paylarının histogramları

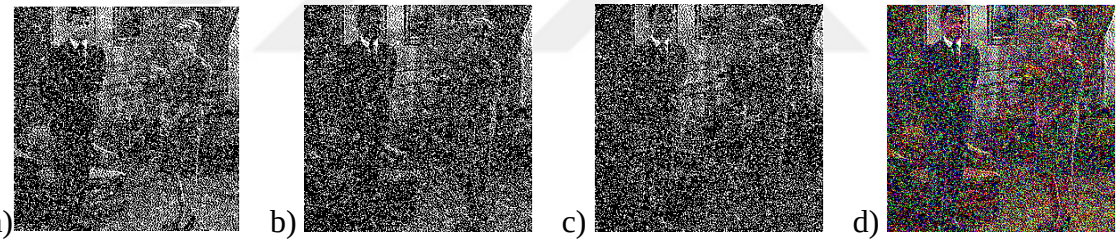
Resim 4.7.'den de anlaşılacağı gibi renk kanallarına ait pay görüntülere başarılı bir şekilde 2D-STLH uygulanmıştır. Şifreli pay görüntülerin histogramları dengeli dağılım göstermektedir. Böylelikle istatistiksel yöntem ile bilgi çıkarmak zorlaşacaktır [24]. Renkli gizli görüntüyü tekrar elde etmek için, önce paylar 2D-STLH'ın işlem basamakları tersi

yönde uygulanarak çözülmüş, her bir renk kanalı için kendi payları üst üste getirilmiş ve sonra RGB kanalları birleştirilmiştir. Birleştirilen RGB kanalları, 0 ile 1 piksel değerlerinden oluşmaktadır. Bu piksel değerleriyle görüntü, renkli olmamıştır. Renkli görüntüyü elde etmek için, 1 piksel değeri yerine 255 piksel değeri konularak, Çizelge 4.2.'de bulunan 8 adet renk, geri elde edilmiştir. Resim 4.8.'de ise geri elde edilen deney görüntüsü verilmiştir.

Çizelge 4.2. Geri elde edilen renkler

Geri Elde Edilen RGB Kanallarındaki Piksel Değerleri	1 Piksel Değerinin 255 Olarak Değiştirilmesi	Elde Edilen Piksellerin Renk Karşılığı
(0, 0, 0)	(0, 0, 0)	Siyah
(0, 0, 1)	(0, 0, 255)	Mavi
(0, 1, 0)	(0, 255, 0)	Yeşil
(0, 1, 1)	(0, 255, 255)	Cyan
(1, 0, 0)	(255, 0, 0)	Kırmızı
(1, 0, 1)	(255, 0, 255)	Magenta
(1, 1, 0)	(255, 255, 0)	Sarı
(1, 1, 1)	(255, 255, 255)	Beyaz

a) b) c) d)



Resim 4.8. Geri elde edilen görüntüler (a) Geri elde edilen R kanalı, (b) Geri elde edilen G kanalı, (c) Geri elde edilen B kanalı, (d) Geri elde edilen deney görüntüsü

RGB kanallarının Jarvis algoritması ile elde edilen görüntüleri ile şifrelendikten sonra geri elde edilen RGB görüntüleri, Eş. 4.1.'de verilen PSNR ile Eş. 4.3.'te verilen SSIM kullanılarak hesaplanmış ve Çizelge 4.3.'te gösterilmiştir.

Çizelge 4.3. Renkli deney görüntüsünün, siyah beyaz RGB kanallarının şifreleme öncesi ve geri elde edildikten sonraki görüntülerinin PSNR ve SSIM değerleri

	R Kanalı	G Kanalı	B Kanalı
PSNR	55,9821	55,8038	55,7185
SSIM	0,9929	0,9925	0,9922

Çizelge 4.3.'deki PSNR ve SSIM değerlerinde de görüldüğü gibi, R, G ve B kanallarının siyah beyaz görüntüsü ile şifrelendikten sonra geri elde edilen R, G ve B kanalları arasında benzerlik olduğu görülmüştür. SSIM değerinin 1'e ne kadar çok yaklaşırsa, orijinal görüntü ile benzerliği o kadar artacaktır. SSIM değerleri de Çizelge 4.3.'te görüldüğü gibi 1'e oldukça yakın çıkmıştır.

4.3. Kaotik Şifrelemeli AT-GSP Şemasına Yapılan Analizler ve Saldırılar

Tezin üçüncü ve son aşamasını oluşturan bu bölümde, yeni oluşturulan şifreleme yöntemine; gizli anahtar boyutu, anahtar duyarlılık analizi, histogram analizi, veri kaybı saldırıları ve tuz-karabiber saldırıları yapılmıştır.

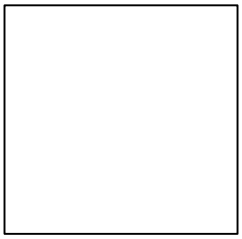
4.3.1. Gizli anahtar boyutu

2D-STLH'da kullanılan gizli anahtarın boyutu 232 bitlik olarak belirlenmiştir. 232 bitlik sayıyı bulmak için en kötü ihtimal ile 2^{232} adet deneme yapmak demektir. Bu da anahtarın kaba kuvvet algoritması ile bulunmasını zorlaştırmıştır. Ayrıca kaos haritalarında anahtar boyutunun en az 2^{100} olması beklenmektedir [56]. Bu da 2D-STLH şifreleme yönteminde kullanılan gizli anahtarın, kaba kuvvet saldırıları ile kolayca bulunamayacağını göstermiştir.

4.3.2. Gizli anahtar duyarlılığı

Uygulamadaki gizli anahtar 232 bit uzunluğunda olup Eş. 3.15'te verilmiştir. Gizli anahtarın en önemsiz biti (LSB) olan en sağdaki rakamı değiştirilmiş ve bu anahtar ile gizli görüntü çözülmeye çalışılmıştır. Resim 4.9.'da şifrelenen anahtar ile çözülmüş olan ve farklı anahtar ile çözülmüş olan görüntüler verilmiştir.

a)  b) 

c)  d) 

Resim 4.9. Lena görüntüsünün farklı anahtar ile çözülmesi, (a) Lena görüntüsü, (b) Jarvis algoritması ile ikili görüntünün oluşması, (c) Şifresi çözülen Lena görüntüsü, (d) Anahtarın değişmesi ile çözülüp elde edilen beyaz renkli görüntü

Resim 4.9. (c) görüntüsünde, Eş. 3.15'te verilen gizli anahtar ile çözülmüş iken, Resim 4.9. (d) görüntüsünde gizli anahtarın LSB'si (Least Significant Bit) "7" olarak çözülmüştür. Çözülen görüntü tamamen kaybedilmiş ve tümüyle renk beyaz olmuştur (Tüm piksel değerleri 1). Renkli görüntüler için de çözülüp elde edilen görüntü beyaz renk olmuştur. Dolayısıyla gizli anahtar duyarlılığı, yapılan çalışmada oldukça yüksektir. En önemsiz bit olan en sağdaki bir bit değişse bile görüntü çözülememiştir. Renkli görüntüler de siyah beyaz görüntülere dönüştürüldüğü için aynı sonuç renkli görüntüler için de geçerli olmuştur.

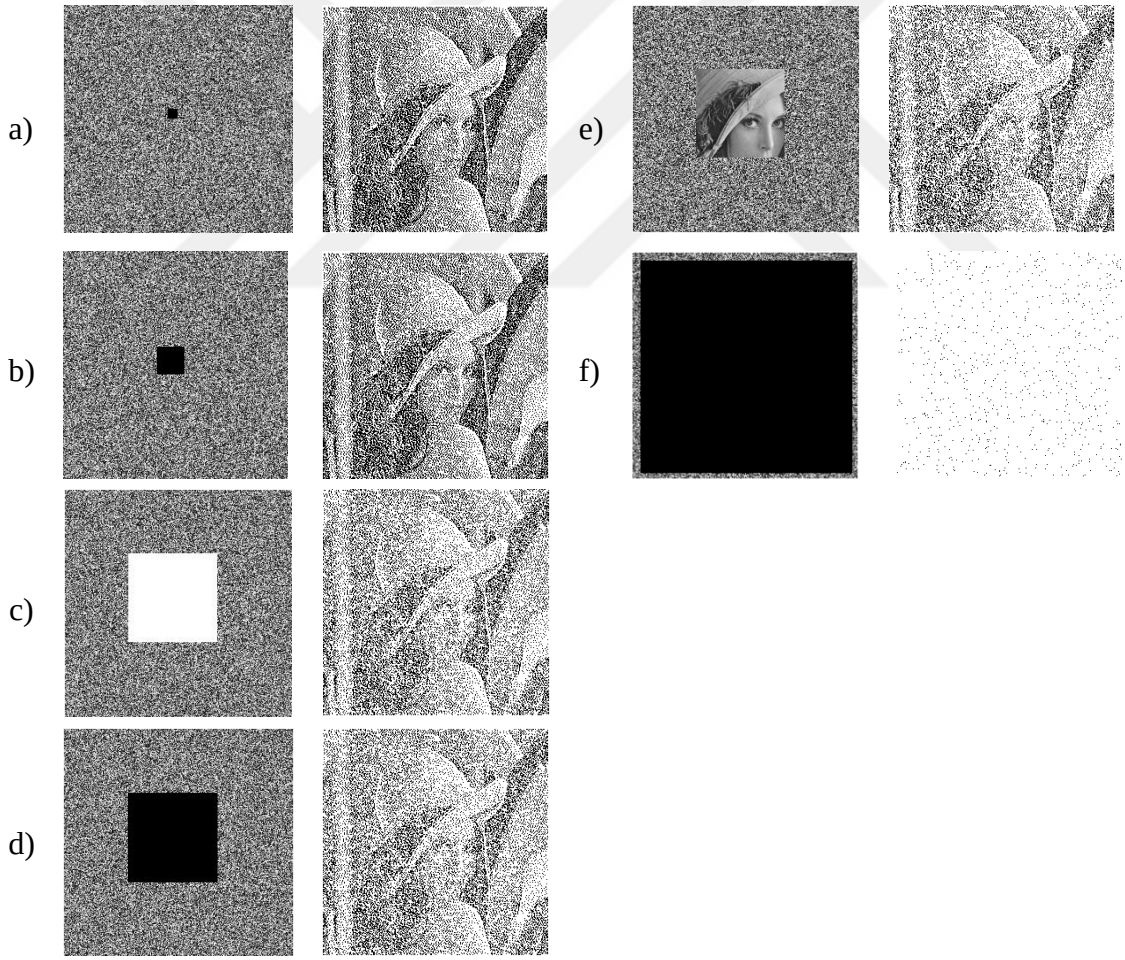
4.3.3. Histogram analizi

Resim 4.3. ve 4.7.'de görülen şifreli görüntülerin histogramları dengeli dağılım gösterdikleri için, şifreli görüntülere yapılan saldırılarla görüntüden bilgi almak çok zordur. Ayrıca histogramların dengeli dağılım göstermesi, istatistiksel yöntem ile yapılan saldırıları da zorlaştırmıştır [25].

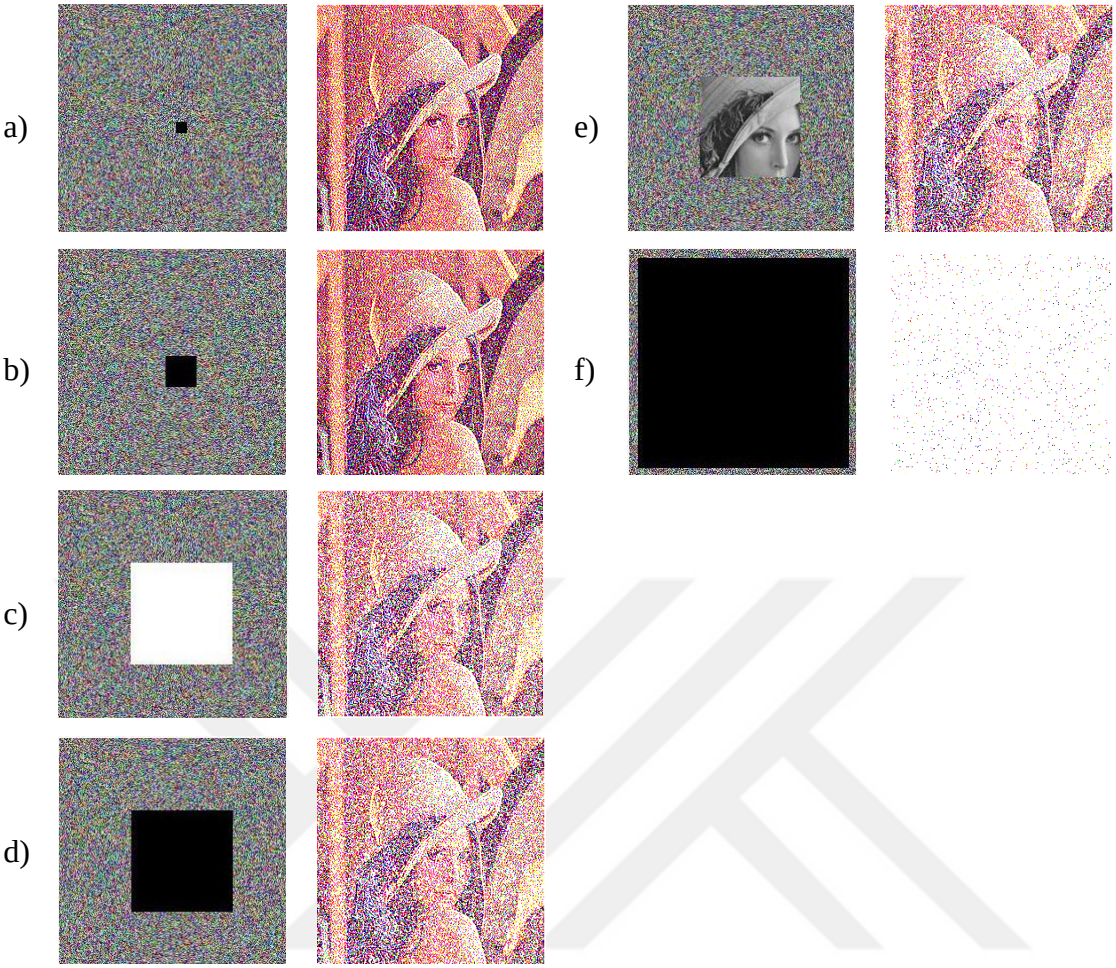
4.3.4. Veri kaybı ve tuz-karabiber saldırıları

Bu bölümde, şifreli görüntülerde oluşabilecek veri kaybı ve tuz-karabiber saldırıları yapılmıştır. Veri kaybı saldırısında, şifreli pay görüntüsünün üzerine siyah veya beyaz bloklar eklenerek şifreli görüntünün bozulması sağlanmıştır. Tuz-karabiber saldırısı ise

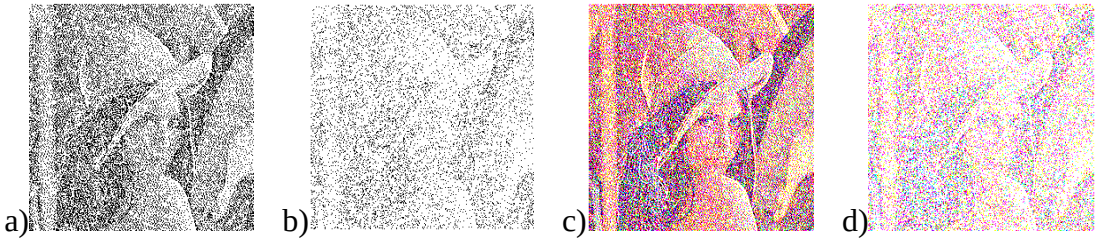
şifreli pay görüntüsüne rastgele siyah ve beyaz piksellerin eklenmesi işlemidir. Burada tuz, beyaz renkli olduğu için beyaz pikseli, karabiber de siyah renkli olduğu için siyah pikseli temsil etmektedir. Bu saldırılarda, gri tonlu Lena görüntüsü 6 adet pay görüntüye ayrılmış ve 2D-STLH ile şifrelenmiştir. Renkli Lena görüntüsü ise ilk olarak RGB kanallarına ayrılmış ve ayrı ayrı pay görüntülere paylaştırılmıştır. Dolayısıyla her bir kanal için 6 adet, toplamda da 18 adet pay görüntüsü olmuştur. 18 adet pay görüntüsü 2D-STLH ile şifrelenmiştir. Her iki görüntü türü için, şifrelenen her bir pay görüntüsüne, aynı saldırı türü, aynı oranda yapılmıştır. Saldırı yapılan şifreli pay görüntüler, şifrelendiği aynı anahtar ile çözülmüştür. Şekil 4.10'da gri tonlu Lena görüntüsü için sadece birinci pay görüntüsüne yapılan saldırı örneği, Şekil 4.11'de sadece R kanalına olan saldırı örneği gösterilmiştir. Şekil 4.12 de ise tuz-karabiber saldırı sonuçları gösterilmiştir.



Resim 4.10. Gri tonlu Lena görüntüsüne yapılan saldırılar, (a) (10×10)'luk siyah kare, (b) (30×30)'luk siyah kare, (c) (100×100)'lük beyaz kare, (d) (100×100)'lük siyah kare, (e) (100×100)'lük görüntü parçası (f) Yüzde 90'lık veri kaybı



Resim 4.11. Renkli Lena görüntüsüne yapılan saldırılar, (a) (10×10)'luk siyah kare, (b) (30×30)'luk siyah kare, (c) (100×100)'lük beyaz kare, (d) (100×100)'lük siyah kare, (e) (100×100)'lük görüntü parçası (f) Yüzde 90'lık veri kaybı



Resim 4.12. Tuz-karabiber saldırı sonuçları (a) Yüzde 1 oranında tuz-karabiber (b) Yüzde 5 oranında tuz-karabiber (c) Yüzde 1 oranında tuz-karabiber (d) Yüzde 5 oranında tuz-karabiber

Resim 4.10. ve 4.11.'da görüldüğü gibi, yapılan (10×10)'luk, (30×30)'luk ve (100×100)'lük siyah ve beyaz kare şeklindeki veri kayıplarına rağmen görüntü kalitesini tam olarak yitirmemiştir. Yüzde 90'lık kayıplarda ise görüntü kaybedilmiştir. Resim 4.12'de ise yüzde 1'lik tuz-karabiber saldırısında, yüzde 5 olan saldırı sonucuna göre, gizli görüntü daha kaliteli kalabilmiştir.

4.3.5. Saldırı sonucu yapılan ölçümler

Yapılan veri kaybı ve tuz-karabiber saldırıları sonucu oluşan görüntüler ile orijinal görüntüler arasında bazı ölçümler yapılmıştır. Bu ölçümlerde kullanılan metrikler; Eş. 4.1'de verilen PSNR, Eş. 4.2'de verilen SSIM ve renkli görüntüler için Eş. 4.11'da verilen CQM (Color Image Quality Measure)'dur.

CQM hesaplamasında, ilk olarak renkli görüntünün RGB kanallarındaki piksel değerleri YUV kanallarına çevrilmiştir. Y parlaklığı, U mavi renk farkını ve V ise kırmızı renk farkını temsil etmektedir. Çevirme işlemleri denklem Eş. 4.10'da verilmiştir.

$$\begin{cases} Y = 0{,}257R + 0{,}504.G + 0{,}098B + 16 \\ U = -0{,}148R - 0{,}291G + 0{,}439B + 128 \\ V = 0{,}439R - 0{,}368G - 0{,}071B + 128 \end{cases} \quad (4.10)$$

YUV kanalları oluşturulduktan sonra R_W ile C_W hesaplanmıştır. R_W ile C_W insan gözündeki koni ve çubuk foto reseptörlerinin ağırlığıdır. $R_W = 0{,}9449$ ile $C_W = 0{,}0551$ olarak bulunmuş ve CQM Eş. 4.11'deki gibi hesaplanmıştır [57].

$$CQM = (PSNR_Y \times R_W) + (\frac{PSNR_U + PSNR_V}{2}) \times C_W \ (dB) \quad (4.11)$$

$PSNR_Y$ değeri, gizli görüntü ile geri elde edilen görüntünün Y kanalının PSNR değeridir. Aynı şekilde $PSNR_U$ ve $PSNR_V$ değerleri de gizli görünü ile geri elde edilen görüntünün U ve V kanallarının PSNR değerleridir. CQM sonucu ne kadar yüksek olursa görüntünün çözünürlüğü o kadar az bozulmuştur.

İlk olarak görüntüler AT-GSP şeması ile 6 adet pay görüntülere ayrılmış, daha sonra bu 6 adet pay görüntüsüne 2D-STLH ile şifreleme yapılmıştır. Görüntüler tekrar çözülmüş ve üst üste getirilmiştir. Elde edilen görüntü ile gizli görüntüler arasında ölçümler yapılmıştır.

Çizelge 4.4.'te ikili ve gri tonlu deney görüntülerin, şifreleme öncesi ile şifreleme sonrası görüntülerinin PSNR ve SSIM değerleri hesaplanmıştır. Çizelge 4.5.'te ise renkli deney görüntülerin, şifreleme öncesi ve sonrası ölçümleri için CQM değerleri hesaplanmıştır.

Deney için kullanılan görüntüler, USC-SIPI Image Database adlı veri tabanından alınan görüntülerdir [58].

Çizelge 4.4. İkili ve gri tonlu görüntülerin kaotik şifrelemeli AT-GSP şeması ile oluşan pay görüntülerinin orijinal görüntüleri ile PSNR ve SSIM değerleri

Deney Görüntüsü	PSNR	SSIM
Siyah beyaz Lena Görüntüsü (256×256)	58,3701	0,9958
Gri tonlu Lena Görüntüsü (256×256)	58,1951	0,9966
Gri tonlu Barbara Görüntüsü (512×512)	57,8817	0,9962
Renkli Biber Görüntüsünün Kırmızı bileşeni (225×225)	58,9144	0,9973
Renkli Biber Görüntüsünün Yeşil bileşeni (225×225)	57,7796	0,9958
Renkli Biber Görüntüsünün Mavi bileşeni (225×225)	56,5663	0,9941

Çizelge 4.5. Renkli görüntülerin kaotik şifrelemeli AT-GSP şeması ile oluşan pay görüntülerinin orijinal görüntüleri ile CQM değerleri

Deney Görüntüsü	CQM
Renkli Biber Görüntüsü $(225 \times 225 \times 3)$	20,6227
Renkli Lena Görüntüsü $(256 \times 256 \times 3)$	22,1913
Renkli Ev Görüntüsü $(256 \times 256 \times 3)$	22,4517
Renkli Jet Görüntüsü $(512 \times 512 \times 3)$	25,8311
Renkli Babun Görüntüsü $(512 \times 512 \times 3)$	20,5208

Çizelge 4.4'deki ve Çizelge 4.5.'teki PSNR, SSIM ve CQM değerleri, şifreleme işlemi sonucunda geri elde edilen görüntülerin, orijinal görüntüleri ile benzerlik olduğunu göstermektedir. SSIM değerlerinin 1'e yaklaşması, benzerliğin çok yüksek olduğunu göstermektedir.

Çizelge 4.6.'da, Resim 4.10.'daki saldırı sonucunda elde edilen gri tonlu görüntüler ile orijinal görüntüler arasında PSNR ve SSIM sonuçları verilmiştir. Çizelge 4.7.'de ise Resim 4.11.'deki saldırı sonucunda elde edilen renkli görüntüler ile orijinal görüntüler arasında CQM sonuçları verilmiştir.

Çizelge 4.6. Gri tonlu Lena görüntüsüne yapılan saldırı sonucu oluşan görüntülerin PSNR ve SSIM değerleri

Yapılan Saldırı	PSNR	SSIM
(10×10)'luk siyah kare	75,7988	1,000
(30×30)'luk siyah kare	67,4142	0,9997
(100×100)'lük beyaz kare	57,6786	0,9959
(100×100)'lük siyah kare	57,6786	0,9959
(100×100)'lük görüntü parçası	57,6762	0,9959
Yüzde 90'lık kayıp	52,0986	0,9728
Yüzde 1 oranında tuz-karabiber	58,7118	0,9971
Yüzde 5 oranında tuz-karabiber	53,5124	0,9834

Çizelge 4.7. Renkli Lena görüntüsüne yapılan saldırı sonucu oluşan görüntülerin CQM değerleri

Yapılan Saldırı	CQM
(10×10)'luk siyah kare	25,4017
(30×30)'luk siyah kare	25,3883
(100×100)'lük beyaz kare	25,3587
(100×100)'lük siyah kare	25,3587
(100×100)'lük görüntü parçası	25,3543
Yüzde 90'lık kayıp	24,9894
Yüzde 1 oranında tuz-karabiber	25,1583
Yüzde 5 oranında tuz-karabiber	25,0015

Çizelge 4.6. ve Çizelge 4.7.'de görüldüğü gibi, aynı saldırı türünün saldırı oranı arttıkça, PSNR, SSIM ve CQM değerlerinde düşüş gözlemlenmiştir. Bunun sonucu olarak da saldırı oranı arttıkça benzerlik oranının azaldığı anlaşılmaktadır. Elde edilen PSNR, SSIM ve CQM değerlerine göre, saldırılara rağmen görüntünün benzerlik oranları yüksek çıkmıştır. SSIM değerleri de 1'e oldukça yakın çıkmıştır. Yalnızca yüzde 90'lık saldırılarda görüntü, görsel olarak kaybedilmiştir. Sonuç olarak, çoğu saldırıya karşı sistemin dayanıklı olduğu görülmüştür.

5. SONUÇLAR VE ÖNERİLER

Bu tez çalışmasında, AT-GSP şemasında oluşan güvenlik açığına, kaotik görüntü şifreleme yöntemlerinden birisi olan 2D-STLH şifreleme yöntemi uygulanarak çözüm getirilmiştir. Önerilen yöntem temel olarak üç ana kısımdan oluşmaktadır. İlk iki kısımda AT-GSP şemasının ve 2D-STLH şifreleme yönteminin nasıl yapıldığı hakkında bilgiler verilmiştir. Tezin son kısmında ise bu iki şifreleme yönteminin birleştirilmesi sonucu ortaya çıkan kaotik şifrelemeli AT-GSP şeması anlatılmış ve yapılan yeni yönteme yönelik analizler ve saldırılar açıklanmıştır.

Bu çalışmanın ilk kısmında, AT-GSP şeması, gizlenmek istenen görüntüyü, kullanıcıların ayrıcalık sırasına göre, pay görüntülere ayıran ve hiçbir geleneksel şifreleme yöntemlerinin kullanılmadığı, sadece insanın görme sistemi ile çözülen bir görüntü şifreleme türüdür. Bu yöntemin avantajları, her bir pay görüntüsünün gizlenecek görüntü ile boyutunun aynı kalması, geleneksel GSP yöntemlerine göre geri elde edilen görüntünün daha iyi kontrasta sahip olması ve her bir payın gizli görüntüyü ortaya çıkarmak için birbirinden farklı kapasiteye sahip olmasıdır.

AT-GSP şemasında, yüksek önceliğe sahip birçok pay görüntüsünün üst üste bindirilmesi sonucu, gizli görüntü, hem görsel olarak ortaya çıkmakta (Bkz. Resim 4.1.) hem de benzerlik oranı PSNR ve SSIM ile hesaplandığında yüksek olduğu görülmektedir (Bkz. Çizelge 4.1.). Bu da gizli görüntüyü elde etmek isteyen üçüncü şahısların tüm pay görüntülerine sahip olmadan gizli görüntüyü görebilecekleri anlamına gelmektedir. Böylece AT-GSP şemasında bir güvenlik problemi olduğu ortaya çıkmıştır. Bu tezde, getirilen çözüm önerisi, pay görüntülerin de ayrıca şifrelenerek bu problemin önüne geçmektir. Şifreleme yöntemi olarak da çok boyutlu kaos tabanlı görüntü şifreleme yöntemlerinin uygun olduğu görülmüştür. Kaos tabanlı görüntü şifrelemenin uygun olmasının temel sebepleri, diğer şifreleme yöntemlerine göre kontrol parametre ve anahtar duyarlılığının, sistemin başlangıç durumunun, tahmin edilemezliğinin, ergodikliğinin, esnekliğinin ve hızının avantajlı olması olarak gösterilmiştir.

Bu çalışmanın ikinci kısmında, çok boyutlu kaos tabanlı görüntü şifreleme yöntemlerinden biri olan 2D-STLH anlatılmıştır. 2D-STLH yönteminde, ilk olarak gizli anahtar (GA)

belirlenmiştir. 232 bitlik olan bu gizli anahtar ile iki adet K_1 ve K_2 kaotik matrisleri oluşturmak için ilk değerler bulunmuştur. Bulunan ilk değerler Eş. 3.12'de 2D-STLH'ın formülünde kullanılmıştır. Çıkan ilk sonuçlar K_1 ve K_2'nin ilk elemanıdır. Daha sonra K_1 ve K_2'nin ilk elemanları da tekrar Eş. 3.12'de işleme sokulmuş ve K_1 ve K_2'nin diğer elemanlar da birbirine bağlı olarak bu yolla elde edilmiştir. Kaotik matrislerin elemanlarının değerleri 0 ile 1 arasında olup bu değerler 0 ile 255 arasında olacak şekilde yeniden düzenlenmiştir. Bunun sebebi, görüntü piksellerin 0 ile 255 arasında olmasından dolayı kaotik matrislerin de buna uygun bir şekilde olacak olmasıdır. Böylelikle birbirleri ile uyumlu olmuştur.

2D-STLH'ın ikinci aşamasında, gizlenecek görüntünün çevresine 0 ile 255 arasında rastgele pikseller eklenmiştir. Bunun sebebi, gizli görüntü aynı anahtar ile şifrelense bile farklı şifreli görüntüler elde edilmesidir. Etrafına rastgele pikseller eklenmiş gizli görüntü ilk olarak K_1 matrisi sırasıyla permütasyon-difüzyon işlemine sokulmuştur. Elde edilen görüntü ile bu sefer K_2 matrisi sırasıyla tekrar permütasyon-difüzyon işlemine sokulmuştur. Böylelikle iki adet döngü tamamlanmıştır. En son elde edilen görüntü, 2D-STLH ile şifrelenmiş bir görüntü olmuştur.

Tezin son aşamasında yeni ortaya çıkan kaotik şifrelemeli AT-GSP şeması anlatılmıştır. Bu yeni yöntemde ikili, gri tonlu ve renkli görüntülerin nasıl uygulandığı ve bu yönteme yapılan analizler ve saldırılar gösterilmiştir. İlk olarak AT-GSP şemasında işlenen görüntüler, ikili görüntüler olmak zorundadır. İkili görüntüler direkt olarak işleme girerken, gri tonlu görüntüler ilk olarak Jarvis algoritması ile ikili görüntülere çevrilmiştir. Elde edilen ikili görüntü AT-GSP şemasında n adet pay görüntüye paylaştırılmıştır. n adet pay görüntü de 2D-STLH şifrelemesi ile şifrelenmiştir. Bu şekilde daha güvenli bir yol önerilmiştir. Şifrelenmiş görüntüyü çözmek için, ilk olarak 2D-STLH'ın işlem basamaklarını ters olarak uyguladıktan sonra pay görüntüler elde edilmiştir. Pay görüntüler de üst üste getirildiğinde gizli görüntü elde edilmiş olacaktır.

Renkli görüntüler de ise ilk olarak RGB kanallarına ayırma işlemi gerçekleşmiştir. RGB kanalları ayrı ayrı Jarvis algoritmasına sokulmuş ve ikili görüntüler elde edilmiştir. Her bir ikili görüntü şeklinde olan renk kanalları AT-GSP şemasına sokularak her bir renk kanalı için n adet pay görüntü elde edilmiştir. Sonuç olarak $3n$ adet pay görüntüsü olmuştur. Bu

pay görüntüleri de 2D-STLH yöntemi ile şifrelenmiş ve renkli görüntüler için şifreleme tamamlanmıştır.

Renkli görüntülerde gizli görüntüyü elde etmek için, şifrelenen her bir pay görüntü, 2D-STLH'ın işlem basamaklarının tersi uygulanarak çözülmüştür. Her bir kanalın payları üst üste getirilmiş ve sonra RGB kanalları birleştirilmiştir. Birleştirilen RGB kanallarında 1 olan piksel değeri, 255 olarak değiştirilmiş, 8 adet renk ortaya çıkmış ve renkli görüntü elde edilmiştir.

Oluşan şifreli pay görüntülere gizli anahtar duyarlılığı, histogram analizi, veri kaybı ve tuz-karabiber saldırıları yapılmıştır. Bu saldırılar hem gri tonlu hem de renkli görüntülere ayrı ayrı uygulanmıştır. Anahtar duyarlılığında, gizli anahtarın en önemsiz biti değişince bile gizli görüntü çözülememiştir. Bu da sistemin anahtar duyarlılığının yüksek olduğunu göstermektedir. Şifreli görüntülerin histogramları, dengeli dağılım göstermiştir. Bunun sonucu olarak da istatistiksel yöntemler ile herhangi bir bilgi çıkarımının yapılması zorlaştırmıştır. Veri kaybı ve tuz-karabiber saldırıları sonucu yapılan ölçüm sonuçları ikili ve gri tonlu görüntüler için PSNR ile SSIM, renkli görüntüler için ise CQM ile ölçülmüştür. Görüntü netliklerine bakıldığında, (10×10), (30×30) ve (100×100)'luk saldırılara nazaran en kötü sonuç yüzde 90'lık kayıpta görülmüştür. Yüzde 1'lik tuz-karabiber saldırısı da yüzde 5'lik tuz-karabiber saldırısına göre daha net bir görüntü elde edilmiştir.

Bu tez çalışmasının benzer çalışmalardan en belirgin özellikleri, GSP ve kaotik şifreleme yöntemleri birlikte kullanılmış, şifreleme aşamasında gri tonlu görüntülere AT-GSP şemasında Jarvis algoritmasının uygulanmış, aynı zamanda, aynı yöntemler renkli görüntülere de uygulanmıştır.

AT-GSP şeması kayıplı bir yöntem olduğu için gizli görüntüyü elde ederken kayıplar yaşanabilmektedir. Ayrıca 2D-STLH ile şifreleme yaparken maliyet olarak süre uzayabilmektedir. İlerleyen çalışmalarda ise bu kayıpları daha aza indirecek çalışmalar yapılması planlanmalıdır.

KAYNAKLAR

1. Pour Hossein, S. (2011). *DNA Desenleri Kullanarak Görüntü Şifreleme*, Yüksek Lisans Tezi, Karadeniz Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Trabzon.

2. Tunçer, S. (2016). *Kaotik Sistem Tabanli Görüntü Şifreleme*, Yüksek Lisans Tezi, Bilecik Şeyh Edebali Üniversitesi, Fen Bilimleri Enstitüsü, Bilecik.

3. Van Tilborg, H. C. A. (2000). *Fundamentals of Cryptology* (Üçüncü Baskı). Dordrecht: Kluwer Academic Publishers, 1-2.

4. National Institute of Standards and Technology. (2001). Advanced Encryption Standard (AES). *FIPS PUB 197, Gaithersburg, Maryland*, 9-25.

5. National Institute of Standards and Technology. (1999). Data Encryption Standard (DES). *FIPS PUB 46, Gaithersburg, Maryland*, 8-15.

6. National Institute of Standards and Technology. (2009). Digital Signature Standard (DSS). *FIPS PUB 186-4, Gaithersburg, Maryland*, 15-19.

7. Kapoor, D., Keshari, S. and Gaur, S. K. (2014). An Overview of Visual Cryptography. *International Journal of Advanced Research in Computer Science and Software Engineering*, 4(2), 103-110.

8. Thien, C. C. and Lin, J. C. (2002). Secret image sharing. *Computers & Graphics*, 26(5), 765-770.

9. Blakley, G. R. (1979). *Safeguarding cryptographic keys.* Proceedings of the National Computer Conference, 48, 313-317, New Jersey, USA.

10. Shamir, A. (1979). How to Share a Secret. *Association for Computing Machinery*, 22(11), 612–613.

11. Naor, M. and Shamir, A. (1995). *Visual Cryptography.* Advances in Cryptography-EUROCRYPT'94, 1–12, Peruiga, Italy.

12. Fang, W. P. and Lin, J. C. (2006). Progressive viewing and sharing of sensitive images. *Pattern Recognition and Image Analysis*, 16(4), 632–636.

13. Hou, Y. C. and Quan, Z. Y. (2011). Progressive visual cryptography with unexpanded shares. *IEEE Transactions on Circuits and Systems for Video Technology*, 21(11), 1760–1764.

14. Jin, D., Yan, W. and Kankanhalli, M. (2005). Progressive color visual cryptography. *SPIE Journal of Electronic Imaging*, 14(3), 1-28.

15. Fang, W. P. (2008). Friendly progressive visual secret sharing. *Pattern Recognition*, 41(4), 1410–1414.

16. Anderson R. J. and Petitcolas, F. A. P. (1998). On the Limits of Steganography, *IEEE Journal of Selected Areas In Communications*, 16(4), 474-481.

17. Wang, R. Z., Chien, Y. F. and Lin, Y. Y. (2010). Scalable user-friendly image sharing. *Journal of Visual Communication and Image Representation*, 21(7), 751–761.

18. Hou, Y. C. (2003). Visual cryptography for color images. *Pattern Recognition*, 36(7), 1619–1629.

19. Chen, C. C., Chen, C. C. and Lin, Y. C. (2009). Weighted modulated secret image sharing method. *Journal of Electronic Imaging*, 18(4), 1-6.

20. Lin, S. J., Chen, L. S. T. and Lin, J. C. (2009). Fast-weighted secret image sharing. *Optical Engineering*, 48(7), 1-7.

21. Li, P., Yang, C. N., Wu, C. C., Kong, Q. and Ma, Y. (2013). Essential secret image sharing scheme with different importance of shadows. *Journal of Visual Communication and Image Representation*, 24(7), 1106–1114.

22. Hou, Y. C., Quan, Z. Y. and Tsai, F. C. (2015). A privilege-based visual secret sharing model. *Journal of Visual Communication and Image Representation*, 33, 358–367.

23. Corrochabo, E. B. (2005). *Handbook of Geometric Computing*, (Birinci baskı). Leipzig: Springer, 231-238.

24. Arroyo, D., Rhouma, R., Alvarez, G., Li, S. and Fernandez, V. (2008). On the security of a new image encryption scheme based on chaotic map lattices. *Chaos Interdisciplinary Journal of Nonlinear Science*, 18(3), 1-8.

25. Hua, Z. and Zhou, Y. (2016). Image encryption using 2D Logistic-adjusted-Sine map. *Information Sciences*, 339, 237–253.

26. Ye, G., Zhao, H. and Chai, H. (2016). Chaotic image encryption algorithm using wave-line permutation and block diffusion. *Nonlinear Dynamics*, 83(4), 2067–2077.

27. Tang, Y. and Guan, X. (2009). Parameter estimation of chaotic system with time-delay: A differential evolution approach. *Chaos, Solitons and Fractals*, 42(5), 3132–3139.

28. Wu, Y., Gelan, Y., Jin, H. and Noonan J. P. (2012). Image encryption using the two-dimensional logistic chaotic map. *Journal of Electronic Imaging*, 21(1), 13014.

29. Ye, G. (2010). Image scrambling encryption algorithm of pixel bit based on chaos map. *Pattern Recognition Letters*, 31(5), 347–354, 2010.

30. Hua, Z., Zhou, Y., Pun, C. M. and Chen, C. L. P. (2015), 2D Sine Logistic modulation map for image encryption. *Information Sciences*, 297, 80–94.

31. Nikate, P. M. and Mujavar, I. I. (2015). Performance Evaluation of Floyd Steinberg Halftoning and Jarvis Halftoning Algorithms in Visual Cryptography. *International Journal of Innovations in Engineering and Technology*, 5(1), 336–342.

32. Yıldızhan, A. ve Doğan, N. (2017). *Gri Tonlu Görüntülerde Kaotik Şifrelemeli Ayrıcalık Tabanlı Görsel Sır Paylaşım Şeması*. 19. Akademik Bilişim Konferansı (AB 2017), Aksaray, Türkiye.

33. Özbek, İ. (2012). *Sır Paylaşım Sistemleri,* Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

34. Landjev, I. (1999). The Mathematical Foundation of Secret Sharing. *International Workshop Information Security in the 21st Century Global Convergence*, 53(9), 1689–1699.

35. McEliece, R. J. and Sarwate, D. V. (1981). On sharing secrets and Reed-Solomon codes. *Association for Computing Machinery*, 24(9), 583–584.

36. Mignotte, M. (1983). *How to share a secret,* Proceedings of the Workshop on Cryptography. 149, 371-375

37. Asmuth, C. and Bloom, J. (1983). A modular approach to key safeguarding. *IEEE Transaction on Information Theory*, 29(2), 208–210.

38. Arda, D. ve Buluş, E. (2009). *Çin kalan teoremini kullanan bir gizlilik paylaşım şeması.* IV. İletişim Teknolojileri Ulusal Sempozyumu, 23–26, Adana, Türkiye.

39. Droste, S. (1996). *New Results on Visual Cryptography*. Advances in Cryptography-CRYPTO ’96. 1109, 401–415.

40. Simmons, G. J., Jackson, W. and Martin, K. (1991). The geometry of shared secret schemes. *Bulletin of the ICA*, 1, 71-88.

41. Hofmeister, T., Krause, M. and Simon, H. M. (2000). Contrast-optimal out of secret sharing schemes in visual cryptography. *Theoretical Computer Science,* 240(2), 471–485.

42. Blundo, C., De Santis, A. and Naor, M. (2000). Visual cryptography for grey level images. *Information Processing Letters,* 75(6), 255–259.

43. De Prisco, R. and De Santis, A. (2013). Color visual cryptography schemes for black and white secret images. *Theoretical Computer Science,* 510, 62–86.

44. Lin, C. C. and Tsai, W. H. (2003). Visual cryptography for gray-level images by dithering techniques. *Pattern Recognition Letters*, 24(1-3), 349–358.

45. Yang, C. N., Sun, L. Z. and Cai, S. R. (2016). Extended color visual cryptography for black and white secret image. *Theoretical Computer Science*, 609(1), 143–161.

46. Wu, C. C. and Chen, L. H. (1998). *A Study On Visual Cryptography*, Yüksek Lisans Tezi, National Chiao Tung University, Institute of Computer and Information Science, Taiwan.

47. Wang, D. S., Yi, F. and Li, X. (2009). On general construction for extended visual cryptography schemes. *Pattern Recognition*, 42(11), 3071–3082.

48. Yang, C. N. (2004). New visual secret sharing schemes using probabilistic method. *Pattern Recognition. Letters*, 25(4), 481–494.

49. Wu, Y. S., Thien, C. C. and Lin, J. C. (2004). Sharing and hiding secret images with size constraint. *Pattern Recognition*, 37(7), 1377–1385.

50. Ateniese, G., Blundo, C., De Santis, A. and Stinson, D. R. (2001). Extended capabilities for visual cryptography. *Theoretical Computer Science*, 250(1-2), 143–161.

51. Tetik, Y. E., Yıldızhan, A. ve Erol, K. (2015). *Görsel Kriptografide Yarı Tonlu Gizli Görüntünün Algılanan Kalitesinin İyileştirilmesi.* 23'üncü Sinyal İşleme ve İletişim Uygulamaları, (SIU 2015), 588-591, Malatya, Türkiye.

52. Liu, W., Sun, K. and Zhu, C. (2016). A fast image encryption algorithm based on chaotic map. *Optics and Lasers in Engineering*, 84(3), 26–36.

53. Wang, X., Teng, L. and Qin, X. (2012). Breaking a novel colour image encryption algorithm based on chaos. *Signal Processing*, 92(4), 1101–1108.

54. Soleyman Zadeh, K. (2012). *Çok Parçalı Sır Paylaşım Şemaları ve Uygulamaları*, Yüksek Lisans Tezi, Karadeniz Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Trabzon.

55. Akbay, C. (2013). *Application of Image Enhancement Algorithms To Improve the Visibility and Classification of Microcalcifications in Mammograms*, Yüksek Lisans Tezi, Ortadoğu Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

56. Alvarez, G. and Li, S. (2006), Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems. *International Journal of Bifurcation and Chaos*, 16(8), 2129-2151.

57. Yalman, Y. and Ertürk, İ. (2013). A new color image quality measure based on YUV transformation and PSNR for human vision system. *Turkish Journal of Electrical Engineering and Computer Sciences*, 21(2), 603–612.

58. İnternet: The USC-SIPI Image Database. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fsipi.usc.edu%2Fdatabase%2Fdatabase.php%3Fvolume%3Dmisc&date=2018-05-07 Son Erişim Tarihi: 07.05.2018.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: YILDIZHAN, Aytekin
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 19.05.1990, Kadirli
Medeni hali	: Evli
Telefon	: 0 (545) 446 36 56
E-Posta	: aytekinyildizhan@gmail.com

Eğitim

Derece	Eğitim Birimi	Mezuniyet tarihi
Yüksek Lisans	Gazi Üniversitesi/Bilgisayar Mühendisliği	Devam Ediyor
Lisans	İzmir Yüksek Teknoloji Enst./Bilgisayar Müh.	2013
Lise	Afyonkarahisar Anadolu Öğretmen Lisesi	2008

İş Deneyimi

Yıl	Çalıştığı Yer	Görev
2016-Devam	Kara Havacılık Okul Komutanlığı	Bilgi İşlem Amiri
2013-2016	Kara Harp Okulu	Öğretim Görevlisi

Yabancı Dil

İngilizce

Yayınlar

Yıldızhan A. ve Doğan, N. (2017). *Gri Tonlu Görüntülerde Kaotik Şifrelemeli Ayrıcalık Tabanlı Görsel Sır Paylaşım Şeması.* 19. Akademik Bilişim Konferansı, (AB 2017), Aksaray, Türkiye.

Yıldızhan A. ve Karakurt, H. B. (2016). *Bilişsel Bilimin Yazılım Maliyetine Yapabileceği Katkılar Üzerine Bir İnceleme.* Elektrik-Elektronik ve Bilgisayar Sempozyumu, (EEB 2016). Tokat, Türkiye.

Tetik, Y. E., Yıldızhan, A. ve Erol, K. (2015). *Görsel Kriptografide Yarı Tonlu Gizli Görüntünün Algılanan Kalitesinin İyileştirilmesi.* 23'üncü Sinyal İşleme ve İletişim Uygulamaları, (SIU 2015), 588-591, Malatya, Türkiye.

Yıldızhan A. ve Çetin, A. (2015). *Yazılımın Bilişsel Karmaşıklığını Ölçme Üzerine Bir İnceleme.* 8'inci Mühendislik ve Teknoloji Sempozyumu, (MTS8), 361-365, Ankara, Türkiye.

Hobiler

Futbol, Basketbol, Koşu, Doğa Yürüyüşü, Kitap Okuma, Sinema

GAZİ GELECEKTİR...