KOCAELİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLİŞİM SİSTEMLERİ MÜHENDİSLİĞİ
ANABİLİM DALI

YÜKSEK LİSANS TEZİ

GÖRÜNTÜ STEGANOGRAFİSİ İÇİN GENETİK ALGORİTMA VE BLOK TABANLI YENİ BİR YÖNTEM

ZEYNEP SARI

KOCAELİ 2022

KOCAELİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BİLİŞİM SİSTEMLERİ MÜHENDİSLİĞİ

ANABİLİM DALI

YÜKSEK LİSANS TEZİ

GÖRÜNTÜ STEGANOGRAFİSİ İÇİN GENETİK ALGORİTMA VE BLOK TABANLI YENİ BİR YÖNTEM

ZEYNEP SARI

Prof. Dr. Mehmet YILDIRIM **Danışman, Kocaeli Üniv.**	**……**
Doç. Dr. Serdar SOLAK **Jüri Üyesi, Kocaeli Üniv.**	**……**
Doç. Dr. Adem TUNCER **Jüri Üyesi, Yalova Üniv.**	**……**

Tezin Savunulduğu Tarih : 15.06.2022

ETİK BEYAN VE ARAŞTIRMA FONU DESTEĞİ

Kocaeli Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım bu tez/proje çalışmasında,

- Bu tezin/projenin bana ait, özgün bir çalışma olduğunu,
- Çalışmamın hazırlık, veri toplama, analiz ve bilgilerin sunumu olmak üzere tüm aşamalarında bilimsel etik ilke ve kurallara uygun davrandığımı,
- Bu çalışma kapsamında elde edilen tüm veri ve bilgiler için kaynak gösterdiğimi ve bu kaynaklara kaynakçada yer verdiğimi,
- Bu çalışmanın Kocaeli Üniversitesi'nin abone olduğu intihal yazılım programı kullanılarak Fen Bilimleri Enstitüsü'nün belirlemiş olduğu ölçütlere uygun olduğunu,
- Kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- Tezin/Projenin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez/proje çalışması olarak sunmadığımı,

beyan ederim.

[X] Bu tez/proje çalışmasının herhangi bir aşaması hiçbir kurum/kuruluş tarafından maddi/alt yapı desteği ile desteklenmemiştir.

[ ] Bu tez/proje çalışması kapsamında üretilen veri ve bilgiler ..... tarafından ..... no'lu proje kapsamında maddi/alt yapı desteği alınarak gerçekleştirilmiştir.

Herhangi bir zamanda, çalışmamla ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçları kabul ettiğimi bildiririm.

……..

Zeynep SARI

YAYIMLAMA VE FİKRİ MÜLKİYET HAKLARI

Fen Bilimleri Enstitüsü tarafından onaylanan lisansüstü tezimin/projemin tamamını veya herhangi bir kısmını, basılı ve elektronik formatta arşivleme ve aşağıda belirtilen koşullarla kullanıma açma izninin Kocaeli Üniversitesi'ne verdiğimi beyan ederim. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak, tezimin/projemin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanımı bana ait olacaktır.

Tezin/projenin kendi özgün çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin/projenin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Tezimde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanılması zorunlu metinlerin yazılı izin alarak kullandığımı ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

Yükseköğretim kurulu tarafından yayınlanan ***"Lisanüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"*** kapsamında tezim aşağıda belirtilen koşullar haricinde YÖK Ulusal Tez Merkezi/ Kocaeli Üniversitesi Kütüphaneleri Açık Erişim Sisteminde erişime açılır.

☐ Enstitü yönetim kurulu kararı ile tezimin/projemin erişime açılması mezuniyet tarihinden itibaren 2 yıl ertelenmiştir.
☐ Enstitü yönetim kurulu gerekçeli kararı ile tezimin/projemin erişime açılması mezuniyet tarihinden itibaren 6 ay ertelenmiştir.
☒ Tezim/projem ile ilgili gizlilik kararı verilmemiştir.

……

Zeynep SARI

ÖNSÖZ VE TEŞEKKÜR

İnternetin ve beraberinde getirdiği teknolojik cihazların büyüyen bir hızla kullanılması verinin güvenliğine ve iletimine dair çalışmaları arttırmıştır. Bu kapsamda tez çalışmasında, genetik algoritma ile veri gizleme algoritması tasarlanmaya çalışılmıştır. Yüksek kapasite veri gizlenirken verinin varlığının gizlenmesi hedeflenmiştir.

Yüksek lisans eğitimim süresince, her türlü konuda benimle bilgi ve birikimlerini paylaşan, yoğun çalışma temposunda, zaman ve mekandan bağımsız olarak çalışmamın tamamlanmasında büyük emeği olan kıymetli danışman hocam Prof. Dr. Mehmet YILDIRIM'a teşekkür ederim. Hocamın örnek kişiliği ile bana kazandırdığı akademik bakış açısı ve gayretle ile ilerleyebilmeyi diliyorum.

Ayrıca, çalışmam sırasında fikirleri ile bana yol gösteren, beni destekleyen hocalarım Doç. Dr. Serdar SOLAK ve Dr. Öğr. Üyesi Adnan SONDAŞ'a, desteği için oda arkadaşım Arş. Gör. Seda BALTA KAÇ'a ve diğer değerli çalışma arkadaşlarıma teşekkür ederim.

Son olarak, beni bugünlere getiren sevgili aileme ve lisans, yüksek lisans eğitimim boyunca hiçbir desteğini esirgemeyen Ozan Utku ARTUK'a, tüm destekleri ve gösterdikleri sabır için teşekkürü bir borç bilirim. Bu yolculukta yalnız olmadığımı biliyor ve emeği geçen herkese teşekkürlerimi sunuyorum.

Mayıs – 2022 Zeynep SARI

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

TABLOLAR DİZİNİ

SİMGELER VE KISALTMALAR DİZİNİ

bpp : Bits Per Pixel (Piksel Başına Bit)
dB : Decibel (Desibel)

Kısaltmalar

ASCII : American Standard Code for Information Interchange (Bilgi Değişimi için Amerikan Standart Kodlama Sistemi)
BER : Bit Error Rate (Bit Hata Oranı)
BDH : Block Data Hiding (Blok Veri Gizleme)
BMP : Bitmap
CMYK : Cyan Magenta Yellow Key (Cam Göbeği, Mor, Sarı, Siyah)
DCT : Discrete Cosine Transform (Ayrık Kosinüs Dönüşümü)
DWT : Discrete Wavelet Transform (Ayrık Dalgacık Dönüşümü)
HVS : Human Visual System (İnsan Görsel Sistemi)
JPEG : Joint Photographic Experts Group (Sayısal Görüntü Kodlama Biçimi)
LCG : Linear Congruential Generator (Doğrusal Eşgüdümlü Üreteç)
LSB : Least Significant Bit (En Düşük Değerlikli Bit)
MSB : Most Significant Bit (En Yüksek Değerlikli Bit)
MSE : Mean Squared Error (Ortalama Hata Karesi)
OPAP : Optimal Pixel Adjustment Process (Optimal Piksel Ayarlama Süreci)
PNG : Portable Network Graphics (Taşınabilir Ağ Grafikleri)
PSNR : Peak Sinyal-to-Noise Ratio (Tepe Sinyal Gürültü Oranı)
RGB : Red, Green, Blue (Kırmızı, Yeşil, Mavi)
RMSE : Root Mean Square Error (Kök Ortalama Kare Hatası)
RS : Regular Singular (Düzenli, Tekil)
SSIM : Structural Similarity Index Measure (Yapısal Benzerlik Oranı)
TIFF : Tag Interchange File Format (Etiket Değişim Dosya Biçimi)

UZAMSAL ALANDA GENETİK ALGORİTMALAR İLE STEGANOGRAFİ TEKNİKLERİ

ÖZET

Haberleşme türlerinin tamamında, özellikle gizli veri haberleşmelerinde, verinin güvenliği önemli bir konudur. Verinin güvenliğini sağlamak için verinin şifrelenmesi, yani kriptoloji klasik yöntemlerden biridir. Verinin şifrelenmesi, veri içeriğinin gizli kalmasını korusa da verinin varlığı gizli olmadığı için istenmeyen kişilerce gözlenebilir veya zarar görebilir. Steganografi verinin varlığının da gizlenmesini sağlayan bilim dalıdır.

Steganografik çalışmalar, verinin varlığını gizlemek için taşıyıcı veya kapak adı verilen medyaları kullanmaktadır. Taşıyıcı medya; video, ses, görüntü veya program dosyaları olabilir. Taşıyıcı medyaya veri gizlenmesi ile elde edilen medyaya stego medya adı verilmektedir. Uzamsal alan görüntü steganografisinde taşıyıcı medya dijital görüntü dosyalarıdır. Veri gizleme işlemleri taşıyıcı görüntünün doğrudan piksel değerlerine yapılmaktadır. Birçok araştırmacı bu alanda teknikler geliştirmiş, teknikler önermişlerdir.

Bu tez çalışmasında, uzamsal alan görüntü steganografisinde kullanılan en az anlamlı bit yer değiştirme tekniğine dayalı yeni bir steganografi tekniği geliştirilmiştir. Önerilen teknik verinin güvenli iletimi için, literatürde de yer alan taşıyıcı görüntünün bloklara ayrılması ve kanal seçimi tekniklerini kullanmaktadır. Steganografinin önemli ve temel ölçütlerinden biri olan verinin güvenliği, blok veri içerisinde genetik algoritma ile kanal seçimi yaparak artırılmaya çalışılmış ve verinin güvenliği genetik algoritmanın ürettiği anahtarla sağlanmıştır. Uygulamada, sabit boyutlu gri ölçekli taşıyıcı görüntüye farklı kapasitede veri gizlemek için, beş farklı boyutta gri ölçekli görüntü dosyaları gizli veri olarak kullanılmıştır. Klasik en az anlamlı bit tekniğindeki taşıyıcı görüntü piksellerinin sırayla seçilmesi yerine, bu seçimi genetik algoritma ile yaparak, verinin anahtar olmadan kolayca geri çıkarılmasının önüne geçilmiştir. Uygulama sonucunda, literatürdeki tekniklere kıyasla hem gizli verinin güvenliğinin artırılabildiği hem de taşıyıcı görüntüdeki bozulma azaltılarak verinin varlığının daha iyi gizlenebildiği gözlemlenmiştir.

Anahtar Kelimeler: Blok Veri Gizleme, Genetik Algoritma, Görüntü Steganografisi, Kanal Seçimi, LSB Veri Gizleme.

GENETIC ALGORITHMS AND STEGANOGRAPHY TECHNIQUES IN THE SPATIAL DOMAIN

ABSTRACT

Data security is an important issue in all types of communication, especially in confidential data communications. Encryption of data, that is, cryptology, is one of the classical methods to ensure the security of data. Encryption of data keeps the data content confidential, but since the existence of the data is not confidential, it can be observed or damaged by undesired persons. Steganography is the science that allows the existence of data to be hidden.

Steganographic studies use media called carriers or covers to hide the existence of data. Carrier media; can be video, audio, image, or program files. The media obtained by hiding data to the carrier media is called stego media. In spatial domain image steganography, the carrier media is digital image files. Data hiding operations are performed directly on the pixel values of the carrier image. Many researchers have developed techniques in this field and suggested techniques.

In this thesis, a new steganography technique was developed based on the least significant bit displacement technique used in spatial domain image steganography. The proposed technique uses the techniques of separating the carrier image into blocks and channel selection, which are also available in the literature, for the secure transmission of data. The security of the data, which is one of the important and basic criteria of steganography, has been tried to be increased by selecting the channel with the genetic algorithm in the block data and the security of the data has been ensured by the key generated by the genetic algorithm. In practice, grayscale image files of five different sizes were used as confidential data in order to hide data of different capacities on a fixed-size grayscale carrier image. Instead of sequentially selecting the carrier image pixels in the classical least significant bit technique, this selection is made with a genetic algorithm, preventing the data from being easily retrieved without a key. As a result of the application, it has been observed that both the security of confidential data can be increased compared to the techniques in the literature and the presence of the data can be better hidden by reducing the deterioration in the carrier image.

Keywords: Block Data Hiding, Genetic Algortihm, Image Steganography, Channel Selection, LSB Data Hiding.

1. GİRİŞ

Hayatın her alanında aktif bir rol almasında ve İnternet kullanımının herkesin ulaşabileceği bir noktaya gelmesinde teknolojinin hızlı gelişiminin rolü büyüktür. Hemen hemen tüm verilerin İnternet üzerinden aktarımının sağlandığı günümüzde, İnternetin en çok kullanılan iletişim aracı olduğundan söz edilebilmektedir. Bu artan teknoloji kullanımıyla beraber, aktarılan verinin güvenliğinin sağlanması da son yılların en önemli problemlerinden biri olmuştur. Bu problemin çözümünde de çeşitli güvenlik yöntemlerinin ve savunma stratejilerinin geliştirildiği görülmektedir.

Tarih boyunca, bilgi her zaman gücün dengi olmuştur. Yazının keşfinden bu yana bilginin çoğaltılabilir, aktarılabilir duruma gelmesi ve aynı şekilde günümüzde bilginin sayısallaştırılabilmesi, sayısallaştırılmış verinin üzerinde işlem yapılabilmesi gibi faktörler, veri aktarımının güvenliğinin de ne kadar önemli olduğunu göstermektedir.

Teknolojinin geldiği bu noktada, iki kişi birbirleriyle haberleşirken üçüncü bir kişi bu iletişime dahil olabilmekte ve veride değişiklik yapabilmektedir. Bu durumun önüne geçilebilmesi adına çeşitli güvenlik sistemlerinin geliştirildiği görülmektedir. Bu sistemlerden biri de çok eski zamanlardan beri kullanılan bir yöntem olan verinin şifrelenmesi, yani kriptoloji bilim dalıdır. Bu yöntemle haberleşmede, iletilecek veri şifreleme algoritmaları ile şifrelenerek iletilir ve alıcı bir anahtar yardımı ile şifreleri çözerek veriyi alır. Ancak, zaman geçtikçe şifrelerin kırılabilmesi sadece şifreleme ile veri güvenliğinin sağlanamayacağını göstermektedir. Bu nedenle, verinin varlığının da gizlenmesi önem arz etmektedir. Verinin varlığını gizleyen bilim dalına da steganografi adı verilmektedir.

İletişimde veri güvenliğinin amacı, iletimin istenmeyen kişilerce fark edilmesini engellemektir. Kriptolojide verinin varlığı açıktır, veri görünür ancak şifrelidir. Verinin iletimi esnasında istenmeyen kişilerce veriye zarar verilebilir. Steganografi, verinin varlığını gizleyerek güvenliği arttırır. Teknolojinin gelişmesi ile birlikte, veri gizleme yöntemleri de gelişmekte ve gelişmeye devam etmektedir.

Steganografide temel fikir gizli verileri bir taşıyıcı medya içerisine tespit edilemeyecek şekilde gizleyebilmektir. İkilik tabanda “0” ve “1” formatındaki gizli veri seçilen bir

algoritmaya göre taşıyıcı medya içerisine yerleştirilir. Aynı şekilde, veri gizleme algoritması içerisinde sadece gönderici ve alıcının bileceği bir anahtar değerine göre gizleme tekniği uygulanabilmektedir. Üretilen anahtar değer, yine taşıyıcı medyaya eklenerek alıcı tarafa ulaştırabilmektedir. Genellikle, bu veri gizleme algoritmaları matematiksel yöntemler kullanılarak gerçekleştirilebilmektedir

İkinci Dünya Savaşı sırasında İngiliz matematikçi Alan Turing'in Alman şifrelerini kırmasıyla birlikte, steganografi üzerine çalışmaların arttığı söylenebilir. Birçok araştırmacı resim, ses ve metin dosyaları içerisine veri gizleme teknikleri üzerine çalışarak bu alanda bilime katkıda bulunmuştur (Bender ve diğ., 1996).

Steganaliz bilimi de steganografi çalışmalarının hız kazanmasıyla paralel olarak gelişmiştir. Steganaliz bilimi, içerisine veri gizlenmiş resim, ses, video vb. dosyalarındaki verinin varlığını tespit etmeyi amaçlamaktadır. Steganalizin temelinde, yapılan her veri gizleme işleminin taşıyıcı medya üzerinde bir iz bıraktığı düşüncesi bulunmaktadır. Steganaliz teknikleri bu izleri tespit ederek verinin varlığını ortaya çıkarmaya çalışmaktadır (Hassan, 2008).

Bu tez çalışmasında, veri alıcı tarafına ulaştığında, üçüncü şahıslardan ziyade mesajı sadece alıcının alabilmesi için, taşıyıcı görüntülerde verinin hangi piksellere gizleneceğini belirleyen bir teknik geliştirilmiştir. Genetik algoritma ile taşıyıcı kanal seçimi yapılarak, seçilen kanallara veri gizlenmiştir.

Çalışma dört bölümden oluşmaktadır. Birinci bölümde, veri gizleme tekniklerinden genel olarak bahsedilirken, alt başlıklarda veri gizleme türlerine yer verilmekte ve steganografinin tarihsel gelişiminden ve temel kavramlarından bahsedilmektedir.

İkinci bölümde, genetik algoritmalar açıklanmakta, uygulama alanları ve genetik algoritmalarda kullanılan doğal seçilim, çaprazlama ve mutasyon operatörlerine yer verilmekte, genetik algoritmaların çözüm kalitesini ve hızını etkileyen parametrelere değinilmektedir.

Üçüncü bölümde, tez çalışması kapsamında geliştirilen genetik algoritma ile görüntü steganografisi tekniği yer almaktadır. Blok veri gizleme ve kanal seçimi tekniklerinin genetik algoritma ile nasıl gerçekleştirilebileceği açıklanmaktadır. Genetik algoritma

operatörlerinde yapılması gereken uyarlamalara yer verilmektedir. Genetik algoritmada kanal seçimi problemine özgü geliştirilen bir amaç fonksiyonu anlatılmaktadır.

Dördüncü bölümde, referans taşıyıcı resimler üzerinde veri gizleme ve veri çıkarma uygulamaları yapılmış, yapılan uygulamaların sonuçları irdelenmekte, elde edilen sonuçlar literatürde yer alan çalışmaların sonuçları ile karşılaştırılmaktadır.

Sonuç ve öneriler bölümünde, tez çalışması kapsamında elde edilen bulgular ve sonraki çalışmalara ışık tutacak önerilere yer verilmektedir.

2. VERİ GİZLEME TEKNİKLERİ

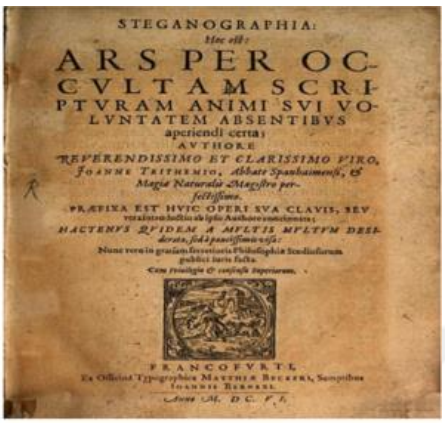
2.1. Steganografinin Tarihçesi

Eski Yunancada "gizlenmiş yazı" anlamına gelen steganografi mesajı başka bir mesajın, fiziksel bir objenin veya dijital dünyada bir görüntü, ses, video veya program dosyasının içerisine yerleştirerek verinin varlığını gizleme sanatıdır. Tarihte, bir kaktüs bitkisi sütünün gizli yazı yazmak için kullanılmasının keşfi, steganografi biliminin ilk örneklerinden biri olduğu düşünülmektedir (Raggo ve Hosmer, 2013). Bu keşif aynı zamanda, I. Dünya Savaşı'nda görünmez mürekkep kullanımına da ilham olmuştur. Yunan tarihçi Herodot tarafından belgelenen dokümanlarda, eski gizli mesajlaşma örneklerinden biri de mesajın tahta bir yüzeye yazıldıktan sonra balmumu ile kaplanmasıdır. Balmumu eritildiğinde mesaj ortaya çıkmaktadır. Bununla beraber, steganografi teriminin ilk defa modern kriptografinin kurucusu kabul edilen Johannes Trithemius (1462-1516) tarafından "Steganographia" adlı kitabı ile kullanıldığı bilinmektedir. Şekil 2.1.'de Trithemius'un kitabının kapağı, Şekil 2.2.'de ise Dr. John Dee tarafından (1591) Trithemuis'un kitabından kopyalanmış bir tablosu bulunmaktadır. Alman bilim insanı ve matematikçi Gaspar Schott (1608-1666), "Schola Steganographica" isimli kitabında, kendi icat ettiği harf ve sayılardan oluşan dört kriptografi durumu anlatmaktadır. Ayrıca, kitabında gizli verileri iletmek için müzik notalarının kullanımından bahsetmektedir (Şahin, 2007).

Yakın geçmişte ise verinin gizlenmesi bir başka deyişle steganografinin bilimsel açıdan ilk olarak 1983 yılında Gustavus J. Simmons tarafından "The Prisoner's Problem and The Subliminal Channel" isimli makalesinde, bir mahkumun gizli mesaj örneği ile anlatılmaktadır (Subhedar, 2014). İlgili çalışma, aynı cezaevinde bulunan Alice ve Bob isimli iki mahkumun kaçış planlarını, gardiyan aracılığı ile birbirlerine ilettiğini ve bu planı gardiyana fark ettirmeden nasıl yaptıklarını konu almaktadır.

II. Dünya Savaşı sırasında geliştirilen "mikro noktalar" mikro film teknolojisi ile verinin varlığı gizlenmiştir. Yine aynı prensip ile, Birleşik Devletler deniz piyadelerinin kullandığı teknik "kod konuşucuları (ing: codetalkers)" basit bir şifreleme ile verilerin varlığını gizleyerek, verinin düz metin şeklinde alıcıya ulaşmasını sağlamıştır (Siper ve diğ., 2005).

Nokta ve mikro nokta kullanımı da bir başka steganografi örneğidir. İngilizler, Yunanlıların aksine sıradan metinler yerine, gazetelerde mürekkep sıçraması gibi görünen noktalarla, gizli verileri mors ve posta kodlarıyla kodlayarak kullanmışlardır (Amirtharajan ve Rayappan, 2013).


STEGANOGRAPHIA:
ARS PER OC-
CVLTAM SCRI-
PTVRAM ANIMI SVI VO-
LVNTATEM ABSENTIBVS
aperiendi certa;
AVTHORE
REVERENDISSIMO ET CLARISSIMO VIRO,
IOANNE TRITHEMIO, Abbate Spanheimensi, &
Magiæ Naturalis Magistro per-
fectissimo.
PRÆFIXA EST HVIC OPERI SVA CLAVIS, SEV
HACTENVS QVIDEM A MVLTIS MVLTVM DESI-
FRANCOFVRTI,
Ex Officina Typographica MATTHIÆ BECKERI, Sumptibus
IOANNIS BERNERI.

Şekil 2.1. Johannes Trithemuis'un "Steganographia" isimli kitabı

Şekil 2.2. Dr. John Dee tarafından Trithemuis'un kitabından kopyalanmış tablo

Günümüzde de steganografi kullanımı popülerliğini sürdürmektedir. Bunun en önemli unsurlarından biri veri iletiminin daha çok dijital olarak İnternet ortamında gerçekleşmesidir. Son yıllarda, gelişen teknoloji ile İnternette veri aktarımının hız kazandığı görülmektedir. Bu da beraberinde önemli bir güvenlik sorununu meydana getirmektedir. Paylaşılan verilerin istenmeyen kişiler veya aracılar tarafından ele geçirilmemesi için çeşitli yöntemler geliştirilmektedir. Genellikle, verinin güvenliği verinin şifrelenmesi ile sağlanır. Verinin şifrelenmesi yani kriptoloji bunun en bilindik yöntemlerindendir. Bu nedenle kriptoloji ve steganografi tanımları çoğunlukla karıştırılmaktadır. Kriptoloji yöntemlerinde gizli veri, gözlemci tarafından görülebilen

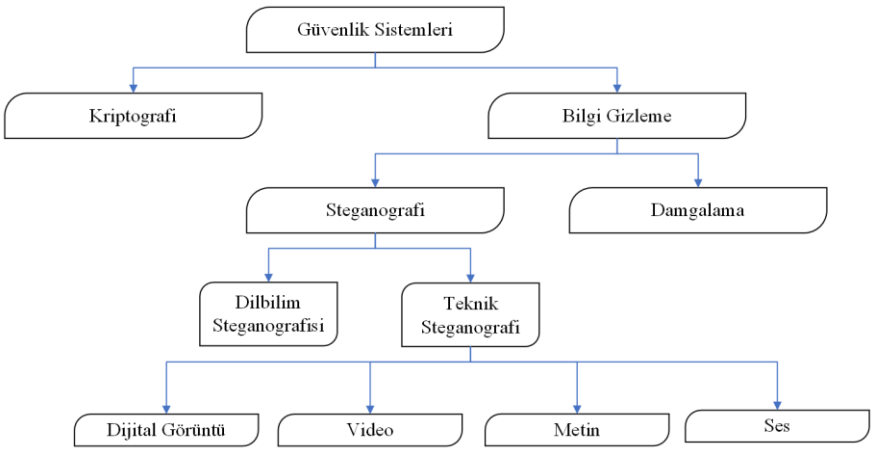
fakat şifre çözme teknikleri kullanılmadan anlaşılamayan veriyi ifade etmektedir. Çünkü, kriptoloji verinin varlığını gizlemez, verinin içeriğini net göremeseler bile, üçüncü kişiler verinin varlığını tespit edebilmektedir. Oysaki, verinin bozulmadan göndericiden alıcıya ulaşabilmesi için varlığının da gizlenmiş olması gerekmektedir. Steganografi doğrudan görülemeyen, gözlemci tarafından fark edilemeyen örtülü yazı olarak da bilinen bilim dalıdır (Raggo ve Hosmer, 2013). Bu sebeple steganografi ve kriptoloji birbirleri ile yakın ilişkili iki bilim dalıdır. Kriptoloji mesajın kendisini şifrelerken, steganografi mesajın varlığını gizlemeyi amaçlamaktadır.

Steganografinin en temel amacının algılanamazlık ilkesinin korunması olduğu bilinmektedir. Zaker ve Hamzeh (2012), çalışmasında veri gizlemenin üç temel gereksinimi olan; algılanamazlık, sağlamlık ve kapasitenin bir üçgenle tanımlanabildiğinden bahsetmiştir. Şekil 2.3.'deki steganografi üçgeninde yer alan gereksinimler arasında, yapılan çalışmaların hedefine göre, her zaman bir denge olduğu görülmektedir. Genel olarak, araştırmacılar üçgenin tepesinde yer alan algılanamazlık ilkesini korumayı hedeflemektedir. Kapasite ile algılanamazlık arasında ters orantı bulunduğu için, veri gizleme yöntemleri geliştirilirken, algılanamazlık ilkesinin korunması öncelikle hedeflenir ve veri gizleme kapasitesi arttırılmaya çalışılmaktadır. Aynı şekilde, saldırılara karşı dayanıklılığın korunması temel unsur olarak karşımıza çıkmaktadır. Sağlamlık veya güvenlik, veri gizleme algoritmasının yani içerisine veri gizlenmiş taşıyıcı medyanın kırpma, döndürme ve ölçeklendirme gibi çeşitli görüntü işleme yöntemlerine maruz kalmasına rağmen dayanıklı olmasını ve gizli verinin bu tekniklerden sonra zarar görmeden sağlam kalma yeteneğini ifade etmektedir. Fridrich ve diğ. (2000, 2002, 2008) yaptığı çalışmalarda, verinin varlığını açığa çıkarma teknikleri olan steganaliz yöntemlerinden ayrıntılı olarak bahsetmektedir.

Şekil 2.3. Veri gizlemede steganografi üçgeni (Zaker ve Hamzeh, 2012)

2.2. Steganografinin Türleri

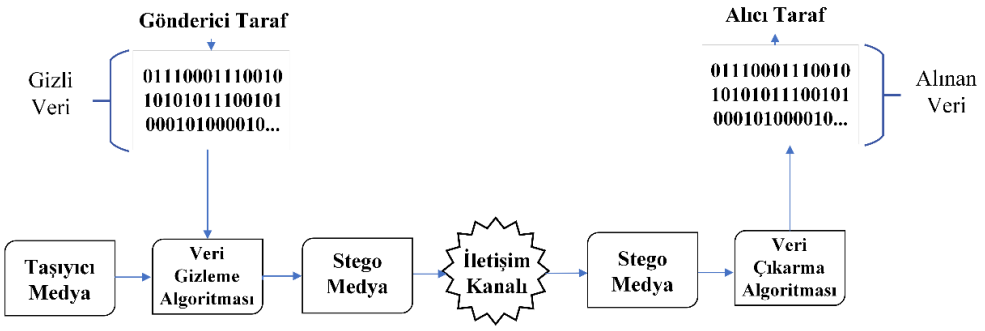
Bilgi gizleme; steganografi ve damgalama olmak üzere iki alt alandan oluşmaktadır. İki alan da mesajı istenmeyen kişilerden korumak için kullanılmaktadır. Damgalama daha çok verinin güvenliğini sağlamak için gizli mesajın bozulmasını veya çıkarılmasını zorlaştırmaktadır. Parmak izi okuyucular örnek uygulama olarak verilebilir.



Şekil 2.4. Bilgi gizleme teknikleri (Cheddad ve diğ., 2010)

Steganografi ise Şekil 2.4.'deki şemada olduğu gibi, kendi içerisinde dilbilim steganografisi ve teknik steganografi olarak alt başlıklara ayrılmaktadır. Dilbilim steganografisinde taşıyıcı metin dosyasıdır (text). Teknik steganografide ise taşıyıcı medya daha geniş bir alana sahiptir; bilgisayar (yazılım, donanım) tabanlı teknikler, görünmez mürekkep, programlama dosyaları.

Steganografi tekniklerinin arkasındaki temel fikir, gizli verileri bir taşıyıcı medya içerisine tespit edilemeyecek şekilde gizleyebilmektir. Şekil 2.5.'deki diyagramda görüldüğü gibi, gizlenecek veriye dair medya formatı verilmemiştir. Gizli veri çalışmalarda kullanılan algoritmalara göre çeşitlilik gösterebilmektedir. İkilik tabanda "0" ve "1" formatındaki gizli veri seçilen bir algoritmaya göre taşıyıcı medya içerisine yerleştirilir. Aynı şekilde, veri gizleme algoritması içerisinde sadece gönderici ve alıcının bileceği bir anahtar değerine göre gizleme tekniği uygulanabilmektedir. Üretilen anahtar değer, yine taşıyıcı medyaya eklenerek alıcı tarafa ulaştırabilmektedir. Genellikle, bu veri gizleme algoritmaları matematiksel yöntemler kullanılarak gerçekleştirilebilmektedir (Kadhim ve diğ., 2019).



Şekil 2.5. Steganografi veri gizleme ve çıkarma diyagramı

2.3. Görüntü Steganografisi

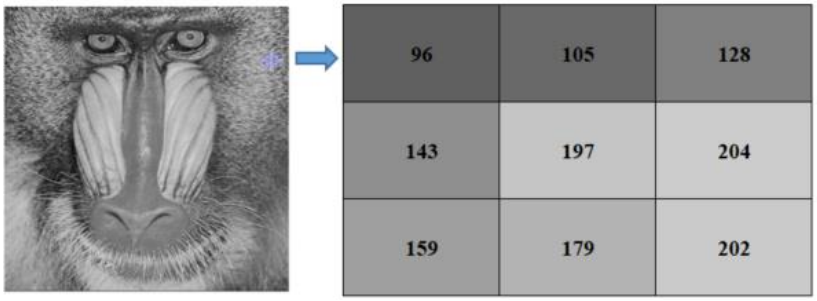
Kapak (ing: cover) veya taşıyıcı medya, gizlenecek verinin bitlerini taşımak için kullanılan medya türüne denilmektedir. İçerisine bilgi gizlenmiş olan taşıyıcı medya bir görüntü ise buna stego görüntü, gizlenmiş veriye de yük adı verilmektedir. Kapasite, taşıyıcı görüntüyü deforme etmeden içerisinde saklanacak veri boyutunu ifade eder ve bpp (ing: bits per pixel) ile temsil edilir (Cheddad ve diğ., 2010).

Taşıyıcı medyanın görüntü olduğu steganografi türü görüntü steganografisidir. Dijital görüntüler N satır ve M sütun ile temsil edilen iki boyutlu dizilerdir. Pikseller de bu iki boyutlu dizinin elemanlarını oluşturan değerlerdir. Renkli görüntü dosyaları RGB (ing: red, green, blue) yani kırmızı-yeşil-mavi renk kanallarına sahiptirler ve çoğunlukla 24 bit ile ifade edilen görüntülerdir. Gri ölçekli görüntüler de tek renk kanalına sahiptirler ve 8 bit ile ifade edilmektedir. Şekil 2.6.'da gri ölçekli görüntü ve görüntünün piksel matrisi Şekil 2.7.'de renkli görüntü ve görüntünün piksel matrisi gösterilmektedir.

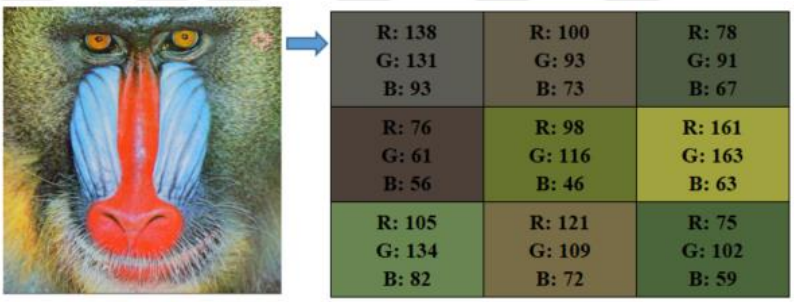
Veri gizleme tekniklerinde taşıyıcı medya seçimi için iki özellik bulunmaktadır; taşıyıcı medya türünün popüler olması ve taşıyıcıdaki değişiklerin gönderici ve alıcı harici kişiler tarafından fark edilememesi gerekmektedir (Hussain ve diğ., 2018). Dijital görüntülerin iletişim kanalı üzerinde iletiminin kolaylığı, yaygın kullanılan medya formatı olması ve kullanım sıklığı gibi faktörler onu steganografi teknikleri için güncel medya haline getirmektedir.

Taşıyıcı görüntü dosyasının içerisine gizli veri olarak metin dosyası ve görüntü dosyası gizlenmesi yine en sık kullanılan çalışmalardandır. Gizli veri bir metin dosyası olduğunda her karakter ASCII kod karşılıkları ile sayısallaştırılır. Sayısallaştırma sonrasında elde

edilen kodun ikilik tabandaki karşılığı taşıyıcı görüntünün piksellerine gizlenmektedir. Gizli veri bir görüntü dosyası olduğunda, görüntüdeki her pikselin sayısal değeri ondalık tabandan ikilik tabandaki karşılığına dönüştürülür ve her bir bit, taşıyıcı görüntünün piksellerine tek tek gizlenmektedir.



Şekil 2.6. Dijital görüntü ve piksel değerleri



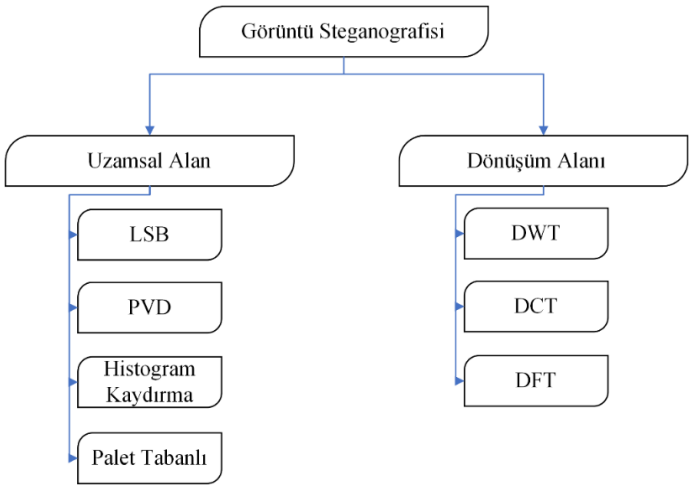
Şekil 2.7. Dijital renkli ölçekli görüntü ve piksel değerleri

2.4. Görüntü Steganografisinin Türleri

Görüntü steganografi teknikleri veri gizleme metotlarına göre iki ayrı alana ayrılmaktadır; uzamsal alan teknikleri ve dönüşüm alanı teknikleri. Uzamsal alan tekniklerinde veri gizlenirken taşıyıcı görüntünün doğrudan pikselleri kullanılır. Gizlenecek verinin bitleri, Şekil 2.8.'de verildiği gibi, çeşitli tekniklerle taşıyıcı görüntünün piksellerine gizlenmektedir.

Dönüşüm alanı tekniklerinde, doğrudan taşıyıcı görüntünün pikselleri kullanılmaz. Öncelikle, ayrık kosinüs veya ayrık dalgacık dönüşümü gibi dönüşümler kullanılarak, taşıyıcı görüntünün frekans katsayıları elde edilmektedir. Gizli verinin bitleri elde edilen bu frekans katsayılarına gizlenir ve gizleme işlemi tamamlandıktan sonra ters dönüşümler

ile stego görüntü yeniden uzamsal alana çevrilmektedir. Dönüşüm alanı tekniklerinde genellikle JPEG görüntü dosyaları üzerinde çalışılmaktadır (Çataltaş, 2018).



Şekil 2.8. Görüntü steganografisi teknikleri (Kadhim ve diğ., 2019)

Kayıplı (ing: lossy) sıkıştırma, dosya verilerini geri alınamaz şekilde azaltabilir ve sıkıştırma işleminden sonra kaybolan veri geri kurtarılamaz. Çoğunlukla kaybolan veri kullanıcının fark edeceği ölçüde değildir.

Kayıpsız sıkıştırma, sıkıştırma işleminden sonra dosyada tutulan veriyi ifade etmektedir. Sıkıştırma öncesi ve sonrasında veriler bozulmadan ve erişilebilir olarak kalmaktadır.

Raster dosyalar, piksel tabanlı görüntü dosyalarını ifade etmek için kullanılmaktadır. Bu dosyalar aynı zamanda bitmap dosyalar olarak da bilinirler.

Jpeg ya da jpg dosya biçimi raster düzenleme olanağına sahip, kayıplı sıkıştırma dosya biçimidir. Web sayfalarında, sosyal medyada, elektronik mail iletimlerinde kullanımı kolay ve pratiktir. Neredeyse tüm cihazların ve tarayıcıların desteklemesi, renk paletinin geniş olması jpeg dosya formatının en sık kullanılan format olmasını sağlamaktadır. Katmanlı dosya yapısı veya saydamlık gerekiyorsa, bu dosya formatı kullanımından kaçınılmalıdır.

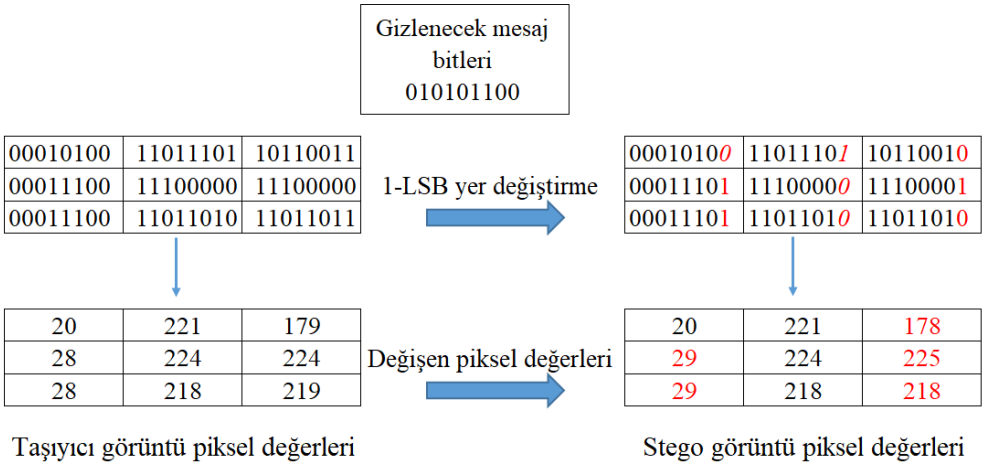
Tiff dosya biçimi kayıpsız sıkıştırmayı destekleyen tarama dosyası türüdür. Jpeg uzantılı dosyalardan daha fazla yer tutarlar. İnternet ortamında sıklıkla kullanılan bu dosya formatı, saydam arka plan, ek düzenleme araçlarına gereksinim duymadan diğer dosya türlerine gömülmede kullanılabilirler.

Yüksek görüntü kalitesine sahip, kayıpsız sıkıştırma dosya biçimidir. Tiff dosyaları CMYK ve RGB renklerini destekledikleri için matbaa basımları için sık kullanılırlar.

2.4.1. En Az Anlamlı Bit Steganografisi

En az anlamlı bit (ing: least significant bit - LSB) steganografisi literatürde en sık kullanılan yöntemlerden biridir. Çeşitli veri gizleme algoritmalarıyla uyumlu çalışabilmesi, taşıyıcı görüntüde çok az değişikliğe neden olması, uygulama tekniğinin basit olması sık kullanılmasının başlıca nedenlerindendir. *n*-LSB yer değiştirme tekniğinde "*n*", taşıyıcı görüntüdeki her bir pikselde değişen bit sayısıdır. Şekil 2.9.'da, 1-LSB yer değiştirme yöntemi ile ilgili temel bir örnek verilmektedir. LSB yer değiştirme tekniğinde, 8 bit ile ifade edilen taşıyıcı görüntünün her bir pikselindeki 2^0 değerlikli biti (son bit), gizlenecek mesajın bir biti ile değiştirilmektedir. Bu işlem, sırasıyla gizli mesaj bitlerinin tamamı taşıyıcı görüntüye gizlenene kadar devam etmektedir.

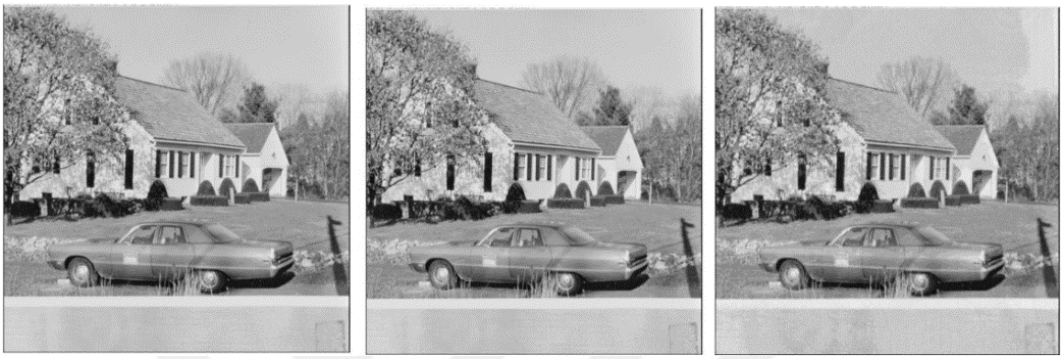
Gizli mesajın varlığının gizlenmesi, taşıyıcı görüntü ile stego görüntü arasında oluşacak farkları insan görsel sisteminin (HVS) yakalayamaması anlamına gelmektedir. LSB yer değiştirme tekniği en az anlamlı biti kullanırken, insan gözünün bu küçük değişiklikleri yakalamayacağı şekilde değişiklik yapmayı hedeflemektedir. Veri gizleme teknikleri için görüntüdeki kalite, stego görüntünün kalitesidir. Bu nedenle, veri gizleme tekniklerinde stego görüntünün kalitesinin yüksek tutulması hedeflenmektedir.



Şekil 2.9. 1-LSB yer değiştirme tekniği örnek

Taşıyıcı görüntünün sadece son bitlerinin değiştirilmesi sonucunda, taşıyıcı görüntü ile stego görüntü arasında fark oluşmamış gibi gözükmektedir. LSB'den MSB'ye doğru veri

gizlemede kullanılacak bitlerin sayısı arttıkça, yapılan değişikler gözle görülür hale gelmektedir. Şekil 2.10.'da görüldüğü gibi, taşıyıcı görüntü piksellerinin son 4 LSB bitlerinin değiştirilmesi sonucunda, stego görüntüde gözle görülür şekilde bozulmalar olduğu açıktır. Böyle bir durumda, herhangi bir steganaliz yapılmasına gerek kalmadan, stego görüntünün içerisinde veri olduğu ortadadır. Sadece son LSB bitlerin değiştirilmesiyle oluşan stego görüntü, taşıyıcı görüntüden farklı gözükmemektedir.



(a) (b) (c)

Şekil 2.10. (a) Taşıyıcı görüntü, (b) 1-LSB Stego görüntü, (c) 4-LSB Stego görüntü

LSB yer değiştirme algoritması, veri gizleme ve veriyi geri almada basit bir teknik olmakla birlikte, steganaliz saldırılına karşı savunmasız kalmaktadır. Ancak, LSB eşleştirmesi (±1 gizleme olarak da bilinir) tekniğinde, taşıyıcı görüntünün LSB değeri gizli veri değeri ile karşılaştırılır ve karşılaştırma sonucuna göre taşıyıcı görüntü pikseline bir eklenir veya çıkartılır (Li ve diğ., 2009).

Fridrich ve diğ. (2001) yaptıkları çalışmada, steganaliz saldırılarından bahsetmiş ve daha çok LSB tekniği ile veri gizlenmiş stego görüntülere uygulanan RS steganalizi ile istatiksel bir LSB yöntemi önermişlerdir. LSB tekniği kullanılarak yerleştirilen gizli verinin, taşıyıcı görüntüdeki değişlikleri temel alarak, neden olduğu ters çevrilmiş pikselleri tahmin etmişlerdir. Yöntemlerini stego görüntüye yapılacak saldırılara karşı güçlendirmişlerdir.

Chan ve Cheng (2004) yaptıkları çalışmada, klasik LSB yer değiştirme algoritması kullanarak elde ettikleri stego görüntüye OPAP algoritmasını uygulamışlardır. OPAP algoritmasıyla, stego görüntünün görüntü kalitesini iyileştirmeyi hedeflemişlerdir.

Çalışmalarında gri renkli taşıyıcı görüntü içine gizli mesaj olarak gri renkli görüntü gizlenmiştir.

Sutaone ve Khandare (2008) çalışmalarında, taşıyıcı görüntü içerisine metin gizlemişlerdir. Klasik LSB yer değiştirme tekniğinde güvenlik sağlamak için, rastgele seçilen piksellerin LSB değerine gizli veriyi gizlemişler, bunun için anahtar kullanmışlardır. Ancak, çalışmalarında veri gizleme kapasitesi düşük tutulmuştur.

Chen (2011) yaptığı çalışmada, modül tabanlı bir LSB yer değiştirme tekniği kullanmıştır. Ayrıca, çalışmasında veri sıkıştırma tekniği de uygulamıştır. Önerilen teknikte, iki farklı 512x512 boyutlarında gri taşıyıcı görüntü içerisine, yedi farklı 256x512 boyutlarında gri görüntü gizlenmiştir. Çalışma sonuçlarını klasik LSB yer değiştirme tekniği, Chang ve diğ.(2003) ve Thien ve Lin'in (2003) uyguladıkları teknikler ile karşılaştırmıştır. Önerdiği yöntemin, karşılaştırma sonuçlarına göre daha yüksek PSNR (ing: peak signal to noise ratio) değeri elde ettiğini belirtmiştir.

Sabeti ve diğ. (2013) çalışmalarında, komşuluk tabanlı karmaşık bir LSB eşleştirmesi önermiştir. Önerdikleri algoritma, veri gizlemek için seçilecek pikselin karmaşık bir dokuya sahip olması için, piksel ve sekiz komşusu arasındaki farkların toplamını dikkat alan bir algoritmadır. Algoritmanın ürettiği sonucu belirli bir eşik değeri ile karşılaştırıp, eğer koşulu sağlıyor ise o piksele veri gizleme tekniğini uygulamıştır. Klasik LSB tekniklerine göre kendi çalışmalarının PSNR değerinin daha yüksek olduğunu belirtmişlerdir.

Rajendran ve Doraipandian (2017) çalışmalarında, bir boyutlu bir lojistik harita kullanarak kaotik dizi yaratmışlardır. Oluşturdukları kaotik diziye göre, taşıyıcı görüntü içerisine gizli mesaj olarak farklı bir görüntü gizlemişlerdir. Çalışmalarını, Bedi ve diğ.'nin (2012) PSO ile yaptıkları çalışmayla, Khodaei ve Faez'in (2010) genetik algoritmayla LSB yer değiştirme tekniğiyle ve klasik LSB tekniğiyle karşılaştırmışlardır. Çalışmalarında veri gizleme kapasitesini düşük tutmuşlardır, ancak önerdikleri yöntemin PSNR değerlerinin daha yüksek olduğunu belirtmişlerdir.

Yukarıda da bahsi geçen steganografik teknikler incelendiğinde, steganaliz saldırılarına karşı etkin iki yöntemin önerildiği görülmektedir (Fridrich ve Soukal, 2006; Chen ve diğ.,

2010 çalışmaları). Bu yöntemler, taşıyıcı görüntünün bloklara ayrılması ve gizli verinin taşıyıcı görüntüde hangi piksele gizleneceğini belirleyen kanal seçimidir.

2.4.2. Blok Veri Gizleme

LSB algoritmasında, taşıyıcı görüntü pikselleri satır satır ve her satır içinde soldan sağa doğru taranmaktadır. Bu, ilk satırdan son satıra kadar devam eden klasik bir yöntemdir. Piksel tarama sırasına, raster sırası da denilmektedir (Kanan ve Nazeri, 2014). Bu işlem, LSB teknikleri ile üretilen stego görüntüden veri çıkarmanın kolay olmasına, ancak verinin de korumasız kalmasına neden olmaktadır.

Blok veri gizleme (ing: blok data hiding – BDH) algoritması matris temelli bir yaklaşım olup, taşıyıcı görüntünün belirli boyutta bloklara bölünmesi ile kullanılmaktadır. Görüntünün matris olarak ele alınması, bloklara ayrılması ve blokların hücre olarak ele alınması ilk olarak Crandall (1998) tarafından ortaya konulmuştur. Westfeld (2001) çalışmasında, Crandall tarafından önerilen algoritmaya kendi algoritması olan F5 algoritmasını dahil ederek ilk uygulama örneklerinden birini oluşturmuştur (Westfeld, 2001).

Gizlenecek mesajın bir kısmı taşıyıcı görüntü bitlerinde değişikliğe neden olurken bir kısmı olmayabilir. Matris temelli algoritmalarda, taşıyıcı görüntüdeki pikselleri en verimli şekilde kullanabilme amacı bulunmaktadır. Bu nedenle, taşıyıcı görüntü bloklara ayrılarak, blok içerisinden en iyi pikseller seçilmeye çalışılmaktadır. Burada, taşıyıcı görüntünün bloklara bölünmesiyle matris tabanlı işlemler yapılması, veri gizleme sürecinde optimal alan yöntemini sağlamaktadır.

Birçok araştırmacı çalışmalarında blok boyutlarını farklı kullanmışlardır. Şekil 2.11.'de verilen matriste, Baboon görüntüsünden alınan ve piksel değerleri gösteren 8x8 bir blok bulunmaktadır. Şekilde, aynı görüntü içerisinden alınan 4x4 ve 3x3 bloklar da gösterilmektedir. Veri gizleme işleminde klasik LSB tekniğindeki gibi pikselleri sıralı seçmek yerine, taşıyıcı görüntüyü bloklarına ayırmak ve ayrılan bloklar içerisinden piksel seçimi yapmak daha güvenlidir.

145	56	49	89	137	90	62	33
116	101	40	67	90	54	65	46
77	114	46	46	98	60	60	47
71	136	95	48	83	120	53	47
87	122	132	50	76	87	74	50
82	76	159	61	72	96	44	46
43	51	134	130	70	122	53	62
33	51	111	153	87	119	48	59

(a)

145	56	49	89
116	101	40	67
77	114	46	46
71	136	95	48

145	56	49
116	101	40
77	114	46

(b)

Şekil 2.11. (a) Taşıyıcı görüntü, (b) Görüntünün 4x4v e 3x3 bloklara ayrılmış temsili

Hesaplama maliyetlerini azaltmak için kullanılan blok veri gizleme algoritması, matris çarpımları ve ek matrisler kullanmadan veri gizleme tekniği sunmaktadır (Nguyen ve diğ., 2016). Taşıyıcı görüntü içerisinden blok seçilerek geliştirilen veri gizleme algoritması o bloktaki piksellere uygulanabilmektedir.

BDH algoritması ile blok içerisinde yalnızca bir veya iki pikselin değiştiği uygulamalar, değiştirilmiş matris veri gizleme algoritmalarından daha fazla bozulmayı azaltabilmektedir. Taşıyıcı görüntü bloklara bölünerek, veri gizleme algoritması kanal seçimi ile birlikte de uygulanabilmektedir (Nguyen ve diğ., 2015). Bloklar içerisinde verinin hangi piksele veya piksellere gizleneceği bir algoritma ile seçilebilmektedir.

2.4.3. Kanal Seçimi

Veri gizleme algoritmalarında, verinin varlığını gizlemek için, steganaliz ataklarından koruyabilmek gerekmektedir. Bu nedenle, verinin hangi piksellere gizleneceğini belirlemek için kanal seçimi yapmak korunma yöntemlerinden biridir. Piksel seçiminde görüntünün karmaşık renk dokusuna sahip bölgesinin seçilmesi avantajlı olacaktır.

Kenar algılama, dijital bir görüntüde görüntü parlaklığının keskin değişimlerini ifade etmektedir. Kenar pikseller, seçilecek pikselin komşuları ile olan farkına bakılarak tespit edilebilmektedir. Görüntünün kenar piksellerini tespit etmek için birçok kenar algılama algoritması geliştirilmiştir. Sobel, Canny, Robert, Prewitt algoritmaları örnek olarak verilebilir (Kumar ve diğ., 2021). Matematiksel yöntemlerle tespit edilebildiği gibi görüntünün gradyan değeri ile de tespit edilebilmektedir.

Fridrich ve Soukal (2006) çalışmalarında, matris tabanlı veri gizleme ile veri gizleme kapasitesini arttırmanın yollarını aramışlardır. Gizli verileri matrise gömmek için rastgele lineer kod kullanarak gizleme verimliliğini arttırdıklarını belirtmişlerdir. Ayrıca, belirtilen yöntemlere ek olarak, matriste yerleştirme için simpleks kodları kullanmışlardır.

Nguyen ve diğ. (2015) yaptıkları çalışmada, blok veri gizleme algoritması ve kanal seçimi ile yeni bir yöntem önermişlerdir. Önerdikleri yöntemde, gizlenecek verinin boyutuna göre görüntüyü bloklara ayırmışlardır. Ayrılan bloklarda, veri gizlemek için seçilecek pikselin komşuları ile aralarındaki farka bakılmıştır. Pikselin dörtten az komşusu var ise, pikselin komşuları ile farkı büyük olan, dört komşuluğu var ise, komşuluk farkının dört sayısına oranlanması ile elde edilen değer dikkate alınmıştır. Çalışmalarında, bu gradyan değerlerini hesaplarken, fark işlemlerinde mutlak değer ile işlemler yapılmıştır. İki ayrı kat sayı değişkeni tanımlayarak, birinci kat sayı elde edilen gradyan değerinin üssü, ikinci katsayı da seçilen pikselin sayısal büyüklüğünün üs değeri üssü alınan gradyan değeri ile üssü alınan pikselin sayısal büyüklüğü birbirine oranlanarak verinin hangi piksele gizleneceği seçilmiştir. Çalışma test sonuçlarını Sabeti ve diğ.'nin (2013) yaptığı çalışma ile karşılaştırmışlar, PSNR sonuçlarının daha yüksek olduğunu belirtmişlerdir.

Sarı ve Yıldırım (2022) çalışmalarında, blok veri gizlemede kanal seçimi ile bir uygulama geliştirmişlerdir. Uygulamada, Şekil 2.12.'de verilen 512x512 boyutlarında taşıyıcı renkli görüntüler kullanılmış olup görüntülerin içerisine de metin dosyası gizlemişlerdir. Taşıyıcı görüntü 4x4 bloklara bölünmüş, her bloktan tek piksel seçilmiştir. Seçilen pikselin son bitine, son iki bitine ve son üç bitine veri gizlenmiştir. Kanal seçimi için iki yöntem kullanmışlardır. Yöntemlerden ilki, seçilen bloktaki piksellerin komşuluklarını hesaplayarak gradyan matrisi oluşturmaktır. Bloktaki maksimum gradyan değerine sahip piksel veri gizleme için seçilen pikseldir. İkinci yöntem ise, bloktaki maksimum piksel değerine sahip pikseli seçmektir. Her iki yöntemde de blokta birden fazla aynı değere sahip maksimum değer varsa ilk maksimum değer değerlendirmeye alınmıştır. İki yöntemde de PSNR değerlerinin birbirine yakın çıktığı belirtilmiştir.

(a) (b) (c)

Şekil 2.12. Taşıyıcı test görüntüleri

Yapılan çalışmada, renkli görüntülerin kırmızı kanalı veri gizleme kanalı olarak seçilmiştir. Tablo 2.1.'de çalışmanın sonuçları verilmiştir.

Tablo 2.1. PSNR, MSE, SSIM değerleri (Sarı ve Yıldırım, 2022).

Payload (bpp)	**Yöntem_1**				**Yöntem_2**				**Resim 512x512**
	PSNR	**SSIM**	**MSE**	**Gizleme Süresi (sn)**	**PSNR**	**SSIM**	**MSE**	**Gizleme Süresi (sn)**	
0.007	63.2475	0.9999	0.0313	0.101	63.2351	0.9999	0.0315	0.116	Baboon
0.015	56.9130	0.9996	0.1324	0.419	56.8668	0.9996	0.1318	0.440	
0.031	50.4573	0.9984	0.5853	0.411	50.4983	0.9984	0.5798	0.412	
0.007	63.1929	0.9998	0.0313	0.149	63.2297	0.9998	0.0311	0.111	Peppers
0.015	56.7597	0.9991	0.1371	0.504	56.7573	0.9991	0.1372	0.440	
0.031	50.4978	0.9964	0.5798	0.502	50.5367	0.9964	0.5747	0.408	
0.007	63.2046	0.9997	0.0313	0.106	63.2582	0.9997	0.0314	0.105	Female
0.015	56.8784	0.9986	0.1334	0.425	56.9472	0.9986	0.1313	0.476	
0.031	50.5212	0.9939	0.5767	0.422	50.4983	0.9938	0.5804	0.459	

Çalışmada taşıyıcı görüntü içerisine gizlenmiş veri yani kapasite (ing: payload) hesabı Denklem (2.1)'de verildiği gibi hesaplanmıştır. Gizlenecek veri miktarının taşıyıcı görüntü bit sayısına bölünmesi ile elde edilen sonuç, piksel başına düşen veri miktarını ifade etmektedir. LSB tekniği genellikle taşıyıcı görüntünün bir pikseline bir gizli veri biti gizler (Setiadi, 2022).

$$\text{bpp} = \frac{\text{gizli mesaj bitleri}}{\text{taşıyıcı görüntü bitleri}} \tag{2.1}$$

2.5. Görüntü Steganografisinde Yaygın Kullanılan Değerlendirme Ölçütleri

Görüntü steganografisinde veri gizlemenin ne kadar kaliteli yapıldığının göstergesi taşıyıcı görüntü ile stego görüntü arasındaki farkın algılanamayacak kadar düşük olmasına bağlıdır. Matematiksel olarak da her iki görüntü arasındaki farkı hesaplayan hata yöntemleri aşağıda verilmektedir.

2.5.1. Ortalama Karesel Hata

Veri gizleme tekniklerinin uygulanmasından sonra, stego görüntünün kalitesini belirlemek için kullanılan en bilindik yöntemlerden biri ortalama karesel hatadır (ing: mean square error – MSE). MSE, taşıyıcı görüntü ile stego görüntü arasındaki piksel değeri farklarının karelerinin toplamını ifade etmektedir. Gizli verinin algılanabilirliğini azaltmak için hata oranının küçük olması istenmektedir. Hata oranı küçük ise görüntüde az bozulma, hata oranı yüksek ise görüntüdeki bozulmanın fazla olduğunu göstermektedir.

$$\mathrm{MSE}= \frac{1}{\mathrm{satırxsütun}} \sum_{i=1}^{\mathrm{satır}} \sum_{j=1}^{\mathrm{sütun}} (T_{i,j}\text{-}S_{i,j})^2 \qquad (2.2)$$

Denklem (2.2)'de i görüntü matrislerinin satır indisini, j sütun indisini, $T_{i,j}$ taşıyıcı görüntünün bitleri ve $S_{i,j}$ stego görüntünün bitleridir.

2.5.2. Tepe Sinyal Gürültü Oranı

Görüntünün kalitesini test etmek için, veri boyutuna bağlı ortalama karesel hatanın kullanılmasından daha ziyade, görüntünün tepe sinyal değerine göre hesaplanan hata büyüklüğü kullanılabilir (Sayood, 1996). Tepe sinyal gürültü oranı (ing: peak signal to noise ratio – PSNR) logaritmik olarak hesaplanan, ortalama karesel hatayı da içeren bir metriktir.

$$\mathrm{PSNR}=10 \log 10 \left(\frac{255^2}{\mathrm{MSE}}\right) \qquad (2.3)$$

Denklem (2.3)'deki PSNR formülü standart bir formül olup, desibel (dB) cinsinden ifade edilmektedir. Stego görüntü kalitesinin iyi olarak kabul edilebilmesi için PSNR değerinin 40 dB üzerinde olması gerekmektedir (Cheddad ve diğ., 2010).

2.5.3. Yapısal Benzerlik Oranı

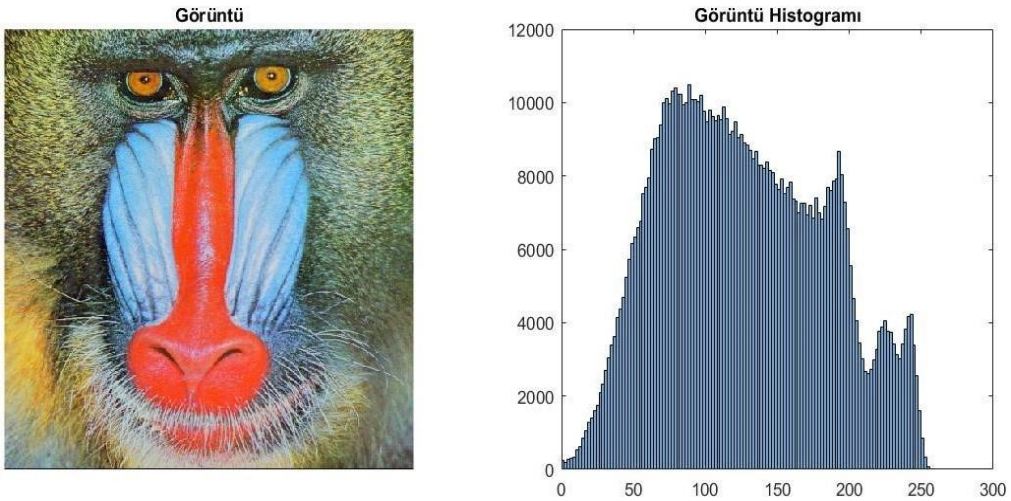
Yapısal benzerlik indeksi ölçüsü (ing: structural similarity index measurement - SSIM) değeri, taşıyıcı görüntü ile stego görüntünün yapısal olarak birbirine benzerliğini ölçmek için kullanılmaktadır. Temel olarak insan görsel sisteminin (HVS) algılayabilirliğine dayanmaktadır (Wang ve diğ., 2003).

$$\mathrm{SSIM}(x,y)=\frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2+\sigma_y^2+C_2)} \tag{2.4}$$

Denklem (2.4)'de SSIM değerini hesaplama formülü verilmektedir. Burada; x ve y değerleri taşıyıcı ve stego görüntüleri ifade etmektedir. Görüntülerdeki piksel yoğunluğu μ ile, standart sapma σ ile ve katsayılar da C ile gösterilmektedir.

2.5.4. Histogram

Görüntü histogramı, görüntüdeki piksel yoğunluk fonksiyonunun grafiksel temsilidir. Taşıyıcı görüntü piksellerine, gizli verinin gömülmesi sırasında, piksel değerlerinde değişiklikler olur ve histogram etkilenir. Taşıyıcı görüntü ve stego görüntü histogramlarına bakılarak, görüntü içerisine veri gizlenip gizlenmediği tespit edilebilmektedir. LSB veri gizleme teknikleri ile veri gizleme işlemi yapıldığında görüntü histogramında girinti ve çıkıntılar oluşmaktadır. Şekil 2.13.'de renkli bir görüntü ve görüntüye ait histogramı gösterilmektedir.



Şekil 2.13. Dijital 24 bit renkli görüntü ve görüntünün histogramı

3. UYGULAMA YÖNTEMİ

Tez çalışmasında, evrimsel programlamanın en yaygın kullanılan algoritmalarından biri olan genetik algoritmalar kullanılmıştır (GA). Genetik algoritmalar, Darwin'in biyolojik evrim sürecini ve doğal seçilimi simüle eden bir arama algoritmasıdır. Evrimsel programlama, 1960'lı yıllarda gündeme gelmiş ve genellikle evrim stratejilerini, genetik algoritmaları kapsamaktadır (Nabiyev, 2016).

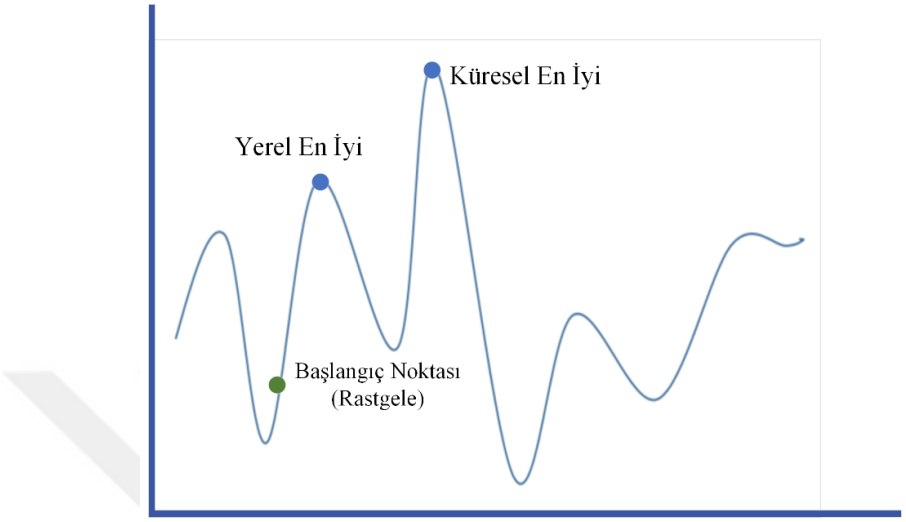
3.1. Genetik Algoritma

Genetik algoritmalar ilk 1970'li yılların ortalarında Michigan Üniversitesi'nde bilgisayar bilimleri uzmanı olan J.Holland tarafından ortaya konulmuştur. Uyarlayıcı ve yapay sistemlerin (ing: artificial systems) incelenmesinde çaprazlama, mutasyon ve seçimi kullanan ilk Holland'dır (Holland, 1975). Çaprazlama, mutasyon ve seçim gibi genetik operatörler problem çözmede genetik algoritmaların temelini oluşturmaktadır. İlk ortaya konulduğundan bu yana, GA birçok problemin çözüm arayışı için kullanılmıştır.

Genetik algoritmaların bu kadar popüler olmasının temel sebebi, karmaşık problemlerle başa çıkabilme, deterministik yöntemler ile kesin çözümü olmayan problemlere kesine çok yakın çözümler üretebilme yeteneğidir. Bunu yaparken de çözümü tek bir noktada aramayıp, çözüm uzayının birçok noktasında paralel olarak arama yapmalarıdır. Problemin parametrelerinin kendisini değil, kodlarını kullanarak arama yapmaktadır. Genetik algoritmalar arama uzayı hakkında bilgi, türev bilgisi, matematiksel işlem gereksinimi duymayan stokastik bir algoritmadır. Problemin çözülebilmesi için, problem ile algoritma arasındaki tek bağ olan amaç fonksiyonun iyi tanımlanması gereklidir.

Arama problemlerinde en önemli sıkıntılardan biri, çözümün yerel en iyi noktasında ve o noktanın çevresinde sıkışmasıdır. Şekil 3.1.'de verildiği üzere, arama uzayında birden fazla yerel en iyi nokta ve küresel en iyi nokta bulunabilmektedir. Genel arama algoritmalarında, yerel arama başlangıç noktası rastgele bir noktadan başladığı için, algoritma çözümde bazen küresel en iyi noktasını bulamamaktadır. Böyle durumlarda, algoritmanın yeniden çalıştırılması gerekmektedir. Başlangıç noktasının rastlantısal olarak küresel en iyi noktasına yakın bir noktadan başlaması, onu komşuları arasından en iyi noktaya götürebilir, ancak bu tamamen rastlantısal bir arama olmaktadır. GA,

mutasyon ve çaprazlama operatörleri ile arama uzayında tüm yerel ve küresel iyi noktaları bulmayı sağlamaktadır. Mutasyon operatörü, algoritmanın yerel en iyi noktada sıkışıp kalmasının önüne geçmektedir.



Şekil 3.1. Yerel en iyi ve küresel en iyi noktalarının gösterimi

GA, amaç fonksiyonu zamanla değişen veya değişmeyen, doğrusal veya doğrusal olmayan, sürekli veya süreksiz, gürültülü optimizasyon problemleri ile ilgilenen, rastlantısal süreçlere dayalı bir algoritma türüdür (Yang, 2021).

Algoritmanın etkili çalışıp, doğru sonuçlar üretmesi için amaç fonksiyonun iyi formüle edilmesi, nüfus büyüklüğünün uygun seçilmesi, mutasyon ve çaprazlama oranlarının probleme yönelik seçilmesi gerekmektedir.

3.2. Genetik Algoritmanın Çalışma Adımları

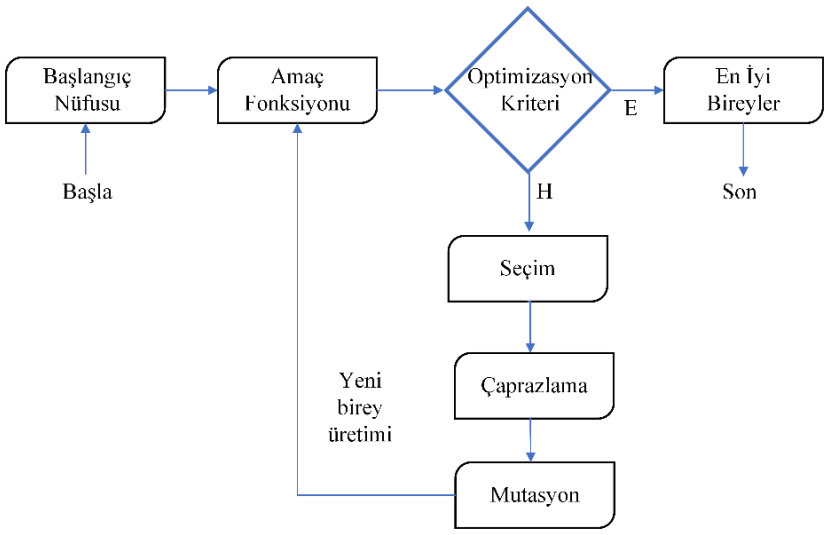
Genetik Algoritmaların akış diyagramı Şekil 3.2.'de gösterilmektedir. Genetik algoritmalar ile bir problemi çözmek için, ilk olarak rastgele meydana getirilmiş başlangıç nüfusunun üretilmesi gerekmektedir. Başlangıç nüfusunun büyüklüğü, birey ve gen sayısı probleme bağlı olarak belirlenmektedir. Nüfus içerisinde yer alan bireyler genetik bilimindeki kromozomları ifade etmektedir. Kromozom sayısı nüfus büyüklüğüne karşılık gelmektedir. Her bir kromozom arama uzayındaki olası bir çözümdür. Genler, kromozomları meydana getiren ve çözümü oluşturan parametreleri temsil etmektedir. Başlangıç nüfusunun büyüklüğü, problemin optimum çözüme ulaşması için gerekli olan aramanın genişliği ve algoritma çözüm süresi için önemli bir seçimdir.

Bir sonraki adımda, nüfus içerisinde her bir bireyin çözüm için ne kadar iyi olduğu tespit edilir. Bunun için kullanılan fonksiyon, aramanın yol haritasını belirleyen amaç fonksiyonudur. Amaç fonksiyonu probleme özgü olarak belirlenmektedir. Amaç fonksiyonunun bir eşik değeri veya iki jenerasyon arasındaki değişimi durdurma kriteri olarak kullanılabilir, durdurma kriteri sağlanana kadar GA çalışmaya devam eder. Kriter sağlandığında algoritmanın çalışması durdurulur.

Amaç fonksiyon değeri, bir sonraki jenerasyonun nüfusunu oluşturacak çocukları üretmek üzere, eşleşmeye girecek olan ebeveyn bireylerin seçilme olasılığını belirlemektedir. Seçim bireylerin seçilme olasılıklarına göre rastgele yapılmaktadır.

Seçilen ebeveyn bireylere çaprazlama ve mutasyon operatörleri uygulanmaktadır. Çaprazlama ile, arama mevcut çözümden daha iyi çözüme doğru yönlendirilirken, mutasyon ile arama uzayının her noktasının aranması yani çeşitlilik sağlanmaktadır.

Üretilen çocuk bireyler ile yeni nüfus oluşturularak amaç fonksiyonu adımına geri dönülür ve bir sonraki jenerasyon için amaç fonksiyon değerleri tekrar hesaplanmaktadır. Yeni bireyler eklendikçe, eski bireyler nüfustan çıkartılarak nüfus büyüklüğünün sabit kalması sağlanmaktadır. En iyi bireyin oluşturduğu çözüm bulunana kadar algoritma çalışmayı sürdürmektedir.



Şekil 3.2. Genetik algoritma akış diyagramı (Yıldırım, 2003).

Genetik algoritmalar, tek bir çözümle değil, çözümlerin yer aldığı bir küme ile arama yapan sezgisel bir algoritmadır. Tekrarlama (İterasyon) yaparak daha iyi çözümü

aramaktadır. Problemlerin parametrelerini değil, kodlarını kullanarak arama yapmaktadır.

Genetik algoritmalar arama uzayı hakkında bilgi, türev bilgisi, matematiksel işlem gereksinimi duymayan stokastik algoritmalardır. Problemin çözülmesi için, probleminin tanımının iyi yapıldığı amaç fonksiyonu gereklidir.

3.3. Genetik Algoritma Operatörleri

3.3.1. Kodlama

Genetik algoritma ile çözüm aranırken bireylerin kodlanması önem taşımaktadır. Bireylerin kodlanmasının nasıl olacağına karar verilmesi, nüfus oluşturulmadan önce karar verilmelidir. İkili kodlama, permütasyon kodlama, gerçel kodlama, ağaç kodlama, değer kodlama gibi kodlama yöntemleri bulunmaktadır (Nabiyev, 2016).

Genellikle kodlama biçimi olarak ikili (binary) kodlama kullanılmaktadır. Bu kodlamada her gen, Tablo 3.1.'deki gibi bir bit ile ifade edilir. Yani 0 ve 1'lerden oluşan bir bit dizisiyle temsil edilmektedir. İkili kodlamada, problemdeki parametre sayısına göre büyük birey vektörleri oluşabilir ancak arama uzayının geniş çaplı aranmasını sağlar.

Tablo 3.1. İkili kodlama temsili

Birey A	1011100101101011100
Birey B	0101101000010000011

Değer kodlama, bireylerin, gerçel sayılardan oluştuğu nüfuslarda kullanılmaktadır. Bu nüfuslarda bireyler, Tablo 3.2.'de verildiği gibi değerler dizisinden oluşmaktadır.

Tablo 3.2. Değer kodlama temsili

Birey A	3.74 6.125 0.27 0.85 0.11
Birey B	(sol),(yukarı),(aşağı),(sağ)

3.3.2. Seçim operatörü

Genetik algoritmada, hangi bireylerin çaprazlamaya katılacağı seçim ile belirlenir. Bu seçilme işlemi, bireylerin amaç fonksiyonu değerleri ile belirlenmektedir. Her bireyin bir seçilme olasılığı vardır ve bu olasılığa göre rastgele seçilirler. Çözüme çok katkı sağlayan

bireylerin amaç fonksiyon değerleri daha uygun oldukları için seçilme olasılıkları da yüksek olmaktadır ve çaprazlamaya daha çok seçilmektedirler. Bu, iyi bireylerin genlerini gelecek kuşaklara daha fazla aktaracaklardır anlamına gelmektedir ve doğada var olan "güçlü olan yaşar" prensibine karşılık gelmektedir. Literatürde yaygın kullanılan seçim yöntemleri rulet tekeri seçimi ve turnuva seçimidir.

3.3.2.1. Rulet Tekeri Seçimi

Bireylerin uygunluk değerleri (amaç fonksiyon değerleri) toplam uygunluk değerine bölünerek bireylere [0,1] aralığında seçilme olasılıkları atanır. Bireylerin seçilme olasılıkları toplamı 1'dir. Bireylerin seçilme olasılıkları bir dairenin dilimlerini temsil ettiği için ve seçilme işlemi rastgele yapıldığından yönteme bu isim verilmiştir.

$$S_i = U_i / \sum_{i=1} U_i \qquad (3.1)$$

Denklem (3.1)'de; U_i *i*. bireyin uygunluk değeri, S_i *i*. bireyin seçilme olasılığıdır. Daireyi oluşturan dilimlerden hangisinin, yani hangi bireyin seçileceği [0,1] aralığında üretilen rastgele sayı ile belirlenmektedir. Bu şekilde çaprazlamaya girecek birey sayısı kadar rastgele birey seçilir.

3.3.2.2. Turnuva Seçimi

Karşılaştırmaya dayalı bir seçim tekniğidir. Rastgele seçilen bireyler arasında uygunluk değeri karşılaştırılarak içlerinden en iyisi seçilir ve seçim bu şekilde ilerler. Örneğin, nüfus içerisinden 4 birey seçilir. Öncelikle, 1 ve 2 numaralı birey karşılaştırılır. Uygunluk değeri daha iyi olan birey seçilir. Daha sonra 3 ve 4 numaralı bireyler karşılaştırılır ve uygunluk değeri iyi olan seçilir. Maksimizasyon problemlerinde uygunluk değeri yüksek olan, minimizasyon problemlerinde uygunluk değeri küçük olan birey seçilmektedir.

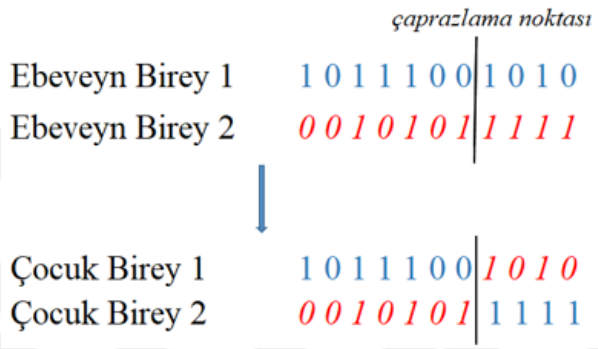
3.3.3. Çaprazlama Operatörü

Çaprazlama, iyi ebeveyn bireylerin genlerinden iyi olanlarını aynı çocuk bireyde buluşturabilmek için yapılmaktadır. Burada amaç, uygunluk değeri iyi ebeveyn bireylerden daha iyi çocuk bireyler üretebilmektir. Çaprazlama arama uzayındaki iyi bir çözümün civarında daha iyi çözümler bulmaya yarar ve yerel optimum çözüme doğru

gidişi hızlandırır. Literatürde kullanılan farklı çaprazlama yöntemleri bulunmaktadır; tek noktalı çaprazlama, iki noktalı çaprazlama, tekdüze (uniform) çaprazlama.

3.3.3.1. Tek Noktalı Çaprazlama

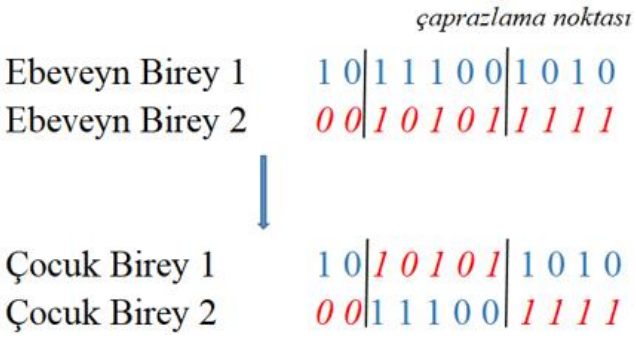
Çaprazlama işlemine girecek iki birey için, ortak bir nokta rastgele belirlenir. Belirlenen bu nokta temel alınarak noktanın öncesi ve sonrasındaki genler bireyler arasında yer değiştirilir. Çaprazlama noktası bir ile bireyin bit sayısından bir eksiği arasında rastgele üretilen bir değerdir. Şekil 3.3.'de tek noktalı çaprazlama örneği verilmektedir.



Şekil 3.3. Tek noktalı çaprazlama

3.3.3.2. İki Noktalı Çaprazlama

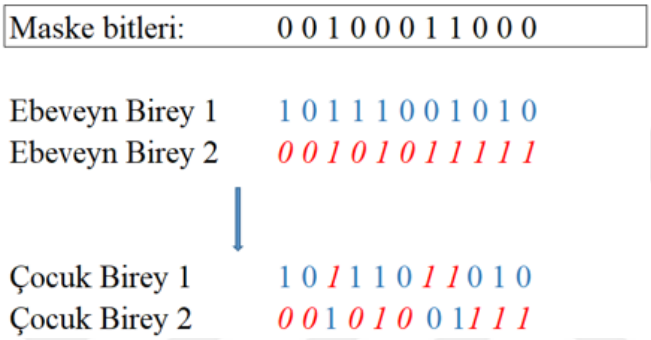
İki noktalı çaprazlama, problemdeki bireyin gen uzunluğuna bağlı kullanılan bir çaprazlama yöntemidir. Problemin değişken sayısı arttıkça çaprazlama noktaları da arttırabilir. Şekil 3.4.'de verilen örnekte, çaprazlama noktaları iki birey için ortak rastgele üretilmiş sayılardır.



Şekil 3.4. İki noktalı çaprazlama

3.3.3.3. Tekdüze Çaprazlama

Tekdüze çaprazlamada, bireylerdeki her bir bit eşit olasılıkla seçilmektedir. Probleme göre olasılık katsayıları değiştirilebilmektedir. Temel ilkesi yazı tura seçimine dayanarak, hangi bitlerin karşılıklı yer değiştireceğini belirleyen bir maske üretmektir. Çaprazlama maskesinde yer alan 1'lerin pozisyonundaki genler yer değiştirilmektedir. Maske ikili kodlardan oluşmaktadır. Şekil 3.5.'de tekdüze çaprazlama işlemine dair örnek verilmektedir.



Şekil 3.5. Tekdüze çaprazlama

3.3.4. Mutasyon Operatörü

Genetik algoritmada mutasyon operatörü, algoritmanın yerel en iyi çözüme takılmasının önüne geçilmesini sağlamaktadır. Nüfus içerisindeki bireylerin birbirlerine benzemesi ve aynılaşması yerel en iyiye takılma anlamına gelmektedir ve bireylerden bir veya birkaçının genlerini rastgele değiştirerek bu benzerlik bozulabilir. Mutasyon, genler üzerinde rastgele değişiklikler yaparak nüfustaki istenen çeşitliliği sağlamaktadır. Mutasyon oranı büyük seçildiğinde, bireyin mutasyona uğrayan gen sayısı artmaktadır. Çok küçük seçilen mutasyon oranı bireyin gen değişiminde fazla rol oynamadığı için, algoritma arama uzayında yerel en iyiye takılabilir.

İkili kodlama için, hangi bireyin hangi geni mutasyona uğrayacak ise o bitin tersi alınır; yani bit 0 ise 1, 1 ise 0 yapılır. Gerçel sayılardan oluşan bireyler için, mutasyon olasılığı mutasyon oranından küçük kalan gen değiştirilir. Değiştirme işlemi de genin değerine mutasyon olasılığının eklenmesi ile olur (Yıldırım, 2003). Mutasyon oranı "0,03" seçilmiş durum için Tablo 3.3. ve Tablo 3.4.'de mutasyona uğrayan birey örnekleri verilmektedir.

Tablo 3.3. İkili kodlama birey için mutasyon

Mutasyon Olasılıkları	0,65	0,13	0,70	**0,01**
Birey (Mutasyon Öncesi)	0	1	0	**0**
Birey (Mutasyon Sonrası)	0	1	0	**1**

Tablo 3.4. Değer kodlama birey için mutasyon

Mutasyon Olasılıkları	0,65	0,13	0,70	**0,01**
Birey (Mutasyon Öncesi)	3,25	2,20	-1,11	**0,75**
Birey (Mutasyon Sonrası)	3,25	2,20	-1,11	**0,78**

3.4. Literatürde Genetik Algoritma Kullanılan Steganografi Çalışmaları

Genetik algoritma kullanılarak görüntü dosyasına veri gizleme konusunda literatür araştırmasında incelenen çalışmalar aşağıda sunulmuştur.

Chang ve diğ. (2009) çalışmasında, taşıyıcı görüntünün çeşitliliğini arttırmak için, renkli görüntülerin sıkıştırma kodlarına veri gizlemeyi ve sadece gri görüntülere uygulanan blok kırpma kodlamasını renkli görüntülere uygulayabilmeyi genetik algoritma kullanarak gerçekleştirmiştir. Ancak, kullanılan yöntem sonucu elde edilen PSNR değerlerinin 40 dB'in altında kaldığı görülmektedir.

Wang ve diğ. (2010), içine veri gizlenmiş stego görüntünün RS analizine dayanıklı olması için, stego görüntü piksel değerlerini değiştiren genetik algoritma tabanlı bir teknik geliştirmişlerdir. İki adımda ilerleyen bu yöntem, öncelikle mesaj bitlerini(LSB)'ye gizleyerek, stego görüntünün RS değerlerinin saldırıya dayanıklı olması için piksel değerlerini değiştirmiştir. Önerdikleri yöntemde taşıyıcı görüntüye gizli verinin nasıl gizleneceğine değil, stego görüntünün saldırılara karşı nasıl dayanıklı olacağına dair uygulama yapılmıştır.

Ghasemi ve Shanbehzadeh (2010) çalışmalarında, taşıyıcı görüntü olarak 512x512 boyutlu gri ölçekli görüntü kullanmışlardır. Taşıyıcı görüntüyü 8x8'lik matrislere bölmüş ve PSNR değerini uygunluk fonksiyonu olarak seçerek, PSNR değeri en yüksek olan en iyi piksel dizisini genetik algoritma ile seçmişlerdir. Seçilen piksel dizisine OPAP kullanmışlardır. Yaptıkları çalışmaları Chang ve diğ. (2008) çalışmasıyla, Lee ve Chen 2007'de yaptıkları çalışma ile ve 4-LSB veri gizlenmesi ile karşılaştırmışlardır. Chang ve diğ.'in (2008) çalışmasına göre, çalışmalarının PSNR değeri düşük kalmasına karşılık

kapasiteyi arttırmışlardır. Diğer karşılaştırma yaptıkları çalışmalara göre de PSNR değerleri daha yüksek sonuç vermiştir. Ancak çalışmalarında PSNR değerinin 40 dB'in altında kaldığı görülmektedir.

Kanan ve Nazeri (2014) çalışmalarında, taşıyıcı görüntü olarak 512x512 boyutunda gri ölçekli görüntü ve gizli veri olarak da 256x256 boyutunda gri ölçekli görüntü kullanmışlardır. Stego görüntünün PSNR değerini maksimum yaparak, veri gizleme için en iyi başlangıç noktasını, tarama sırasını bulmak için genetik algoritma kullanmışlardır. Tarama sırası olarak verilen parametre, taşıyıcı görüntüde raster seçim yapmak yerine, genetik algoritmanın verdiği sıraya göre ilerlemektir. Yaptıkları çalışmanın ortalama PSNR değerinin 45.13 dB olduğu gösterilmiştir.

Nosrati ve diğ. (2015), genetik algoritmayı taşıyıcı görüntündeki pikselleri seçmek için kullanmışlardır. Çalışmalarında, taşıyıcı görüntünün LSB matrisini çıkartmışlar, 0 ve 1'lerden oluşan bir matris olarak saklamışlardır. Gizli veri de ikilik tabanda bir dizi olarak işleme alınmıştır. Daha sonra, taşıyıcı görüntü ve gizli veri dizilerini blok setlerine dönüştürmek için segmentasyon işlemi uygulanmıştır. Taşıyıcı görüntü olarak 1000x800 boyutlarında BMP formatlı gri ölçekli resim kullanılmıştır. Hangi bloklarda hangi piksellerin kullanıldığı bilgisi bir anahtar dizisinde saklanmıştır. Çalışmanın deneysel sonucuna örnek olarak da taşıyıcı görüntünün ve içerisine veri gizlenmiş görüntünün histogram grafikleri karşılaştırılmıştır. Uygulamalarında PSNR ve SSIM değerlerinden bahsedilmemiştir.

Sethi ve Kapoor (2016), görüntü steganografisi ile kriptolojiyi birleştirmiş ve verinin gizleneceği piksel seçimini genetik algoritma ile yapmışlardır. Taşıyıcı görüntü piksellerine veri gizlenmeden önce AES algoritması ile şifrelenmiştir.

Gu ve Sun (2018) çalışmalarında, 512x256, 384x256, 256x256, 128x256 boyutlu renkli taşıyıcı görüntüler kullanmışlardır. Veri gizleme işleminden önce taşıyıcı görüntüyü şifrelemişlerdir. Taşıyıcı görüntü Arnold Dönüşümü ile dönüştürme işlemlerinden geçmiştir. Genetik algoritmada kodlama olarak gerçel kodlama kullanmışlardır. Amaç fonksiyonu olarak da PSNR değerinin maksimum olması hedeflenmiştir. Çalışma sonuçları klasik LSB yer değiştirme tekniği ile karşılaştırılmış, PSNR değerlerinin klasik LSB tekniğine göre daha iyi olduğu ileri sürülmüştür.

Shah ve Bichkar (2018) çalışmalarında, kayıpsız veri için uzamsal alan görüntü steganografisinde genetik algoritma ve LCG yöntemlerini kullanmışlardır. Taşıyıcı görüntü olarak 256x256 boyutlu gri ölçekli görüntüler ve gizli veri için de 64x64 boyutlu gri ölçekli görüntü kullanmışlardır. Önerilen teknikte, taşıyıcı görüntünün ¼'üne gizli mesaj bitlerini, geri kalan ¾'lük kısmına da katsayı değerlerini gizlemişlerdir. Seçilen her piksele 2 bit (2-LSB) veri gizleyerek gizli veriyi taşıyıcı görüntü piksellerine yerleştirmişlerdir. Gizli veriler oluşturulan bir katsayı matrisine göre taşıyıcı görüntüye gizlenmiştir. Katsayı matrisinin boyutu 128x128 olarak verilmiştir. Katsayı matrisi bitlerinin taşıyıcı görüntü piksellerine yerleştirilmesi LCG ile yapılmıştır. Ancak, burada gizlenecek veri kapasitesi küçük, verinin kayıpsız geri alınabilmesi için gerekli olan katsayı matrisi boyutu büyük seçilmiştir. Yani verinin alıcı tarafından düzgün alınabilmesi için gereken anahtarın boyutu iletilen verinin boyutundan büyüktür. Önerilen tekniğin sonuçları aynı kapasitede veri gizlenerek klasik LSB yer değiştirme tekniği ile karşılaştırılmış ve PSNR değerlerinin birbirine yakın olduğu görülmüştür.

Shah ve Bichkar (2020) çalışmalarında, genetik algoritmaya dayalı bir veri gizleme algoritması önermişlerdir. Taşıyıcı görüntü 256x256 boyutlu gri ölçekli resimlerden, gizli veri de 64x128 boyutlu gri ölçekli görüntülerden oluşmuştur. Önerilen teknikte, taşıyıcı görüntüler ve gizli veri istatiksel olarak analiz edilmiştir. Analizde verilerdeki 0 ve 1'lerin istatiksel olarak oranlarına bakılmıştır. 1000 resimden oluşan veri tabanından bu istatiksel oranlara bakılarak 10 adet taşıyıcı görüntü seçilmiştir. Gizli veri bloklara ayrılmıştır ve bloklar arasında LCG kullanılarak sıralama yapılmıştır. Genetik algoritma yardımıyla en iyi piksellerin yerleri belirlenmiş, belirlenmiş piksel bloklarına gizli veri blokları yerleştirilmiştir. Burada, gizli veri piksel yerleri değiştirildiği için, gizlenecek veri bir görüntü olmadığında, veride tutarsızlık oluşabilir. Çalışmalarında 54 bit uzunluğunda anahtar kullanılmıştır ve anahtar taşıyıcı görüntünün 2. LSB'sine gizlenmiştir. Önerdikleri tekniği, klasik LSB yer değiştirme tekniği sonuçları ile karşılaştırmış ve tekniklerinin PSNR değerinin daha yüksek olduğunu belirtmişlerdir.

Shah ve Bichkar (2021) genetik algoritma ile veri gizleme tekniği önermişlerdir. Taşıyıcı görüntü için 512x512 boyutlarında gri ölçekli görüntüler, gizli veri için 128x256 boyutlu gri ölçekli görüntü kullanmışlardır. Ayrıca, çalışmalarında genetik algoritmanın nüfusu oluşturan bireyleri için esnek kromozom adlı bir kavram kullanmışlardır. Bireylerin

genleri, yani problemin parametreleri gizli veri bitlerine göre değişebildiği için esnek kromozom diye adlandırmışlardır. Önerilen teknikte, gizli veri yeniden düzenlenerek taşıyıcı görüntü piksellerine gizlenmiştir. Çalışmalarını, klasik LSB tekniği, klasik genetik algoritma birey yapısı ile karşılaştırmışlardır. Esnek kromozom yapısı ile her iki çalışmaya göre daha yüksek PSNR sonucu aldıklarını belirtmişlerdir.

Shyla ve arkadaşları (2021), taşıyıcı medya için 256x256 boyutunda gri ölçekli görüntüler ve gizli veri için 64x128 boyutunda gri ölçekli görüntü seçmişlerdir. Önerilen teknikte, 1000 adet görüntüden oluşan görüntü veri tabanından veri gizleme için en uygun olan görüntünün taşıyıcı görüntü olarak seçilmesi genetik algoritma ile yapılmıştır. Bir eşik değer belirlenmiş ve veri tabanındaki görüntülerden PSNR ve RMSE değerleri eşik değerden büyük olanlar genetik algoritma ile seçilmiştir. Seçim işleminde uygunluk fonksiyonu için bir olasılık fonksiyonu tanımlanmıştır. Seçim işlemi tamamlandıktan sonra, gizli veriyi taşıyıcı görüntüye klasik LSB veri gizleme tekniğini kullanarak gizlemişlerdir. Deneysel çalışma sonuçlarını, Gu ve Sun (2018), Shah ve Bichkar (2021) çalışmaları ile karşılaştırmışlardır. Karşılaştırma sonucunda, önerdikleri tekniğin, diğer iki çalışmanın PSNR değerlerinden yüksek olduğunu belirtmişlerdir.

4. GENETİK ALGORİTMA İLE KANAL SEÇİMİ

Uygulamada kullanılan taşıyıcı ve gizli mesaj görüntülerin bir kısmı USC-SIPI görüntü veri tabanından elde edilmiştir. Bir kısmı da MATLAB programının kendi demo görüntüler klasöründen elde edilmiştir.

Uygulama tasarlanırken taşıyıcı görüntü olarak 256x256 piksel (65 KB) boyutunda gri ölçekli dijital görüntüler kullanılmıştır. Gizlenecek veri olarak da 16x32 piksel (512 B), 32x32 piksel (1 KB), 32x64 piksel (2 KB), 64x64 piksel (4 KB) ve 64x128 piksel (8 KB) boyutlarında gri ölçekli dijital görüntüler kullanılmıştır. Denklem (2.1)'deki hesaplama ile gizli veri kapasiteleri sırasıyla, 0.007 bpp, 0.015 bpp, 0.031 bpp, 0.0625 bpp ve 0.125 bpp'dir. Dijital görüntüler tiff uzantılı görüntü dosyalarıdır. Uygulamada kullanılan taşıyıcı görüntüler Şekil 4.1.'de, gizli veri görüntüleri Şekil 4.2.'de verilmektedir.

Veri gizleme algoritma adımları:

Girdi**:** Taşıyıcı görüntü T_{mxn}, Gizli veri M_{mxl} $(l = \{1,2,4,8,16\})$
Çıktı**:** Stego görüntü S_{mxn}
1. Taşıyıcı görüntüyü 4x4 bloklara bölün.
2. Görüntüyü satır satır tarama işlemini blok blok tarama olacak şekilde taşıyıcı görüntü matrisini $T_{4096x16}$ olacak şekilde yeniden boyutlandırın.
3. Gizli veri görüntüsünü ikili dosyaya dönüştürüp sırasıyla 16x32, 32x32, 32x64, 64x64 ve 64x128 boyutlu gri görüntüleri M_{4096x1}, M_{4096x2},M_{4096x4}, M_{4096x8}, $M_{4096x16}$ boyutlarında matrislere yerleştirin.
4. Nüfus büyüklüğü: 50 ve tekrarlama sayısı: 3000
5. GA için rastgele kromozomları oluşturun. Kromozomların gen sayısını gizli verinin sütun sayısına göre ayarlayın.
6. Nüfus içerisinden rulet tekerleği ile kromozomların uygunluk değerlerine göre iki kromozom seçin.
7. Kromozomlara çaprazlama işlemini ve mutasyon oranını uygulayın (mutasyon oranı: 0.02).
8. En iyi kromozomu elitist kromozom olarak ayırın.
9. 3000 jenerasyon için 6 – 8 arası adımları uygulayın.
10. Çözüm için en uygun seçilen kromozomu anahtar dizisi olarak saklayın.

11. Taşıyıcı görüntü anahtar dizisi ile verilen konumdaki piksellerinin son bitleri ile gizli veri bitlerini LSB yer değiştirme tekniği ile değiştirin.
12. Anahtar değerini stego görüntü piksellerinin 2.LSB'lerine klasik LSB yer değiştirme tekniği ile yerleştirin.

Veri çıkarma algoritma adımları:

Girdi**:** Stego görüntü S_{mxn}
Çıktı**:** Gizli veri M_{mxl} $(l = \{1,2,4,8,16\})$
1. Stego görüntünün 2.LSB'sinden anahtar dizisini çıkartın.
2. Anahtarı kullanarak stego görüntünün piksellerinden gizli veriyi çıkartın.

4.1. Uygulamada Kullanılan Görüntüler

Uygulama tasarlanırken taşıyıcı görüntü olarak 256x256 boyutunda gri ölçekli dijital görüntüler kullanılmıştır. Gizlenecek veri olarak da 16x32, 32x32, 32x64, 64x64, 64x128 boyutlarında gri ölçekli dijital görüntüler kullanılmıştır. Dijital görüntüler tiff uzantılı görüntü dosyalarıdır.

Şekil 4.1. Taşıyıcı test görüntüler (Baboon, Pirate, House, Zelda)

Şekil 4.2. Gizli veri görüntüleri (Cameraman, Female, Lake, Peppers, Livingroom)

4.2. Taşıyıcı Görüntülerin Bloklara Ayrılması

Uygulamada, 256x256 piksel boyutlu gri ölçekli görüntüler, 4x4 bloklara ayrılmış, her bir blok kendi içinde değerlendirmeye alınarak veri gizleme tekniği uygulanmıştır. 256x256 piksel boyutlu bir görüntü, 4x4 boyutunda bloklara ayrıldığında, 64x64 boyutlu bir hücre matrisi elde edilmektedir. Şekil 4.3.'de (a) taşıyıcı görüntünün 4x4 bloklara ayrılmış hücre matrisi olarak gösterimi, (b) hücre matrisinin ilk bloğunda yer alan piksel değerleri gösterilmektedir.

cover_matris_cell

{} 64x64 cell

	1	2	3	4
1	*4x4 uint8*	*4x4 uint8*	*4x4 uint8*	*4x4 uint8*
2	*4x4 uint8*	*4x4 uint8*	*4x4 uint8*	*4x4 uint8*
3	*4x4 uint8*	*4x4 uint8*	*4x4 uint8*	*4x4 uint8*
4	*4x4 uint8*	*4x4 uint8*	*4x4 uint8*	*4x4 uint8*

(a)

cover_matris_cell {1,1}

	1	2	3	4
1	102	65	93	53
2	97	69	80	58
3	95	101	79	57
4	51	121	102	58

(b)

Şekil 4.3. (a) Taşıyıcı görüntü hücre matrisi, (b) Hücre matrisi blok gösterimi

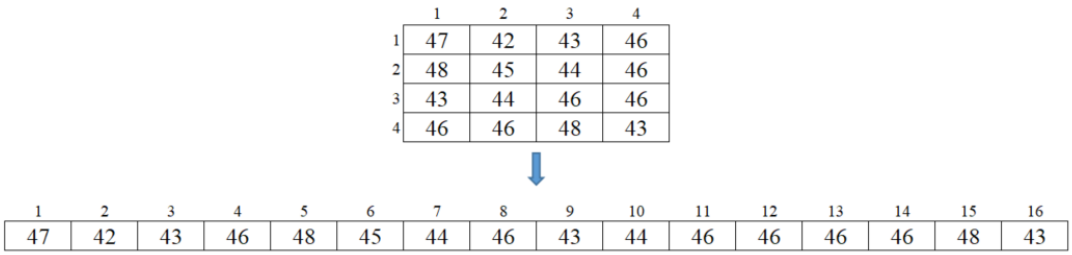
Uygulamada veri gizleme kapasitesi, her blok içerisinde sırasıyla 1 piksel, 2 piksel, 4 piksel, 8 piksel ve 16 piksel olarak belirlenmiştir. 256x256 piksel boyutlu gri ölçekli bir görüntü bloklara bölünmeden, piksel değerlerinin sadece son bitlerine 1-LSB veri

gizleme tekniği uygulandığında, 65.536 bit uzunluğunda bir veri gizlenebilecek demektir. Diğer taraftan, taşıyıcı görüntü 4x4 piksel boyutunda bloklara bölündüğünde ise, her blok içinde 16 piksel olduğundan, bir bloğun bit gizleme kapasitesinin 16 olduğu açıktır. Bu çalışmada yapılmaya çalışılan, en uygun piksel veya pikseller seçilerek, her blok içerisine sırasıyla 1 bit, 2 bit, 4 bit, 8 bit ve 16 bit veri gizlemektir.

Her piksel değeri 8 bit ile ifade edilmektedir. Her blok içerisinde sadece 1 pikselin son bitine veri gizleme işlemi yapılacağı zaman, 4.096 (64x64) bit veri gizlenebilecek demektir. Eğer gizlenecek veri görüntü ise, bunun için gerekli olan gizli görüntü boyutu 16x32 piksel olmalıdır. Aynı şekilde, her blok içerisinde 2 piksele veri gizlendiğinde, 8.192 bit veri gizlenebilecek; 4 piksele veri gizlendiğinde, 16.384 bit veri gizlenebilecek; 8 piksele veri gizlendiğinde, 32.768 bit veri gizlenebilecek; 16 pikselin tamamına veri gizlendiğinde ise, 65.536 bit veri gizlenebilecektir.

4.3. Taşıyıcı Görüntü Bloklarının ve Gizli Verinin Düzenlenmesi

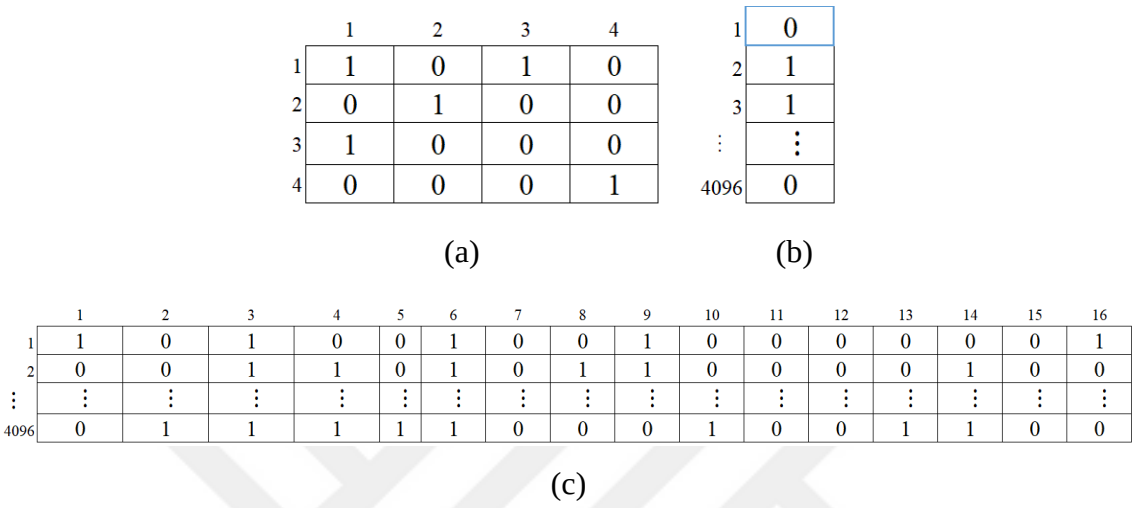
Bölüm 2.4.2.' de bahsedildiği gibi, LSB algoritmasında tarama işlemi satır satır, soldan sağa doğrudur. Matrisi bloklara bölüp, her blok için işlem yapıldığında tarama düzeni değişmemektedir. Bu nedenle uygulamada, taşıyıcı görüntü 64x64 boyutunda bloklardan oluşan bir matris yerine, 16 sütun (1 blok) 4096 satır boyutunda matris olarak işleme alınmıştır. Şekil 4.4'de, 4x4 boyutunda bir bloğun, 1x16 boyutunda satır matrisi olarak gösterimi bulunmaktadır.



Şekil 4.4. 4x4 Boyutlu matrisin 1x16 boyutlu satır matrisi

Şekil 4.4. incelendiğinde, 4x4 matrisin tarama düzeninin değişmeden satır matrisine çevrildiği görülmektedir. Aynı işlem, gizlenecek görüntüler için de uygulanmaktadır. 16x32 piksel boyutundaki gri görüntü 4096x1 ikili sütun matrisine, 32x32 piksel boyutundaki gri görüntü 4096x2 boyutlu ikili matrise, 32x64 piksel boyutundaki gri

görüntü 4096x4 boyutlu ikili matrise, 64x64 piksel boyutundaki gri görüntü 4096x8 boyutlu ikili matrise ve 64x128 piksel boyutundaki gri görüntü 4096x16 boyutlu ikili matrise dönüştürülmüştür. Bu matrislerin tamamında, 1-LSB kullanılacağından, piksel değerleri yerine son bitleri yer almaktadır (Şekil 4.5.).



Şekil 4.5. (a) Taşıyıcı görüntü son bitleri, (b) Gizli veri bitleri, (c) Taşıyıcı görüntü bitlerinin yeniden düzenlenmiş matrisi

4.4. Uygulamada Kullanılan GA Parametreleri ve Amaç Fonksiyon

Genetik algoritmanın iyi bir sonuç üretebilmesi için, başlangıç nüfusunun probleme uygun seçilmesi, mutasyon oranının ve jenerasyon sayısının belirlenmesi, amaç fonksiyonunun problemi iyi tanımlaması önem arz etmektedir. Genetik algoritmada çalışma için gerekli parametreler belirlendikten sonra, algoritma jenerasyon sayısı kadar arama uzayını taramaktadır.

Genetik algoritma ile bulunmak istenen, gizlenecek verinin taşıyıcı görüntüde hangi piksele gizleneceğidir. Bunun için, gizli verideki gizlenecek bitler, taşıyıcı görüntü piksellerinin LSB değerlerinden çıkartılarak, farklar toplamı minimum yapılmaya çalışılmaktadır. Denklem (4.1)'de, bir bloğa bir bit saklamak için kullanılan amaç fonksiyon verilmektedir.

$$\min \sum_{i=1}^{4096} |T(i,j) - S(i,1)| \quad , \quad j \in (1,16) \tag{4.1}$$

Denklem (4.1)'de; $T(i,j)$ taşıyıcı görüntünün i. satır j. sütundaki bit değeri, $S(i,1)$ gizli görüntünün i. satırdaki bit değeridir. Genetik algoritma ile bulunmaya çalışılan, hangi j

değerinde (blok içerisinde hangi piksel) farklar toplamının mutlak değeri minimum olmaktadır. Bu, gizli veri taşıyıcı görüntü içerisine gömüldüğünde, LSB bitlerinde minimum değişme, yani maksimum PSNR anlamına gelmektedir.

Tez çalışması kapsamında, yapılan çok sayıda deneme sonucunda genetik algoritma çalışma parametreleri aşağıdaki gibi belirlenmiştir:

- ✓ Başlangıç nüfus büyüklüğü : 50
- ✓ Tekrarlama (jenerasyon) sayısı : 3000
- ✓ Mutasyon oranı : 0.02
- ✓ Seçim : Rulet Tekeri Seçimi

Genetik algoritmanın parametre değerleri belirlendikten sonra, algoritma amaç fonksiyonun minimum olan değerini aramaya başlar. Arama işlemi sırasında, optimizasyon kriteri sağlandığında algoritma sonlanır ve minimum amaç fonksiyonu değerini veren kromozomun genleri belirlenmiş yani kanal seçimi gerçekleşmiş olur. Üretilen bu dizi aynı zamanda alıcıya iletilecek anahtar dizisi olacaktır.

Amaç fonksiyonu minimum yapan kanallar taşıyıcı görüntünün tüm blokları için geçerlidir. Tüm bloklarda, sırasıyla, seçilen kanallardaki taşıyıcı görüntü bitleri ile gizli veri bitleri değiştirilmektedir.

4.5. Veri Gizleme

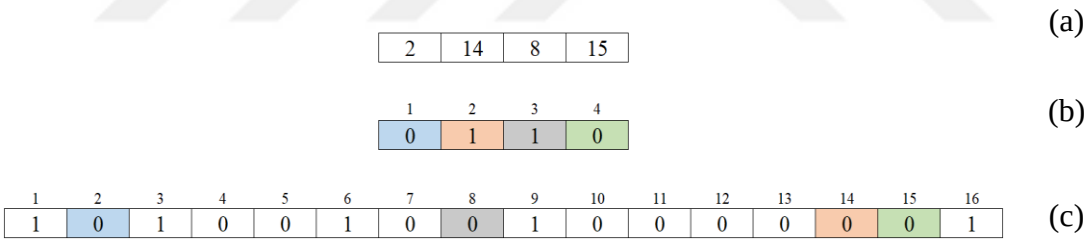
Genetik algoritmada kullanmak üzere, taşıyıcı görüntü ve gizli görüntünün matris boyutlarının yeniden düzenlenmesi yukarıdaki bölümlerde bahsedilmişti. GA, düzenlenmiş taşıyıcı görüntü ve gizli görüntü verilerini kullanarak, minimum amaç fonksiyonu değerine ulaşmak için çözüm arar ve bulduğu en iyi kromozom en iyi kanal seçimini göstermektedir. Seçilen kanallar aynı zamanda anahtar olarak veri gizleme sürecinde kullanılmıştır. Anahtarın kendisi de ayrıca, stego görüntü içerisine gizlenerek gönderilmektedir.

Taşıyıcı görüntü matrisi, 4x4 bloklara bölündüğü için, bir blok içerisinde 16 hücre bulunmaktadır. Bloklar 4x4 boyutundan 1x16 boyutuna düzenlendiğinden, en fazla 16 adet kanal seçimi yapılabilmektedir. Kromozom uzunluğu da, bu nedenle, en fazla 16

genden oluşmaktadır. Her bir gen blok içerisindeki bir hücrenin konumunu göstermektedir. Kromozom içerisindeki genler blok içerisindeki piksellere işaret eden işaretçiler gibi düşünülebilir. En iyi kromozom anahtar olarak karşı tarafa stego görüntü içerisinde gönderileceğinden, anahtar uzunluğu ikili olarak, gen sayısı x 4 bit olarak hesaplanmaktadır.

Şekil 4.6. (a) GA'da kullanılan 4 gen içeren bir kromozomu, yani anahtarı göstermektedir. Gen sayısının 4 olması, 16 piksel içeren bir bloğun 4 pikseline veri gizleneceği anlamına gelmektedir. Kromozomdaki genlerin değerleri, hangi piksellere veri gizleneceğine işaret etmektedir. Şekil 4.6. (a)'da gizli veri, Şekil 4.6. (c)'de ise anahtarın gösterdiği konumlara veri gizlenmiş taşıyıcı görüntü bloğu gösterilmektedir.

Anahtar boyutu bloklarda gizlenecek bit sayısına göre değişmektedir. Blok içerisinde bir bit veri gizlendiğinde, tek piksel seçileceği için, anahtar 1x1 boyutunda matris olacak ve stego görüntü içerisinde ikili 4 bit olarak yer alacaktır. Sırasıyla, iki bit gizlemek için anahtar 1x2 boyutunda matris olacak ve stego görüntü içerisinde ikili 8 bit olarak yer alacaktır. 4, 8 ve 16 bit gizlemek için de aynı yöntem izlenecektir.



Şekil 4.6. (a) Taşıyıcı görüntüde seçilen kanalları gösteren GA kromozomu, (b) Blok içerisine gizlenecek olan veri bitleri, (c) Gizli veri yerleştirilmiş taşıyıcı görüntü bloğundaki LSB değerleri

Veri, alıcıya gönderilmeden önce, taşıyıcı görüntünün anahtardaki indislerine sıra ile gizlenmektedir. Anahtar da stego görüntünün 2. LSB'lerine klasik LSB yer değiştirme tekniği ile gizlenmektedir. Verinin alıcı tarafta kayıpsız olarak geri alınabilmesi için anahtar bilgisi gereklidir.

4.6. Veri Çıkarma

Veri çıkarma işleminde, ilk işlem, stego görüntünün 2. LSB'lerinden anahtar değerlerinin alınmasıdır. Anahtar stego görüntüden çıkarıldıktan sonra, anahtarın işaret ettiği konum değerlerine göre, görüntülerden veriler kayıpsız olarak çıkarılmaktadır.

Gizlenen veri ile alınan verinin aynı olduğunu, kayıpsız şekilde geri çıkartılabildiğini görmek için kullanılan formül Denklem 4.2'de verilmektedir. Denklemdeki *n* değeri, gizlenen verinin uzunluğunu, *M* değeri gizlenen veriyi, *C* değeri de geri alınan veriyi temsil etmektedir. BER değer aralığının 0-1 arası olması gerekmektedir. BER değeri 0 ise, gönderilen veri ile alınan verinin birebir aynı olduğunu, veri gizleme ve çıkarma algoritmalarının doğru yapıldığını göstermektedir.

$$BER=\frac{\sum_{i=0}^{n}(M_i \oplus C_i)}{n} \tag{4.2}$$

4.7. Uygulama Sonuçları

Bu bölümde, önerilen GA tekniği ile tez çalışması kapsamında yapılan steganografi ve steganaliz çalışmalarının sonuçları yer almaktadır. Veri gizleme tekniklerinde taşıyıcı görüntü ile stego görüntü boyutlarının aynı olması gerekmektedir. Veri gizlemeden önce taşıyıcı görüntünün boyutu ne ise veri gizleme işlemlerinden sonra ortaya çıkan stego görüntünün boyutu da aynı olmalıdır.

Veri gizleme kapasitesine göre, taşıyıcı ve elde edilen stego görüntülerin sonuçları Şekil 4.7.'de verilmektedir. Şekilde, taşıyıcı görüntü olarak *baboon* görüntüsü örnek olarak gösterilmektedir. Şekil 4.7.(a) taşıyıcı orijinal görüntü, Şekil 4.7. (b-f) ise taşıyıcı görüntünün 4x4 bloklarının her birine, sırasıyla 1, 2, 4, 8 ve 16 bit gizlenmiş stego görüntüleri verilmektedir. Şekil 4.8.'de taşıyıcı görüntüye gizlenen gizli veri görüntüleri gösterilmektedir. Gizleme kapasitesine göre gizlenen veri boyutu da değişiklik göstermektedir.

(a) (b) (c)

(d) (e) (f)

Şekil 4.7. (a) Orijinal görüntü, (b)-(f) Stego görüntüler

16x32 32x32 32x64 64x64 64x128

Şekil 4.8. Gizli veri dijital görüntü boyutları

Tez çalışması kapsamında GA'ya dayalı geliştirilen yöntemin sonuçları, Sarı ve Yıldırım'ın (2022) yaptıkları 4x4 bloklarda en yüksek gradyan değerine sahip pikselin seçilmesine dayanan çalışma ve klasik LSB yer değiştirme tekniği ile karşılaştırılmıştır.

Tablo 4.1.'de, taşıyıcı görüntünün her bir bloğunda bir bit verinin gizlendiği karşılaştırma sonucu yer almaktadır. Bir bit gizlendiği için gizli veri boyutu 16x32 piksel alınmıştır. Farklı taşıyıcı görüntüler içerisine farklı gizli görüntüler gizlenmiştir. Tüm gizleme işlemlerinde, önerdiğimiz GA_LSB tekniğine ait PSNR değerleri Grad_LSB ve klasik LSB tekniklerine ait PSNR değerlerinden az da olsa daha yüksek çıkmıştır. SSIM

değerleri karşılaştırıldığında ise, GA_LSB tekniğine ait SSIM değeri diğerlerine göre eşit veya daha yüksek bulunmuştur. Tüm uygulamalarda BER değeri sıfır olarak elde edilmiş olup veri kaybı söz konusu olmamıştır.

Tablo 4.1. Her blokta 1 bit veri gizleme

Gizli Veri (16x32)	**Taşıyıcı Görüntü (256x256)**	**PSNR**			**SSIM**			**BER**
		GA_LSB	**Grad_LSB**	**LSB**	**GA_LSB**	**Grad_LSB**	**LSB**	
Peppers	Baboon	63.2701	63.2057	63.1611	1.0000	0.9999	0.9999	0
Lake	Pirate	63.2680	63.2206	63.2615	1.0000	0.9999	0.9999	0
Livingroom	House	63.2314	63.1506	63.1759	0.9999	0.9998	0.9998	0
Cameraman	Pirate	63.3370	63.2853	63.2658	1.0000	0.9999	0.9999	0
Female	Zelda	63.2550	63.2615	63.2422	0.9999	0.9998	0.9998	0

Tablo 4.2.'de, taşıyıcı görüntünün her bir bloğunda iki bit verinin gizlendiği karşılaştırma sonucu yer almaktadır. İki bit gizlendiği için gizli veri boyutu 32x32 piksel alınmıştır. Tüm gizleme işlemlerinde, önerdiğimiz GA_LSB tekniğine ait PSNR değerleri Grad_LSB ve klasik LSB tekniklerine ait PSNR değerlerinden daha yüksek çıkmıştır. SSIM değerleri karşılaştırıldığında ise, GA_LSB tekniğine ait SSIM değeri diğerlerine göre eşit veya daha yüksek bulunmuştur. BER değeri sıfır olarak elde edilmiş olup veri kaybı söz konusu olmamıştır.

Tablo 4.2. Her blokta 2 bit veri gizleme

Gizli Veri (32x32)	**Taşıyıcı Görüntü (256x256)**	**PSNR**			**SSIM**			**BER**
		GA_LSB	**Grad_LSB**	**LSB**	**GA_LSB**	**Grad_LSB**	**LSB**	
Peppers	Baboon	60.3066	56.4553	60.1382	0.9999	0.9996	0.9999	0
Lake	Pirate	60.3384	56.3379	60.1382	0.9999	0.9994	0.9999	0
Livingroom	House	60.2728	55.9779	60.1582	0.9997	0.9991	0.9996	0
Cameraman	Pirate	60.3165	56.4230	60.2253	0.9999	0.9995	0.9999	0
Female	Zelda	60.2533	56.2011	60.2007	0.9998	0.9988	0.9997	0

Tablo 4.3.'de, taşıyıcı görüntünün her bir bloğunda 4 bit verinin gizlendiği karşılaştırma sonucu yer almaktadır. 4 bit gizlendiği için gizli veri boyutu 32x64 piksel alınmıştır. Tüm gizleme işlemlerinde, önerdiğimiz GA_LSB tekniğine ait PSNR değerleri Grad_LSB ve klasik LSB tekniklerine ait PSNR değerlerinden daha yüksek çıkmıştır. SSIM değerleri karşılaştırıldığında ise, GA_LSB tekniğine ait SSIM değeri diğerlerine göre eşit veya daha yüksek bulunmuştur. BER değeri sıfır olarak elde edilmiş olup veri kaybı söz konusu olmamıştır.

Tablo 4.3. Her blokta 4 bit veri gizleme

Gizli Veri (32x64)	Taşıyıcı Görüntü (256x256)	PSNR			SSIM			BER
		GA_LSB	Grad_LSB	LSB	GA_LSB	Grad_LSB	LSB	
Peppers	Baboon	57.2707	44.5105	57.1353	0.9999	0.9945	0.9999	0
Lake	Pirate	57.2772	44.3099	57.1702	0.9999	0.9918	0.9998	0
Livingroom	House	57.2827	42.8510	57.2495	0.9995	0.9816	0.9994	0
Cameraman	Pirate	57.2772	44.3625	57.1527	0.9999	0.9916	0.9993	0
Female	Zelda	57.2745	44.3667	57.1553	0.9995	0.9824	0.9995	0

Tablo 4.4.'de, taşıyıcı görüntünün her bir bloğunda 8 bit verinin gizlendiği karşılaştırma sonucu yer almaktadır. 8 bit gizlendiği için gizli veri boyutu 64x64 piksel alınmıştır. Tüm gizleme işlemlerinde, önerdiğimiz GA_LSB tekniğine ait PSNR değerleri klasik LSB tekniğine ait PSNR değerlerinden daha yüksek çıkmıştır. SSIM değerleri karşılaştırıldığında ise, GA_LSB tekniğine ait SSIM değeri diğerlerine göre genel olarak daha yüksek bulunmuştur. BER değeri sıfır olarak elde edilmiş olup veri kaybı söz konusu olmamıştır.

Gradyan değeri yüksek olan pikselin seçilerek veri gizlenmesi klasik LSB yöntemine göre verinin tespitinde daha güvenli olabilmektedir. Ancak, her blok içinde maksimum gradyan değeri arandığı ve blok içinde birden fazla maksimum değer olması halinde ilk değerin seçilmesi sebebiyle, veri gizleme kapasitesi düşük bir tekniktir. Tablo 4.4 ve 4.5.'de görüldüğü üzere, Grad_LSB (gradyan değerine dayalı LSB) tekniğinde gradyan hesaplanamadığı için sonuç alınamamıştır. Grad LSB tekniğinde, genel olarak PSNR ve SSIM değerleri GA'ya dayalı LSB ve klasik LSB tekniklerinden düşük kalmıştır.

Tablo 4.4. Her blokta 8 bit veri gizleme

Gizli Veri (64x64)	Taşıyıcı Görüntü (256x256)	PSNR			SSIM			BER
		GA_LSB	Grad_LSB	LSB	GA_LSB	Grad_LSB	LSB	
Peppers	Baboon	54.2449	-	54.1756	0.9998	-	0.9997	0
Lake	Pirate	54.2265	-	54.1673	0.9997	-	0.9994	0
Livingroom	House	54.2455	-	54.1551	0.9992	-	0.9993	0
Cameraman	Pirate	54.2236	-	54.1281	0.9997	-	0.9994	0
Female	Zelda	54.2455	-	54.1423	0.9992	-	0.9989	0

Tablo 4.5'de, taşıyıcı görüntünün her bir bloğunda 16 bit verinin gizlendiği karşılaştırma sonucu yer almaktadır. 16 bit gizlendiği için gizli veri boyutu 64x128 piksel alınmıştır. Tüm gizleme işlemlerinde, önerdiğimiz GA_LSB tekniğine ait PSNR değerleri klasik LSB tekniğine ait PSNR değerlerinden daha yüksek çıkmıştır. SSIM değerleri

karşılaştırıldığında ise, GA_LSB tekniğine ait SSIM değeri diğerlerine göre daha yüksek bulunmuştur. BER değeri sıfır olarak elde edilmiş olup veri kaybı söz konusu olmamıştır.

Tablo 4.5. Her blokta 16 bit veri gizleme

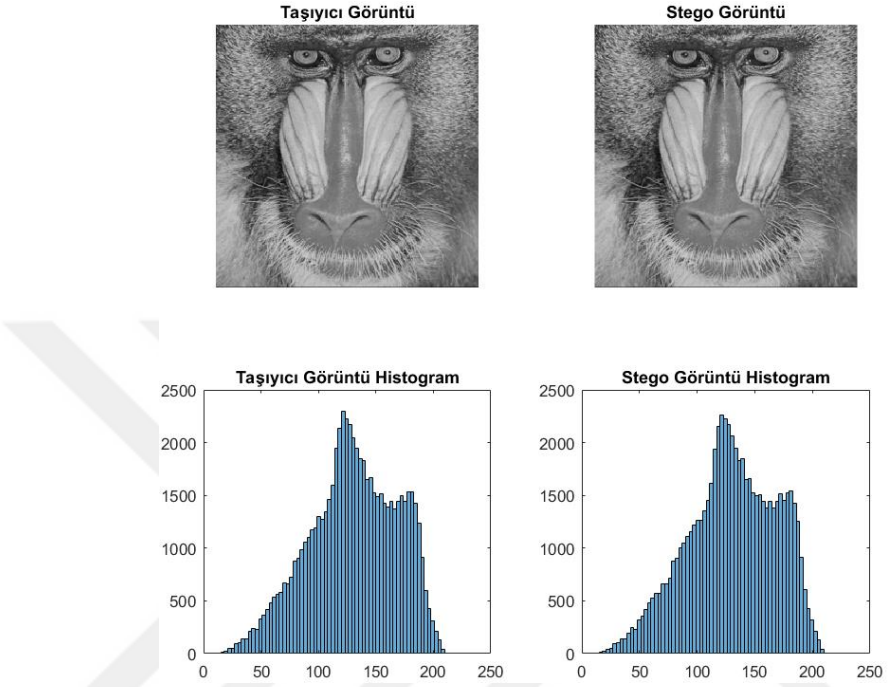
Gizli Veri (64x128)	Taşıyıcı Görüntü (256x256)	PSNR			SSIM			BER
		GA_LSB	Grad_LSB	LSB	GA_LSB	Grad_LSB	LSB	
Peppers	Baboon	51.2400	-	51.1385	0.9996	-	0.9993	0
Lake	Pirate	51.2311	-	51.1629	0.9995	-	0.9985	0
Livingroom	House	51.5096	-	51.1565	0.9988	-	0.9986	0
Cameraman	Pirate	51.2283	-	51.1017	0.9995	-	0.9984	0
Female	Zelda	51.2206	-	51.1533	0.9988	-	0.9978	0

Grad_LSB yönteminin, klasik LSB yönteminden daha güvenli olduğu ileri sürülse de, taşıyıcı görüntüdeki maksimum gradyan değerini bulmak ve bu değerdeki pikselleri kontrol etmek, iletişim ağındaki istenmeyen kişiler için zor değildir. Bu nedenle, kanal seçiminin genetik algoritma ile gerçekleştirilmesi gizli verinin çıkartılması için bir anahtar kullanma gerekliliği sağlamıştır. Anahtar olmadan, hangi kanalda verinin olduğu bilinemez. Bu da veriye güvenlik sağlamaktadır. Tüm taşıyıcı görüntü, gizli görüntü ve tüm gizleme kapasitelerinde yapılan uygulama sonuçları, önerilen GA_LSB tekniğine ait MSE hata değerlerinin klasik LSB tekniğine ait MSE değerlerinden daha düşük olduğunu göstermiştir (Tablo 4.6).

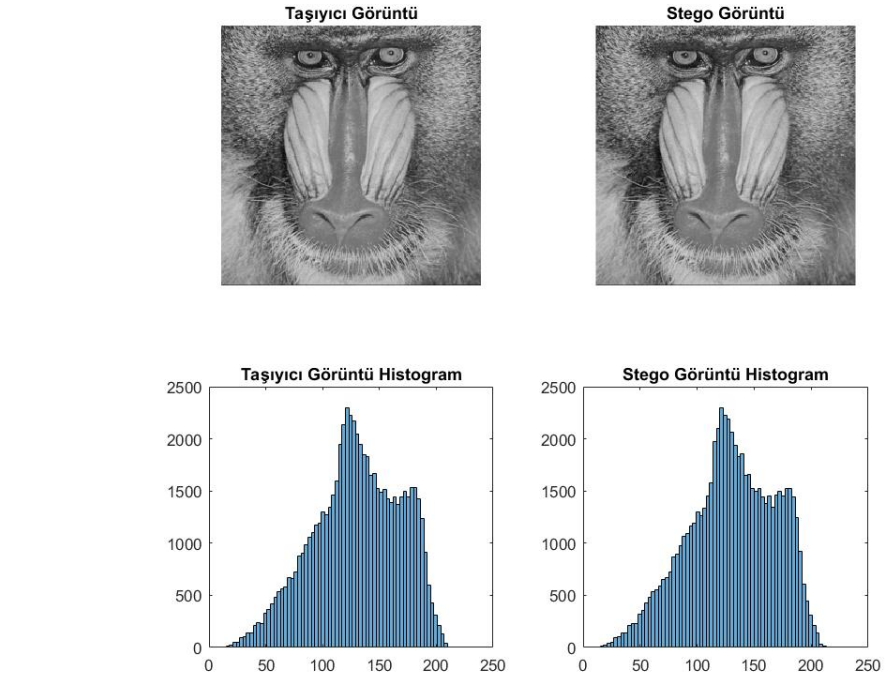
Tablo 4.6. MSE değerleri

Taşıyıcı Görüntü (256x256)	Gizli Veri		MSE	
			GA_LSB	LSB
Baboon	**16x32**	**Peppers**	0.0306	0.0314
	32x32		0.0606	0.0630
	32x64		0.1219	0.1258
	64x64		0.2447	0.2486
	64x128		0.4871	0.5003
Pirate	**16x32**	**Lake**	0.0306	0.0307
	32x32		0.0602	0.0630
	32x64		0.1217	0.1248
	64x64		0.2457	0.2491
	64x128		0.4897	0.4975
House	**16x32**	**Livingroom**	0.0309	0.0313
	32x32		0.0611	0.0627
	32x64		0.1216	0.1225
	64x64		0.2445	0.2498
	64x128		0.4893	0.4982
Pirate	**16x32**	**Cameraman**	0.0302	0.0307
	32x32		0.0605	0.0617
	32x64		0.1217	0.1253
	64x64		0.2456	0.2513
	64x128		0.4901	0.5046
Zelda	**16x32**	**Female**	0.0307	0.0308
	32x32		0.0610	0.0621
	32x64		0.1217	0.1252
	64x64		0.2446	0.2506
	64x128		0.4909	0.4986

Uygulama çalışmasının sonuçları klasik LSB yer değiştirme tekniği sonuçları ile kıyaslanmıştır. Uygulama sonuçlarının klasik LSB tekniğine göre daha iyi olduğu görülmektedir. Şekil 4.9. ve 4.10.'da aynı kapasitede gizli veri görüntüsüne sahip iki ayrı yöntemin taşıyıcı görüntü ve histogramı, stego görüntü ve histogramı verilmiştir.

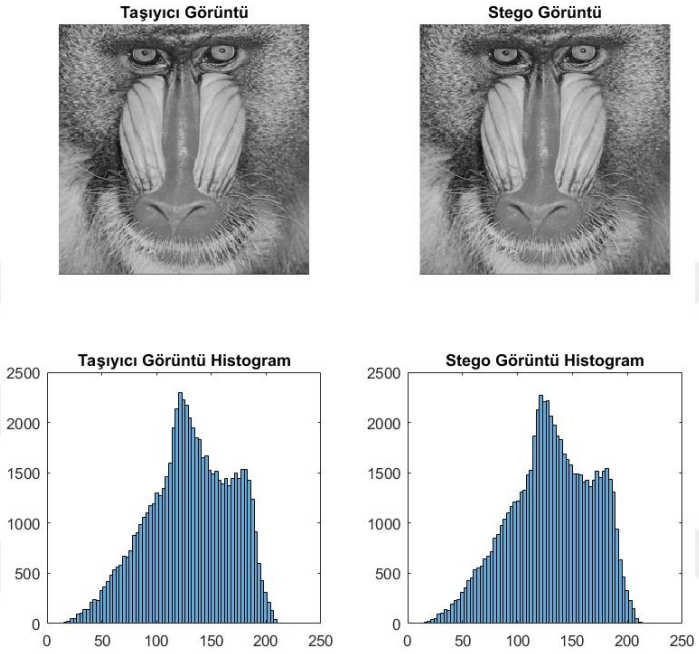


Şekil 4.9. Klasik LSB tekniği ile 32x64 gizli veri gizleme

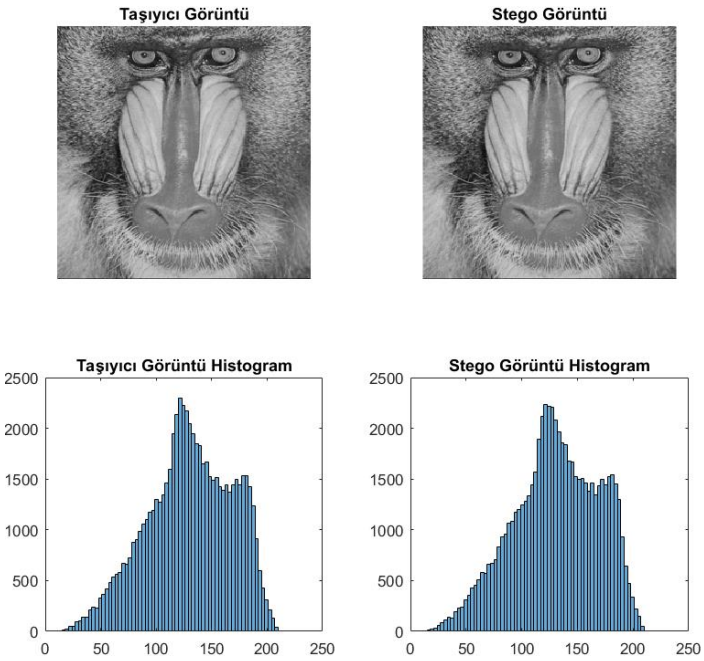


Şekil 4.10. GA_LSB tekniği ile 32x64 gizli veri gizleme

Şekil 4.11. ve 4.12.'de taşıyıcı görüntünün tüm piksellerinin son bitlerine gizli verinin yerleştirilmesiyle elde edilen sonuçlar verilmektedir. Klasik LSB tekniğinde taşıyıcı görüntü bitleri raster düzen ile taranıp gizli verinin bitleri ile değiştirilmiştir. GA_LSB tekniğinde ise GA'nın ürettiği kromozomun koordinatlarına göre taşıyıcı görüntü bitleri gizli veri bitleri ile değiştirilmiştir.



Şekil 4.11. Klasik LSB tekniği ile 64x128 gizli veri gizleme



Şekil 4.12. GA_LSB tekniği ile 64x128 gizli veri gizleme

5. SONUÇLAR VE ÖNERİLER

Steganografinin arkasındaki temel fikir, gizli verileri bir taşıyıcı medya içerisine tespit edilemeyecek şekilde gizleyebilmektir. İkilik tabandaki gizli veri seçilen bir algoritmaya göre taşıyıcı medya içerisine yerleştirilir. Aynı şekilde, veri gizleme algoritması içerisinde sadece gönderici ve alıcının bileceği bir anahtar değerine göre gizleme tekniği uygulanabilmektedir. Üretilen anahtar değer, yine taşıyıcı medyaya eklenerek alıcı tarafa ulaştırabilmektedir.

Bu tez çalışmasında, uzamsal alan görüntü steganografisinde GA ile kanal seçimi yapılmıştır. GA verinin gizleneceği pikselleri tespit ettikten sonra, gizleme tekniği olarak klasik LSB yer değiştirme tekniği kullanılarak taşıyıcı görüntünün sadece son bitlerine veri gizlenmiştir. Gönderici ve alıcı arasındaki iletişimde, verinin güvenliğini sağlamak için veri gizleme sürecinde anahtar kullanılmış ve anahtar boyutu çok küçük tutulmuştur.

Klasik LSB yer değiştirmede, gönderici ve alıcı tarafı dışındaki kişilerce gizli verinin alınması olasıdır. Bu güvenlik probleminin önüne geçilebilmesi için, klasik LSB tekniğindeki gibi, gizli veri bitlerini sıralı şekilde gizleme yerine, taşıyıcı görüntü önce 4x4 bloklara bölünmüş ve daha sonra bloklarda kanal seçimi uygulanmıştır. Genetik algoritma, gizlenecek verinin bitleri ile taşıyıcı görüntü bitlerini karşılaştırarak, taşıyıcı görüntüde en az değişim olacak kanalların seçimini yapmıştır.

Çalışma kapsamında her blokta, sırasıyla, 1,2,4,8 ve 16 piksel seçilerek veri gizleme teknikleri uygulanmıştır. Verinin kapasitesi arttırıldıkça anahtarın da uzunluğu artmaktadır. Ancak uygulama kapsamında en uzun anahtar 64 bit uzunluğundadır. Anahtarın boyutu büyük olmadığı için, taşıyıcı görüntünün son bitlerine veri gizlenirken, 2. LSB'lerine de anahtar gizlenmiştir. Anahtar, klasik LSB tekniği ile yani piksellere sıralı olarak yerleştirilmiştir. Alıcı anahtarı aldıktan sonra seçilen kanallardan veriyi kayıpsız şekilde geri alabilmektedir.

Uygulama tasarlanırken taşıyıcı görüntü olarak 256x256 piksel boyutunda gri ölçekli dijital görüntüler kullanılmıştır. Gizlenecek veri olarak da 16x32 piksel, 32x32 piksel, 32x64 piksel, 64x64 piksel ve 64x128 piksel boyutlarında gri ölçekli dijital görüntüler kullanılmıştır. Dijital görüntüler .tiff uzantılı görüntü dosyalarıdır.

Tüm gizleme işlemlerinde, önerdiğimiz GA_LSB tekniğine ait PSNR değerleri Grad_LSB ve klasik LSB tekniklerine ait PSNR değerlerinden daha yüksek çıkmıştır. SSIM değerleri karşılaştırıldığında ise, GA_LSB tekniğine ait SSIM değeri diğerlerine göre eşit veya daha yüksek bulunmuştur. Veri gizleme kapasitesi 0.007 bpp için ortalama PSNR değeri 63.26 dB, 0.015 bpp için ortalama PSNR değeri 60.29 dB, 0.031 bpp için ortalama PSNR değeri 57.27 dB, 0.0625 bpp için ortalama PSNR değeri 54.23 dB, 0.125 bpp için ortalama PSNR değeri 51.28 dB olarak hesaplanmıştır. BER değeri sıfır olarak elde edilmiş olup veri kaybı söz konusu olmamıştır.

Ayrıca, tüm taşıyıcı görüntü, gizli görüntü ve tüm gizleme kapasitelerinde yapılan uygulama sonuçları, önerilen GA_LSB tekniğine ait MSE hata değerlerinin klasik LSB tekniğine ait MSE değerlerinden daha düşük olduğunu göstermiştir.

Çalışmanın önemli noktalarından biri, verinin gizleme öncesi ve çıkartıldıktan sonra aynı olmasıdır. Veride herhangi bir kaybın bulunmamasıdır. Diğer bir husus ise, taşıyıcı görüntünün tüm bloklarına uygulanabilecek optimal bir kanal seçimi yapıldığı için, anahtar uzunluğu diğer çalışmalarda kullanılan anahtar uzunluklarından çok daha küçük bulunmuştur. Önerilen yöntem ile karmaşık bir anahtar yapısı kullanmadan klasik LSB tekniğine göre daha güvenli veri iletimi sağlanmıştır.

KAYNAKLAR

Amirtharajan, R., Rayappan, J. B. B. (2013). Steganography-time to Time: A review. *Research Journal of Information Technology*, *5*(2), 53-66.

Bedi, P., Bansal R., Sehgal, P. (2011). Using PSO in Image Hiding Scheme Based on LSB Substitution. *ACC 2011: Advances in Computing and Communications, 192.* Springer, 259-268.

Bender, W., Gruhl, D., Morimoto, N., Lu, A. (1996). Techniques for Data Hiding, *IBM Systems Journal*, *35*, 313-336.

Chen, S., K. (2011). A Module-Based LSB Substitution Method Eith Lossless Secret Data Compression. *Computer Standarts&Interfaces, 33*(4), 367-371.

Chan, C.K., Cheng, L.M. (2004). Hiding Data in Images by Simple LSB Substitution. *Patern Recognition, 37*(3), 469-474.

Chang, C.C., Hsiao, J.Y., Chan, C.S. (2003). Finding Optimal Leat-Significant-Bit Substitution in Image Hiding by Dynamiz Programming Strategy. *Pattern Recognition, 36*(7), 1583-1595.

Chang, K.C., Chang, C.P., Huang, P.S., Tu, T.M. (2008). A Novel Image Steganographic Method Using Tri-way Pixel-Value Diffrencing. *Journal of Multimedia, 3(2),* 37-44. DOI:10.4304/jmm.3.2.37-44

Chang, C.C., Chen, Y.H., Lin, C.C. (2009). A Data Embedding Scheme for Color Images based on Genetic Algorithm and Absolute Moment Block Truncation Coding. *Soft Comput 13***,** 321–331.

Cheddad, A., Condell, J., Curran, K., Mc Kevitt, P. (2010). Digital Image Steganography: Survey and Analysis of Current Methods. *Signal Processing, 90*(3), 727-752.

Crandall, R. (1998). Some Notes on Stegaography.

Çataltaş, Ö. (2018). Görüntü Steganografisinde Yeni Bir Yöntem. Yüksek Lisans Tezi, Selçuk Üniversitesi, Fen Bilimleri Enstitüsü, Konya, 489362.

Fridrich, J., Long, M. (2000). Steganalysis of LSB Encoding in Color Images. *IEEE International Conference on Multimedia and Expo. ICME2000. Proceedings. Latest Advances in the Fast Changing World of Multimedia, 3*,1279-1282.

Fridrich, J., Goljan, M., Du R. (2001). Detecting LSB Steganography in Color, and Gray-Scale Images. *IEEE Multimedia, 8* (4), 22-28.

Fridrich, J., Goljan, M., Hogea, D. (2002). Steganalysis of JPEG Images: Breaking the F5 Algorithm. F.A.P (Ed.), *International Workshop on Information Hiding*, 310-323. Berlin: Springer.

Fridrich, J., Soukal, D. (2006). Matrix Embedding for Large Payloads. *IEEE Transaction on Information Forensics and Security, 1* (3), 390-395.

Ghasemi, E., Shanbehzadeh, J. (2010). An Imperceptible Steganographic Method based on Genetic Algorithm. *2010 5th International Symposium on Telecomminications,* Tahran, İran, 04-06 Aralık 2010.

Goldberg, D.E. (1989). *Genetic Algorithms in Search, Optimization and Machine Learning.* Boston: Addison-Wesley Publishing Company Inc.

Gu, X., Sun, Y. (2018). Image Transformation and Information Hidig Technology based on Genetic Algorithm. *EURASIP Journal on Image and Video Processing, 115.*

Hassan, M.D. (2008). Steganaliz Yaklaşımlarının Karşılaştırılması. Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Ankara, 233706.

Holland, J.H. (1975). Adaptation in Natural and Artificial Systems. Ann Arbor AMichigan: University of Michigan Press,

Hussain, M., Wahab, A.W., Idris, Y.I.B., Ho, A.T.S., Jung, K.H. (2018). Image Steganography in Spatial Domain: A Survey. *Signal Processing: Image Communication, 65,* 46-66.

Judge, J. C. (2001). Steganography: Past, Present, Future. *SANS white paper, 30.*

Kadhim, I.J., Premaratne, P., Vial, P.J., Halloran, B. (2019). Comprehensive Survey of Image Steganography: Techniques, Evaluations, and Trends in Future Research. *Neurocomputing, 335,* 299-326.

Kahn, D. (1996). The History of Steganography. Anderson, R. (Ed.), *Information Hiding, Lecture Notes in Computer Science, 1174,* Berlin: Springer.

Kanan, H.R., Nazeri, B. (2014). A Novel Image Steganography Scheme with High Embedding Capacity and Tunable Visual Image Quality Based on a Genetic Algorithm. *Expert Systems with Applications, 41*(14), 6123-6130.

Khodaei, M., Faez, K. (2010). Image Hiding by Using Genetic Algorithm and LSB Substitution. *ICISP 2010, Lecture Notes in Computer Science, 6134,* 404-411.

Kodovský, J., Fridrich, J. (2008). Influence of Embedding Strategies on Security of Steganographic Methods in the JPEG Domain. *In Security, Forensics, Steganography, and Watermarking of Multimedia Contents X , 6819,* 681902. International Society for Optics and Photonics.

Kumar, S., Upadhyay, A.K., Dubey, P., Varshney, S. (2021). Comparative Analysis for Edge Detection Techniques. *2021 International Conference on Computing, Communication, and Intelligent Systems,* Greater Nodia, Hindistan, 19-20 Şubat 2021.

Lee, Y.K., Chen, L.H. (2000). High Capacity Image Steganographic Model. *IEEE Proceedings Image and Signal Processing, 147*(3), 288-294.

Li, X., Yang, B., Çeng, D., Zeng, T. (2009). A Generalization of LSB Matching. *IEEE Signal Precessing Letter, 16*(2), 69-72.

Nabiyev, V.V. (2016). *Yapay Zeka* (5). Seçkin Teknik, Ankara: Seçkin Yayıncılık.

Nosrati, M., Hanani, A., Karimi, R. (2015). Steganography in Image Segments Using Genetic Algorithm. *2015 fifth International Conference on Advanced Computing & Communication Technologies,* Haryana, Hindistan, 21-22 Şubat 2015.

Nguyen, T.D., Arch-int, S., Arch-int, N. (2015). A Novel Secure Channel Selection Rule for Spatial Image Steganography. *2015 12th International Joint Conference on Computer Science and Software Engineering (JCSSE),* Songkhla, Tayland, 22-24 Temmuz 2015.

Nguyen, T.D., Arch-int, S., Arch-int, N. (2015). A Novel Secure Block Data-Hiding Algorithm Using Cellular Automata to Enhance the Performance of JPEG Steganography. *Multimed Tools Application, 74,* 5661-5682.

Nguyen, T.D., Arch-int, S., Arch-int, N. (2016). An Adaptive Multi Bit-Plane Image Steganography Using Block Data-Hiding. *Multimed Tools Application, 75,* 8319-8345.

Okkalı, A. (2013). Genetik Algoritmalar ile Aydınlatma Hesabı Optimizasyonu. Yüksek Lisans Tezi. Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü, Kocaeli, 342554.

Pevny, T., Fridrich, J. (2008). Detection of Double-Compression in JPEG Images for Aplications in Steganography. *IEEE Transactions on Information Forensics and Security, 3*(2), 247-258.

Raggo, M., Hosmer, C. (2013). *Data Hiding Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols.* Elsevier. USA: Waltham.

Rajendran, S. ve Doraipandian, M. (2017). Chaotic Map Based Random Image Steganography Using LSB Technique. *International Journal of Network Security, 19* (4), 593-598.

Sethi, P., Kapoor, V. (2016). A Proposed Novel Architecture for Information Hiding in Image Steganography by Using Genetic Algorithm and Cryptography. *Procedia Computer Sicence, 87,* 61-66.

Setiadi D.,R.,I.,M. (2022). Improved Payload Capacity in LSB Image Steganography Uses Dilated Hybrid Edge Detection. *Journal of King Saud University-Computer and Information Sciences, 34* (2), 104-114.

Sabeti, V., Samavi, S., Shirani, S. (2012). An Adaptive LSB Matching Steganography Based on Octonary Complexity Measure. *Multimedia Tools and Applications, 64*(16), 777-793.

Sarı, Z., Yıldırım, M. (2022). Uzamsal Alan Görüntü Steganografisi için Blok Veri Gizlemede Kanal Seçimi. *Avrupa Bilim ve Teknoloji Dergisi, Ejosat Special Issue 2022 (ICAENS-1), 34,* 305-310.

Sayood, K. (1996). *Introduction to Data Compression,* (3rd ed.). USA: San Francisso, Elsevier.

Simmons, G.J. (1984). The Prisoners' Problem and the Subliminal Channel. In: Chaum, D. (eds) Advances in Cryptology. Springer, Boston: MA.

Siper, A., Farley, R., Lombardo, C. (2005). The Rise of Steganography. *Proceedings of student/faculty research day,* CSIS, Pace University.

Shah, P.D., Bichkar, R.S. (2018). A Secure Spatial Domain Image Steganography Using Genetic Algorithm and Linear Congruential Generator. Dash, S., Das, S., Panigrahi, B. (Ed) *International Conference on Intelligent Computing and Applications. Advances in Intelligent Systems and Computing, 632,* 119-129. Springer, Singapore.

Shah, P.D., Bichkar, R.S. (2020). Genetic Algorithm based Approach to Select Suitable Cover Image for Image Steganography. *2020 International Conference for Emerging Technology (INCET),* Balgaum, Hindistan, 05-07 Temmuz 2020.

Shah, P.D., Bichkar, R.S. (2021). Secret Data Modification based Image Staganography Technique Using Genetic Algorithm Having a Flexible Chromosome Structure. *Engineering Science and Technology, an International Journal, 24*(3), 782-794.

Shyla, M.K., Kumar, K.B.S., Das R.K. (2021). Image Steganography Using Genetic Algortihm for Cover Image Selection and Embedding. *Soft Computing Letter, 3.*

Sugathan, S. (2016). An Improved LSB Embedding Technique for Image Steganography. *2016 2nd Internation Conference on Applied and Theoretical Computing and Communication Technology(iCATccT),* Bangalore, Hindistan, 21-23 Temmuz 2016.

Sutaone, MS., Khandare OG. (2008). Image Based Steganography using LSB Insertion Technique. *2008 IET Interonational Conference on Wireless, Mobile and Multimedia Networks,* Beijing, 11-12 Ocak 2008.

Şahin, A. (2007). Görüntü Steganografide Kullanılan Yeni Metodlar ve Bu Metodların Güvenirlikleri. Doktora Tezi, Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Edirne, 199963.

Thien, C.C., Lin, J.C. (2003). A Simple and High-Hiding Capacity Method for Hidng Digit-by-Digit Data in Images Based on Modulus Function. *Pattern Recognition, 36*(12), 2875-2881.

Wang, Z., Simoncelli, E.P., Bovik, A.C. (2003). Multiscale Structural Similarity For Image Quality Assessment. *The Thirty-Seventh Asilomar Conference on Signals & Computers,* Pacific Grove, USA, 09-12 Kasım 2003.

Wang, S., Yang, B., Niu, X. (2010). A Secure Steganography Method based on Genetic Algorithm. *Journal of Information Hiding and Multimedia Signal Processing. 1*(1), 28-35.

Wang, Y., Tang, M., Wang, Z. (2020). High-capacity Adaptive Steganography Based on LSB and Haming Code. *Optik, 213.*

Westfeld, A. (2001). F5 A Steganographic Algorithm High Capacity Despite Better Steganalysis. Moskowitz, I.S. (Ed.) *Information Hiding. Lecture Notes in Computer Science, 2137,* (289-302). Berlin: Springer.

Yang, X.S. (2021). Chapter 6- Genetic Algorithms. Yang, X.S. (Ed.), *Nature-Inspired Optimization Algorithms* (2nd ed.), 91-100. UK, London: Academic Press.

Yıldırım, M. (2003). Genetik Algoritmalar ve Benzetilmiş Tavlama ile Uzun Dönem Üretim Genişletme Planlaması. Doktora Tezi, Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü, Kocaeli, 135971.

Zaker, N., Hamzeh, A. (2012). A Novel Steganalysis for TPVD Steganographic Method Based on Differences of Pixel Difference Histogram. *Multimed Tools Appl*, *58*, 147–166.

URL-1: https://sipi.usc.edu/database/, (Erişim Tarihi: 25 Mart 2022).

URL-2:https://www.widen.com/blog/whats-the-difference-between-png-jpeg-gif-and-tiff , (Ziyaret Tarihi: 24 Nisan 2022).

URL-3: https://en.wikipedia.org/wiki/Edge_detection, (Erişim Tarihi: 26 Nisan 2022).

KİŞİSEL YAYIN VE ESERLER

Sarı, Z., Yıldırım, M. (2022). Uzamsal Alan Görüntü Steganografisi için Blok Veri Gizlemede Kanal Seçimi. *Avrupa Bilim ve Teknoloji Dergisi, Ejosat Special Issue 2022 (ICAENS-1), 34,* 305-310.

ÖZGEÇMİŞ

Lise öğrenimini İzmir'de tamamladı. 2009 yılında Çukurova Üniversitesi Kozan Meslek Yüksekokulu Bilgisayar Teknolojisi ve Programlama önlisans programından mezun oldu. 2014 yılında girdiği Kocaeli Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü'nden 2020 yılında mezun oldu. Ardından Kocaeli Üniversitesi Bilişim Sistemleri Mühendisliği bölümünde yüksek lisans eğitimine başladı. Yüksek lisans eğitiminde Genetik Algoritma ile Görüntü Steganografisi konusunda çalışmaları bulunmaktadır.

2011-2016 yılları arasında Erzincan Binali Yıldırım Üniversitesi'nde Bilgisayar İşletmeni olarak ve 2016-2021 yılları arasında Kocaeli Üniversitesi'nde Bilgisayar İşletmeni olarak görev yaptı. 2021 yılından beri Kocaeli Üniversitesi Teknoloji Fakültesi Bilişim Sistemleri Mühendisliği Bölümü'nde Araştırma Görevlisi olarak çalışmaktadır.