Araştırma Makalesi

GÖRÜNTÜLER İÇİN ALFA KANALINI MASKELEYEREK VERİ GİZLEME TEKNİĞİ VE UYGULAMASI

Mehmet ŞANVEREN†, Mustafa Cem KASAPBAŞI††

† İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Ana Bilim Dalı, İstanbul, Türkiye

††İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Ana Bilim Dalı, İstanbul, Türkiye

mehmetsanveren1029@gmail.com, mckasapbasi@ticaret.edu.tr

0009-0002-6920-9390, 0000-0001-6444-6659

Atıf/Citation: ŞANVEREN, M., KASAPBAŞI, M. C., (2023). Görüntüler İçin Alfa Kanalını Maskeleyerek Veri Gizleme Tekniği ve Uygulaması, Journal of Technology and Applied Sciences 6(2) s.21-35, DOI: 10.56809/icujtas.1328818

ÖZ

Dijital görüntüler günümüzde büyük bir değer taşımaktadır. İnternetin yaşam kaynaklarımızı desteklediği hızlı iletişim çağında iletişim oldukça önemli hale gelmiştir. Bu bağlamda, veri iletişimi ve transferi konularında birtakım çalışmalar yapılmıştır. Gerçekleştirilen saklı veri transferler tekniklerine steganografi adı verilir. Steganografi, gizli mesajların çeşitli teknikler kullanılarak taşıyıcı nesnelerde saklandığı bir yöntemdir. Bu taşıyıcı nesneler, görüntü, ses, video veya metin gibi dosya türlerinden oluşabilir ve içerisinde gizli mesajlar barındırabilir. Eğer gizli mesaj, taşıyıcı nesne üzerinde görsel olarak fark edilmeyecek bir şekilde saklanıyorsa, bu yönteme görüntü steganografisi denir. Bu çalışmada, görüntüler üzerindeki veri gizleme teknikleri üzerinde durulmuş ve yeni bir uygulama geliştirilmiştir. C# programlama dili kullanılarak kodlama yapılmıştır. En Düşük Değerlikli bit (LSB-Least Significant Bit) tekniği, RGB kanallarının yanı sıra alfa kanalını da (R, G, B, A) kullanmaktadır. Çalışmanın yapısının ve kalite başarısının testini gerçekleştirmek amacıyla MATLAB ortamında kodlama yapılarak, Tepe Sinyal Gürültü Oranı (PSNR-Peak Signal to Noise Ratio), Ortalama Karesel Hata (MSE-Mean Squared Error), Yapısal Benzerlik İndeksi (SSIM-Structural Similarity Index), ve entropi testleri gerçekleştirilmiştir. Elde edilen sonuçlar değerlendirildiğinde, insan gözüyle fark edilemeyen bir durumu ve kalite ölçümlerinin literatür değerlerine uygun şekilde başarılı olduğunu göstermektedir. Bu çalışma, arka planı şeffaf olan resimler için başarılı bir şekilde kullanılabilecek bir teknik sunmaktadır. Mahremiyet ve gizli iletişim konularında alınan önlemler göz önüne alındığında, bu çalışmanın görsel steganografiye katkı sağlayarak arka planı şeffaf olan resimlerde yaşanan problemlere çözüm getireceği düşünülmektedir.

Anahtar Kelimeler: LSB, Steganografi, Veri Gizleme, Görsel Steganografi

DATA HIDING TECHNIQUE AND ITS APPLICATION BY MASKING THE ALPHA CHANNEL FOR IMAGES

ABSTRACT

Digital images are of great value today. Communication has become very important in the age of fast communication, when the Internet supports our life resources. In this context, a number of studies have been conducted on data communication and transfer issues. The stored data transfer techniques performed are called steganography. Steganography is a method by which hidden messages are stored in carrier objects using various techniques. These carrier objects can consist of file types such as images, audio, video, or text, and may contain hidden messages inside. If the hidden message is stored on the carrier object in such a way that it is not visually noticeable, this method is called image steganography. In this study, data hiding techniques on images were focused on and a new application was developed.

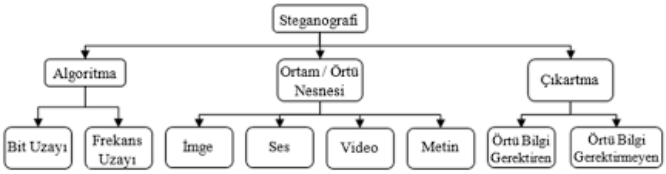
Geliş/Received : 17.07.2023
Gözden Geçirme/Revised : 25.07.2023
Kabul/Accepted : 28.07.2023

Coding has been done using the C# programming language. The Least Significant bit (LSB) technique uses the alpha channel (R, G, B, A) as well as the RGB channels. In order to test the structure and quality achievement of the study, PSNR (Peak Signal to Noise Ratio), MSE (Mean Squared Error), SSIM (Structural Similarity Index), and entropy tests were performed by coding in MATLAB environment. When the results obtained are evaluated, it shows a condition that cannot be noticed by human eyes and that the quality measurements are successful in accordance with the literature values. This study presents a technique that can be successfully used for paintings with a transparent background. Considering the measures taken on the issues of privacy and confidential communication, it is thought that this study will provide solutions to the problems experienced in pictures with transparent background by contributing to visual steganography.

Keywords: LSB, Steganography, Data Hiding, İmage Steganography

1. GİRİŞ

Steganografi, gizli bir mesajı bir örtü nesnesine saklayarak karşı tarafa iletme uygulamasıdır. Başka bir ifade ile steganografi, bir mesajın herhangi bir dosya içerisine gömülerek karşı taraftaki iletilen kişinin veya dışarıdan erişim sağlamaya çalışan kişinin anlamayacağı şekilde veri iletişim yöntemidir. Steganografi bilgi gizleme yöntemlerinin önemli bir dalı olarak ifade edilir. Tarihte yaşamış olan bir çok kavim yaşantıları boyunca, iletişim için güvercinleri kullanmak, kadınların küpelerine nakış işlemek ve harf noktalarının vuruşlarını değiştirmek gibi farklı bir çok teknik kullanmıştır. "Steganografi" kelimesinin mucidi Johannes Trithemius'dir (Syndics of Cambridge University Library). Stego görüntünün görüntü kalitesi, kontrol sonucu, stego görüntü üretilene kadar asla bilinmez. Aslında steganografinin temeli, iletişimle başlamıştır. Çünkü doğadaki var olan her canlı tıpkı insanlar gibi iletişim kurarlar. Steganografi insanlar veya nesneler arasındaki gerçekleşen iletişimi sadece iletişim kuran kişilerin anlayacağı hale bürünmesi için gerekli ortamı hazırlamaktır. Steganografi ile ilgili tarihteki örneklere bakacak olursak, belki de en iyi bilinen yöntemi geçmiş dönemlerde kullanılan görünmez ismini verdikleri mürekkeptir. Tarih boyunca insanlar birbirleri ile iletişim kurabilmek adına sayısız yöntemler denemiş ve bu yöntemlerde sirke, bal, şeker gibi sıvılarda kullanmışlardır. Bazı dönemlerde kölelere dövme yapılarak iletişim sağlanmıştır. İnsanoğlu var oluşundan beri iletişim ihtiyacı hissetmiştir. Günümüzde ultra mega boyutlarda teknikler ve algoritmalar geliştirilmiştir. Bir çok farklı yazılım dilinde stego araçları geliştirilebilir ve bu teknikler ile resimler farklı algoritmalara dahil edilerek saklanabilmektedir. Veri gizleme, temel bir ifadeyle Steganografi (Kadhim vd., 2019) ve Filigran (Petitokolas vd., 1999, Wan vd., 2022). olmak üzere ikiye ayrılır.



Şekil 1. Steganografi Algoritması

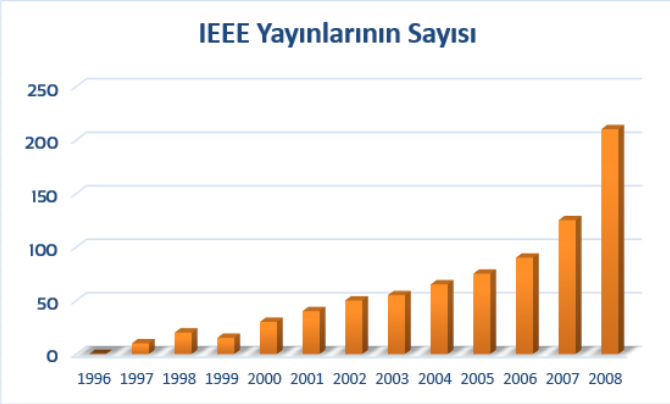
Steganografi, 1978'de Viktor Korchnoi ile Anatoly Karpov arasında gerçekleşen Dünya Satranç Şampiyonluğu maçında tartışma konusu haline gelmiştir. (Jessica, 2007). Bir maçta, Karpov'un yardımcıları ona yoğurtlu bir tepsi uzattı. Bu, oyun sırasında oyuncu ile takımı arasındaki iletişimi yasaklayan kurallara aykırı bir davranıştı. Korchnoi'nin heyetinin başkanı Petra Leeuwerik, Karpov'un ekibinin gizli mesajlar ilettiğini iddia ederek hemen itiraz etmiştir. Örneğin, mor bir yoğurt, Karpov'un beraberlik teklif etmesi gerektiği anlamına gelebilirken, dilimlenmiş bir mango, oyuncunun beraberliği reddetmesi gerektiğini ifade edebilirdi. Yemek servisi zamanlaması da ek mesajların iletilmesi için kullanılabilirdi (Gonzalez, 2007).

Bu çalışmada, LSB algoritmalarına katkıda bulunmak amacıyla PNG görüntü formatları üzerinde arka planı şeffaf olan resimler için yeni bir algoritma geliştirilmiştir. Geliştirilen bu algoritma arka planı şeffaf olan PNG görüntüler için alfa kanalı üzerinde maskeleme yaparak, steganografi tekniklerinden en düşük değerlikli bit (LSB), tekniğinin başarılı bir şekilde kullanılabildiğini göstermektedir.

Geliştirilen algoritmanın başarısını test etmek amacıyla performans metrikleri ve analizleri yapıldığında teorik değerler elde edilmiştir. Bölüm 3'te dijital görüntülerden ve R,G,B,A kanallarından bahsedilmiştir. Geliştirilen algoritmanın adımlarına yer verilmiştir. Tartışma kısmında, literatürde yer alan ve önerilen algoritmada kullanılan tekniğin birebir aynısı olmaması sebebiyle en yakın çalışmalar baz alınmış, bu çalışmaların karşılaştırılması yapılmıştır. Son bölümde ise sonuçlardan ve gelecekte yapılacak olan çalışmalardan bahsedilmiştir.

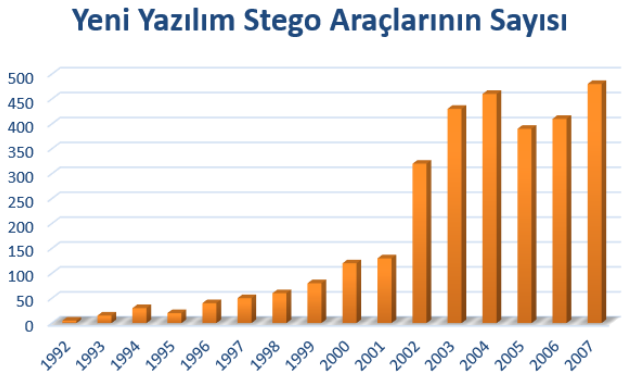
2. LİTERATÜR TARAMASI

Dijital görüntü, piksel adı verilen küçük resim elemanlarının matematiksel değerlerle temsil edildiği bir 2B veya 3B görsel nesnelerden oluşmaktadır. Her piksel, genellikle bir matris veya dizi içinde konumlandırılır ve bir gri tonlama veya renk değeriyle ilişkilendirilir. Renkli görüntülerde yaygın olarak kullanılan renk modeli RGB'dir. RGB, kırmızı (Red), yeşil (Green) ve mavi (Blue) bileşenlerin birleşiminden oluşan bir renk uzayıdır. Her pikselin RGB değeri, bu üç bileşenin yoğunluklarını belirtir. Genellikle 8 bit kullanılarak, her bileşen 0 ile 255 arasında bir sayıyla temsil edilir. Örneğin, beyaz renk (255, 255, 255) olarak temsil edilirken, siyah renk (0, 0, 0) olarak temsil edilir. Bunun yanı sıra, gri tonlamalı görüntüler sadece parlaklık değerini içerir. Gri tonlamalı bir pikselin parlaklık değeri genellikle 0 ile 255 arasında bir sayıdır, 0 siyahı temsil ederken 255 beyazı temsil eder. Dijital görüntüler, çeşitli işlemlere tabi tutulabilir. Örneğin, filtreleme, kesme, yeniden boyutlandırma, dönüşüm veya kompresyon gibi işlemler dijital görüntü işlemeyle gerçekleştirilebilir. Görüntüler ayrıca farklı dosya formatlarında (JPEG, PNG, GIF, BMP vb.) saklanabilir ve iletişim için kullanılabilir. Dijital görüntü teknolojisi, bilgisayarlı görüntü, video oyunları, medya yayıncılığı, sinema, tıbbi görüntüleme ve daha birçok alanda geniş bir uygulama alanına sahiptir (Johnson, 2008). Görmüş olduğumuz renkli dijital görüntüler bir takım piksellerden ve bu pikselleri temsil eden bir takım kodların birleşmesi ile meydana gelmektedir. Oluşan bu renkleri tanımlamak için kullanılan matematiksel modellere ve bütün renkleri temsil edecek şekilde oluşturulmasına genel olarak renk modeli denilmektedir (Yılmaz, 2002). Dijital görüntüler genellikle raster, palet, dönüşüm ve vektör olmak üzere dört temel biçimde temsil edilir. Günümüzde doğal görüntülerin en yaygın temsili olan popüler transform-domain formatı PNG ve JPEG'tir. Steganografi alanında gerçekleştirilen çalışmaların yıllara göre istatistikleri Şekil 2, Şekil 3 ve Şekil 4'de sunulmuştur.



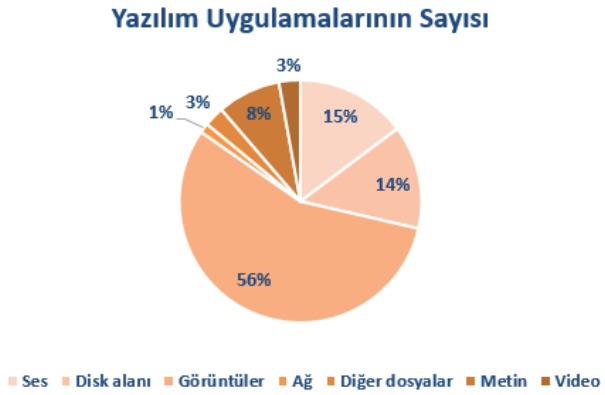
Şekil 2. Steganografi Anahtar Kelimeleri İçeren Yayınların Sayısı

Şekil 2'de her yıl yayınlanan ve "steganografi" veya "steganaliz" anahtar kelimelerini içeren makalelerin sayısı, alanın büyümesine tanıklık etmektedir (Jessica, 2007,a).



Şekil 3. Stego Araçlarının Sayısı

Şekil 3'de Dijital ortamda ve metinde veri saklayabilen yeni çıkan uygulamaların veya mevcut programların yeni sürümlerinin sayısını göstermektedir. (Jessica, 2007,b).



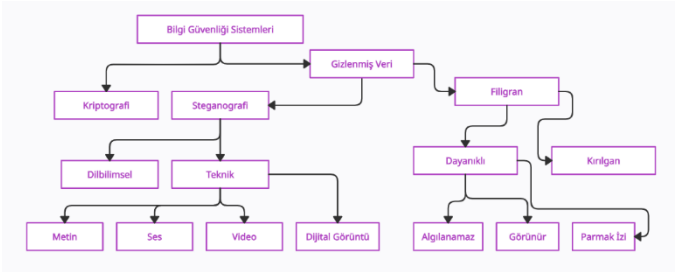
Şekil 4. Stegonagrafi Yazılım Uygulamalarının Sayısı

Şekil 4'de Haziran 2008 itibariyle elektronik ortamda veri saklayabilen steganografik yazılım uygulamalarının sayısı (Jessica, 2007,c).

Görüldüğü gibi steganografi kelimesini içeren yayınlar ve araçlar 90'lı yıllardan 2008 yılına kadar ciddi bir artış göstermiş, sonrasında ise günümüze kadar neredeyse sayılamayacak kadar çok artmıştır. Steganografi bir çok alanda veri gizleme amacıyla kullanılır. Watermarking, dijital içeriklere benzersiz bir kimlik veya sahiplik bilgisi eklemek için kullanılan bir yöntemdir. Watermarking, genellikle telif hakkı koruması veya sahtecilik tespiti gibi amaçlarla kullanılır. Watermark, içeriğin üzerine eklenen veya gömülen bir imza, logo veya metin şeklinde olabilir.

Watermark, genellikle açıkça görünür veya algılanabilir bir şekilde eklenir ve içeriğin sahipliğini veya orijinalliğini göstermek için kullanılır. Steganografi ise, gizli mesajların başka verilerin içine saklandığı bir yöntemdir. Steganografi, mesajın varlığını gizlemek için medya dosyalarını (görüntü, ses, metin) kullanır. Mesaj, taşıyıcı veriye gömülerek veya üzerine eklenerek saklanır ve genellikle insan algısı için göze veya kulağa çarpmayan bir şekilde gerçekleştirilir. Steganografi, mesajın gizliliğini sağlamak ve iletişimdeki taraflar arasında güvenli bir şekilde bilgi paylaşımı yapmak için kullanılır (Cox I., Miller J. 2002).

Görüntü işleme konferansı (ICIP) ve multimedya ve güvenlik çalıştayı (ACM) 1996'da Cambridge'de ilk Bilgi gizleme çalıştayı düzenlendi ve o zamandan beri bu çalıştaylar dizisi, veri gizleme teorisi ve uygulamalarında en son gelişmeleri sunmak için birinci sınıf yıllık toplantı yeri haline gelmiştir (Jessica, 2007, ICIP 2022). Stego dosyasının silinmesi veya algoritmasına müdahale edilmesi durumunda gizli bilgilerin kaybolacağını unutmamak önemlidir (Morkel, et al., 2005).



Şekil 5. Detaylı Steganografi Görseli

Telif hakkı korumasının artan önemi nedeniyle, filigran tekniği birçok araştırmacının ilgisini çekmektedir. Bilgisayar uzmanları ve güvenlik araştırmacıları, steganografinin yasadışı kullanımının bir tehdit haline gelebileceğini belirtmişlerdir. Steganografi teröristlerin gizlice iletişim kurmasına kolluk kuvvetlerinin bundan haberi olmadan izin verebilir. Bu tehdit nedeniyle, araştırmacılar mevcut steganografi sistemlerinde kusurları bulmayı hedeflemişlerdir (Kovaçiç & Jones, 2002).

İnternette 1 dakikada neler olduğu sorusu aslında steganografi için de oldukça önem arz etmektedir. Çünkü bu istatiksel çalışmaya göre hangi alanda yoğun kullanım olduğunu tespit edebiliriz.

Şekil 6. İnternette 1 Dakikada Gerçekleşen Değişim (Navarra, 2022).

E-mail: 231 milyon, Yazı: 16 milyon, Google: 5.9m arama, Snapchat: 2.4m snap Facebook: 1.7m gönderi, Tinder: 1.1m swipes, Twitter: 347k twit, Instagram: 66k Fotoğraf, YouTube video yükleme süresi: 500 saat

İnternette 1 dakikada gerçekleşen muazzam bir veri akışı tablosu yukarıda sunulmuştur.
Şekil 6'da yer alan istatistiklere istinaden değerlendirme yapıldığında, veri iletişimi günümüz için muazzam şekilde ilerlemiştir. Bu ortamda veri güvenliğinin önemi artmakla beraber, güvenlik zaafiyeti sonucunda çok ciddi kayıplar yaşanabilmektedir. Veri gizleme tekniklerinden biri olan steganografi veri güvenliğinde de önemli bir değer taşımaktadır.

3. MATERYAL VE METOT

Bu bölüm, çalışmada kullanılan R,G,B ve Alfa kanalını kısaca gözden geçirmektedir.

3.1. Dijital Görüntülerde R,G,B ve Alfa Kanalı

Steganografi, bilgi veya veri gizlemenin bir yöntemidir ve çeşitli taşıyıcı ortamların içine gizli mesajları yerleştirme işlemidir. RGB (Red, Green, Blue) renk modeli, piksellerin kırmızı, yeşil ve mavi bileşenlerini kullanarak renklerin oluşturulduğu bir modele işaret eder.

Alfa kanalı ise bir renk modelindeki dördüncü bir bileşendir ve genellikle opaklık seviyesini temsil eder. Alfa kanalı, bir pikselin ne kadar saydam veya opak olduğunu belirler. Bu kanal, görüntülerin yarı saydam piksellerini ve görüntü üzerine eklenmiş olan katmanları kontrol etmek için kullanılır (Ghaith, 2014).

Steganografi genellikle görüntü dosyalarında kullanılan bir yöntemdir ve RGB renk modeli ile birlikte Alfa kanalı da görüntülerin saklanan mesajları taşımak için maskeleme yapılarak kullanılabilir. Görüntüdeki piksellerin her bir bileşeni (RGB) ve Alfa kanalı, gizli mesajı saklamak için kullanılabilecek değerleri temsil edebilir. Bu şekilde, görüntü dosyasının görünümünde çok az fark oluşturularak gizli mesajı taşıyabilirsiniz.

Alfa kanalı, bir renk modelinde dördüncü bir bileşendir ve genellikle opaklık veya saydamlık seviyesini temsil eder. İngilizce "Alfa channel" terimi, görüntü işleme ve grafik tasarım alanlarında sıklıkla kullanılır. Bir pikselin opaklık düzeyini belirtmek için 0 ile 255 arasında değerler kullanır. Bu değerler, pikselin tamamen saydam (0) veya tamamen opak (255) olduğunu gösterebilir. Aradaki değerler, kısmi saydamlık veya yarı saydamlık oluşturmak için kullanılabilir.

Alfa kanalı, genellikle RGBA renk modeliyle birlikte kullanılır. RGBA, Red (kırmızı), Green (yeşil), Blue (mavi) ve Alfa (opaklık) bileşenlerini temsil eder. Bu renk modeli, özellikle transparan (saydam) görüntülerin veya katmanların kullanıldığı grafik tasarım ve görüntü işleme uygulamalarında sıkça kullanılır.

RGBA, RGB renk modelini alfa değeriyle genişletir. Alfa kanalı 1971'de "Catmull" ve "Smithin" tarafından icat edilmiştir (Alvy, 1995). Görüntüdeki her pikselde saydamlık için ayrılmış bir veri bölümü vardır.Bir görüntüdeki saydamlığı ve opaklığı kontrol eden bilgi, alfa kanalıdır. Görüntülerdeki her piksele ayrı ayrı uygulanır ve pikselin çevreleyen piksellerle nasıl birleştiğini ve arka plana ne kadar karıştığını kontrol etmek için kullanılır. Alfa kanalı, görüntünün veya katmanın yalnızca belirli bir bölümünün görünmesini sağlayarak karmaşık görüntü efektleri oluşturabilir ve daha esnek bir görüntü düzenlemesi imkanı sunar.

4. ŞİFRELEME İÇİN ÖNERİLEN ALGORİTMA

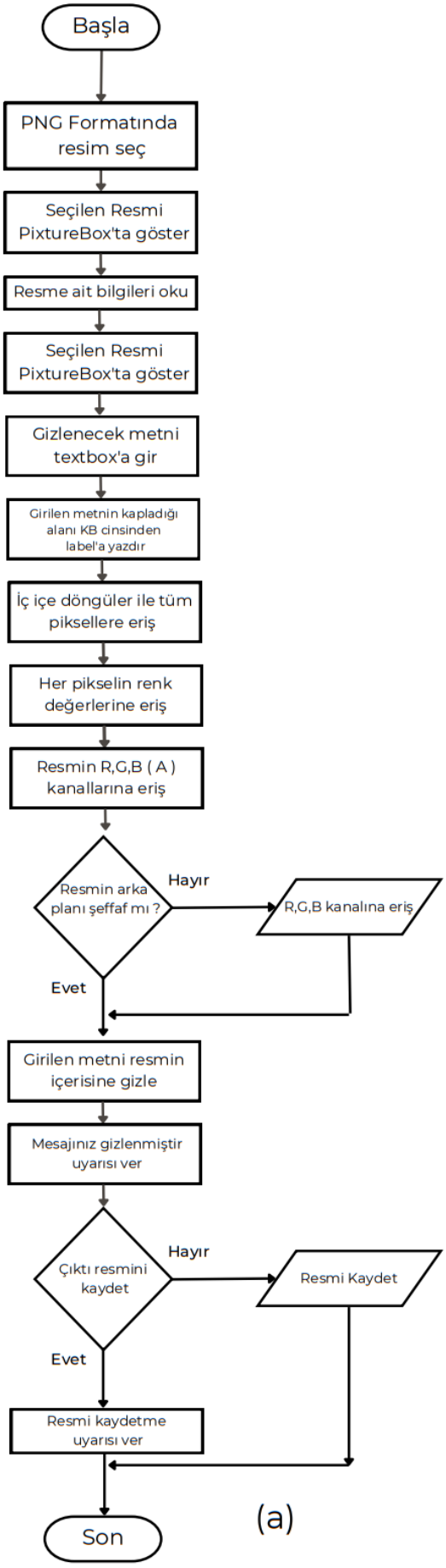
Bu makalede görüntü şifreleme işleminde kullanılacak teknik için yeni bir algoritma geliştirilmiştir. Bu işlemlerin gerçekleştirilebilmesi için kullanılacak ortam C# yazılım dili ile kodlanmıştır. Uygulama sayesinde son kullanıcı dahi kolaylıkla bilgi gizleyebilir ve çözebilir. Geliştirilen uygulama için grafikler özel olarak tasarlanmış ve bir form sayfası hazırlanmıştır. Gizleme mantığının tersi olarak çözme algoritması çalışmaktadır. Her pikselin renk kanallarına erişilerek en az anlamlı bitler elde edilir. ReverseBits metodu üzerinden gizli mesaj elde edilir.

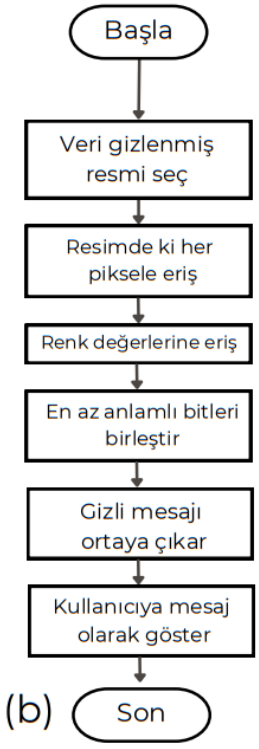
4.1. Şifreleme İşlemi

Adım 1. İlk olarak uygulama başlatılır.
Adım 2. Dosya Seç butonu ile kullanıcıdan PNG formatında resim seçmesi istenir. (PNG harici uzantıya izin verilmez, özel olarak filtrelenmiştir.)
Adım 3. Seçilen resim pixtureBox üzerinde gösterilir.
Adım 4. Seçilen resme ait fileİnfo komutu ile bilgiler okunur. (Dosya yolu, Dosya boyutu KB-MB, Dosya uzantısı, Dosya boyutu px.)
Adım 5. Kullanıcıdan textBox alanına gizlenmesini talep ettiği metni girmesi istenir.
Adım 6. Kullanıcı textBox alanına yazmaya başladıkça canlı olarak label üzerinde o metnin dönüşüm olarak hesaplanmış KB cinsinden uzunluğu tutulur.
Adım 7. Resim üzerinde piksel bazında dolaşarak her bir pikselin renk değerlerine erişilir.
Adım 8. Resmin arka planının şeffaf olup olmadığı kontrol edilir. Alfa kanalı sorgulanır.
Adım 9. Resmin arka planı şeffaf ise alfa kanalında maskeleme yapılır.
Adım 10. Resmin arka planı şeffaf değilse RGB kanallarında işlem yapılır.
Adım 11. Her pikselin renk değerleri RGB (kırmızı, yeşil, mavi) ve A (alfa) kanallarından oluşur. Bu kanalların her biri 8 bit (0-255 arası değer) ile temsil edilir.
Adım 12. Gizleme işlemi, metni en az anlamlı bitlere saklama mantığına dayanır. Yani, her bir renk kanalının en az anlamlı bitleri değiştirilerek metin gizlenir
Adım 13. Örneğin, R (kırmızı) kanalının en az anlamlı biti, G (yeşil) kanalının en az anlamlı biti, B (mavi) kanalının en az anlamlı biti ve A (alfa) kanalının en az anlamlı biti metin bitlerini saklamak için kullanılabilir.(Alfa kanalında maskeleme yapılması gerekmektedir.)
Adım 14. Her pikseldeki renk kanallarının en az anlamlı bitleri sırasıyla değiştirilerek metin bitleri yerleştirilir.
Adım 15. Kullanıcı Gizle butonuna tıkladığı anda gizleme algoritması çalışmaya başlar.
Adım 16. Her pikseldeki renk kanallarının en az anlamlı bitleri sırasıyla değiştirilerek metin bitleri yerleştirilir.
Adım 17. Kullanıcı Gizle butonuna tıkladığı anda gizleme algoritması çalışmaya başlar.
Adım 18. Metnin tamamı işlenip gizlendikten sonra, elde edilen resim gizli mesajı içerir ve bu resim normal bir resim gibi görünür.

4.2. Şifre Çözme İşlemi

Adım 1. İçerisine gizli bilgi kaydedilmiş resim kullanıcı tarafından resim seç butonu ile seçilir.
Adım 2. Bilgiyi çöz butonu ile arka planda çözme algoritmasına erişilir.
Adım 3. Resimdeki her bir pikselin renk değerlerine erişilir.
Adım 4. Her pikselin renk değerlerindeki en az anlamlı bitler elde edilir.
Adım 5. Bu en az anlamlı bitler birleştirilerek ReverseBits metodu üzerinden gizli mesaj elde edilir.
Adım 6. Gizli mesaj ortaya çıkar ve okunabilir hale gelir.
Adım 7. Ekran üzerinde messageBox kısmında gizlenmiş olan mesaj kullanıcıya gösterilir ve gizli mesaj iletilir.



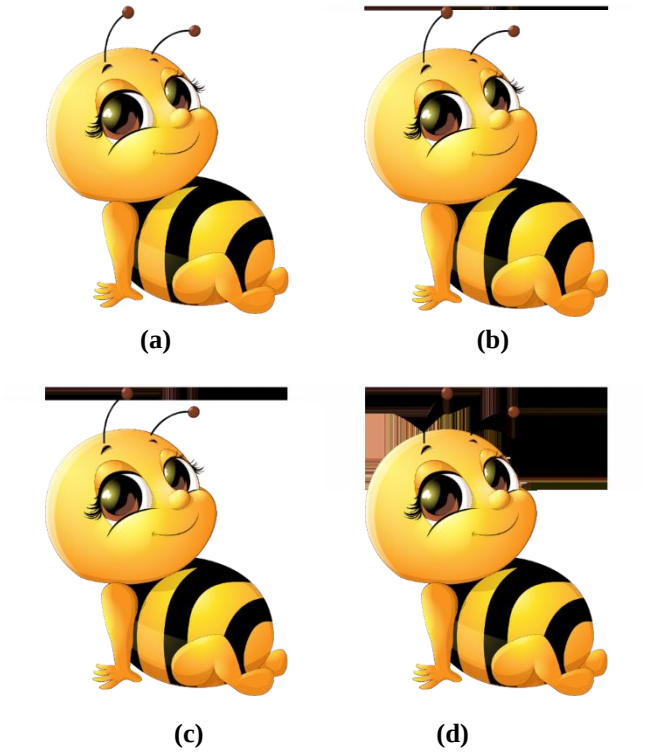


(a) Geliştirilen Uygulamanın veri gizleme işlemlerinin akış şeması

(b) Geliştirilen Uygulamanın veri çözme akış şeması

Not*: Uygulama örnek için 512x512px resim kullanılmıştır. Resim kalite ölçüm sonuçları resim boyutu ve kapladığı boyuta göre değişebilmektedir.

Şekil 7. Geliştirilen Uygulamanın Akış Şeması



Şekil 8. (a) Alfa kanalı maskelenmiş hali (b, c, d) Alfa kanalı maskelenmemiş hali

Yukarıda 4 adet (a, b, c, d) numaralı görsellerde arka planı şeffaf olan bir PNG arı resmine farklı KB uzunluklarında metinler gizlenmiştir. Alfa kanalı dâhil edilmediği takdirde (b, c, d) şekillerinde gözüktüğü gibi, gizlenen metin boyutu yükseldikçe arka plandaki şeffaf kısımlar farklı piksel renklerle gösterilmektedir. Alfa kanalı maskelendiğinde ise şekil (a) üzerinde gösterildiği gibi arka planda herhangi bir değişiklik olmamaktadır. Bu nedenle alfa kanalının maskelenmesi, steganografi çalışmalarında arka planı şeffaf olan resimler için kullanılmaktadır. Ayrıca makine öğrenme yöntemleri ve insan gözü ile fark edilmemesi için önem arz etmektedir.

5. PERFORMANS ANALİZİ

Bu bölüm, önerilen algoritmanın başarı kalitesini ölçmek amacıyla literatürde yer alan kalite ölçüm metriklerinin sonuçlarını sunar. Geliştirilen algoritmanın arkaplanı şeffaf olan resimlerde bilgi gizleme amacı taşıması sebebiyle aşağıdaki bölümlerde sunulan, arı,kulaklık ve yılan resimleri üzerinde testler gerçekleştirilmiştir.

5.1. Ortalama Kare Hata Metodu (MSE)

Veri gizleme tekniklerinin uygulanması neticesinde, stego görüntünün kalitesini belirleyebilmek amacıyla bazı yöntemler kullanılır. Bir kalite ölçüm yöntemi olan MSE (Mean Square Error veya Türkçe karşılığıyla ortalama kare hata), taşıyıcı görüntü ile stego görüntü arasındaki piksel değeri farklarının karesel toplamını temsil eder. Bu yöntem, steganografi uygulamalarında kullanılır ve iki görüntü arasındaki gizli veri gömülme veya çıkarma işlemlerinin başarısını değerlendirmek için kullanılır. Gizli verinin algılanma durumunu azaltmak için hata oranının çok küçük olmasını beklenmektedir. Normal olarak hata oranı yüksekse görüntü bozulur, düşük ise daha temiz ve net bir görüntü elde edilir.

$$MSE = \frac{\sum_{i=1}^{n}(C_i - C,i)^2}{n} \quad (1)$$

5.2. Tepe Sinyal Gürültü Oranı (PSNR)

Görüntünün mevcut kalitesini ortaya çıkartarak test etmek için, veri boyutuna bağlı ortalama karesel hatanın kullanılmasından daha önemli olan tepe sinyal gürültü oranı kullanılabilir. Tepe sinyal gürültü oranı olarak ifade edilen (PSNR) logaritmik olarak hesaplanır. Ortalama karesel hatayı da içermektedir.

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

Yukarıdaki denklemde olduğu gibi standart bir formül olup, gürültü desibel (dB) cinsinden ifade edilir. Stego görüntünün kaliteli sayılabilmesi için kalitesinin analizi yapıldığında PSNR değerinin 40 dB üzerinde olması gerekir (Cheddad ve diğ., 2010).

5.3 Yapısal Benzerlik İndeksi (SSIM)

Yapısal benzerlik indeksi SSIM olarak ifade edilir. Değeri taşıyıcı görüntünün stego görüntü ile birbirine benzeyip benzemediğini ortaya çıkartmak ve ölçmek için kullanılır. Temel mantığı insan görsel sistemi olan (HSV) algılanmasına dayanır.

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y+\mathrm{C}_1)(2\sigma_x\sigma_y+\mathrm{C}_2)}{(\mu_x 2+\mu_y 2+\mathrm{C}_1)(\sigma_X 2+\sigma_y 2+\mathrm{C}_2} \quad (3)$$

Yukarıdaki denklemde SSIM değerinin hesaplama formülü paylaşılmıştır. Burada x ve y değerleri taşıyıcı ve stego görüntüleri ifade etmek amacıyla belirtilir. Görüntülerdeki piksel yoğunluğu μ ile, standart sapma σ ile ve katsayılar da C ile ifade edilerek formülde sunulmuştur.

5.4. Entropi

Entropi, bir sistemdeki düzenlilik veya belirsizlik seviyesini ölçmek için kullanılır. Bir veri kümesinin entropisi, veri setindeki değerlerin çeşitliliği ve dağılımının bir ölçüsüdür. Eğer bir veri kümesindeki değerler benzer veya tekrarlayan ise, entropi düşük olur çünkü daha az belirsizlik vardır. Ancak, eğer bir veri kümesindeki değerler farklı ve çeşitli ise, entropi yüksek olur çünkü daha fazla belirsizlik vardır.

Entropi, bilgi sıkıştırma, veri analizi, şifreleme ve veri iletimi gibi birçok alanda kullanılır. Örneğin, sıkıştırma algoritmaları, düşük entropiye sahip verileri daha etkin bir şekilde temsil ederek veri boyutunu azaltır. Denklem (4) te gösterilmiştir.

$$H(m) = \sum_{i=0}^{M*N-1} P(m_i) log_2 \frac{1}{p_{(m1)}} \quad (4)$$

Entropi, bir görüntünün istatistiksel düzensizlik veya belirsizlik derecesini ölçer. Steganografi işlemi sırasında, gizli mesajın görüntüye eklenmesi, görüntünün entropi değerinde bir değişiklik yapar. Eğer gizli mesaj doğru bir şekilde eklenirse, görüntünün entropi değeri değişmeden veya sadece minimal bir değişiklikle neredeyse aynı kalır. Görüntüdeki entropi, piksellerin renk dağılımı ve örüntüleri ile ilgilidir. Düşük entropi, görüntünün daha düzenli ve tahmin edilebilir olduğunu gösterirken, yüksek entropi daha fazla rastgelelik ve düzensizlik içerdiğini gösterir.

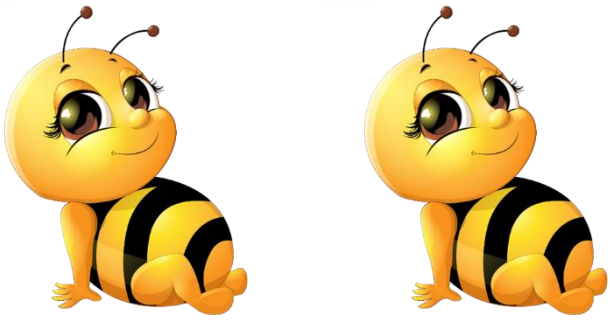
Steganografi (veri gizleme) tekniklerine uygun olarak hazırlanmış olan bu çalışma C# programlama dili kullanılarak Visual Studio. NET ortamında özel bir form tasarlandıktan sonra kodlanarak gerçekleştirilmiştir. Bu uygulamada LSB tekniği kanalı üzerinde RGB kanallarının yanı sıra alfa kanalı da dâhil edilmiştir

(R,G,B,A). Gerçekleştirilen bu çalışmanın yapısının ve başarısının testini gerçekleştirmek amacıyla, PSNR, MSE, ENTROPİ testleri ve ölçümleri MATLAB ortamında tekrardan kodlanarak gerçekleştirilmiştir.

Geliştirilen uygulamada başarılı işlemlerin yanı sıra son kullanıcıya hitap edecek şekilde bir form ara yüzü tasarlanmış ve resmi gizlemeden önce resme ait bazı parametre ve değerler kullanıcıya ekranda gösterilmiştir. Ayrıca ek bir özellik olarak kullanıcı textbox alanına gizlenecek bilgiyi yazmaya başladığı andan itibaren, yazdığı her harfin ne kadar KB boyut yer kapladığı bir label üzerinde kullanıcıya canlı olarak gösterilmektedir. Böylece kullanıcı gizleyeceği bilgiyi yazarken bunun toplam boyutunu görebilmektedir. LSB algoritmasında mesajın 1 karakteri resmin 8 baytına kopyalanmaktadır.

Farklı KB boyutlarında bilgi içeren metinlerin gizlendiği resimlerin kalite karşılaştırmaları yapılmıştır. PSNR değeri için 40 dB üzeri literatürde başarılı kabul edilmektedir (Bayam, 2018). Bu çalışmayla beraber gizlediğimiz bilgi sonucunda oluşan resimlerin değerleri tablo olarak sunulmuştur. Çıkan sonuçlar incelendiğinde literatüre göre başarılı kabul edilmektedir. Çeşitli boyutlarda metinler hazırlanarak resim içerisine gizlenmiştir. Metin uzunlukları 1,5,10,20,30 Kilobayt olacak şekilde test edilmiştir. Bu sonuçlar bir tablo haline getirilerek sunulmuştur. Gizlenmiş olan mesajın anlaşılmaması için geliştirilen uygulama içerisinde 50 KB, 60 KB olarak da veriler saklanabilmektedir.

Ancak literatür karşılaştırması için yukarıda belirlenen değerler üzerinden test edilmiştir. Farklı boyutlara sahip metinlerin Arı, Kulaklık ve Yılan isimli PNG dosyalarına gizlenmesi sonucunda ortaya çıkan resimlerin, kalite ölçüm sonuçları tablo olarak sunulmuştur.



(a) **(b)**

Şekil 9. (a) Orijinal arı resmi **(b)** Şifrelenmiş arı resmi

Tablo 1. Farklı boyutlarda veri gizlenmiş resmin kalite ölçüm sonuçları

Metin Büyüklüğü	PSNR	MSE	SSIM	ENTROPİ
1KB	48.222	1	0.9995	6.752
5 KB	48	1.03	0.9989	6.755
10 KB	47.91	1.06	0.9983	6.757
20 KB	47.63	1.13	0.9972	6.761
30 KB	47.38	1.2	0.9964	6.766

Tablo 1'de farklı boyutlara sahip verilerin arka planı şeffaf olan 512x512 piksel boyutundaki arı resmine gizlenmesi sonucunda oluşan kalite farkını göstermek için ifade edilen, ortalama karesel hata, tepe sinyal gürültü oranı, yapısal benzerlik indeksi ve entropi metrikleri kullanılmıştır.
Ortaya çıkan tablodaki veri sonuçlarına göre, 48.2 gibi yüksek bir PSNR değeri, iyi bir kalite performansı gösterdiğini işaret eder. Düşük MSE değerleri, stego görüntünün taşıyıcıya yakın bir kaliteye sahip olduğunu gösterir. 1.2 gibi düşük bir MSE değeri, iyi bir kalite performansını ifade eder. SSIM değerinin 1 olması, stego görüntünün taşıyıcı görüntüyle büyük bir yapısal benzerlik taşıdığını ifade eder.

(a) **(b)**

Şekil 10. (a) Orijinal kulaklık resmi **(b)** Şifrelenmiş kulaklık resmi

Tablo 2. Farklı boyutlarda veri gizlenmiş kulaklık resminin kalite ölçüm sonuçları

Metin Büyüklüğü	PSNR	MSE	SSIM	ENTROPİ
1KB	45.05	2	0.9997	4.107
5 KB	44.98	2.07	0.9984	4.108
10 KB	44.91	2.1	0.9977	4.109
20 KB	44.77	2.16	0.9967	4.110
30 KB	44.65	2.22	0.9958	4.113

Tablo 2'de farklı boyutlara sahip verilerin arka planı şeffaf olan 512x512 piksel boyutundaki kulaklık resmine gizlenmesi sonucunda oluşan kalite farkını göstermek için ifade edilen, Ortalama Karesel Hata, Tepe Sinyal Gürültü Oranı, Yapısal Benzerlik İndeksi, Entropi metrikleri kullanılmıştır.

Ortaya çıkan tablodaki veri sonuçlarına göre, 45.05 gibi yüksek bir PSNR değeri, iyi bir kalite performansı gösterdiğini işaret eder. Düşük MSE değerleri, stego görüntünün taşıyıcıya yakın bir kaliteye sahip olduğunu gösterir. 2 gibi düşük bir MSE değeri, iyi bir kalite performansını ifade eder. SSIM değerinin 1 olması, stego görüntünün taşıyıcı görüntüyle büyük bir yapısal benzerlik taşıdığını ifade eder. Bu sonuçlar değerlendirildiğinde kulaklık resminin, arı resmine yakın değerler elde edildiği görülmüştür.

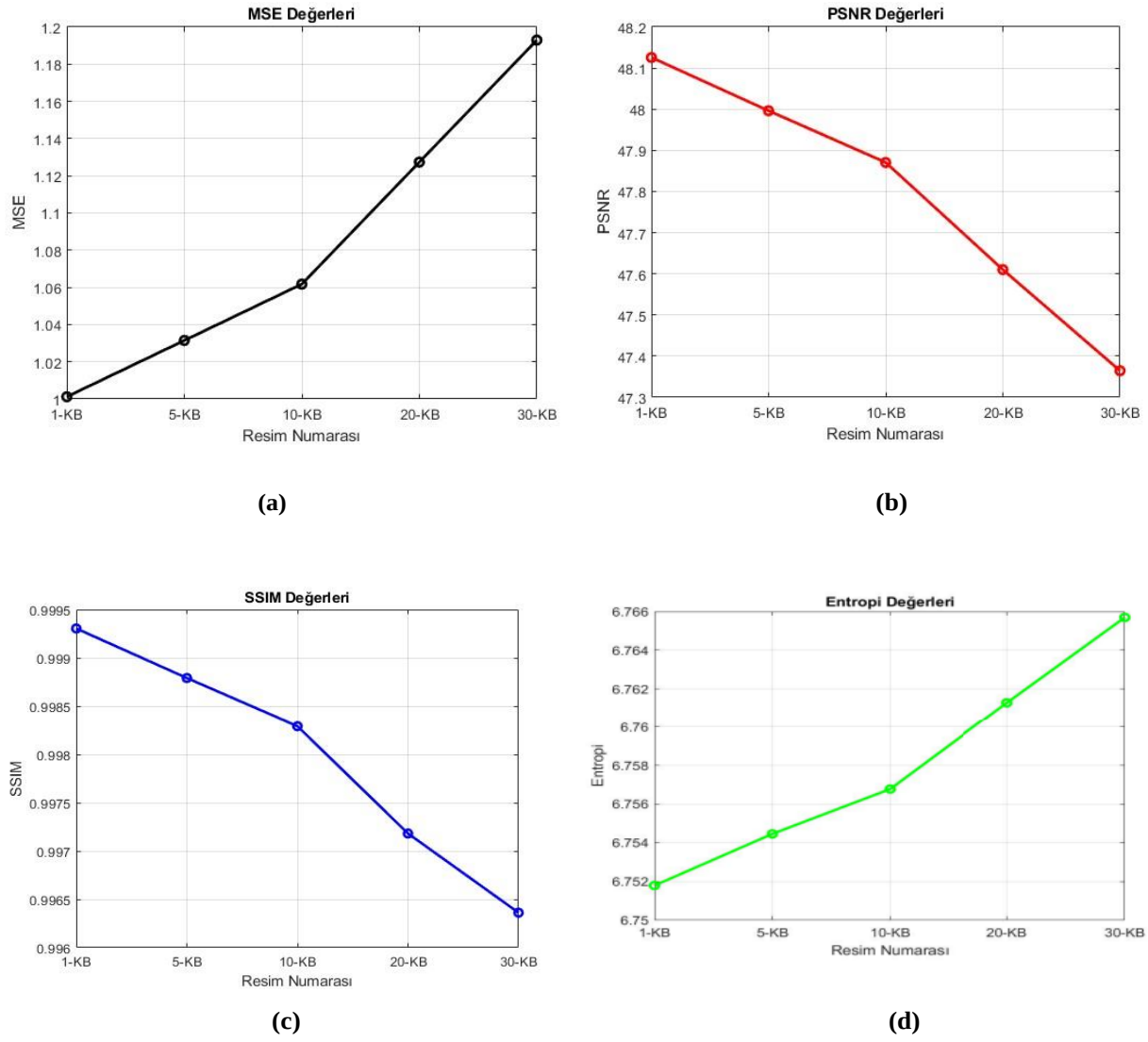
(a) **(b)**

Şekil 11. (a) Orijinal yılan resmi **(b)** Şifrelenmiş yılan resmi

Metin Büyüklüğü	PSNR	MSE	SSIM	ENTROPİ
1KB	47.28	1.22	0.9980	4.0712
5 KB	47.15	1.25	0.9975	4.0707
10 KB	47.09	1.28	0.9970	4.0703
20 KB	46.85	1.35	0.9958	4.0701
30 KB	46.62	1.41	0.9950	4.0698

Tablo 3'de farklı boyutlara sahip verilerin arka planı şeffaf olan 512x512 piksel boyutundaki yılan resmine gizlenmesi sonucunda oluşan kalite farkını göstermek için ifade edilen, ortalama karesel hata, tepe sinyal gürültü oranı, yapısal benzerlik indeksi ve entropi metrikleri kullanılmıştır.

Ortaya çıkan tablodaki veri sonuçlarına göre, 47.28 gibi yüksek bir PSNR değeri, iyi bir kalite performansı gösterdiğini işaret eder. Düşük MSE değerleri, stego görüntünün taşıyıcıya yakın bir kaliteye sahip olduğunu gösterir. 1.22 gibi düşük bir MSE değeri, iyi bir kalite performansını ifade eder. SSIM değerinin 1 olması, stego görüntünün taşıyıcı görüntüyle büyük bir yapısal benzerlik taşıdığını ifade eder. Bu sonuçlar değerlendirildiğinde yılan resminin, kullanılan kulaklık ve arı resmine yakın değerler elde ettiği görülmüştür. Bu nedenle değerlendirmeler başarılı olarak gözlemlenmiştir.



Şekil 12. (**a, b, c, d**) **arı** resmi referans alınarak, ortalama karesel hata, tepe sinyal gürültü oranı, yapısal benzerlik indeksi ve entropi metrikleri kullanılarak MATLAB üzerinde elde edilen grafik sonuçları sunulmuştur.

6. BULGULAR VE TARTIŞMA

Tablo 4'de şimdiye kadar gerçekleştirilen çalışmalar ile önerilen alfa kanalı filtreli algoritmanın karşılaştırması yapılmıştır.

Tablo 4. Literatürde yer alan çalışmalar ile karşılaştırma

İlgili Çalışma	PSNR	MSE	SSIM	ENTROPİ
(Andaç, 2007)	20,16	626,619	X	X
(Öztürk ve ark, 2007)	54,05	0,255	X	X
(Olcay ve Saran, 2013)	57,60	0,1128	X	X
(Sarayreh, 2014)	46,14	0,270	X	X
(Karakış ve ark, 2020)	64,48	0,005	0,99	X
(Karaduran, 2020)	42,53	3,65	X	X
Önerilen Alfa Kanalı Filtreli Çalışma	48.222	1	0,999	6,752

Tablodaki değerlere bakıldığında önerilen algoritmanın literatürdeki çalışmalarla kıyaslanması sonucunda alfa kanalı maskelenmiş olmasına rağmen oldukça iyi sonuç verdiği görülmüştür.

Alfa kanalı filtreli olarak gerçekleştirilmiş olan çalışma, birebir aynı değerleri ve testleri içeren çalışmalar olmaması sebebiyle en yakın değerlere sahip çalışmalar ile kıyaslanmıştır. Literatürde, tepe sinyal gürültü oranı (PSNR) için 40 dB üstü sonuçlar başarılı kabul edildiğinden (Bayam, 2018) diğer metrik ölçümleri incelendiğinde yapılan çalışmanın başarılı sonuç ürettiğinin bir göstergesidir.

İnternetin günümüz dünyasında oldukça hızlı ilerlediği ve anlık olarak 1 dakikada milyonlara veri transferi gerçekleştiği bilinmektedir. Günümüzde resim dosyaları hem boyut olarak fazla yer kaplamaması ve hem de insanlar tarafından en kolay şekilde bir çok farklı platform aracılığı ile transfer edilebilmektedir.

Bu makalede steganografik tekniklerinden LSB tekniği kullanılarak R,G,B renk kanallarının yanı sıra Alfa kanalı üzerinde işlemler gerçekleştirilmiştir. Geliştirilen uygulamada son kullanıcının kolaylıkla kullanımına uygun bir görsel ara yüz tasarlanmış ve özelleştirilmiştir.

7. SONUÇLAR VE GELECEKTEKİ ÇALIŞMALAR

Sonuçlar dikkate alındığında, önerilen yöntem ile resim içerisine gizlenen metinlerin başarılı bir şekilde gizlendiği ve çıkartıldığı sorunsuz bir şekilde işlem yapılabildiği tespit edilmiştir.

Kalite ölçümlerinin gerekli değerleri karşıladığı ve arka planı şeffaf olan resimler için bu tekniğin başarılı bir şekilde rahatlıkla kullanılabileceği belirlenmiştir.

Mahremiyet ve gizli iletişim hakkında günümüzde çok ciddi önlemler alınmaktadır. Bu hususta değerlendirme yapıldığında önerilen bu teknik ve gerçekleştirilen bu çalışma görsel steganografi üzerinde bu problemin çözümüne katkı sağlayacağı düşünülmektedir.

Dijital görüntüler için yeni görüntü formatları ortaya çıktıkça kodlama dilleri üzerinde daha iyi performans/analiz uygulamaları geliştirilmesi araştırılacaktır.

Sosyal medya uygulamalarının bilgi gizlenmiş olan resimlerin algoritmasını bozmaması için koruma sağlayan bir algoritma gerçekleştirilmesi araştırılacaktır.

Steganografi, mahremiyet ve gizlilik alanında birçok uygulama potansiyeline sahip olması sebebiyle, gelecekte bu çalışmanın sonuçlarından yola çıkarak steganografinin yeni alanlarda kullanımı araştırılabilir. Dijital iletişim, ve veri saklama gibi farklı alanlarda steganografinin kullanımı incelenecektir.

Kapasite ve hız iyileştirmeleri yapılabilir. Şu anda kullanılan LSB tekniği, resim dosyasının en düşük anlamlı bitlerinde gizlenen metinleri destekler. Ancak, daha yüksek kapasiteli ve hızlı veri gizleme yöntemleri üzerinde çalışmak, daha fazla bilgiyi resme gizlemek ve işlemleri hızlandırmak için fırsatlar sunabilir.

REFERANSLAR

Alvy, R. S. (1995). Alpha and the History of Digital Compositing. Microsoft Tech Memo, 7, p. 8-15.

Balcı, D. & Karakış, R. & Güler, İ. (2020). Tıbbi DICOM Veri Güvenliğinde Hibrit Yöntemlerin Kullanılması. Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 1303-1304.

Bayam, İ., (2018). Kaotik Yöntem İle En Düşük Değerlikli Bit Steganografi Modeli ve Uygulaması, 78

Cheddad, A., Condell, J., Curran, K. ve Mc Kevitt, P., 2010, Digital image steganography: Survey and analysis of current methods, Signal Processing, 90 (2010)

Cox, I. J., Miller, M. L., & Bloom, J. A. (2002). Digital Watermarking (2nd ed.). Morgan Kaufmann.(2002)

Ghaith Salem Sarayreh, Text Hiding in RGBA Images Using the Alpha Channel and the Indicator Method (2014)

Gonzalez, R. C., & Woods, R. E. (2008). Digital Image Processing. Pearson Education. Pratt, W. K. (2007). Digital Image Processing. John Wiley & Sons. (2007)

Jessica Fridrich, 2007. Binghamton University, State University of New York (SUNY). Steganography in digital media, Principles, Algorithms, and Applications in book, 117, 118, 119. (2007)

Jessica Fridrich, 2007. Binghamton University, State University of New York (SUNY). Steganography in digital media, Principles, Algorithms, and Applications in book, 7-8. (2007)

Jessica Fridrich, 2007. Binghamton University, State University of New York (SUNY). Steganography in digital media, Principles, Algorithms, and Applications in book.(2007)

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.

Karaduran, A. & Turan M. (2020). Cebirsel Şifrelenmiş LSB Yöntemi. Avrupa Bilim ve Teknoloji Dergisi, (Special Issue), 73-80.

Kovacich, G. & Jones, A. (2002). What infosec professional should know about information warfare tactics by terrorists. Computer & Security, 21(1), 35-41.

Morkel, T., Eloff, J. H., & Olivier, M. S. (2005, June). An overview of image Steganography. In Information Systems Security Association (ISSA), pp. 1-11.

N. F. Johnson and P. Sallee. Detection of hidden information, covert channels and information flows. In John G. Voeller, editor, Wiley Handbook of Science Technology for Homeland Security. New York: Wiley & Sons, Inc, April 4, (2008).

Olcay, C. & Saran, N. (2013). İmge İçine Bilgi Gizlemede Kullanılan LSB Yöntemlerinin Karşılaştırılması. C¸ ankaya University Journal of Science and Engineering Volume 10 (2013), No. 1, 17–32

Öztürk, E. & Şahin, A. & Mesut, A. (2011). LSB Ekleme Yönteminde Bilgi Gizleme İçin Tek Renk Kanal Kullanımının Güvenliğe Etkileri. 4. Ağ ve Bilgi Güvenliği Sempozyumu. -444

Şahin, A., (2007). Görüntü Steganografide Kullanılan Yeni Metodlar ve Bu Metodların Güvenirlikleri, 81-82.

Wan, W., Wang, J., Zhang, Y., Li, J., Yu, H., & Sun, J., 2022. A Comprehensive Survey on Robust Image Watermarking. Neurocomputing. https://doi.org/10.1016/j.neucom.2022.02.083.

Yılmaz İ. Renk Sistemleri, Renk Uzayları ve Dönüşümler, Selçuk Üniversitesi Jeodezi ve Fotogrametri Mühendisliği Öğretiminde 30.Yıl Sempozyumu, Konya, 10, (2002)

İNTERNET KAYNAKLARI

https://tr.wikipedia.org/wiki/Viktor_Korchnoi (03.06.2023)

https://autonom.com.tr/goruntu-olusumu (03.06.2023)

https://digitalage.com.tr/internette-bir-dakika-matt-navarra (03.06.2023)

https://www.lib.cam.ac.uk/university-archives/glossary/ Syndics of Cambridge University Library (03.06.2023)

Not: *Bu makale, İstanbul Ticaret Üniversitesi Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı'nda, Doç.Dr. Mustafa Cem Kasapbaşı danışmanlığında, Mehmet ŞANVEREN tarafından yürütülecek olan, "Görüntüler Üzerinde Alfa Kanalı Filtreli Veri Gizleme Tekniği ve Uygulaması" başlıklı yüksek lisans tezinin ön çalışmalarından yararlanılarak hazırlanmıştır.*