Koc. Üni. Fen Bil. Der., 4(1): (2021) 1-5

Kocaeli Üniversitesi

Kocaeli Üniversitesi Fen Bilimleri Dergisi

http://dergipark.org.tr/koufbd

Çoklu Görsel Nesnelere Veri Gizleme (Steganografi)

Data Hiding (Steganography) into Multiple Visual Objects

Hasan YAĞCIOĞLU[1,*], Adnan SONDAŞ[2]

[1] *Bilişim Sistemleri Mühendisliği, Kocaeli Üniversitesi, Kocaeli, Türkiye,* ***Orcid:*** *0000-0002-9737-6180*
[2] *Bilişim Sistemleri Mühendisliği, Kocaeli Üniversitesi, Kocaeli, Türkiye,* ***Orcid:*** *0000-0003-4559-3463*

Araştırma Makalesi

Gönderilme Tarihi : *27/04/2020*
Kabul Tarihi : *06/01/2021*

Anahtar Kelimeler

Bilgi Güvenliği
Resim Steganografi
LSB
Veri Gizleme

Özet

Çağımızda internet kullanımının yaygınlaşmasıyla beraber veri alışverişi ve bilgi paylaşımı büyük bir oranda artmış, bilgi güvenliği önemli hale gelmiştir. Bu çalışma kapsamında C# programla dili ve resim steganografide en az anlamlı bite gizleme yöntemi (LSB) kullanılarak uygulama geliştirilmiştir. Geliştirilen uygulamada belirlenen PNG ve BMP resim dosyaları içerisine LSB kullanarak metin verisi gizleme işlemi gerçekleştirilmiştir. Gizleme işleminin başarım sonuçları ise MSE ve PSNR sonuçları ile değerlendirilmiştir.
Geliştirilen uygulama ile birden fazla resim dosyasına veri gizleme işlemi yapılmaktadır. Bildiride, 1500 karakterlik bir metnin tek bir resme ve 5 farklı resme gizlenmesinin sonuçları karşılaştırılmıştır. Elde edilen sonuçlara göre verinin 5 parçaya bölünerek gizlenmesi sonucunda ilgili örtü-resminde oluşan bozulma değerlerinin düştüğü görülmüştür.

Research Paper

Received Date : *27/04/2020*
Accepted Date : *06/01/2021*

Keywords

Information Security
Image Steganography
LSB
Data Hiding

Abstract

With the widespread use of internet in our age, data exchange and information sharing have increased largely and information security has become important. Within the scope of this study, an application was developed by using the C# language and the Least Significant Bit (LSB) method in the picture steganography. By using the developed application, a text data is hidden into PNG and BMP image files using LSB method. The performance results of the concealment were evaluated with MSE and PSNR results.
With the developed application, data hiding is made to more than one image file. In the paper, the results of hiding a 1500 character text in a single picture and 5 different pictures were compared. According to the obtained results, it was observed that the distortion values in the related cover-image decreased as a result of hiding the data into 5 parts.

1. Giriş

Son yıllarda bilgi teknolojilerinin gelişmesi ve gün geçtikçe hayatımıza daha çok girmesiyle beraber, işlemlerimizin birçoğu elektronik ortamlarda yapılır hale gelmiştir. Bu ortamlarda işlenen, saklanan ve gönderilen verilerin güvenliğinin sağlanması ise oldukça gerekli bir durumdur. Veri iletiminin gerçekleştirildiği dijital ortamlarda, göndericiden alıcıya iletilen veriye yetkisiz kişilerin erişimi, verinin değiştirilmesi ve hatta verinin kaybolması gibi birçok güvenlik tehdidi bulunmaktadır. Bu güvenlik tehditlerinin ortadan kaldırılmasına yönelik farklı yaklaşımlar sürekli geliştirilmektedir.

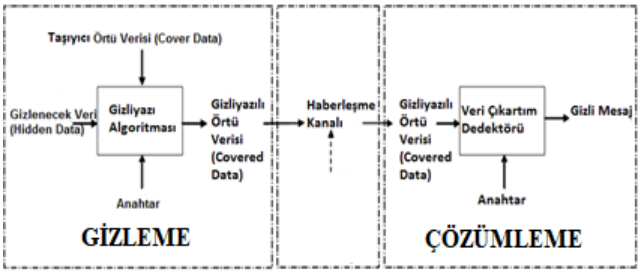
Veri güvenliğinin sağlanmasına yönelik geliştirilen farklı yaklaşımlardan birisi ise steganografidir. Steganografinin amacı veriyi, istenmeyen kişileri şüphelendirmeden ilgili hedefe ulaştırmaktır. Bu özelliğinden dolayı steganografi, gizli iletişim yöntemi olarak da bilinmektedir. Mesaj gönderilirken, üçüncü kişilerin şüphe etmeyeceği şekilde gizlenerek gönderilir ve üçüncü kişilerin eline geçse bile ellerinde gizlenmiş mesaj olduğunu anlayamayacaklardır. Böylelikle gönderilen mesajın açığa çıkması da engellenmiş olacaktır.

* Sorumlu Yazar *(Corresponding Author)*: hasan.yagcioglu@hotmail.com

Tarihi çok eskiye dayanan bir bilim dalı olan steganografi, Antik Yunan ve Heredot dönemine kadar uzanmaktadır [1]. Steganografi, kelime anlamı "gizlenmiş yazı" veya "örtülü yazı" anlamına gelmektedir [2]. Steganografide ilgili veriyi gizlemek için bir taşıyıcı nesneye ihtiyaç duyulmaktadır. İçerisine bilgi gizlenecek olan bu taşıyıcı nesneye örtü-nesnesi (cover object), gizleme işlemi sonrası oluşan nesneye ise stego-nesnesi (stego object) adı verilir [3]. Bu nesneler, bütün sayısal dosya formatları (ses, fotoğraf ve video gibi) olabileceği gibi, herhangi bir görüntü içerisine gizlenmiş başka bir görüntü dosyası veya ses dosyası da olabilir [4]. Örtü-nesnesi içerisine gizli verileri saklama ve stego-nesneden gizli verileri tekrar elde etme aşamalarında kullanılan fonksiyonlar ise anahtar olarak tanımlanmaktadır [5].

Steganografide amaç örtü-nesnesine maksimum boyutta veri gizlenebilmesi ve buna karşılık örtü-nesnesinde en az seviyede bozulma olmasıdır.

Şekil 1'de steganografinin genel aşamaları yer almaktadır. Görüldüğü üzere, gizleme fonksiyonu kullanılarak örtü-nesnesi içerisine veri gizlenmekte ve stego-nesnesi elde edilmektedir. Çözme aşamasında ise stego-nesne üzerine çözme fonksiyonu uygulanılarak gizli veri tekrar elde edilmektedir.



Şekil 1. Steganografinin genel aşamaları.

Bu çalışmada, en az anlamlı bite gizleme (Least Signification Bit; LSB) yöntemi kullanılarak örtü-nesnelerine veri gizleme işlemi yapılmaktadır. Bu amaçla, Visual Studio C# programlama dili kullanılarak bir arayüz tasarımı geliştirilmiştir. Bu arayüz aracılığıyla gizlenmek istenen veri, birden fazla resim üzerine bölünerek gizlenmektedir. Beklendiği üzere, resim sayısı arttıkça gizlenebilecek veri boyutu da artmaktadır. Ayrıca geliştirilen uygulama sayesinde, stego-resimler içerisine gizlenen veriler tekrar elde edilebilmektedir.

2. Yöntem

LSB yöntemi, görüntü steganografide en çok kullanılan yöntemlerden birisidir. Bu yöntem uygulanırken, gizlenmek istenen verinin bitleri sırası ile örtü-nesnesinin (resim dosyasının) piksellerine ait renk değerlerinin en az anlamlı bitine yazılmaktadır. Yapılan değişiklikler sonucunda resmin renk tonlarında çok az miktarda ton değişikliği oluştursa da bu değişim insan gözü ile algılanamayacak seviyededir.

Tablo 1'de, "Y" harfinin ASCII karakter karşılığı olan "01011001" verisinin bir görüntüye gizlenmesi işlemi özetlenmiştir. Görüldüğü üzere bu işlem sonucunda bazı bitler değişirken (kırmızı) bazıları ise aynı kalmaktadır (mavi).

Tablo 1. 'Y' harfinin gizlenmesi işlemi.

Piksel No	Eski Renk Değeri	Gizlenecek Veri	Yeni Renk Değeri
1	1001010101	0	1001010100
2	0101101011	0	0101101010
3	0011011010	0	0011011010
4	0100011010	1	0100011010
5	1011011101	0	1011011100
6	0111100111	0	0111100110
7	0111110001	0	0111110000
8	1110001101	0	1110001101
9	0110001111	0	0110001110
10	1011010101	1	1011010101

Geliştiren uygulamanın Türkçe karakterleri de destekleyebilmesi için bütün karakterlerin ASCII karşılıkları 10-bit olacak şekilde ayarlanmıştır. Daha kısa ASCII değerine sahip olan karakterlerin değerlerinin başına ise 10 bite tamamlayacak sayıda "0" değeri eklenerek resim içerisine gizleme işlemi yapılmıştır.

Geliştirilen uygulamada, girilen metin yüklenen resim sayısına göre parçalara ayrıştırılarak metin gizleme işlemi gerçekleştirilmiştir. Örneğin "YAĞCIOĞLU" kelimesi 3 adet resim içine gizlendiğinde, 1. resim içine "YCĞ" harfleri, 2. resim içine "AIL" harfleri ve 3. resim içine "ĞOU" harfleri gizlenmektedir.

Veri gizleme aşamasının algoritması aşağıdaki gibidir;

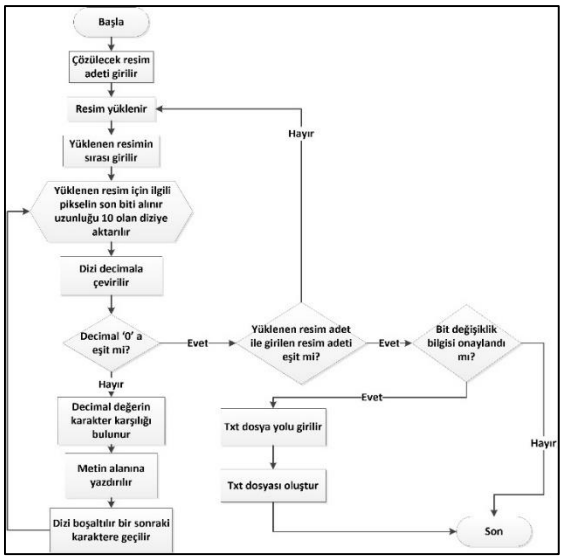
1) Gizleme işleminin kaç farklı görüntü üzerinde yapılacağı belirlenir.

2) Gizlenmek istenen mesajın karakterlerinden hangilerinin hangi resme gizleneceği belirlenir. Bunun için karakter sırası, mod (görüntü adedi) ile belirlenen resim içerisine gömülecek şekilde planlama yapılır.

3) Belirlenen karakterler sıra ile ilgili resimlerin piksel değerlerine LSB yöntemi ile gizlenir.

4) İlgili resimlerde karakter gizlemenin bittiğinin anlaşılabilmesi için her resimde en son karakterden sonra NULL "0000000000" değeri eklenir. Bu değer mesajın geri elde edilmesi aşamasında kullanılacaktır.

Örtü-resmi içerisine veri gizlenme aşamasının akış şeması Şekil 2'de verilmektedir.



Şekil 2. Veri gizleme aşamasının akış şeması.

Çözümleme aşamasının algoritması aşağıdaki gibidir;

1) Çözümleme işleminin kaç farklı resim üzerinde yapılacağı belirlenir.

2) Sıra ile resimler ele alınır, piksellerinin son bitleri tespit edilir.

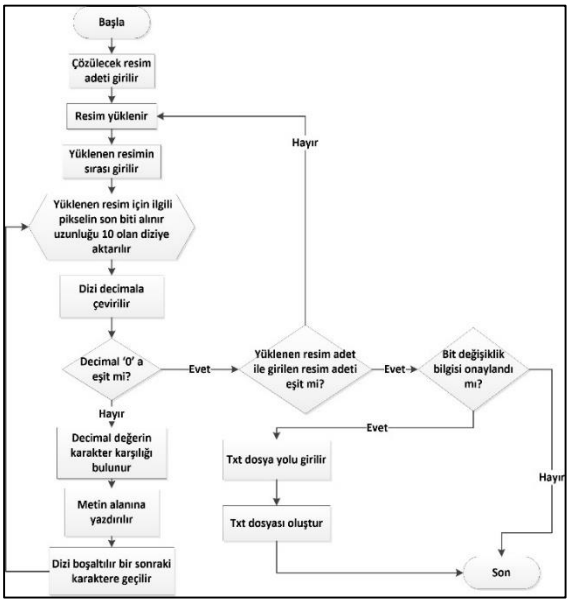
3) 10 adet bit alındıktan sonra ilgili değere karşılık gelen harf belirlenir.

4) Eğer alınan değer NULL "0000000000" ise bir sonraki görüntü içerisindeki değerler alınmaya başlanır.

5) Bütün görüntülerdeki karakterler tespit edildikten sonra mesajın karakterleri sıralanır. Bu aşamada, ilgili resimlerden elde edilen verilerin önce ilk karakterleri sıra ile yerleştirildikten sonra bir sonraki sırada bulunan karakterleri yerleştirilmektedir.

6) Böylece ilgili mesaj tekrar elde edilir.

Stego-resim içerisinden veri çıkartılması aşamasının akış şeması ise Şekil 3'te verilmektedir.



Şekil 3. Veri çıkarımı aşamasının akış şeması.

3. Bulgular ve Tartışma

Steganografi çalışmalarının başarısı, örtü-resmi ile stego-resmin birbiri ile karşılaştırılması sonucunda belirlenir. Örtü nesnesi üzerindeki değişimler veya bozulma oranlarının belirlenmesi için bazı ölçme metotları geliştirilmiştir. En çok kullanılan ölçme metotları MSE ve PSNR değerlerinin hesaplanmasıdır. Bu oranlar, örtü nesnesi üzerine gizleme işlemi yapılmadan önce ve yapıldıktan sonraki farkları görmemizi sağlayan matematiksel fonksiyonlardır.

MSE, örtü-resmi ile stego-resim arasındaki benzerlik oranını verir ve iki resim bire bir aynı ise MSE değeri 0 hesaplanır. MSE değerinin düşük çıkması, benzerliğin yüksek olduğunu ve steganografik çalışmanın başarılı bir şekilde uygulandığını belirtmektedir. MSE değeri hesaplanırken Denklem 1 kullanılır.

$$MSE=\frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[I(i,j)-K(i,j)\right]^2 \quad (1)$$

Denklemdeki;

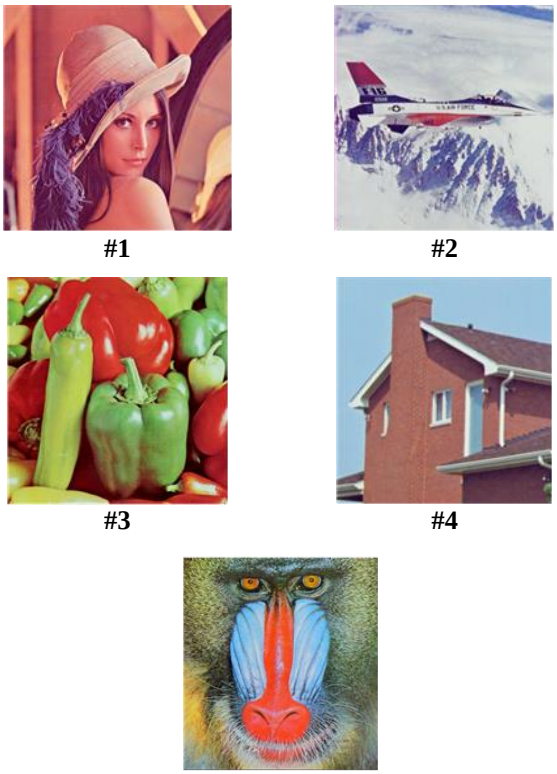
- I(i,j) değeri örtü resmini belirtmektedir.
- K(i,j) değeri stego-resmi belirtmektedir.
- m, n ise resmin ebatlarını temsil etmektedir.

PSNR, stego-resmin bozulumuna sebep olan en yüksek seviye sinyal ile bozulmaya diğer bir neden olan gürültü değerinin arasındaki orana denir. PSNR değerinin yüksek hesaplandığı durumlarda resim kalitesinin yüksek olduğu anlamına gelir. Eğer karşılaştırılan iki resim aynı ise PSNR değeri sonsuzdur. PSNR değerinin hesaplanmasında Denklem 2 kullanılır.

$$PSNR=10\log10\left(\frac{R^2}{MSE}\right) \quad (2)$$

Görüldüğü üzere PSNR değeri hesaplanırken MSE değeri de kullanılır. Denklemde kullanılan "R" değeri ise 8-bitlik bir resim için 2^8-1= 255 dir.

Şekil 4'te, geliştirilen uygulamanın test aşamasında kullanılan 24-bit renk çözünürlüğüne sahip, 256×256 piksel boyutundaki ve "bmp" formatındaki 5 adet resim verilmiştir.



#1 **#2**

#3 **#4**

#5

Şekil 4. Uygulamada kullanılan farklı resimler.

Öncelikle geliştirilen uygulama ile 1500 karakterlik 'Son yıllarda bilgi teknolojilerinin gelişmesi ve gün geçtikçe hayatımıza daha çok girmesiyle beraber yapılan birçok işlemin elektronik ortamlarla sağlanması, bu ortamlarda saklanan, işlenen, gönderilen verilerin güvenliğinin sağlanması önem arz etmektedir. Veri iletimi gerçekleştirilen ortamlarda göndericiden alıcıya iletilen veriye yetkisiz erişim, veriyi değiştirme ve hatta veriyi silme gibi birçok güvenlik tehditi bulunmaktadır. Bu güvenlik tehditlerin ortadan kaldırılmasına yönelik teknikler devamlı geliştirilmektedir. Veri güvenliğinin sağlanmasına yönelik iki ana yöntem bulunmaktadır. Bunlar steganografi ve kriptografidir...' mesajının tamamı 1 adet Lena resmine (#1) gizlenmiştir. İşlem sonucunda elde edilen MSE ve PSNR değerleri Tablo 2'de verilmiştir.

Tablo 2. 1 adet Lena resmine ait MSE ve PSNR değerleri.

	MSE	PSNR(dB)
1 adet resim (#1)	0,1162416	57,477193

Daha sonra aynı 1500 karakterlik mesaj, 5 adet Lena resmine (#1) bölünerek tekrardan gizlenmiştir. İşlem sonucunda her bir resme ait elde edilen MSE ve PSNR değerleri ise Tablo 3'te verilmiştir. Görüldüğü ve beklendiği üzere mesaj, birden fazla resme bölünerek gizlendiğinde ilgili örtü-resimlerinde Tablo 2'ye göre daha düşük bozulma değerleri elde edilmiştir.

Tablo 3. 5 adet Lena resmine ait MSE ve PSNR değerleri.

	MSE	PSNR(dB)
1. Resim (#1)	0,02389526	64,34768
2. Resim (#1)	0,02359009	64,40350
3. Resim (#1)	0,02374268	64,37550
4. Resim (#1)	0,02307129	64,50008
5. Resim (#1)	0,02333069	64,45152

Aynı 1500 karakterlik mesaj, Şekil 4'te verilen 5 farklı resme gizlendiğinde elde edilen MSE ve PSNR değerleri ise Tablo 4'te verilmiştir. Görüldüğü üzere bu durumda da beklendiği üzere Tablo 2'deki sonuçlara göre daha iyi değerler elde edilmiştir.

Tablo 4. 5 farklı resme ait MSE ve PSNR değerleri.

	MSE	PSNR (dB)
Resim #1	0,02357483	64,40631
Resim #2	0,00595855	70,37939
Resim #3	0,00591278	70,41288
Resim #4	0,02307129	64,50008
Resim #5	0,00555038	70,68757

4. Sonuçlar

Günümüzde internet kullanımının artmasıyla beraber veri alışverişi ve bilgi paylaşımında bilgi güvenliği önemli hale gelmiş durumdadır. Bu çalışma kapsamında C# programla dilinde, resim steganografide LSB yöntemi kullanan bir uygulama geliştirilmiştir. Bu uygulama sayesinde, belirlenen PNG ve BMP resim dosyaları içerisine metin verisi gizleme işlemi gerçekleştirilebilmektedir.

Bu uygulamada, gizli mesaj birden fazla örtü-resmine paylaştırılarak gizlendiğinde (beklendiği üzere), toplam gizlenebilecek veri boyutu da artmaktadır. Bildiride, 1500 karakterlik bir metnin tek bir resme ve 5 farklı resme gizlenmesinin sonuçları karşılaştırılmıştır. Elde edilen sonuçlara göre verinin 5 parçaya bölünerek gizlenmesi sonucunda ilgili örtü-resminde oluşan bozulma değerlerinin düştüğü görülmüştür.

Ancak veri gizleme işleminin baştan başlayarak sıra ile yapılması, verinin tespit edilmesini kolaylaştırmaktadır. Bu şekilde uygulandığında, gizli veri başkaları tarafından geliştiren algoritmalar ile tespit edilebilir. Bunun önüne geçilebilmesi için uygulamada mesajın öncelikle şifrelenmesi ve daha sonra ilgili resimlere gizlenmesi gerçekleştirilebilir. Böylece gerçek metni elde etmek oldukça zorlaşacaktır.

Çıkar Çatışması Beyanı:

Yazarlar tarafından herhangi bir çıkar çatışması belirtilmemiştir.

Etik Standartlar Beyanı:

Yazarlar bu çalışmada kullanılan materyal ve yöntemlerin etik kurul izni ve yasal-özel izin gerektirmediğini beyan eder.

Kaynaklar

[1] Ganbat B., Steganografi ile Bilgi Güvenliği, Yüksek Lisans Tezi, Ankara Üniversitesi, Fen Bilimleri Enstitüsü, Ankara, 2017, 467467.

[2] Cummins J., Diskin P., Lau S., Parlett R., Steganography and Digital Watermarking, School of Computer Science, 2004, **14**(60), 5-10.

[3] Razavi N., LSB Steganografi Yönteminde Yüksek Kapasiteli Veri Gizleme, Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Ankara, 2017.

[4] Sahin A., Buluş E., Sakallı M.T., Gri Seviye Resimler Üzerinde Rasgele Lsb Yöntemini ve Sayi Teorisini Kullanarak Bilgi Gizleme ve Steganaliz, Akademik Bilişim Konferansları, Denizli, Türkiye, 9-11 Şubat 2006.

[5] Patel Z. V., Gadhiya S. A., A Survey Paper on Steganography and Cryptography, International Multidisciplinary Research Journal, 2015, **2**(5), 2349-7637.