Genlik Modülasyonu Algoritması ile Görüntü İçerisine Veri Gizleme

Andaç Mesut [1], Bora Aslan[2], M. Tolga Sakallı[1], Füsun Yavuzer Aslan[1]

[1] Trakya Üniversitesi, Bilgisayar Mühendisliği Bölümü, Edirne

[2] Kırklareli Üniversitesi, Bilgisayar Programcılığı Bölümü, Kırklareli

andacs@trakya.edu.tr, bora.aslan@kirklareli.edu.tr, tolga@trakya.edu.tr, fusunyavuzer@gmail.com

Özet: Teknolojinin gelişmesi ile birlikte bilgiler artık dijital ortam aracılığı ile iletilmektedir. Bu noktada bilgi güvenliği kavramı önem kazanmaktadır. Günümüzdeki en değerli meta bilgidir. Bilginin güvenli yollar ile iletilmesi için birçok yöntem tasarlanmıştır. Bu yöntemlerden olan şifreleme mesajın içeriğinin korunmasını amaçlarken, steganografi mesajın varlığının gizlenmesini amaçlamaktadır. Yunanca kelime anlamı "gizlenmiş yazı" olan steganografi, verinin varlığını saklamayı amaçlamıştır. Bu çalışmada steganografi algoritmalarından olan genlik modülasyon algoritması incelenmiştir.

Anahtar Sözcükler: Steganografi, genlik modülasyonu algoritması, bilgi gizleme.

Information Hiding in Image Using Amplitude Modulation Algorithm

Abstract:. With the help of improvements in technology, the information can be gained through digital media. At this point, information security becomes very important. Today's most valuable thing is information. Many methods are designed in order for the information to be transferred in safe manners. Cryptography which is one of these methods aims at protecting the message content. On the other hand, steganography aims at covering the presence of message. Steganography, the meaning of which is "concealed writing", aims at hiding the presence of the data. In this paper, amplitude modulation algorithm which is present in steganography algorithms is examined.

Keywords: Steganography, amplitude modulation algorithm, information hiding.

1. Giriş

Steganografi önemli bir bilgi gizleme yöntemidir [1]. Bilgi gizleme çok eski çağlardan bu yana kullanılmaktadır. Gelinen süreçte, ilkel yöntemlerin yerine gelişmiş algoritmalar ile bilgi gizleme işlemi yapılmaktadır.

Günümüzde sayısal (dijital) nesneler üzerinde steganografi uygulamaları yapılmaktadır ve gelişen teknoloji nedeniyle, verileri korumak amacıyla son yıllarda sıklıkla kullanılmaya başlanmıştır. Steganografi, Dilbilim Steganografi ve Teknik Steganografi olmak üzere kendi içerisinde ikiye ayrılmaktadır. Dilbilim steganografi, taşıyıcı verinin metin olduğu steganografi koludur. Teknik Steganografi ise birçok konuyu içine almaktadır. Bunlar; görünmez mürekkep, gizli yerler, microdotlar ve bilgisayar tabanlı yöntemler gibi başlıklar altında toplanabilmektedir.

Steganografinin amacı gizli mesaj ya da bilginin varlığını saklamaktır. Taşınmak istenen mesaj bir başka masum görünüşlü ortamda saklanarak, üçüncü şahısların iletilen mesajın varlığından haberdar olması engellenir.

Metin, ses, sayısal resim, video dosyaları üzerine veri saklanabilir. Bu veriler metin dosyası olabileceği gibi, herhangi bir görüntü

içerisine başka bir görüntüyü gizlemekte mümkündür. Yine aynı şekilde bir ses dosyasının içine bir metin dosyası da saklanabilmektedir [2] [3].

Bir Stego-sistemde, bilgi gizlenen ortam cover-data (örtü verisi) ve oluşan ortama da stego-text veya stego-object denilmektedir [4].

Steganografi ile şifreleme birbirlerine yakın olmasına rağmen birçok noktada ayrılmaktadır. Şifreleme bilginin korunarak anlaşılamayacak şekle dönüşmesini amaçlar iken steganografi bilginin bir ortama gömülerek sezilmemesini sağlamayı amaçlamaktadır. Bu anlamda düşünüldüğünde steganografi, kriptolojiye güvenliği arttırıcı bir özellik katmaktadır.

Steganografi, kullanım alanları açısından üçe ayrılmaktadır [5]. Bunlar metin, görüntü ve ses steganografidir.

Metin (text) steganografi, bilgi gizlenecek olan ortamın metin olduğu stenografi alanıdır. Genellikle kelimelerin anlamları veya dizilişleri, noktalama işaretleri, ekstra boşluk kullanımı veya ASCII kodları gibi çeşitli yöntemler ile gizlenecek metin başka bir metin içerisine eklenebilir.

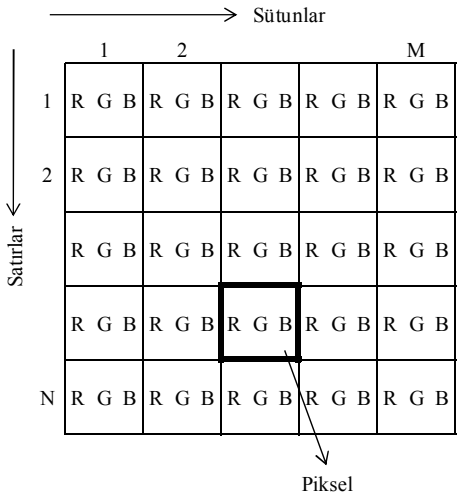
Görüntü (image) steganografi, dijital görüntülerin gelişmesi ile beraber en çok kullanılan steganografi yöntemidir. Görüntüdeki pikseller içerisindeki renk bitlerine veri gömülebilir. Genellikle en önemsiz bite veri saklama, maskeleme ve filtreleme, algoritmalar ve dönüşümler gibi yöntemler kullanılarak görüntü içerisine bilgi gizlenebilir.

Ses (audio) steganografi kullanımı zor olan bir steganografi dalıdır. Ses sinyallerinin düşük bit kodlaması ile veri gizleme en çok tercih edilen ses steganografi yöntemi olmakla beraber aşama kodlama, tayf yayılması, yankı veri gizlemesi diğer yöntemler arasındadır.

Bu çalışmada görüntü steganografi algoritmalarından olan genlik modülasyonu (amplitude modulation) algoritması incelenmiştir.

2. Sayısal Görüntünün Yapısı

Bir sayısal görüntü N satır ve M sütundan oluşan bir dizi şeklindedir. Dizinin her elmanı piksel olarak adlandırılır. En basit görüntülerde piksel değeri 1 veya 0 olabilir. Bu tip görüntülere ikili görüntü adı verilir. Genellikle 24 bitlik görüntüler üzerine veri gizleme işlemi yapılır. Bu tip görüntülerde bir piksel başına 3 byte kullanmaktadır. Her pikselin rengi; Kırmızı (red), Yeşil (green), Mavi (blue) olmak üzere üç ana renkten elde edilmektedir. Buna pikselin RGB değeri denmektedir [6].



Şekil 1. 24 bitlik görüntü yapısı

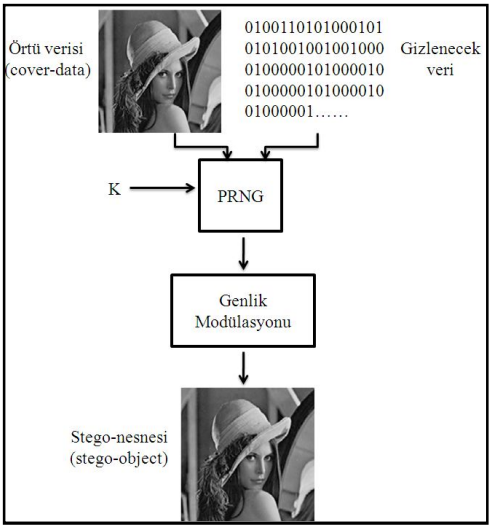
24 bitlik bir görüntüde her renk 0 ile 255 arasında değer alabilen ikili kodlar olarak ifade edilir. Örneğin turkuaz renkli bir pikselin RGB kodu aşağıdaki gibidir.

R	=	48	=	00110000
G	=	214	=	11010110
B	=	200	=	11001000

2. Genlik Modülasyonu

Genlik modülasyonu [7] mavi renk kanalı üzerine veri gizlemeyi amaçlayan bir algoritmadır. Genel olarak algoritma veri gizlenecek pikselin mavi kanal değerinin ışığın oranına veya bitin değerine göre arttırılıp azaltılması üzerine kuruludur.

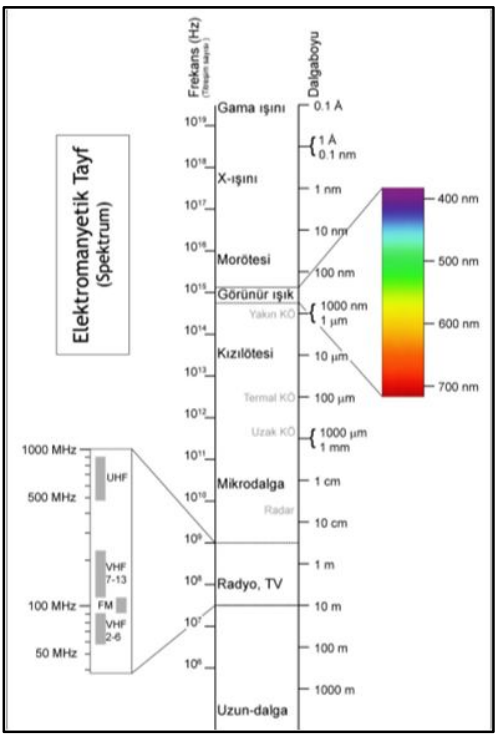
Genlik modülasyonu yöntemine göre veri gizleme işleminin şeması şekil 2'de gösterilmiştir.



Şekil 2 Genlik Modülasyonu (veri gizleme)

İnsan gözü 400 nm(nanometre) ile 700 nm arasındaki renk değerlerini görebilir (Şekil 3). Mavi renk ise görülebilir alanda kalan ilk bölüm olan 400 nm ile 500 nm arasındadır. Dolayısı ile diğer renklere göre değişimin en az fark edileceği renk mavidir. Eğer veri gizlemek için mavi kanal üzerinde küçük değişiklikler yapılır ise gizli verinin sezilebilirliği zorlaştırılmış olacaktır.

Veri gizlenecek koordinatlar, K anahtarı ile rastgele sayı üreteci sayesinde üretilen noktalarda saklanmaktadır.



Şekil 3. Elektromanyetik Spektrum

Saklanacak veri her seferinde rastgele olarak seçilen i ve j koordinatlarına sırayla yerleşmektedir.

- $\mathbf{B_{(i,j)}}$, i,j koordinatındaki mavi renk tonunu göstermektedir.
- $\mathbf{L_{(i,j)}}=0.299R_{(i,j)}+0.587G_{(i,j)}+0.114B_{(i,j)}$
- **S** değeri saklanacak bit (0 veya 1)
- **q** değeri ise saklanacak bilginin sezilmesini engellemek amacıyla 0 ile 1 arasında seçilen bir sabit değerdir.

Yukarıdaki formüller ve değerler yardımıyla i,j koordinatı için yeni mavi kanal renk değeri denklem 1'e göre hesaplanmaktadır.

$$B'_{ij} = B_{ij} + (2s-1)L_{ij}q \qquad (1)$$

Hesaplanan B'_{ij} değeri pikselin yeni mavi renk kanalı değeridir.

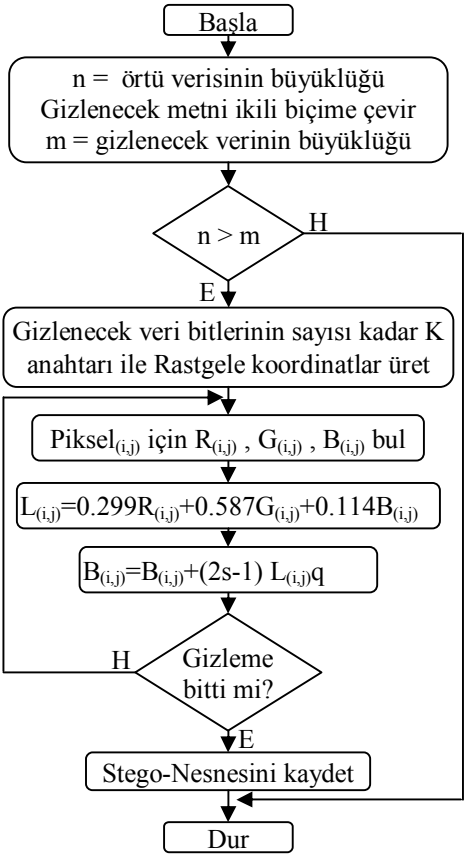
Örnek olarak 11000001 verisi gizlenmek istensin. Gizlenmek istenen veri dizisinin ilk

elemanı olan 1'in gizlenmesi için rastgele olarak seçilen ilk i,j koordinatının RGB değerleri sırası ile 125, 91, 136 olsun.

L=0.299 * 125 + 0.587 * 91 + 0.114 * 136
=37.375 + 53.417 + 15.504 = 106.296
B=136 + (2 * 1 - 1) * 106.296 * 0.5= 189.148

Hesaplanan değerlere göre pikselin yeni RGB kodları sırası ile 125, 91, 189 olacaktır. Bu değişim sayısal olarak büyük gözükmektedir fakat mavi renk kanalı üzerinde yapılan değişiklikler göz tarafından daha az sezildiği için resimdeki değişim hissedilemeyecek derecede küçük olmaktadır. Benzer şekilde gizlenecek verinin diğer bitleri de belirlenen koordinatlara gizlenir.

Veri gizleme algoritmasının akış çizelgesi şekil 4'te gösterilmiştir.



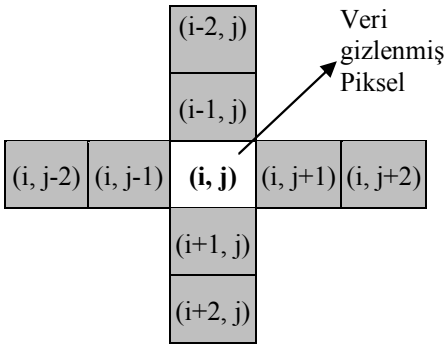
Şekil 4. Veri gizleme algoritması

Genlik modülasyonu algoritması ile içine veri gizlenmiş bir stego-nesneden veriyi geri çekmek için örtü verisinin orijinal mavi renk değerlerinin tahmin edilmesi gerekmektedir. Bu tahmin pikselin komşularının mavi kanal değerlerinin lineer kombinasyonuna dayanmaktadır. Eski mavi kanal renginin tahmin edilmesi için en iyi yöntem, pikselin komşularının değerleri üzerinden hesaplama olacaktır.

Öncelikle veri gizleme koordinatlarını tekrardan üretebilmek için gizleme anında kullanılan K anahtarı ile değiştirilmiş piksellerin yerleri tespit edilir. Daha sonrasında denklem 2 kullanılarak veri gizlenmiş pikselin komşuları dikkate alınarak eski mavi kanal rengi tahmin edilir.

$$\hat{B}_{ij} = \frac{1}{4c}\left(\sum_{k=-c}^{c} B_{i+kj} + \sum_{k=-c}^{c} B_{ij+k} - 2B_{ij} \right) \qquad (2)$$

Denklem 2'deki c değeri piksel için kontrol edilecek komşularının sayısıdır.

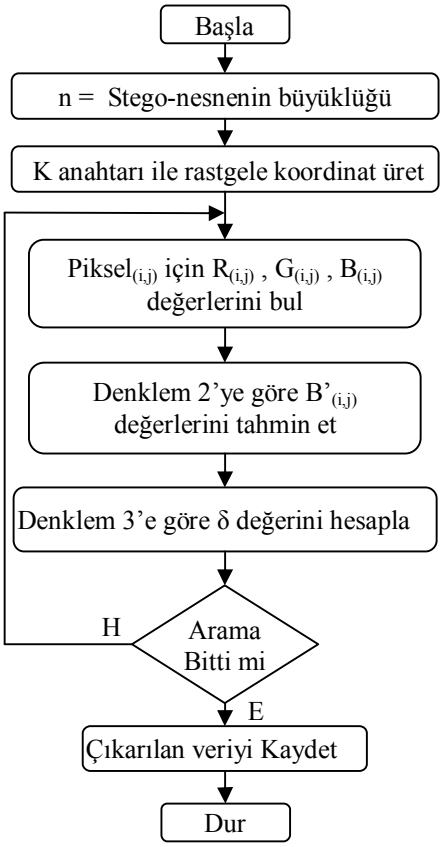


Şekil 5. c=2 için piksel komşuları

Pikselin değeri tahmin edildikten sonra denklem 3 sayesinde tahmin edilen mavi kanal değeri ile mevcut mavi kanal değerinin farkı alınır. Bu farkın işareti, gizlenen bitin değerini ifade etmektedir.

$$\delta = \hat{B}_{ij} - B_{ij} \qquad (3)$$

Buna göre veriyi elde etme işlemlerinin akış şeması şekil 6'da ifade edilmiştir.

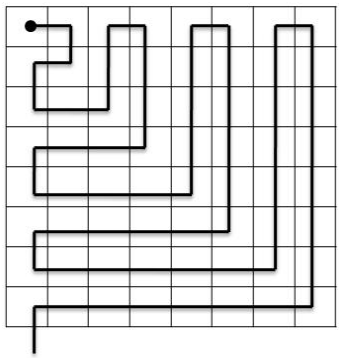


Şekil 6. Gizli veriyi elde etme işlemlerinin akış şeması

Birden fazla veri gizleme işlemlerinde veri gizleme veya çıkarma işlemleri için kullanılacak rastgele koordinatlar belirli bir düzende sıralanması gerekmektedir. Bu durumlarda yatayda veya dikeyde sıralama saldırıları kolaylaştırıcı bir etmek oynamaktadır. Bunu yerine şekil 7'deki gibi zikzak şeklinde bir sıralama yapmak saldırganın işini zorlaştıracaktır.

3. Örnek Çalışma

2048 (16384 bit) karakterlik, 304 kelimelik bir mesaj Abidin Dino'ya ait olan şekil 8(a)'daki 662x529 piksellik resme gizlenmiş ve şekil 8(b)'de bulunan resim oluşturulmuştur. Şekil 8(b)'deki değişim insan gözü ile fark edilemeyecek seviyededir fakat şekil bilgisayar yardımı ile incelendiğinde piksellerdeki değişim görülebilir. Örneğin örtü verisinde i=100, j=252 koordinatlarındaki pikselin renk değerleri R:100, G:106, B:118 iken 1 değeri bu piksele gizlendiğinde renk değerleri R:100, G:106, B:171 olarak değişmiştir.



Şekil 7. Zikzag şeklinde veri gizleme

(a)

(b)

Şekil 8. Örnek veri gizleme

5. Sonuçlar

Bu çalışmada, genlik modülasyonu algoritması ile görüntü içerisine metin verisi gizleme yöntemi anlatılmıştır. Stego-görüntüde yapılabilecek bulanıklaştırma, JPEG kodlama, döndürme ve başka bir görüntü ile birleştirme gibi işlemlere karşı dayanıklı olan bu yöntemin birkaç dezavantajı mevcuttur.

Her piksele sadece bir bit gizlenmesi sebebiyle uzun bir metin gizlenebilmesi için çok büyük boyutta bir resim kullanılması gerekebilecektir. Yada gizlenecek verinin önceden sıkıştırılması daha uygun olabilecektir.

Verinin geri elde edilmesi aşamasında komşu piksellerin çok faklı renklere sahip olması durumunda hatalı tahmin yapılma olasılığı çok yüksek olmaktadır.

Bu sebeplerden dolayı bu yöntem daha çok görüntü içerisine metin gizlemek yerine görüntü içerisine görüntü gizlemek için kullanılmaktadır.

Güvenliğin arttırılması açısından gizlenecek veriler daha öncesinde AES [8] gibi bir şifreleme algoritması ile şifrelenerek görüntü içerisine gizlenebilir. Böylelikle saldırgan gizlenmiş verileri bulsa dahi çözümlemesi için deşifreleme anahtarına da ihtiyaç duyacağından gizli veriye ulaşabilmesi oldukça zor olacaktır.

6. Kaynaklar

[1] Petitcolas F.A.P., Anderson R.J., Kuhn M.G., "Information Hiding–A Survey", Proceedings of the IEEE, **Special Issue on Protection of Multimedia Content**, 87(7):1062-1078, July 1999.

[2] Memon N., Wong, P., "Protecting digital media content", **Communications of the ACM,** vol 41, no. 7 , pp. 34–43, July 1998.

[3] Wang H., Wang S., "Cyber Warfare: Steganography vs. Steganalysis", **Communications of the ACM**, vol. 47, no. 10, October 2004.

[4] Şahin A., Buluş E., Sakallı M.T., "24-Bit Renkli Resimler Üzerinde En Önemsiz Bite Ekleme Yöntemini Kullanarak Bilgi Gizleme", **Trakya Üniversitesi Fen Bilimleri Dergisi**, Edirne-Haziran-2006.

[5] Şahin A., "Görüntü Steganografide Kullanılan Yeni Metodlar ve Bu Metodların Güvenilirlikleri", **Doktora Tezi**, 2007.

[6] Morkel T., Eloff J.H.P., Olivier M.S., "An Overview of Image Steganography", **Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005)**, Sandton, South Africa, June/July 2005

[7] Kutter M., Jordan F., Bossen F., "Digital Signature of Color Images using Amplitude Modulation", **Proceedings of SPIE storage and retrieval for image and video databases**, San Jose, USA, February 13-14, 1997.

[8] Advanced Encryption Standard (AES), **Federal Information Processing Standard Publication (FIPS 197)**, 26 November 2001.