Journal of Naval Science and Engineering
2009, Vol. 5 , No.1, pp. 107-118

İMGE KARELERİ KULLANAN YENİ BİR STEGANOGRAFİ YÖNTEMİ

Dz.Kd.Ütğm.Ömer KURTULDU, Yrd.Doç.Y.Müh.Kd.Bnb. Nafiz ARICA

Deniz Harp Okulu, Bilgisayar Mühendisliği Bölüm Başkanlığı
Tuzla,İstanbul, Türkiye
okurtuldu@dho.edu.tr, narica@dho.edu.tr

Özetçe

Bu çalışmada imge karelerini kullanan yeni bir steganografi yöntemi önerilmektedir. Önerilen yöntem, örtü imgesini karelere bölerek her kareye kare boyutuna bağlı uzunlukta mesaj bitini saklar. Kare içinde değişik yönlerdeki satır/sütunlardaki piksellerin en önemsiz bitlerinde (EÖB) arama yaparak mesaj bit dizisine en yakın satır/sütun bulunur. Bulunan satır/sütunun en önemsiz bitleri mesaj bit dizisiyle değiştirildikten sonra mesajın geri elde edilebilmesi amacıyla değiştirilen satır/sütunun çerçeve biti işaretlenir. Önerilen yöntemin steganografi analizlerine karşı performansı imge bozulma oranlarıyla ölçülmüş ve rastgele seçilen 100 imge ve gizli mesaj bitlerinde yapılan deneylerde Ortalama Karesel Hata ve Sinyal/Gürültü Oranı kullanılmıştır. Yöntemin literatürde yayınlanan imge uzayı tabanlı yöntemlerden daha düşük bozulma oranlarına sahip olduğu tespit edilmiştir.

A NEW STEGANOGRAPHY METHOD USING IMAGE BLOCKS

Abstract

In this study we propose a new steganography method using image blocks. The proposed method splits the cover image into square blocks and embeds a sequence of message bits into each block. It performs a search on least significant bits (LSB) of raw/column pixels at different directions and find the most similar raw/column to the message bits. It then changes the LSBs of raw/column pixels with the message bits. Finally the message embedded raw/column is pointed out using the frame pixels of block. The performance

of proposed method against steganalysis is evaluated using the measure of distorted pixels. İn the experiments performed on randomly selected 100 different images and message bits, Mean Square Error (MSE) and Peak Signal-to-Noise Rate (PSNR) measures are used. The method outperforms the other steganography techniques based on image domain published in the literature.

Anahtar Kelimeler: *Imge Steganografisi, Bilgi saklama*
Keywords: *Image* Steganography*, Information hiding*

1. GİRİŞ

Kısaca bilgi saklama sanatı olarak tanımlanan steganografide amaç gizli bir mesajı bilinen başka bir mesaj içinde saklayarak ilgili yere ulaştırmaktır. Bir başka deyişle steganografi veri içine veri gömerek gömülen verinin varlığını saklar. Gizli verinin gömülmesi için metin, ses, imge veya video gibi bir örtü verisi (cover data) kullanılır. Gizli verinin varlığını saklamak için gömme işlemi sonucunda örtü verisinin en az bozulmaya uğraması hedeflenir. Ayrıca örüntü verisine maksimum büyüklükte gizli veri saklamaya çalışılır [1][2].

Steganografinin kriptografiden (şifreleme) en önemli farkı steganografide saklı mesajın varlığının gizlenmesidir. Yani saklı verinin örtü verisi içine gömüldüğü bilgisi sadece mesajın alıcısı tarafından bilinir ve örtü verisine sahip olan bir başkası saklı verinin varlığını farkedemez. Kriptografide ise gönderilen verinin gizli olduğu herkes tarafından bilinir. İçeriği gizli anahtar olmadan anlaşılamaz ve gizli verinin anlaşılabilmesi için çok büyük çabanın ve zamanın harcanması gerekir. Eğer birbirleri ile gizli olarak haberleşen iki kişiyi gözletleyen üçüncü bir kişi haberleşmenin gizliliğini farkedecek olursa steganografi esas amacına ulaşamamış olacaktır. [3]

Steganografi ile sayısal damgalama (digital watermarking) arasındaki fark ise örtü verisindeki bozulmadan kaynaklanır. Steganografide gizli mesajın gömülmesiyle örtü verisinde farkedilmeyecek derecede de olsa bozulmaya izin verilirken, damgalama uygulamalarında gizli mesaj örtü

verisinin bir parçası olarak saklanır ve genellikle örtü verisinin bozulmasına izin verilmez.

İmge steganografisinde kullanılan yöntemler imge uzayı ve dönüşüm uzayı tabanlı yöntemler olmak üzere iki ana başlık altında toplanırlar [2]. İmge uzayını kullanan yöntemler imge piksel değerlerinin ikili düzendeki En Önemsiz Bitlerini (Least Significant Bit- LSB) kullanırlarken, dönüşüm uzayı tabanlı yöntemler imge verisini frekans uzayına dönüştürüp saklama işlemini bu uzayda gerçekleştirirler [2]. İmge uzayında yapılan işlemler göreceli olarak daha basit olmakla birlikte imge üzerinde yapılacak ufak değişmelere (filtreleme, boyutlarını değiştirme, sıkıştırma vb.) hassastırlar. Dönüşüm uzayında yapılan veri gizleme yöntemleri ise söz konusu değişikliklere daha fazla dayanıklılık göstermektedir. Ancak görüntü uzayına saklanan veriden daha az oranda veri saklama kapasitesine sahiptir [8].

Bu çalışmada LSB tabanlı yeni bir steganografi yöntemi önerilmektedir. Yöntem, imgeyi karelere bölerek gizlenecek veri bitlerini kare piksellerinin en önemsiz bitlerine saklar. Kare piksel değerleri en az bozulmaya uğrayacak şekilde gizli veri bit dizisi uygun satır veya sütuna saklanır. Önerilen yöntemin performans ölçümü steganografi analizlerine karşı güçlülüğünün değerlendirilmesiyle yapılmıştır. Bu amaçla, 100 farklı örtü imgesi kullanılarak rastgele seçilen gizli mesajların gömülmesi sonucunda imgelerin bozulma oranları hesaplanmıştır. Yapılan deneylerde önerilen yöntemin örtü imgelerini literatürdeki diğer LSB tabanlı yöntemlerden daha az bozduğu görülmüştür.

2. İMGE UZAYINI KULLANAN TEKNİKLER

İmge uzayını kullanan yöntemler bir mesajı örtü imgesine gömmek için imge piksellerinin en önemsiz bit veya bitlerini (LSB) kullanırlar. Bu amaçla mesaj bitleri seçilen piksellerin en önemsiz bitleriyle değiştirilir (EÖB değiştirme-LSB replacement) veya eşleştirilir (EÖB eşleştirme-LSB matching). EÖB değiştirmede çift sayı olan piksel değerleri bir arttırılır veya

değişmeden bırakılırken, tek sayılar bir azaltılır veya değişmeden bırakılır. EÖB eşleştirmede ise mesaj bitleriyle piksel bitleri eşleştirmeye çalışılır eğer eşleşmiyorlarsa örtü imgesi pikseli değeri rastgele olarak arttırılır ve azaltılır [7].

En basit şekliyle LSB değiştirme işlemi imgedeki satır veya sütunlara sıralı olarak yapılabilir. Ancak bu klasik yöntemde mesajın geri elde edilmesi kolaylaşır. Yöntemi daha güvenli hale getirmek ve mesajın geri elde edilmesini zorlaştırmak amacıyla mesaj bitlerinin gömüleceği imge pikselleri daha karmaşık bir şekilde seçilir. Örneğin ayrık logaritma fonksiyonu ile değiştirilecek pikseller rastgele belirlenir [8].

Diğer bir yöntemde [2][5], mesaj gömülecek imge pikselleri kenar bilgisi kullanılarak seçilir. Öncelikle imge kenar pikselleri Laplacian kenar bulma algoritmasıyla çıkartılır. Elde edilen piksel değerlerine bir eşik seviyesi uygulanarak mesajın gömüleceği pikseller belirlenir. Gömme işleminin hangi sırada yapılacağını belirlemek amacıyla bir yer seçim algoritması kullanılır. Gizli mesajın tekrar elde edilmesinde de aynı işlemler uygulanır. Kenar piksellerinin kullanılmasıyla yöntemin güvenliği arttırılmış ve steganaliz tekniklerinden daha iyi sonuç elde edilebilmektedir [2].

Referans [6]'da anlatılan veri gizleme işlemi için örtü imgesinde kullanılacak piksel ve piksel değerleri bir matematiksel algoritma ile belirlenir. Seçilen bu değerlerin hepsinin çift olması için ilk once ön işlemden geçirilir. Tüm tek değerlikli pikseller çift değerlere dönüştürülmekte, Müteakiben gizlenecek veri ile karşılaştırılmaktadır. Eğer gizlenecek veri tek ise piksel değeri tek olmakta, çift ise değişikliğe uğramamaktadır. Verinin geri alınması ise piksel değerlerinin tek veya çift olmasına bakılarak bulunur .

Bir başka çalışmada [1] ise örtü imgesi içine başka bir imge gömülmesi hedeflenmektedir. Öncelikle örtü imgesi karelere ayrılır ve her kareye gizlenecek imgenin bir pikseli saklanır. Saklama işleminde bir kare içerisinde saklanacak piksel değerine en yakın piksel bulunur. Bulunan bu

piksel saklanacak piksel değeri ile değiştirilerek stego-imge elde edilmiş olur.

EÖB Eşleştirme yönteminde EÖB değiştirme yöntemi üzerinde modifikasyon yapılarak gizli verinin kapak resmine işlenmesini öngörmektedir. İmge içerisinde veri gizleme işlemi herbir bit için ayrı ayrı yapılmak yerine piksel çiftleri kullanılır ve rastgele olarak örtü imgesinde seçilen piksel çiftlerinin değerleri arttırılır/azaltılır [7]. Bu şekilde normal LSB yönteminde gizlenen veri oranı değişmemiş olur ancak örtü imgesindeki değişen piksel değerlerinin değişim oranının azalması sağlanır [7]. Sonuç olarak bu yöntemin klasik LSB yöntemine istinaden örtü imgesinde değişim azalmakta ve analizlere karşı dayanıklılığı artmaktadır [7].

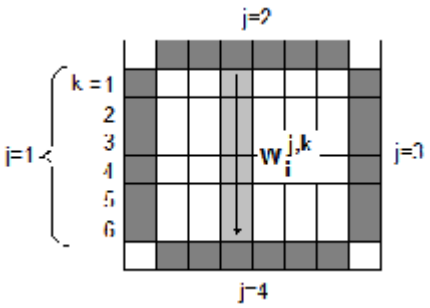
3. ÖNERİLEN YÖNTEM

Bu çalışmada önerilen yöntem örtü imgesini karelere böler ve kare boyutuyla orantılı sayıda mesaj bitini söz konusu karenin en önemsiz bitlerine gömer. Her kare içinde en az sayıda pikseli değiştirmek amacıyla mesaj bitlerinin gömüleceği en uygun satır veya sütunu seçer. Soldan sağa ve sağdan sola tüm satırlar ile yukarıdan aşağıya ve aşağıdan yukarı sütunlarda arama yapılarak gizlenecek mesaj bit dizisine en yakın olan satır/sütun bulunur. Gizli mesaj bulunan satır/sütuna gömülür.

Ancak geri dönüşüm için gömme işleminin yapıldığı satır/sütunun işaretlenmesi gerektiğinden örtü imgesindeki karelerin çerçeve pikselleri işaretleme amacıyla kullanılır ve mesaj gömme bu piksellerde yapılmaz. Şekil 1'de gösterilen örnek imge karesinde işaretleme pikselleri koyu renkle boyanmıştır.

Matematiksel olarak ifade edecek olursak; bir imgenin n adet kareye bölündüğünü ve her karenin w_i, $i=1...n$, m adet satır ve sütuna sahip olduğunu varsayalım.

Karelerin *1.* ve *m.* satır ve sutunları (çerçeve) işaretleme amacıyla kullanılacağından bir kareye *m-2* bitlik mesaj parçası, msg_i gömülebilir. Dolayısıyla imgeye *nx(m-2)* bit uzunluğunda bir mesaj saklanabilir.



Şekil 1: İmge karelerinde arama yapılan satır/sütunlar

Saklama işleminde, msg_i'ye w_i içindeki en yakın satır veya sütunun bulunması;

$$(p, r) = \min_{j,k} \left\{ d\left(msg_i, w_i^{j,k}\right) \right\} \quad j = 1...4 \;,\; k = 1...m - 2 \qquad (1)$$

olarak ifade edilebilir.

Yukarıdaki denklemde *j* değişkeni soldan sağa ve sağdan sola satırlar ile yukarıdan aşağı ve aşağıdan yukarı sütunları ifade etmektedir. Bir başka deyişle *4* farklı satır ve sütun yönünü belirtmektedir. Değişken *k*, ise her yöndeki *m-2* adet satır/sütunu gösterir. Şekil-1'de örnek imge karesinde bu değişkenler gösterilmiştir. Uzaklık ölçümünde *d(.)*, Manhattan uzaklık fonksiyonu kullanılmaktadır. Özetle kare içindeki toplam *4x(m-2)* adet alternatif bit dizisi arasından msg_i'ye en yakın olan satır/sütunun hangi yönde, *p*, ve kaçıncı sırada olduğu, *r*, bulunur.

Bu işlemin sonucunda bulunan satır/sütundaki pikseller, LSB değiştirme yönteminde olduğu gibi, çiftten teke veya tekten çifte dönüştürülerek mesaj

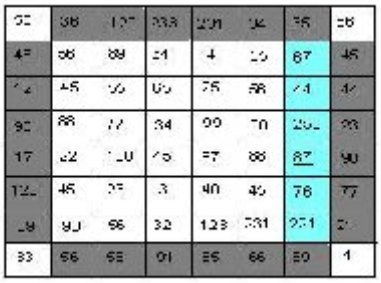
bit dizisiyle değiştirilirler. Değiştirilen satır/sütunun başındaki çerçeve biti $S_{p,r}$ işaretlenir. İşaretleme işlemi de benzer şekilde çiftten teke veya tekten çifte dönüştürerek yapılır.

Yukarıda anlatılan yöntemi bir örnek üzerinde açıklayacak olursak; örtü imgesinin 8X8'lik karelere bölündüğünü ve örnek karemizin şekil-2.a'daki piksellere sahip olduğunu varsayalım. Söz konusu imge karesine saklamak istediğimiz mesaj bit dizisi ise : [1 0 0 1 0 1] olsun.

Kare içindeki piksellerin en önemsiz bitleri üzerinde yapılan (1)'deki arama işlemi ile mesaj bit dizisine en yakın satır/sütun bulunur. Çerçeve satır ve sütunlar işaretleme amacıyla kulllanıldığından 8x8'lik karede 6 bit uzunluğundaki bit dizileri üzerinde arama işlemi yapılır. Bu örnekte yukarıdan aşağıya 6. sütundaki pikseller mesaj bit dizisine en yakın olarak bulunmuştur. Bir başka deyişle (1)'deki işlemin sonucu (2,6) olarak hesaplanır. Şekil-1'de de gösterildiği gibi 2 yukarıdan aşağıya sütunları 6 ise bu sütunlardan kaçıncısı olduğunu ifade etmektedir.

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	04	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	55	07	[illegible]
[illegible]	45	[illegible]	[illegible]	[illegible]	[illegible]	44	[illegible]
11	[illegible]	[illegible]	04	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	67	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
08	[illegible]	[illegible]	32	[illegible]	[illegible]	22	[illegible]
[illegible]	[illegible]	[illegible]	81	[illegible]	[illegible]	[illegible]	[illegible]

(a)



(b)

Şekil 2: Örnek 8X8'lik imge karesine 1 0 0 1 0 1 mesajının saklanması; (a) Orjinal kare, (b) Saklama işleminde değiştirilen pikseller.

Söz konusu sütunda, [67, 44, 250, 86, 76, 221] piksel değerlerinin en önemsiz bitleri kodlandığında [1 0 0 0 0 1] değeri elde edilir. Mesaj bitin saklanması için sadece 4. biti 0'dan 1'e dönüştürmek yeterli olacaktır. Bu işlem yapıldığında 86 piksel değeri 87 olarak değiştirmiş olur. Daha sonra (2,6) çerçeve pikselin en önemsiz biti, $S_{2,6}$, işaretlenir ve 34 olan değeri 35 ile değiştirilir.

Saklanan mesajın geri elde edilmesinde ise imge karelere bölündükten sonra her kare içinde hangi çerçeve bitinin değiştiği tespit edilir. Bu bitin işaretlediği satır/sütundaki piksellerin en önemsiz bitleri alınarak gizli mesaj çıkarılır.

4. DENEYLER

Steganografi yöntemlerinin performansı, steganaliz yöntemlerine karşı güçlülüğüyle değerlendirilmektedir. Steganaliz yöntemleri öncelikle bir örtü verisinde bilgi gizlenip gizlenmediğini tespit ederler, bu işleme sezme (detection) adı verilir. Daha sonra gizli bilgi saklandığı tespit edilen verideki bilgiyi elde etmeye çalışılır. Bu işleme ise çelme (extraction) denir.

Sezme işleminin başarısız olabilmesi için gerçek imge üzerinde yapılacak değişikliklerin en az seviyede tutulması gereklidir. Bu nedenle örtü imgesi

ile gizli veri işlendikten sonra stego-imgesi arasındaki ortalama karesel hatanın bulunması ve PSNR'nın değerinin elde edilmesi geliştirilen yöntemlerin başarısı hakkında fikir elde etmemizi sağlayacaktır [2].

Ortalama karesel hata iki imge arasındaki farkı belirtmek için kullanılmaktadır :

$$\mathrm{MSE} = \frac{1}{\mathrm{MN}} \sum [\mathrm{I1(m,n)} - \mathrm{I2(mn,)}]^2 \qquad (2)$$

Yukarıda I_1 ve I_2 sırasıyla örtü imgesi ve stego imgelerini, M ve N imge boyutlarını göstermektedir. R bir pikselin alabileceği en yüksek değeri belirtmek üzere, PSNR ise MSE'ye bağlı olarak örtü imgesinde yapılan değişikliğin analizinde kullanılmaktadır :

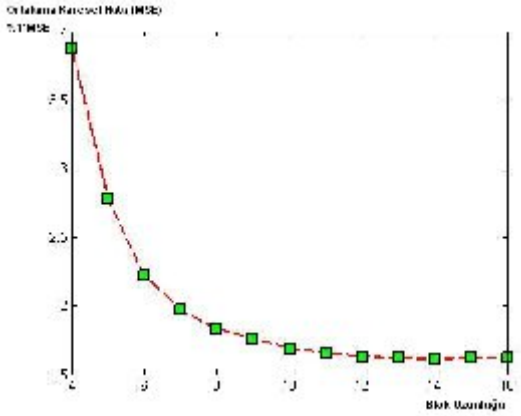
$$PSNR = 10 \log_{10} \frac{R^2}{MSE} \qquad (3)$$

Steganalizin sezme aşamasında imge pikselleri arasındaki farklılıklar gözlenmektedir. Eğer bu farklılıklar beklenen değerlerin aksine değişiklik gösterirse bu imgede gizli veri var denilebilir. Bunun önüne geçebilmek için steganografide örtü imgesi mümkün olduğunca aynı bırakılmaya çalışılmaktadır. Bu sebeple MSE ve PSNR ölçümleri steganografi yöntemlerinin performans değerlendirmesinde kullanılan yöntemlerdendir.

Önerilen yöntem rastgele seçilen 256x256 boyutunda 100 adet gri seviyeli imgelerde denenmiştir. Deneylerde değişik kare boyutları kullanılarak imge bozulmasını en aza indirgeyen kare boyutu bulmaya çalışılmıştır. Şekil-3'de gösterilen grafikte 4 ile 16 arasındaki kare boyutlarında Ortalama Karesel Hata değerleri plotlanmıştır. Önerilen Yöntem bölümünde anlatıldığı gibi her imge karesine kare boyutuna bağlı uzunlukta mesaj biti saklanabilmektedir. Tüm imgede saklanabilecek mesaj uzunluğu kare boyutu yükseldikçe azalmaktadır. Örneğin 4x4'lük kare boyutunda 8192 bit mesaj saklanabilirken 16x16 karelerde 3584 bit

saklanabilmektedir. Deneylerde MSE ölçümünü eşit şartlarda yapmak amacıyla tüm kare boyutlarında en düşük mesaj boyutu olan 3584 bit uzunluğunda rastgele mesaj biti kullanılmıştır. Şekil-3'de görüldüğü üzere en düşük MSE oranı 14x14'lük kare boyutlarında elde edilmiştir.

Önerilen yöntemin literatürdeki diğer çalışmalarla karşılaştırmasında en iyi sonucun alındığı 14x14'lük kare boyutları kullanılmış ve bu kare boyutuna bağlı olarak 3888 bit uzunluğunda mesaj saklanmıştır. Karşılaştırma yapılan diğer tüm çalışmalarda da söz konusu mesaj uzunluğu kullanılmıştır.



Şekil 3: Blok (kare) uzunluğuna bağlı MSE değerleri

Karşılaştırma / Yöntemler	MSE	PSNR
LSB	0.028402	63,63
A New Algorithm for Hiding Gray Images Using Blocks [1]	0.407495	52,06
Hiding Secret Message in Edges of the Image [2]	0.029459	63,47
An Architecture Platform for Grey LeveI Modification Steganography [6]	0.029875	63,41
LSB Matching Revisited [7]	0.021988	64,74
Önerilen Yöntem	**0.017593**	**65,71**

Tablo 1 : Değişik yöntemlerin ve önerilen yöntemin MSE ve PSNR olarak karşılaştırılması

Tablo 1'den de anlaşılacağı üzere yapılan deneyler sonucunda 100 resmin ortalaması alındığında en düşük MSE değeri önerilen yöntemde elde edilmektedir. Bunun sonucu olarak en yüksek PSNR değeri de önerilen yöntemle bulunmuştur. Ayrıca önerilen yöntemde, gizlenecek verinin uzunluğunun % 29,6'sı (% Gizlenecek mesajın işlenmesi için örtü imgesinde değişmesi gereken bitlerin sayısı / toplam gizlenecek mesajın bit sayısı) oranında işaretlenen örtü imgesi piksellerinde değişiklik yapılması gerektiği görülmektedir.

5. SONUÇ

Bu çalışmada örtü imgesini kareler bölerek her kareye bir dizi mesaj biti saklayan yeni bir steganografi yöntemi önerilmiştir. Kare içerisinde gizlenecek mesaja en uygun dizinin (satır/sütun) yeri tespit edilerek işaretlenmekte ve seçilen dizi uygun modifikasyon işlemlerine tabi tutulmaktadır.

Örtü imgesinin bozulmamasını temin etmek ve güvenli iletiminin yapılabilmesini sağlamak steganografik yöntemlerin en önemli amaçlarından ikisini oluşturmaktadır. Bu nedenle yapılan çalışmalarda MSE ve PSNR'ler dikkate alınmaktadır. 100 imge üzerinde ve rastgele üretilen gizli mesaj bitlerinde yapılan deneylerle önerilen yöntem literatürdeki diğer imge uzayı kullanan çalışmalarla karşılaştırılmıştır. Deneyler sonucunda önerilen yöntemin diğer yöntemlere göre daha düşük oranda MSE ve daha yüksek oranda PSNR elde ettiği görülmüştür.

Önerilen tekniğin iyileştirilmesi kapsamında müteakip yapılacak çalışmalarda MSE'nin en aza indirilmesinin ve güvenli iletimin sağlanması amacıyla karelerin sırayla işlenmesi yerine rastgele seçilmesinin faydalı olacağı değerlendirilmektedir. Ayrıca gelecek çalışmalarda imge ve dönüşüm uzayının birlikte kullanıldığı melez bir algoritma geliştirilmesi planlanmaktadır.

KAYNAKÇA

[1] Samer Atawneh, A New Algorithm for Hiding Gray Images Using Blocks, *IEEE 2006, Information Systems Security, Volume 15, Issue 6 December 2006.*

[2] Kh.Manglem Singh, L.Shyamsudar Singh, A.Buboo Singh, Kh.Subhabati Devi, Hiding Secret Message in Edges of the Images, *Information and Communication Technology Conferance, 2007.*

[3] Jian Liu, Xiangjian He, A Review Study on Digital Watermarking*, Information and Communication Technologies Conferance, 2005.*

[4] Vidyasagar M.Potdar, Song Han, Elizabeth Chang, A Survey of Digital Image Watermarking Techniques*, 3rd IEEE International Conference 2005.*

[5] Mrs.ShantalaSureh, Dr.Vishvanath, "Edge-Steganography" for Secure Communication, *2006 IEEE Region 10 Conference.*

[6] Muhammad A.Khan, Vidyasagar Potdar, Elizabet Chang, An Architecture Platform for Grey LeveI Modification Steganography, *The 30th Annual Conference of the IEEE Industrial Electronics Society, November2-6, 2004.*

[7] Jarno Mielikainen, LSB Matching Revisited, *Signal Processing Letters, IEEE 2006.*

[8] Andaç Şahin, Görüntü Steganografide Kullanilan Yeni Metodlar ve Bu Metodlarin Güvenilirlikler, *Trakya University 2007.*