STEGANOGRAFİK KÜTÜPHANE

Zekeriya ERKİN[1] **Bülent ÖRENCİK**[2]

[1,2]Bilgisayar Mühendisliği Bölümü

Elektrik-Elektronik Fakültesi
İstanbul Teknik Üniversitesi, 34469, Maslak, İstanbul
[1]e-posta: erkin@ce.itu.edu.tr [2] e-posta: orencik@ce.itu.edu.tr

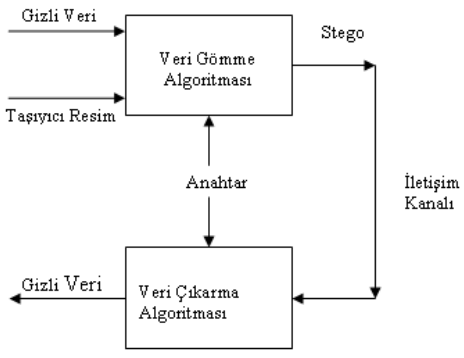
Anahtar sözcükler: Steganografi, Kriptografi, Gizli Yazı, İnternet Güvenliği, Gizli İletişim

ABSTRACT

This paper presents a new software library in which there are several novel studies proposed on Steganography. Library is implemented with an object oriented programming language enabling its users to add new methods easily. The efficiency of the methods implemented in the library is also presented in this paper.

1. GİRİŞ

Steganografi, gizli verinin masum içeriğe sahip ve taşıyıcı olarak adlandırılan bir başka veri içersinde saklanması olarak tanımlanabilir. Bu saklama işlemi için kullanılan algoritma gizli değildir ancak güvenlik algoritma için kullanılan anahtar ile sağlanmaktadır. İçersinde gizli veri bulunduran taşıyıcıya "stego" adı verilmektedir. Stego herhangi bir yolla alıcıya ulaştırılır. Alıcı veri saklama algoritmasının tersi olan bir işlemle gizli veriyi, anahtarı da kullanarak ortaya çıkarır (Şekil 1).



Şekil 1: Steganografi Sistemi

Bu çalışmada temel steganografik yöntemler özetlenmekte ve akademik olarak üzerinde yeni yoğunlaşılan bu konu üzerindeki problemler ortaya konulmaktadır. En temel problemlerden biri olan test ortamının hizmete sunulması için hazırlanan steganografi kütüphanesi ele alınacaktır. Araştırmacıların karşılaştığı yazılım güçlüğüne bir çare olarak düşünülen steganografik kütüphane resim dosyalarını taşıyıcı olarak kullanmakla beraber ses dosyaları da yapısı gereği kütüphaneye kolayca eklenebilir.

2. STEGANOGRAFİDEKİ TEMEL YÖNTEMLER

Steganografi, Yunanca "gizli yazı" anlamına gelmektedir. Bruce Schneider steganografiyi, gizli mesajı masum başka bir mesajın içerisinde varlığını saklamak amacıyla gömme işlemi olarak tanımlamaktadır[1]. Günümüz bilgi teknolojisinin bize sağlamış olduğu ortamda resim, ses, metin dosyaları gizli mesajın saklanması açısından elverişli bir ortam sunmaktadır. Bunlara ek olarak sabit disklerin ve disketlerin kullanılmayan alanları, IP paketlerinin başlık kısmındaki ayrılmış alanları gibi ortamlar gizli mesajın saklanması açısından elverişlidir. Tüm bu geniş olanaklara karşın sağlamış olduğu yüksek miktardaki ham veri miktarıyla resim dosyaları steganografi konusunda çalışan birçok araştırmacının gizli mesajı saklamak için tercih ettiği bir dosya türüdür[2].

Resim dosyaları piksel adı verilen renk değerlerinin belirli bir düzenle bir araya gelmesiyle anlamlı bir görüntü oluşturmaktadır. Renk değerlerinin ve resmin büyüklüğü resim dosyasının barındırdığı veri miktarını belirlemektedir. 600x800 piksel büyüklüğündeki bir resim dosyasında her bir renk değeri tek bir bayt ile temsil edildiğinde 464 KB'lık bir veri yığını, 3 bayt ile temsil edildiğinde 1,5 MB'lık bir veri yığını ortaya çıkmaktadır. Bu büyüklükteki veri içerisinde gizli mesaj saklamak için çeşitli yöntemler geliştirilmiştir. Bu yöntemlerden en basiti, renk değerlerinin en düşük anlamlı bitlerinin değiştirilmesi ilkesi ile çalışır. Bu yöntem değiştirilen düşük anlamlı bit sayısına bağlı olarak yüksek

miktarda gizli bilginin resim dosyasında saklanmasına olanak sağlamaktadır. Ancak, oldukça kolay bir şekilde uygulamaya geçirilebilecek bu yöntemde, resim dosyası resim işleme tekniklerine karşı oldukça duyarlıdır. Resmin parlaklığının küçük bir değişimi bile içerisinde barındırdığı gizli mesajın yok olmasına neden olur. Bu yöntemin zayıf noktasından hareketle steganografik algoritma sonucunda içerisinde gizli bilgi barındıran resim dosyasının görüntü işleme tekniklerine dayanıklı olması gerektiği ortaya çıkmaktadır. Bu işleme yöntemlerinden en önemlisi sıkıştırma işlemidir. 1,5 MB ve hatta 464 KB'lık resim dosyaları İnternette paylaşmak için oldukça büyük sayılmaktadır. Bu nedenle çeşitli algoritmalarla sıkıştırılmaktadırlar. Bu sıkıştırma işlemi için kullanılan algoritmalardan en yaygın olanı JPEG sıkıştırmasıdır. Bu algoritma, ayrık kosinüs dönüşümü ile resim dosyasını oluşturan veriyi frekans düzlemine çekmekte ve bu düzlemde resmin tekrar oluşturulması için gerekmeyen frekanslardaki katsayılar yok etmektedir. Bu yöntem resim dosyasının kalitesini değiştirmekle beraber 40 kata varan oranda sıkıştırma sağlamaktadır. JPEG sıkıştırmasına dayanıklı bir steganografik yöntemin ayrık kosinüs dönüşümünü hesaba katması gerektiği ortadır. Önerilen yöntemler frekans katsayılarının gizli mesajın bitlerini barındırmak üzere değiştirilmesine dayanır[4], [5], [6]. Ancak, birçok durumda resmin gözle görülebilir bir şekilde bozulması bu yöntemlerde engellenememektedir. Önerilen başka bir yöntem yine frekans düzleminde çalışmaktadır ancak, gizli bilgi saklanmadan önce frekans spektrumunda yayılır[7], [8]. Spektrumu genişletilen mesaj görüntü işleme tekniklerine karşı oldukça dayanıklıdır. Yapı itibariyle birden fazla banda yayılan mesaj, bir veya birden fazla bantta bozulsa bile geri kalan bantlar yardımıyla gizli mesaj oldukça başarı bir şekilde alıcı tarafından ortaya çıkarılmaktadır. Ne var ki, bu yöntemde gizli mesajın birden fazla frekans bandına yayılması ve alıcının gizli mesajı okuma olasılığını arttırmak için kullanılan hata düzeltme kodları gönderilebilecek veri miktarını azaltmaktadır.

Akademik dünyada resim dosyalarının içerisinde gizli mesaj saklamak için önerilen yöntemler arasında resmin istatistiksel değerleriyle oynanması suretiyle alıcıya mesaj gönderme de vardır. Bu yöntemlerden birinde resim rasgele iki parçaya bölünür ve bu parçalardan birinin her renk değeri gömülecek bilgi bitine karşılık artırılır veya aynı kalır[9]. Karşı taraf, bu iki parçanın ortalama renk değerini hesaplayarak karşı tarafın "0" veya "1" gönderip göndermediğini inceler. Yöntemden de anlaşıldığı üzere gönderilebilecek bilgi miktarı bir kaç biti geçmemektedir. Bunun dışında gönderilmek istenen gizli mesajdan hareketle resim oluşturulması da araştırma konusudur. Ancak bu yöntem ile oluşturulan yapay resimler çıplak gözle bile kolayca kendini ele vermektedir[10].

3. STEGANOGRAFİK KÜTÜPHANE

Bu çalışmada amaç steganografi üzerinde çalışan araştırmacıların bir önceki bölümde ana hatlarıyla ortaya konulan temel yöntemler üzerinde çalışmalarına olanak vermektedir. Ne yazık ki yapılan birçok akademik çalışmanın yayınlanması aşamasında yöntemlere ilişkin ayrıntılar ortaya konulamamaktadır. Görüntü ve işaret işleme tekniklerinin yoğun olarak kullanıldığı steganografide ortaya konulan çalışmalardaki ölçümleri incelemek ve gerekirse tekrarlamak ve yine bahsi geçen yönteme ilişkin iyileştirmeler yapmak için yayınlanan çalışmanın aslı gerekmektedir. Maalesef çalışmada kullanılan asıl yazılım araçlarına ulaşmak her zaman mümkün olmamaktadır.

Steganografik kütüphane steganografi konusunda yayınlanmış önemli çalışmaların gerçeklendiği bir ortam sunmaktadır. Amacı araştırmacılara inceledikleri yöntem hakkında irdeleme ve gerekirse iyileştirme yapma olanağı sağlamak olduğu için platformdan bağımsız bir kütüphane çalışması gerçekleştirilmiştir. Kütüphane yazılımı için seçilen Java programlama dili, nesneye dayalı bir programlama dilidir ve platformdan bağımsızdır. Kütüphane için nesneye dayalı bir dilin kullanılması araştırmacılara geliştirme ortamı sunmak için önemlidir.

Kütüphanede temel olarak dört ana paket bulunmaktadır:

- Yer değiştirme algoritmalarına dayanan yöntemlerin bulunduğu paket
- Frekans düzleminde katsayıların değiştirilmesine dayanan yöntemlerin bulunduğu paket
- Yayılmış spektrum kullanımına dayanan yöntemlerin bulunduğu paket
- İstatistiksel algoritmalara dayanan yöntemlerin bulunduğu paket

Yer değiştirme algoritmalarına dayanan yöntemlerin bulunduğu pakette, steganografi konusunda gerçekleştirilen ilk nesil çalışmalar ortaya konulmaktadır. Bu algoritmalar gerçekleştirilmesi kolay olmakla beraber güvenliğin yüksek düzeyde gerektiği ortamlar için oldukça zayıftırlar. Ancak, sağlamış oldukları yüksek veri saklama imkânı ile birçok düşük güvenlik düzeyindeki uygulamalar için oldukça elverişlidirler.

Bu pakette yer alan yöntemler temelde insan gözünün küçük değişimleri fark edememesi ilkesini kullanmaktadır. Resim dosyalarında temsil edilen renk değerleri ile oynanarak büyük miktarda veri saklamak mümkündür. [3] renk değerlerinin dosyada hangi büyüklükte saklanırsa, dosya içerisinde ne kadar veri saklanabileceğini yansıtmaktadır.

Verinin renk değerlerinin en düşük anlamlı bit değerlerinde saklanabilmesi için önerilen birçok yöntem vardır. Kütüphane dâhilinde bu yöntemlerden en belirgin olanlar gerçeklenmiştir. Veri saklamak için ardışık ve rasgele renk değerlerini kullanan yöntemler geliştirilmiştir. Ayrıca, gizli verinin her bir renk değerinde bir bitinin saklanması yerine belirli bir blokta tek bir bitin eşlik biti hesaplanması yöntemine göre saklanması yine bu pakette yer almaktadır. Açıkça görülebileceği gibi bahsedilen ilk iki yöntemde her biri bitin değişikliğe uğrama ihtimali %50 iken, eşlik biti hesabına dayanan yöntemde seçilen bölgede yalnızca tek bir bit %50 ihtimalle değişime uğrayacaktır. Ancak, bu önemli avantajına karşılık kapasite kullanımı seçilen bölge büyüklüğü ile ilintili olarak azalmaktadır.

Kütüphanede bulunan ikinci pakette, frekans düzleminde çalışan algoritmalar gerçeklenmiştir. Renk değerleri ayrık bir işaretin katsayıları olarak kabul edilirse, bu işaretin frekans düzlemine taşınması ve tekrar frekans düzleminden renk değerlerinin hesaplanması mümkündür. Ancak, renk değerlerinden oluşan ayrık işaretin frekans düzlemine taşınmasındaki asıl amaç, birçok sıkıştırma algoritmasının frekans düzleminden geri dönerken kayıplı bir yöntem izlemesinden kaynaklanmaktadır. Geri dönüşteki kayıp tekrar oluşturulan resmin kalitesi ile ters orantılı olmakla beraber birçok durumda bu kayıplı geri dönüş işlemi resim dosyasının boyutunu ciddi bir şekilde küçültürken, kayıptan kaynaklanan değişim gözle görülemeyecek kadar önemsizdir. Steganografi, sıkıştırma algoritmalarından en çok kullanılan JPEG sıkıştırma algoritmasında kullanılan yöntemi resim içerisinde veri saklamak için kullanmaktadır. Pakette frekans düzleminde sıkıştırma amacıyla feda edilemeyecek katsayılar özenle seçilip, saklanacak gizli veri bitine uygun olarak değiştirilmelerini öngören yöntemler gerçeklenmiştir. Bu yöntemle oluşturulan ve içerisinde gizli verinin bulunduğu resim dosyalarının basit görüntü işlemleri ve JPEG sıkıştırmasına karşı dayanıklı olması beklenmektedir.

Yer değiştirme ve frekans düzleminde katsayılar üzerinde oynama işlemi yapan algoritmalar çeşitli düzeyde güvenlik ihtiyacının hissedileceği uygulamalara uygun olmakla beraber, beraberinde getirdikleri bazı teknik sorunlardan dolayı yüksek güvenliğin gerektirdiği aktif dinleyici senaryosunda yararlı olamamaktadırlar. Steganografi için sayısal ortamda aktif dinleyicinin çeşitli saldırılarına karşı dayanıklı olduğu öne sürülen spektrum yayılmasına dayanan yöntem yine steganografik kütüphaneye alınmıştır. Temeli askeri iletişimde kullanılan yönteme dayanan bu konudaki çalışmalarda, saklanmak istenen veri gerektiğinden çok daha fazla frekans bandına yayılır ve bu şekilde resme gürültü olarak eklenir. İletim ortamında gerçekleşecek birçok saldırı sonucunda yeterli frekans bandında veri bulunması durumunda gizli veri bozulmamış bir şekilde alıcı tarafından elde edilebilmektedir.

Kütüphanenin son paketinde istatistiksel yöntemler incelenmiştir. Bu pakette yer alan yöntemler resmin bütününde işlem gerektirmektedir. Alıcı ve gönderenin üzerinde anlaştığı bir *f* hipotez fonksiyonu resme uygulandığında fonksiyon *"0"* veya *"1"* gönderilip gönderilmediğini ortaya koymaktadır. Ancak bu şekilde çalışması planlanan sistemlerde en büyük sorun uygun bir *f* fonksiyonunun bulunmasıdır.

4. STEGANOGRAFİK KÜTÜPHANENİN BAŞARIMI

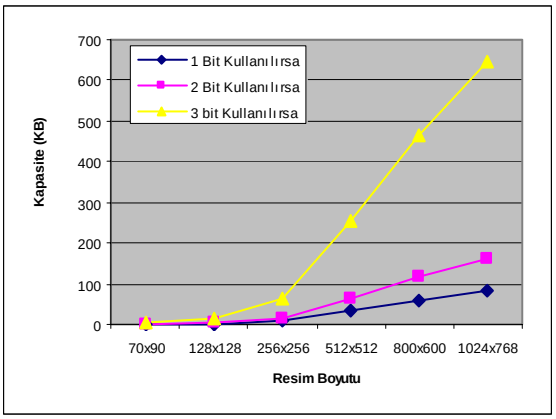
Steganografik bir yöntem önerildiğinde temel olarak 3 ana başlık altında bu yöntem incelenmektedir:

- Yöntemin kapasite kullanım miktarı
- Yöntemin taşıyıcı üzerinde gerçekleştirdiği değişim miktarı
- Yöntemin saldırılara dayanıklılığı

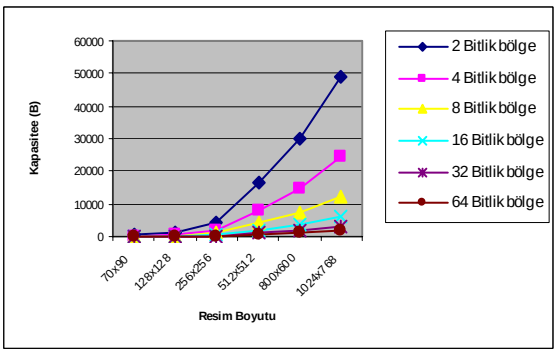
Steganografinin amacı, gizli bilginin karşı tarafa başka hiç kimseye fark ettirilmeden taşınması olarak tanımlanırsa taşıyıcının kapasite miktarının önemli olduğu ortaya çıkmaktadır. Öte yandan, taşıyıcının saldırılara dayanıklı olması istense de, steganografiyi gizli damgadan (watermarking) ayıran en önemli özellik, steganografinin yüksek kapasite ihtiyacıdır. Oysa gizli damgada küçük miktardaki veri olası tüm saldırılara karşı korunmak istenmektedir. Ancak, her iki yöntemde de taşıyıcının ciddi bir şekilde değişmemesi asıldır.

Kütüphanede gerçeklenen her paketteki örnek yöntemler, yukarda belirtilen özellikler çerçevesinde incelenmiştir.

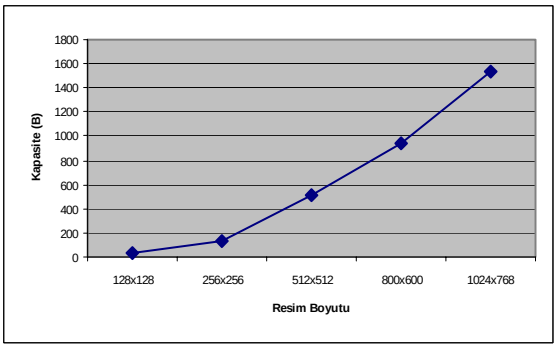
Şekil 2'de ardışık ve rasgele seçilen renk değerlerinin en düşük anlamlı bitlerinin değiştirilmesi ile saklanabilecek veri miktarı gösterilmektedir. Şekil 3'de resim içerinde çeşitli boyutlarda seçilecek bölgeler için eşlik biti hesaplama yöntemiyle saklanabilecek veri miktarı; Şekil 4'de de frekans düzleminde katsayıların değiştirilmesi yöntemiyle gerçeklenen yöntemlerin veri saklama kapasitesi verilmektedir.



Şekil 2: Yer değiştirme algoritmalarına dayanan yöntemlerin bilgi gömebilme miktarı



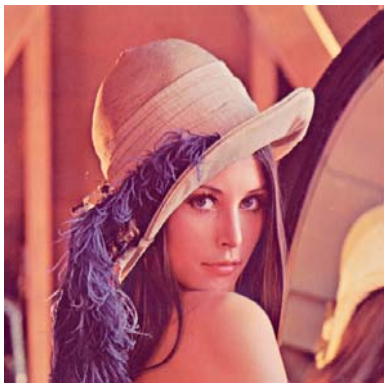
Şekil 3: Eşlik biti hesabına dayanan yöntemlerin kapasite miktarı



Şekil 4: Frekans düzleminde katsayı değiştirmeye dayanan yöntemlerin kapasite miktarı

Spektrum yayılmasına dayanan yöntemlerde saklanabilecek veri miktarı seçilen dikey kod uzunluğuna bağlıdır. Ancak, seçilen dikey kod uzunluğu resim renk değerlerinin sayısını geçemez ve dikey kodun büyüklüğü ile beraber işlem yükü artar. İstatistiksel yöntemlerin birçoğu her resim dosyası başına 1 bit gömebilmektedir.

Steganografik kütüphanede gerçeklenen algoritmalar dayanıklılık açısından da incelenmiştir. İlk pakette yer alan yer değiştirme algoritmalarına dayalı yöntemler öngörüldüğü gibi en ufak görüntü işleme yöntemlerine karşı bile oldukça dayanıksızdır. Şekil 5'teki taşıyıcı resme, Şekil 6'te gösterilen resim dosyası gizlenmiştir. İçerisinde gizli veri taşıyan resim dosyasının parlaklık bilgileri ile oynandığında, gizli veri tekrar elde edilememiştir.



Şekil 5: Taşıyıcı resim

Şekil 6: Gizli veri

Benzer şekilde, Şekil 5'teki taşıyıcı resim içerisine Şekil 6'teki gizli veri, ikinci pakette yer alan frekans düzleminde katsayıların değiştirilmesine dayanan yöntemlerle gizlenmiştir. Parlaklığın artırılması ve benzer resim değiştirme işlemleri gizli verinin tekrar elde edilmesine engel olamadığı gibi JPEG algoritması ile gerçekleştirilen ve taşıyıcının %40 resim kalitesi ile sıkıştırılması durumunda dahi gizli veri elde edilebilmektedir. Ne var ki, bu yöntemde sıkıştırma işlemine dayanıklılık arttırıldığında resimde insan gözünün algılayabileceği bozulmalar gerçekleşmektedir.

Şekil 7: Taşıyıcı resim

Şekil 7 içerisine Şekil 6'ta gösterilen gizli veri spektrum yayılmasına dayanan yöntemle

gömülmüştür. Beklendiği gibi, taşıyıcı dosya üzerinde gerçekleştirilen ciddi bozulmalara rağmen, gizli veri bu yöntemle alıcı tarafında başarıyla elde edilmektedir (Şekil 8).

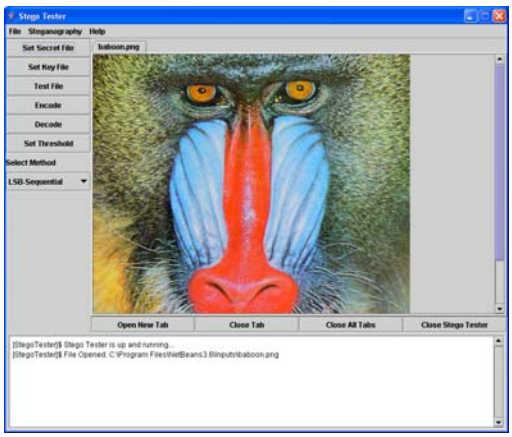
Şekil 8: Bozulmuş taşıyıcı resim

Steganografik kütüphanede yer alan son pakette istatistiksel yöntemler gerçeklenmiştir. Ancak, taşıyıcı resim dosyası başına saklanabilen *"1"* bit oldukça düşük bir kapasite miktarını yansıttığı gibi başarılı bir *f* hipotez fonksiyonun bulunmasının güçlüğü ortaya çıkmıştır. Çalışmalarda önerilen hipotez fonksiyonlarının taşıyıcı resimdeki küçük değişimlere karşı duyarlı olduğu kütüphanede gerçeklenen yazılım dâhilinde tespit edilmiştir.

5. SONUÇLAR VE OLASI ÇALIŞMALAR

Steganografik kütüphane araştırmacıların steganografi alanında araştırma yaparken incelemek isteyecekleri en temel yöntemleri içeren bir ortam sağlamaktadır. Kullanılan nesneye dayalı programlama dili ve sağlanan belgeler ile geliştirilmeye açıktır.

Kütüphanenin kullanımını göstermek için grafiksel bir ara yüz (Şekil 9) hazırlanmıştır. Bu ara yüz ile kütüphane dâhilindeki tüm yöntem sınıflarının ve bu sınıflara ait yöntemlerin nasıl kullanılacağı gösterilmektedir.



Şekil 9: Steganografik kütüphane ara yüzü

Steganografik kütüphane, ara yüzü ve belgeler ile tamamlanmıştır. Ancak, yeni yöntemler araştırmacılar tarafından kolayca eklenebilir durumdadır. Steganografik kütüphanedeki algoritmaların sağlamlığını arttırmak amacıyla hata düzeltme kodlarının ve ticari uygulamalarda kullanılabilmeleri için şifreleme algoritmalarının eklenmeleri gerekmektedir.

KAYNAKLAR

[1] **Schneier, B**., 1996. Applied Cryptography-Protocols, Algorithms and Source Codes in C, *2. Baskı*, John Wiley and Sons, New York.

[2] **Zilnerr, J., Federrath, H., Klimat, H., Pfitzmann, A., Piotraschke, R., Wesfeld, A., Wicke, G. and Wolf, G**., 1998. Modeling the Security of Steganographic Systems, *Proc. 2nd Workshop on Information Hiding*, Nisan, LNCS 1525, Springer-Verlag, Portland.

[3] **Chandramouli, R., Memon, N.**, 2001. Analysis of LSB Based Image Steganography Techniques, *Proceedings of the International Conference on Image Processing*, Thessalonica, Ekim, Yunanistan, 1019-1022.

[4] **Katsenbeisser, S. and Petitcolas, F.,** 2000. Information hiding Techniques for Steganography and Digital Watermarking, Artech House, Boston.

[5] **Ogihara, T., Nakamura, D. and Yokoya, N.,** 1996. Data Embedding into Pictorial Images with Less Distortion Using Discrete Cosine Transform, Proc. 13th IARP Int. Conference on Pattern Recognition, **1** , 675-679.

[6] **Zhao, J. and Koch, E.,** 1995. Embedding Robust Labels into Images for Copyright Protection, Proceedings of the International Conference on Intellectual Property Rights for Information, Knowledge and New Techniques, Münih, 242-251.

[7] **Pickholtz, R. L., Schilling, D. L. and Milstein, L. B.,** 1982 .Theory of Spread-Spectrum Communications-A Tutorial,. *IEEE Transactions on Communications*, **30(5)**, 855–884.

[8] **Marvel, L. and Retter, C.,** 1999. Spread Spectrum Image Steganography, *IEEE Transactions on Image Processing*, **8(8)**, 1075-1083.

[9] **Pitas, I.**, 1999. A Method for Signature Casting on Digital Images , *IEEE International Conference on Image Processing*, (3), 215-218.

[10] **Sandford, M. T., Bradley, J. N. and Ettinger, J. M**., 1996. Data Embedding Method, *Proceeding of the SPIE 2615, Integration Issues in Large Commercial Media Delivery Systems*, 226-259.