Çok Katmanlı Steganografi Tekniği Kullanılarak Mobil Cihazlara Haberleşme Uygulaması

Hakan Kutucu1, Ahmet Disli2, Mustafa Akca3
1 Karabük Üniversitesi, Bilgisayar Mühendisliği Bölümü, Karabük
2 Karabük Üniversitesi, Bilgisayar Mühendisliği Bölümü, Karabük
3 Karabük Üniversitesi, Bilgisayar Mühendisliği Bölümü, Karabük
hakankutucu@karabuk.edu.tr, ahmetdisli@outlook.com, mustafa.akca@ogr.ktu.edu.tr

Özet: Çok katmanlı veri yerleştirme sayısal görüntü steganografi de kullanılan en güvenli yaklaşımlardan bir tanesidir. Görüntü steganografi teknikleri stego görüntüdeki bozulmayı minimize etmeye ve aynı zamanda güvenli olmasına çalışırlar. Böylece literatürde bilinen steganaliz tekniklerinin büyük bir çoğunluğundan saklanabilmektedir. Bu yöntemde kaynak fotoğraf bloklara bölünerek gizli veri bitlerinin gömüleceği en uygun satır/sütun aranır. Arama işlemi piksel değerlerinin hem en önemsiz bit katmanında hem de daha üst katmanlarda yapılarak resim bozulması en aza indirgenir. Arama uzayını genişletmek için sadece en önemsiz bitlerin olduğu katmanda değil üst katmanlarda da arama yapılır. Fotoğrafın her bloğunun sondan bir önceki katmanında, saklama işleminin hangi katmanda yapıldığı işaretlenir. Arama sonucu bulunan katman satır/sütun bilgisi son katmanda işaretlenir. Fotoğrafın yapısındaki bozulmayı en az seviyede tutmak için blok içindeki son iki katman hariç her katmana veri gömülmesi ve işaretlemenin son iki katmanda yapılması gerçekleştirilir. Bahsi geçen steganografi tekniği kullanılarak, android cep telefonları için mesajları fotoğraflara yerleştiren ve alıcı kişiye gönderen, alıcı tarafında ise göndericiden aldığı fotoğrafı tersinir bir algoritmayla çözen ve metni fotoğraf içerisinden çıkaran bir uygulama geliştirilmiştir.

Anahtar Sözcükler: Çok Katmanlı Stenografi, Steganaliz, Veri Gizleme, Android

Abstract: Multistage data embedding is one of the most secure approaches used in the steganography of digital images. Image steganography techniques try to minimize the embedding distortion in the stego image and also to make it secure. Thus, they can be invisible under the many steganalysis techniques in the literature. In this method, the image is divided into blocks and the most similar rows/colums to embed the secret bit sequence are investigated. Investigation is performed not only in the Least Significant Bit (LSB) layer but in the higher layers of the blocks for minimizing the distortion in the cover image. The frame pixels of the blocks are used for marking the row/column in which the secret bits are embedded. The rows and colums of higher layers generated by the binary representation of pixel values are also added to the search space. The location of row/colum and its differences from the secret data is then marked by modifying minimum number of bits in the Least Significant Bits of the blocks. The main purpose of this method is to increase the capacity of data embedding without increasing the cover image degradation. In this case, the bit sequence is embedded in each layer and marking is done in the last layer. Using the proposed steganography technique, we have been developed an android application to insert the hidden messages into the photos and to sent the recipient. Then the recipient extracts the hidden message from the photo by the same android application.

Keywords: Multistage Steganography, Steganalysis, Hiding Information, Android

1-Giriş:

Son yıllarda bilgi güvenliği ve bilginin taşınmasında ortaya çıkan ihlaller gittikçe artmaktadır. Teknolojinin çok hızlı gelişmesi ve mobil cihaz kullanımlarının hızlı artışı ile birlikte geliştirilen yeni uygulamalar sayesinde artık insanlar kişisel bilgilerini sürekli olarak paylaşmaktadır. Böyle bir paylaşma ortamında bilginin güvenli bir şekilde saklanması ve gerekli platformlar aracılığı ile güvenli bir şekilde taşınması gittikçe zorlaşmaktadır. Bilgi paylaşımındaki bu zorluk insanların kişisel bilgileri, özel hayatları, sırları gibi birçok bilginin kolay bir şekilde erişilebilirliğini arttırmaktadır. Bilgi güvenliği alanında önemli dallardan biri kapalı bilgi alış verişidir. Bu sebeple şifreleme (kriptografi), veri gizleme (steganografi) gibi çeşitli teknikler kullanılmaktadır. Şifrelemede veriler şifrelendikten sonra aktarıldığı için insanlar şifrelenmiş veriyi görebilirler fakat içerdiği bilgiyi anlayamayabilirler. Steganografi de ise amaç bilginin bir medya üzerinde saklanarak aktarılmasıdır. İnsanlar o medya nesnesinde bilgi

olduğunu bile anlayamayabilirler [1]. Eğer medya nesnesinde gizli mesajın varlığı anlaşılırsa steganografi amacına ulaşamamış sayılmaktadır [2]. Steganografi ve şifreleme aslında aynı değildir. Steganografinin amacı bir mesajın varlığını gizlemektir, şifrelemede ise mevcut mesajı anlaşılmaz hale dönüştürmektir. Bu sebeple verinin saklanması sonucu uğrayabileceği muhtemel saldırılara karşı dayanıklı olması steganografinin başlıca amaçları arasında yer almaktadır.

2-Steganografinin Tanımı ve Tarihçesi:

Steganografi kelimesi yunanca "Gizlenmiş yazı" anlamına gelmektedir. Steganografinin kullanılması M.Ö. 5. yüzyıla kadar uzanmaktadır. Yunanlı tarihçi Heredot'un kayıtları steganografinin kullanıldığına yönelik en eski belgeleri oluşturmaktadır. Antik çağdaki ilk steganografi yöntemlerine örnek olarak: Susa kralı Darius tarafından tutsak alınan Histiaeus'un oğlu Aristagoras'ın saçlarının kazınıp gizli mesajın kafasına dövme yaptırılarak gömülmesi ve saçları uzayınca haberci olarak kullanılması, Demeratus tarafından Yunanistan'ın işgal edileceği haberinin tahtanın üzerine balmumu kaplanmasıyla Sparta'ya ulaştırılması, normal yazıların satır aralarına süt veya meyve suyu kullanılarak gizli yazının saklanması verilebilir.

16. yüzyılda gizlenecek mesajın harflerinin, gönderilecek nesne üzerindeki belirli alanlara gelecek şekilde yazılarak gömme işlemi gerçekleştirilmiştir. Alıcı taraf ise yazı üzerine konulacak delikli bir kağıt yardımı ile gizli mesaja ulaşmaktadır. Bu yöntemde kullanılan delikli kağıt Cardan Grille tablosu olarak anılmaktadır.

İkinci dünya savaşında gizli mesajlar el mendillerine bakır sülfat solüsyonu ile yazıldıktan sonra alıcıya gönderilmiştir. Ayrıca Alman casuslar tarafından gizli verinin iletiminde şifrelenmemiş yani açık ve dikkat çekmeyecek mesajlarının her bir kelimesine ilk veya belirlenecek harflerin birleştirilmesi ile gizli verinin kullanılması steganografinin tarihteki örnekleri olarak gösterilebilmektedir.

3-Steganografi'nin kullanım alanları:

Steganografi çeşitli medya ortamlarında bilgi gizlemek için kapsamlı yöntemleri bulunmaktadır. Dijital imza, görünmez mürekkep karmaşık kanallar veya yaygın spektrum iletişim gibi yöntemler kullanılmaktadır. Günümüzde ise verilerin dijitalleşmesi ile birlikte metin, görüntü, ses ve sinyaller içerisinde de mesajlar gizlenebilmektedir.

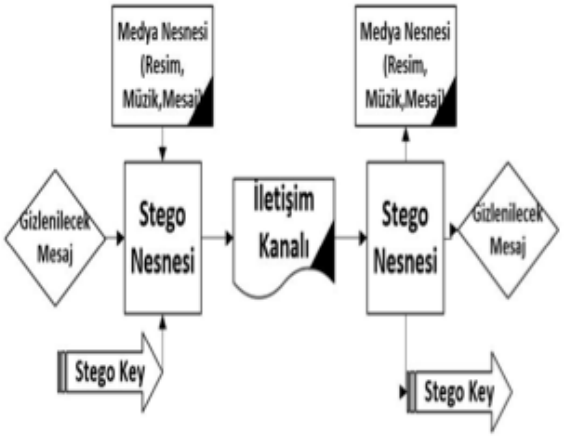
Herhangi bir üreticinin üretmiş olduğu görüntü, video veya ses gibi nesnelerde bir ticari işaret veya özelliğin gizlice depolanmasına damgalama (Watermarking), seri numarası veya diğer karakteristik bir özelliğin nesneye gizlenmesine de parmak izi (finger print) denilmektedir. Damgalama ve parmak izi işlemleri ile korsan işlerin önüne geçmek ve yasal sürece yardımcı olarak telif hakları ihlallerinin önüne geçilmesi için oluşturulmaktadır. Bu yöntemler vasıtası ile bir bilgiyi gizleyerek başka bir yere taşımak yerine ürünlerin sahiplik haklarının veya çoğaltılma izinlerinin korunması sağlanmıştır. Bu sayede aslında gizlenecek veri sayesinde gizlenen medyanın haklarının korunması amaçlanmış olmaktadır.

4-Steganografi ile Şifrelemenin(kriptoloji) Karşılaştırılması:

Steganografinin şifrelemeden en önemli farklı steganografide mesajın varlığının gizlenmesidir. Verinin gizlendiği bilgisi sadece alıcı tarafından bilindiği için aynı gizlenmiş medyaya sahip olan bir başkası, verinin varlığını fark edemez. Şifrelemede ise gönderilen verinin gizli olduğu herkes tarafından bilinmektedir. İçeriği gizli anahtar olmadan anlaşılamaz ve gizli verinin anlaşılabilmesi için çok büyük çabaların ve zamanın harcanması gerekir. Şifrelemede kullanılan algoritmaların deneme saldırılarına karşı dirençli olması nedeniyle gizli verinin elde edilmesi çok güç olmaktadır. Steganografide ise mesajın bir nesnede saklandığı anlaşıldığında gizli veriye ulaşılması daha kolay olmaktadır. Steganografi işlemlerinden herhangi biri ile veri iletilirken içerdiği bilgi şifreleme teknikleri ile şifrelenebilir. Böylece güvenlik arttırılmış olup, daha zor bir şekilde gizlenmiş veriye ulaşılması sağlanabilir. Hiçbir gizli veri çözülemez değildir. Steganografide de şifreleme tekniklerinde de amaç, bit veriyi olabilecek en iyi şekilde gizlemektir.

5-Genel Steganografi Modeli:

Steganografi genel modeli 3 temel elemandan oluşmaktadır; gizli mesaj, stego key ve medya dosyasıdır. Gizli mesaj gönderici tarafından alıcıya güvenli bir şekilde aktarılmak istenilen mesajdır. Stego key gönderici ve alıcı arasında gönderilme mesajının gizleme işlemi için kullanılan bilgiyi içerir. Medya nesnesi ise mesajın stego key vasıtası ile gizleneceği formattır. Günümüzde teknolojisinde veriler dijital ortamlarda saklanmaktadır. Veriler alışveriş yapılırken tüm dijital dosyalar bitler şeklinde saklanmaktadır. Bunun sayesinde herhangi bir resim, video, ses dosyası içerisine gizlenme işlemi yapılabilmektedir.



Şekil 1 – Genel Görüntü Steganografi Modeli

Şekil-1'deki modelde gönderici sadece alıcının bileceği bir stego key ile gönderilmesini istediği mesajı şifreleyip stego nesnesini oluşturur. Oluşan stego nesnesi iletişim kanalları ile birlikte alıcı tarafa ulaşır alıcı taraf ulaşan şifrelenmiş nesneyi çözerek istenilen mesajı görmüş olur.

6-Steganografi Yöntemlerinin Performansı:

Steganografi yöntemlerinin performansı steganaliz yöntemlerine karşı dirençleri ile değerlendirilmektedir. Steganaliz yöntemleri öncelikle bir medya nesnesine bilgi gizlenip gizlenilmediğini tespit ederler, bu işleme tespit (detection) adı verilir. Tespit işlemi tamamlandıktan sonra tespit edilen medyadan gizlenmiş mesajın bulunması işlemine geçilir, bu işlemede çıkarma (extraction) denir.
Sezme işleminden kaçabilmek için gerçek resim unsuru üzerinde yapılacak değişikliklerin en az seviyede tutulması gereklidir. Gizleme işlemi sonrasında resim nesnesinde bozulma ne kadar az ise frekans ve resim uzayında yapılacak analizler sonucunda tespit işlemi o kadar başarısız olmaktadır.

Mesaj gizlenmesi sırasında kullanılan resim üzerinde bozulma ne kadar az olur ise kullanılan yöntem steganalizlere karşı ters orantılı olarak o kadar çok dayanıklı olacaktır.

Steganalizlerde genel veri araştırma yöntemi olarak gizlenmesi yapılan resim uzayında yada frekans uzayındaki sonuçlara dayanmaktadır. Bu sonuçlar orijinal resmin sonuçları ile karşılaştırılarak veya analiz sonucundaki, veri türüne göre olan bit bazındaki dağılımlardaki farklara göre oluşturulmaktadır.

Steganografi yapılmış bir resim unsurunun steganalizlerde en az oranda görüntülenebilmesi için işlemlerden sonra orijinal resimdeki bozulmanın en aza indirilmesinden kaynaklanmaktadır. Bu durumun yapılabilmesi için orijinal resimde yapılan analizler sonucunda saklanacak olan bilgilerin düzgün şekilde yerleştirilmesi gerekmektedir.

6.1-Görüntü Steganografi:

Günümüz teknolojisinde dijital verilerin kullanımı sıklaşmıştır. İnternet üzerinde çok yaygın şekilde kullanılan ve gerekli veri gizleme alanlarına sahip oldukları için fotoğraflar ve görüntüler steganografinin kapsama alanına girmektedirler.

Görüntü steganografisinde kullanılan nesneler jpg, jpeg, gif, bmp gibi değişik formatlarda olabilirler. Görüntü steganografisinde veri gizlenmesi olayı nesnelerinin piksel değerleri üzerindeki değişiklikler ile yapılmaktadır. Her bir piksel 8 bit değerinden oluşmaktadır. Bit değerlerinin karşılıkları sayesinde piksellerin renk durumları oluşmaktadır ve bu durum tüm pikseler sayesinde resmin gerçek görüntüsünü sağlamaktadır. Bu bitler üzerinde yapılacak değişiklikler sayesinde resim dosyasında insan gözünün, hatta steganaliz yöntemlerinin algılayamayacağı değişikliklerin yapılması mümkündür.

Görüntü steganografisi için birçok yöntem geliştirilmiş ve üzerinde çalışmalar devam etmektedir.

6.2-En Önemsiz Bitlerin Değişimi Yöntemi:

Görüntülerin piksel değerlerindeki en önemsiz bitlerindeki değişimler bu kategoriye girmektedir. Örneğin 8 bitlik [1000 0001] verisinde en sağdaki bit en önemsiz bit (EÖB) olarak adlandırılmaktadır. Bu yöntem steganografinin en basit yöntemi olarak uygulanmaktadır. Bu yöntem ortalama olarak resmin sahip olduğu piksel değerlerinin yarısı kadarlık bit değişimi ile veri saklanmasına olanak sağlamaktadır.

Örneğin gizlenmek istenilen mesajın [0101] olduğunu varsayalım.

Orijinal görüntümüzün;
1.Piksel değeri [1001000]
2.Piksel değeri [0001011]
3.Piksel değeri [1001101]
4.Piksel değeri [1110000] şeklinde olduğunu kabul edelim. 3. pikseldeki son bitin 0, 4. Pikseldeki son bitin 1 olarak değiştirilmesi ile gerçek piksel değerlerindeki -1 ve +1 değişimler sonucunda veri gizlenmiş olacaktır. Son durumda ori-

jinal görüntü pikselleri:

1.Piksel değeri [1001000]
2.Piksel değeri [0001011]
3.Piksel değeri [1001101]
4.Piksel değeri [1110000] olarak değişmiş olacaktır. Bu durumda orijinal resimden 2 bit değişimi yapılarak istenilen veri gizlenmiş olacaktır. Bir piksel 8 bitten oluştuğundan dolayı değeri en fazla 255 sayısal değerini alabilmektedir. En son bitte yapılan bir değişiklik piksel değerini +1 veya -1 olarak değiştirmektedir. Böyle bir değişim sonucunda oluşacak değişimlerden orijinal görüntü ile yeni oluşan stego nesnesi arasında insan gözünün algılayamayacağı küçük değişiklikler olmuş olacaktır. Ancak EÖB değişimi kesme-yapıştırma, döndürme, sıkıştırma vb. gibi basit saldırılara karşı çok hassastır. Ayrıca EÖB yer değiştirme yöntemi sonucu oluşan değişimler resim pikselleri ile bağlantılı olmasından dolayı basit analizler ile tespit edilebilmektedir. Eğer bitlerin yerleştirilme durumu karışık pikseller seçilerek yapılır ise analizciler tarafından fark edilmesi daha zor olacaktır.

EÖB yer değiştirme yönteminin zayıf yönlerinin geliştirilmesi için çalışmalar devam etmektedir. Bu yöntemlerden birisi olan piksel steganografi yöntemi ile piksel değişikliğinin yapılacağı en güvenli yerler seçilmektedir. En güvenli yerler piksellerin çabuk değişime uğradığı köşe, çizgi sonları ve renk değişikliklerin olduğu noktalardır [3].

6.3-EÖB Eşleştirme Yöntemi:

EÖB eşleştirme yönteminde gömülecek veriye göre görüntü içerisindeki piksellerin arttırılması yada azaltılması esasına dayanır. Eğer görüntü pikselindeki veri gizlenecek veri ile uyuşursa değişiklik yapılmaz. Eğer uyuşmazsa piksellin arttırılması veya azaltılması ile gizlenecek veri yerleştirilir. Bu yöntem sayesinde analizler sonucunda gizlenen verinin bulunması zorlaştırılmış olur [5].

J. Mielkainen, EÖB eşleştirme yöntemini geliştirerek, her bir piksel çiftinin, özel şartlara sahip bir fonksiyona bağlı olarak arttırılmasını sağlar. Bu şekilde her görüntü piksel çiftine iki bit gizlenmek istenilen veri gömülmüş olur. Bu sayede EÖB yöntemine karşın daha az sayıda piksel değeri değişmesine neden olur.

Aşağıdaki algoritma yardımı ile EÖB eşleştirme yöntemi uygulanabilir [6].

$$
\begin{aligned}
&\text{if } m_i = \text{EÖB}(x_i)\\
&\quad \text{if } m_{i+1} != f(x_i, x_{i+1})\\
&\qquad y_{i+1} = x_{i+1} + 1\\
&\quad \text{else}\\
&\qquad y_{i+1} = x_{i+1}\\
&\quad y_{i+1} = x_i\\
&\text{else}\\
&\quad \text{if } m_{i+1} = f(x_{i-1}, x_{i+1})\\
&\qquad y_i = x_i - 1\\
&\quad \text{else}\\
&\qquad y_i = x_i + 1\\
&\quad y_{i+1} = x_i + 1
\end{aligned}
$$

Algoritmada x ile seçilen resim piksel değerleri, m ile de gizli veri çifti ifade edilmiştir.

EÖB ise : $EÖB([x_i/2] + x_{i+1}) = f(x_i, x_{i+1})$ şeklinde ifade edilmektedir.

(y_i,...) ile düzenlenmiş stegı resim değerleri ifade edilmektedir.

Bu yöntem ile birlikte her bir pikselin değişim ihtimali %35-50 arasında tutularak resim nesnesinin bozulma seviyesi azaltılmaktadır. En büyük dezavantajı ise gömülecek veri miktarının sadece piksel sayısı kadar olmasıdır.

6.4-Görüntü Blokları Tabanlı EÖB Değiştirme Yöntemleri:

Blok tabanlı EÖB yöntemlerinde resim nesnesi sabit boyutlu parçalara ayrılmaktadır. Gizlenecek veri her bir bloğa eşit sayıda bit gelecek şekilde parçalara ayrılır ve her bir bloğun içerisine resim nesnesinin EÖB'leri ile en fazla uyuşma sağlayacak satır veya sütunlarına eşleştirilerek gömülür. Bir mesaj gizlenirken her blok içerisinde en az sayıda pikseli değiştirmek amacıyla mesaj bitlerinin gömüleceği en uygun satır veya sütun seçilir. Gizli mesaj bulunan satır/sütuna gömülür.

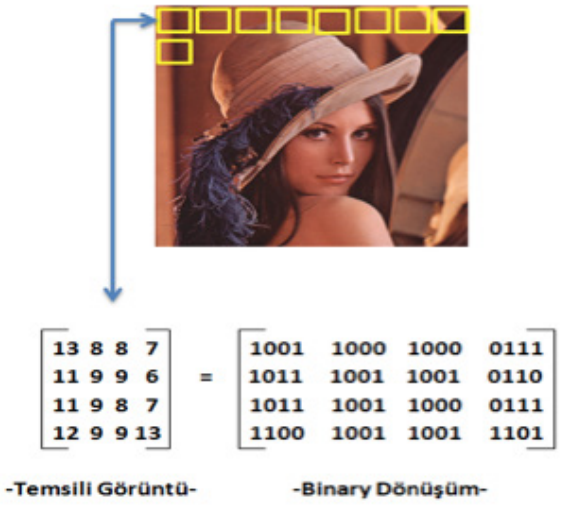
Alıcı tarafından mesajı çözümlenmesi gerektiğinden hangi satır/sütunların işaretlenmesi yapıldığı çevre piksellere yazılır. Çevre piksellere mesaj girilmesi işlemi yapılmaz.

Bloklara ayrılmış resim nesnesi üzerinden 1. ve sonuncu satır işaretleme için kullanılacağından bir bloğa satır sayısının iki eksiği kadar mesaj parçası gömülebilir. Bu nedenle blok sayısının satır sayısının iki eksiği kadarlık bitlere mesaj gizlenmesi yapılabilmektedir.

Saklama işleminde resim nesnesinin bir bloğundaki en yakın satır veya sütun aşağıdaki bulunabilir.

$$(p,r) = min_{j,k}\{Uzaklık(S_i, H_{i,(j,k)})\} j = 1 \dots d, k = 1 \dots m$$

Bu formülde i blok numarasını, m satır sayısını, d sütun sayısını, k değişkeni her yöndeki m-2 adet satır/sütunu, Uzaklık() uzaklık ölçümünü, S gizlenecek sayıyı, H bitin gerçek değerini göstermektedir. Sonuç olarak S ye en yakın olan satır/sütunun hangi yönde p ve kaçıncı sırada olduğu r, bulunur. Temsili olarak 4x4 lük bloklara ayırma yaparsak ve bir pikselin 4 bit olduğu düşünülürse, bloklara ayırma işleminin Şekil-2'deki gibi olduğunu söyleyebiliriz.



Şekil 2- Bloklara Ayırma İşlemi

6.5-Görüntü Katmanlarına Dayalı Yöntem:

Görüntü blokları tabanlı EÖB yönteminde her bir bloğa blok boyutunun 2 bit eksiği kadar veri biti gömülmektedir. Ayrıca 4 yönlü arama yapıldığında her blok için arama uzayı 4x(blok boyutu-2) olmaktadır. Görüntü katmanlarına dayalı yöntem EÖB yöntemi ile aynı olarak resim bloklarına blok boyutuyla orantılı sayıda verinin saklanması esasına dayanmaktadır. Fakat farklı olarak EÖB haricindeki bitlere de gömme işlemi yapılabilmektedir.

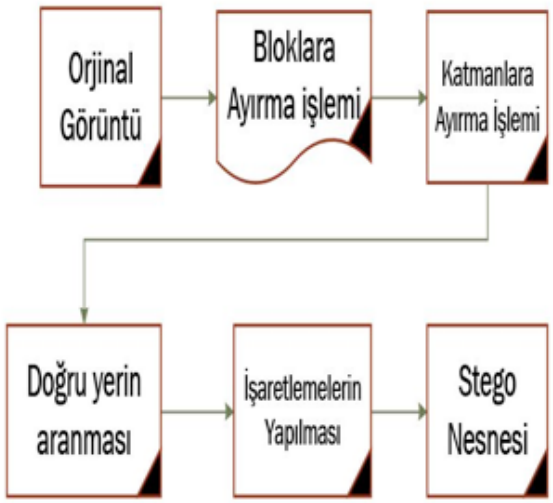
Öncelikle resim bloklara ayrılır her bir bloktaki piksel değerleri bit değerlerine dönüştürülür. İlgili bloktaki tüm piksellerin aynı indislerdeki pikselleri bir araya getirilerek katmanlar oluşturulur. 7. ve 8. katmana gömme işlemi yapılmaz bu katmanlar yapılan değişikliklerin nerede yapıldığının ve nasıl yapıldığının tutulacağı katmanlar olarak ayrılmıştır.

Arama algoritması her bloğun katmanları arasında istenilen gizli veri dizisine en yakın satır veya sütunu bulmaya çalışır. 7. ve 8. katman hariç tüm bit katmanları arama sürecine dahildir. En fazla benzerliğe sahip satır/sütun bulunduğunda veri gizlenmesi yapılmaya başlanır. Kullanılan herhangi bir katmanın belirlenmesi için gömme işleminde kullanmadığımız 7. katmanın, ilgili katman indisli satırı önceden belirlenmiş işaretçiyle işaretlenir. Böylelikle gömme işleminde kullanılan katman bilinmiş olunur. Bu sayede değişiklik yapılan katman 7. katman üzerinden belirtilmiş olmaktadır.

Yapılan değişiklikler, 8.katmanda ilgili satır/sütün farklı bir işaretçiyle işaretlenerek ve indisine bakılarak nerede, nasıl bir değişiklik olduğu bilinir. Bu sayede değişiklik yapılan konum 8. katman üzerinden belirtilmiş olmaktadır.

Eğer arama sonucunda gizlenecek veriler ile ilgili katmanlardaki satır/sütun eşleşmesi birebir yapılırsa sadece 7. ve 8. katmandaki işlem yapılır.

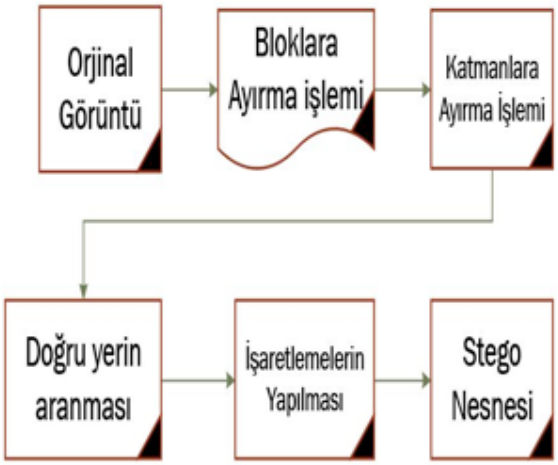
Algoritma sonucunda bit katmanlarında gizli veri dizisi ile en fazla eşleşen satır veya sütun bulunmuş olacaktır. Böylelikle değişikliğin en az düzeyde tutulması sağlanacaktır.



Şekil 3 – Mesaj Gizleme Adımları

Geliştirilen hibrit algoritma ile mesajın gömülme adımları aşağıdaki gibidir.
1- Görüntü bloklara ayrılır. Bit matrisleri oluşturulur.
2- Her bir bloktaki tüm piksellerin aynı indislerdeki pikselleri bir araya getirilerek katmanlar oluşturulur.
3- En büyük indisli iki katman haricinde en uygun yer satır ve sütunlarda aranır. Bulunan yere veri gömme işlemi yapılır.

4- 7.katmanda gömme işleminde kullanılan katman indisi işaretlenir.
5- 8.Katmanda gömme işleminin yapıldığı satır/sütun işaretlenir.



Şekil 4 - Gizlenmiş Mesajın Çıkarılma Adımları

Geliştirilen hibrit algoritma ile gizli mesajın elde edilme adımları aşağıdaki gibidir.
1- Görüntü bloklara ayrılır. Bit matrisleri oluşturulur.
2- Her bir bloktaki tüm piksellerin aynı indislerdeki pikselleri bir araya getirilerek katmanlar oluşturulur.
3- 7. ve 8. katmanda işaretlenmiş alanlar aranır. Bulunan indislere göre mesaj birleştirilir.

7-Geliştirilen Mobil Uygulama

Android uygulaması geliştirilirken Eclipse Android Sdk kullanılarak, çalışılacak cihaz düzeyi andro-id 4.3 olarak ayarlanmış, çalışma aralığında android 4.0 ile 4.4 seçilmiştir.

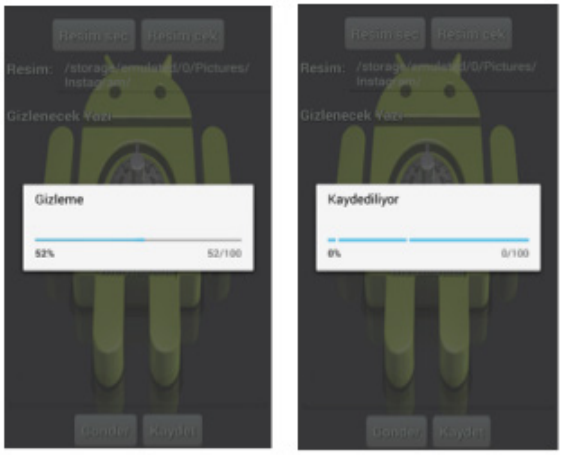
Şekil 5 - Uygulama Karşılama Ekranı

Uygulama 3 farklı ara yüzden oluşmaktadır. Şekil 5 uygulama karşılama ekranıdır. Bu ekranda mesajı gizle ve Mesajı çöz olmak üzere 2 buton bulunmaktadır. Mesajı gizle butonuna basıldığında mesaj gizleme işleminin gerçekleştirileceği arayüz (şekil 6) gelmektedir.

Şekil 6 - Mesaj Gizleme Arayüzü

Şekil-4 de görüldüğü gibi verinin gizleneceği resmin seçilmesi için akıllı telefonun resimleri arasından veya kamera yardımı ile çekilecek olan bir resim kullanılabilmektedir. Bu işlemlerden herhangi biri yapıldığı zaman işlenecek resim Bitmap şekline dönüştürülerek işlenmesi kolay bir hale getirilmektedir. Gizleme işleminin yapılacağı yazı yazıldıktan sonra gömme işleminin ayarlandığı algoritma çalışarak gömme işlemini tamamlayıp tekrardan neredeyse ilk resmin aynısı olan resim oluşacaktır. Gönder kısmı ile oluşturulan resim bir media intenti vasıtası ile telefon üzerinde resmi kullanılabilecek uygulamaları göstermektedir. Bu aşamada eğer bir sıkıştırma algoritması kullanan bir uygulama (Facebook, Instagram, WhatsApp (bedava versiyonu)) seçilir ise veri kayıpları oluşacağından sağlıklı sonuçlar elde edilemeyecektir. Fakat eğer mail, cloud hesapları veya resim sıkıştırma algoritması kullanılmayan bir uygulama seçilir ise gönderilmek istenen kişiye eksiksiz bir şekilde stego nesnesi ulaştırılabilmektedir.

Kaydet butonu ile de oluşturulan stego nesnesi telefon hafızasına kaydedilmektedir. Bu işlemlerin yapıldığı ekran görüntüleri Şekil 7'deki gibidir.



Şekil 7 – Gizleme ve Kaydetme İşlemleri

İlk arayüzde 'Mesajı Çöz' butonu tıklanır ise resimden veri çıkarma işlemini gerçekleştirecek olan algoritma çalıştırılarak resim üzerinden gizlenen veri elde edilerek kullanıcıya gösterilmektedir. Eğer gömme işleminin yapıldığı algoritma kullanılarak gizlenmiş bir veri yok ise kullanıcıya verinin olmadığı belirtilmektedir. Şekil 8 de mesaj çözme işlemi sonucu görülmektedir.

8-Sonuç :

Çok katmanlı steganografi teknikleri kullanılarak oluşturulan algoritma ile verilerin resim nesnelerine güvenli bir şekilde saklanması sağlanabilmektedir. Bu tekniklerden görüntü blokları tabanlı olan ve görüntü katmanları tabanlı olan algoritmalar birleştirilip geliştirilerek hibrit bir algoritma elde edilmiştir. Geliştirilen bu yöntemde medya nesnesi içerisine gizli veri saklanmasından sonra görüntünün bozulmasının en aza indirgenmesi, steganaliz yöntemlerinden en az derecede etkilenmesi amaçlanmıştır. Geliştirilen bu algoritma temel alınarak, Android arayüzü ile mobil cihazlar üzerinde çalıştırılacak uygulama geliştirilmiştir. Bu mobil uygulama, kullanıcının seçeceği veya kameralardan alacakları görüntüler üzerine istenilen verinin gizlenmesi ve çeşitli iletişim uygulamaları vasıtasıyla alıcıya iletilmesinden sonra sadece alıcı tarafından güvenli bir şekilde gizli verinin tekrar elde edilmesini sağlanmıştır.

9-Kaynaklar

[1] M. M Amin, M. Salleh, S.Ibrahim, M.R.Katmin, and M.Z.I. Shamsuddin,"Information Hiding Using Steganography", 4 th. National Conferance on Telecommunication Technology Proceedings, Shah Alam, Malaysia, 0-7803-7773-7/03, 2003 IEEE.
[2] Johnson, Neil F., "Exploring Steganography: Seeing the Unseen." IEEE Computer 30.2 (1998): 26-34.
[3]Mrs.ShantalaSures, Dr.Vishvanath, "Edge-Steganography for Secure Communication", 1-4244-0549-1/ 2006 IEEE.
[4] Kh.Manglem Singh, L Shyamsudar Singh, A. Buboo Sİngh and Kh.Subhabati Devi, "Hiding Secret Message in Edge of The Image", Internatioanl Conference on Information and Communication Technology,ICICT 2007, 7-9 March 2007, Dhaka, Bangladesh.
[5] Jarno Mielikainen, "LSB Matching Revisited", Signal Processing Letters,IEEE, Publication Date: May 2006Volume : 13, Issue : 5, On page(s): 285- 287.
[6] Chi-Shiang Chan, Chin-Chen Chang, "A Survey of Information HidingSchemes for Digital Images", IJCSES International Journal of Computer Sciences and Engineering System, Vol.1, No:3, July 2007.