mühendislikdergisi
Dicle Üniversitesi Mühendislik Fakültesi
Cilt: 7, Sayı: 3,501-514
Eylül 2016

İmgeler için farklı bir veri gizleme yaklaşımı

Ferdi DOĞAN[*,1], Resul DAŞ[2], İbrahim TÜRKOĞLU[2]

[1]*Adıyaman Üniversitesi, Kahta Meslek Yüksekokulu, Bilgisayar Teknolojileri Bölümü, Kahta, Adıyaman*
[2]*Fırat Üniversitesi, Teknoloji Fakültesi, Yazılım Mühendisliği Bölümü, Merkez, Elazığ*

Makale Gönderme Tarihi: 18.03.2016 Makale Kabul Tarihi: 18.05.2016

Öz

Günümüz teknolojilerinde bilginin dış ortamlara karşı korunması çok önemli olmakla birlikte zorunlu hale gelmiştir. Bu sebeple bilginin korunması için geliştirilen ve uygulanan birçok yöntem vardır. Bunlardan biri de stenografidir. Stenografik teknikler kullanılarak imge içerisine bilgiler güvenli şekilde karşı tarafa iletilmesi amaçlanır. Burada temel amaç imge üzerinde yapılacak değişikliklerin, üzerindeki bozulmayı en aza indirgeyerek gizli bilginin varlığının saklanmasıdır. Dijital görüntüler üzerinde değişiklikler yapılarak, imge içerisine pek çok bilgi yerleştirilebilir. Ancak bu değişikliklerin fark edilmemesi gerekmektedir. İnternetin günümüz dünyasında her alanda kullanıldığı düşünülecek olursa her an dijital görüntülüler içerisinde olduğumuz görülecektir. Sosyal paylaşım siteleri, sosyal ağlar, internet siteleri içerisinde dolaşan sayısız dijital görüntü içerisine stenografik tekniklerle bilgin gizlenmesi mümkündür. Bununla beraber böyle bir dijital ortamda gizlenen bilginin fark edilebilmesi neredeyse imkânsızdır. Bu makalede stenografik veri gömme teknikleri üzerinde en çok kullanılan LSB kodlama, 2bit LSB kodlama, RGB kodlama, R kodlama teknikleri kullanılarak birbirleri üzerindeki üstünlükleri karşılaştırılmıştır. Bu yöntemler üzerine analizler yapılarak yeni bir veri kodlama tekniği sunulmuştur. Önceki yöntemler ile geliştirilen 0. ve 2. bite gömme yöntemi karşılaştırılmıştır. Geliştirilen yeni yöntemin önceki yöntemlere göre bilinmemesi, gizli veriye ulaşılması bakımından daha zor olacaktır. Önceki yöntemler ile geliştirilen yeni yöntem veri gizleme uygulamaları yapılmış ve PSNR (Peak Signal to Noise Ratio), MSE (Mean Squared Error), SSIM (Structural Similarity) analizleri ile resim üzerindeki bozulma oranları çıkarılmıştır. Ortaya çıkan sonuçlara bakarak veri gömme yöntemlerinin birbirlerine göre avantaj çıkarımları yapılmıştır.

Anahtar kelimeler: *Bilgi güvenliği; steganografi; veri gizleme; LSB*

[*]Yazışmaların yapılacağı yazar: Ferdi DOĞAN. fdogan*@adiyaman.edu.tr*; Tel:

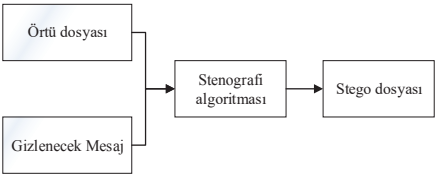
Giriş

Verinin gizlenmesi sanatı olarak bilinen stenografi; eski yunanlılardan pek çok dile de geçen steno gizli yada gizlemiş anlamına gelen ve resim yada grafik üzerine çizmek ya da yazmak anlamına gelmektedir (Anguraj vd., 2011). Stenografide bir mesaj bir imge içerisine yerleştirilerek, mesajın varlığı gizlenir. Gizli mesajı çıplak gözle görülebilme imkânı yoktur. Herkes bu mesaja ulaşamaz ve mesajın varlığından haberdar olamaz (Shahadi ve Jidin, 2014). Günümüzde internet gibi herkese açık olan bir sistemde Stenografik teknikler güvenlik ve gizlilik açısından önem kazanmaktadır (Rai ve Dubey, 2012).

İnternet ortamındaki ses ve görüntü iletişimi insanlar arasında önemli oranda yer almaktadır. Sosyal medya uygulamaları, mobil uygulamalar bu noktada büyük yer tutmaktadır. Bilgilerin böyle bir ortamda yer alması bilgi güvenliği konusunda riskler oluşturmaktadır. Bu sebeple güçlü stenografik ve kriptolojik yaklaşımlar sosyal medyanın geliştiği günümüzde çok önem arz etmektedir (Sethi ve Sharma, 2012).

Stenografi ve kriptoloji birbirleriyle karıştırılmaktadır. Fakat her ikisi de birbirinden farklı yapıya sahiptir. Stenografide temel amaç gizli bilginin varlığının bilinmemesidir. Kriptolojide ise gizli bilgi olduğu bilinmekte ve bu gizli bilgi çözümü için bir gizli anahtara sahip olunması gerekmektedir. (Behnia vd., 2014). Benzer bir durum stenografide water marking arasında da yapılmaktadır. Bu iki yaklaşım da birbirlerinden farklıdır. Stenografide gizli bilgi yerleştirilmiş bir resim üzerinde gerçekleşecek bir bozulma gizli bilgiye ulaşılmasını engeller. Ancak watermarking yani damgalamada obje içerisine yerleştirilmiş bir filigran vardır ve obje üzerinde gerçekleşebilecek bir bozulma filigranı bozmaz (Hayati, 2007).

Dijital görüntülerde gizli anahtar fikrini ilk kez Shamir ve Barkey tarafından ortaya atılmıştır (Shamir, 1979; Blakley, 1979). Stenografide iki temel unsur vardır. Bunlar örtü dosyası ve gizlenecek olan mesaj. Gizlenecek olan mesaj örtü dosyası içerisine gizlenerek varlığı korunmaya çalışılır. Mesaj+örtü dosyasına, stego dosyası denir. Bu durum aşağıda şekil 1'de gösterilmektedir (Rai ve Dubey, 2012).



Şekil 1:Stenografi Şeması

Stenografi açısından imge görüntüleri üzerinde yapılan değişimler çıplak gözle bakıldığında anlaşılmamalıdır. Yapılan değişikliğin anlaşılması, gizli bilgi olduğu şüphesini taşımaktadır. Bu durumda üçüncü kişilerin gizli metine ulaşabilmesi için imge görüntüleri üzerinde işlemler yapmasına olanak sağlar. Bu sebeple veri gizleme tekniklerinin bu tarz yapılara karşı dayanıklı olması beklenir(Doğan vd., 2013).

Stenografiden elde edilen stego objesi orijinal görüntüsü ile karşılaştırıldığında gözle görülebilecek bir farklılık göstermez. Bu farklılığın fark edilebilmesi için dijital ortamda bazı çalışmalar yapılması ve test edilmesi gerekir. Stego objesi içerisinde gizli bir bilginin bulabilmesi için yapılan çalışmaya steganaliz denir. Steno objesi içerisindeki gizli verinin varlığının tahmin edilmesi steganalizin alanına girer. Gizli verilerin tespitini yapmak için kullanılan bazı yöntemler vardır. Bu yöntemler;

- Histogram Analizi
- $\chi 2$ Testi
- RS Steganalizi
- RQP Yöntemi
- Görsel Ataklar

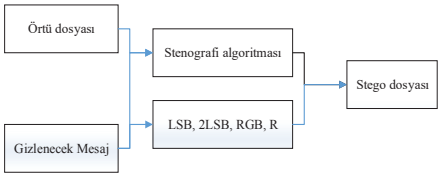
olarak gösterilebilir (Fridrich ve Goljan, 2002).

Günümüz teknolojilerinde bilgiye rahat ve kısa yoldan ulaşabilmek oldukça kolaydır. İnternet, bilgi paylaşımını sağlayan en uygun ortamdır. Bu ortam içerisinde yer alan her türlü bilgi ve teknolojiler savunmasız ve açık durumdadır. Savunmasız durumda bulunan bu ortam için herkesin ulaşmaması gereken bilgilerin aktarımı için pek çok yol mevcuttur. Bir bilginin gizli bir şekilde, sadece ulaşılması istenilecek kişiye gönderilmesi için kullanılacak olan yöntemlerden biride stenografik yaklaşımlardır. Bu yaklaşımda dijital görüntüler kullanılarak, iletilmesi istenilen veriler resim içerisine gömülerek karşı tarafa iletilir.

Metaryal ve Yöntem

Verinin dijital görüntü üzerine gömülmesi için farklı yaklaşımlar mevcuttur. Bu konuda bazı yöntem ve algoritmalar yer almaktadır. Özellikle görüntü üzerinde oluşabilecek bozulmaları en aza indirgemek için pek çok algoritma geliştirilmiştir. Gömülecek olan verinin görüntü dosyası üzerinde filtreleme yapılarak görüntüdeki bozulma oranı azaltılmaya çalışılmıştır. Bununla beraber dijital görüntü içerisine gizlenebilecek veri miktarı da önem taşımaktadır. Gizlenebilecek veri miktarı arttıkça, bozulmada yaklaşık oranda artmaktadır. Bozulmanın fazla olması stenografide istenmeyen bir durumdur.

Dijital görüntü içerisine bilgi gizlenirken gerçekleştirilen algoritmalar genellikle filtreleme ile gömü yapılabilecek pikselleri seçmektedir. Algoritma ile beraber verilerin pikseller üzerinde nasıl bir yapı ile kullanılacağınında belirlenmesi gerekmektedir. Literatürde yapılan çalışmalarda en önemsiz bite (Least Significant Bit) yerleştirilerek yapmak bozulmayı en aza indirgemiştir. Bazı yöntemlerde ise gizlenecek veri boyutunun fazla olması sebebiyle en önemsiz bite yerleştirmek verinin tamamının imge içerisine gizlenmesine olanak sağlamaz. Bu sebeple farklı tipte yöntemler kullanılır. Bunlardan bir diğeri de 2LSB tekniğidir. İmge üzerinde, en önemsiz bit kullanılarak yapılan veri gizleme tekniğinden biraz daha fazla bozulma gerçekleşir. İmgede pikseli gösteren değerin son iki biti değişmektedir. Ancak gözle görülmesi imkânsızdır. Çok küçük değişiklikler yer alır ancak gömülebilecek veri miktarı biraz daha fazladır. Kullanılabilecek başka bir teknik ise RGB ve R ağılıklı kodlama tekniğidir. Gizli mesaj bu teknikler kullanılarak çok daha fazla bilgiyi barındırabilir. Böylelikle çok büyük bilgilerde bu yöntemler aracılığı ile gizlenebilir. Bir bilginin sağlıklı şekilde korunması için veri gizleme algoritmasının iyi bir şekilde tasarlanması gerekmektedir (Matam ve Lowe, 2009). Dijital görüntü ve gizli mesajın birleşimiyle oluşturulan stego objesi için şekil 2'de gösterilen bir blok şeması oluşturulabilir.



Şekil 2: Stenografi blok diyagramı

Bu çalışmada kullanılan stenografik veri gizleme teknikleri ve geliştirilen teknik şu şekildedir.

1. RGB kodlama tekniği;
2. R kodlama tekniği;
3. LSB kodlama tekniği;
4. 2LSB kodlama tekniği;
5. 0 ve 2 Bite kodlama tekniği;

RGB Kodlama Tekniği

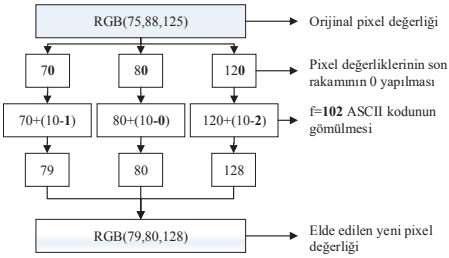
Bu kodlama tekniğindeki temel mantık bir piksel içerisine bir ASCII karakterinin gömülmesi mantığına dayanmaktadır. Bir piksel içerisinde yer alan Red Green ve Blue değerliklerinin içerisine bir Ascii karakter kümesinin sayısal değerliğinin yerleştirilmesiyle oluşur. Bir karakterin ascii kod karşılığı 3 haneden oluşur (Ching-Yu, 2009). Burada örnek olarak f harfini alacak olursak; f=102 Ascii değerine sahiptir. Bu değerlikte her bir hane,

pikseldeki renk kodlarından R,G ve B değerliklerine yerleştirilir. Ancak buradaki işlem yürütülürken Ascii karakter karşılığındaki rakamın her bir hanesi f 'nıntümleyeni olarak alınır. Bu alınan değerlik f' olarak tanımlanır. 102 değeri tümleyeni alındıktan sonra 908 olarak görünür. f'=908 olur.

Pikseldeki RGB değerliğinde ise her bir değerin sonu önce 0 değerini alır. Alınan örnek piksel değerliğinin RGB (75, 88, 125) olduğunu düşünecek olursak; R=75, G=88, B=125'tir. Her değerin son hanesi 0 yapılır. Bu durumda R=70, G=80, B=120 olacaktır. Ve görüntü içerisindeki piksel değerliğinin sonuna buradaki her bir hane yerleştirilir.

R=70+9=79
G=80+0=80
B=120+8=128 olacaktır.

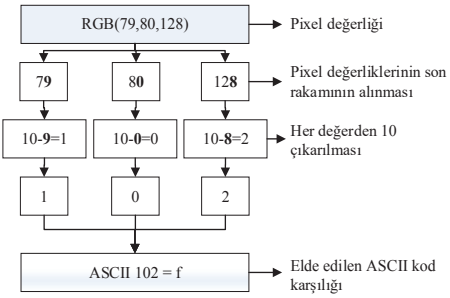
RGB kodlama ile veri gizleme şeması şekil3'te anlatılmıştır.



Şekil 3:RGB kodlama ile veri gömme

Yeni oluşan RGB değeri ise RGB (79, 80, 128) şeklinde olacaktır. RGB kodlama tekniği ile veri gömüldükten sonra resim üzerinde bozulmalar meydana gelecektir. Hassasiyeti diğer duyu organlarından daha az olan gözün, oluşan bu bozulmaları görmesi pek mümkün değildir (Erçelebi ve Subaşı, 2006).

Gizlenmiş olan verinin yeniden elde edilmesi için gömme işleminin tersi uygulanır. Öncelikle bir piksel değerliği alınır. RGB (79, 80, 128). Her bir ağırlıktaki değerin son hanesi yani birler basamağındaki rakam alınır. Alınan rakamların tümleyeni alınarak, yani 10 çıkarılarak ASCII karakter kod karşılığı elde edilir. R=79, G=80, B=128'dir. Her bir değerliğin son hanesini alıp 10'dan çıkaracak olursak elde edilecek olan değerler 1, 0, 2'dir. Yan yana getirilecek olan bu değer 102 ASCII karakter kodu olan f harfinin bulunmasını sağlar. Bu durum şekil 4'te gösterilmektedir.



Şekil 4: RGB kodlama ile verinin elde edilmesi.

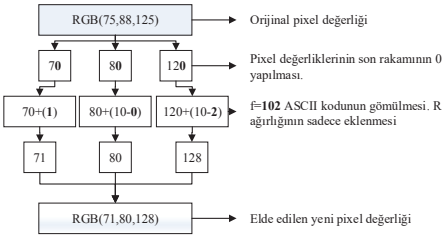
R kodlama Tekniği

R ağırlıklı kodlama tekniği RGB ağırlıklı kodlama tekniğine benzer şekilde işler. Ancak burada işlem yapılırken R ağırlıklı renk değerindeki son hane 0 yapılmadan ASCII kod karşılığındaki ilk basamak değerini alır. Diğer renk değerlikleri yine RGB kodlama tekniğinde anlatıldığı şekilde işler(Akar ve Selçuk, 2004;Akar vd, 2014). Önek olarak f harfini alacak olursak; "f"=102 ascii karakter koduna sahiptir. Piksel değerliğimiz ise RGB (75, 88, 125) olduğunu düşünecek olursak; öncelikle piksel değerliklerin son basamak değerliklerini 0 yaparız. R=70, G=80,B=120 olarak tanımlanır. Daha sonra f ASCII kodlu olan 102 değerliğinin ikinci ve üçüncü basamağındaki değerliklerin 10'a tümleyenini alırız. Eğer sonuç 10 ise bunu 0 olarak değerlendiririz. Buna göre 102 gömü değerindeki 0 değerliği için ilk basamak değerine dokunulmaz ve ikinci basamak değeri için 10-0=0 olur. 102 gömü verisindeki son basamak olan 2 değeri için ise 10-2=8 olacaktır. Yeni ASCII değerlikli

kodumuz ise 108 olacaktır. Gömme işlemine geçildiğinde ise her hanedeki değerlikler RGB piksel değerliklerinin birer basamağına yerleşecektir. Burada 108 gömü verisindeki 1 değerliği R ağırlığının son hanesine, 0 değeri G ağırlığının son hanesine ve 8 değeri B ağırlıklı değerin son hanesine yerleştirilecektir.

R=70+1=71
G=80+0=80
B=120+8=128 olacaktır.

Oluşacak olan yeni piksel değerliği RGB (71, 80, 128) olacaktır. Bu durum şekil 5'te gösterilmektedir.

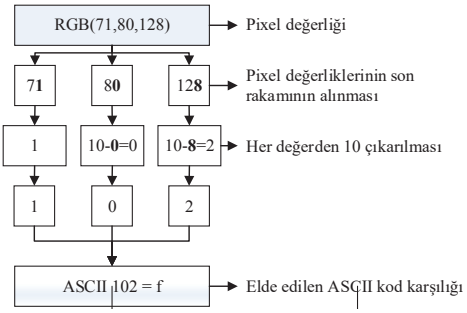


Şekil 5: R Kodlama ile veri gömme.

Gömülen verinin tekrar elde edilmesi ise yukarıda anlatılan işlemin tersi ile mümkün olacaktır. Önce piksel değerliği okunur. RGB (71, 80, 128) elde edilen piksel değerliğindeki her ağırlığındaki son haneler alınır. R ağırlığı hariç diğer ağırlıkların son hane değerlerinden 10 çıkarılır. Yani 10'a tümleyeni alınır. R=71, G=80, B=128. Ve buradan son haneler alınır. R=1 G=10-0,B=10-8. Buradan R=1,G=0,B=2 olur. Ve elde edilen ascii karakter kodu 102 olur. Buradan elde edilen karakter f'dir. Şekil 6'da gösterilmektedir.

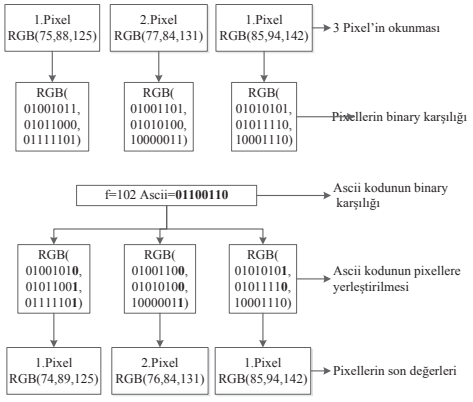
LSB Kodlama Tekniği

LSB (Least Significant Bit) stenografik uygulamalar için yeni bir başlangıçtır (Coşkun vd., 2013). LSB kodlama tekniği literatürde en çok kullanılan ve karşılaşılan tekniktir (Neeta, 2006; Charudhary ve Vasavada, 2012). Çok fazla kullanılmasının sebebi ise veri gizlendikten sonra resim üzerindeki bozulmaların bilinen



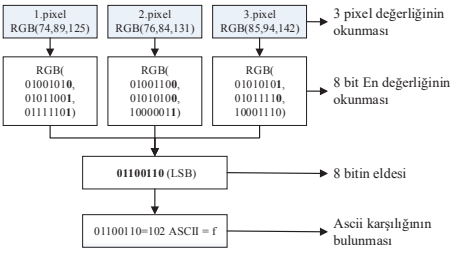
Şekil 6: R kodlama ile verinin elde edilmesi.

tekniklere göre oldukça az olmasıdır. Bu teknikte piksel değerliğinin en az ağırlıklı olan son biti ardışık olarak değiştirilerek gerçekleştirilir (Singh vd., 2007). Piksel değerlikleri binary'e çevrilerek son bitlerine gömülecek olan verinin binary kodu yerleştirilir. Bir Ascii karakter kodunun gömülebilmesi için 3 piksele ihtiyaç vardır. 8 bitlik bir Ascii kod karşılığı olan bir karakterin yerleştirilmesi için 3 pikseldeki 9 değerlikten 8 değerliğe gömülme işleminin yapılması gerekmektedir. En önemsiz bite yerleştirilecek olan bitler değiştirilerek gerçekleşir. Resim üzerinde gerçekleşecek bu değişim gözle görünmeyecek kadar az olacaktır. Aşağıdaki şekil 7'de 3 piksel okunur ve devamın da Ascii karakter kodunun karşılığı binary'e çevrilir. Ve en önemsiz bit olan son bite yerleştirilir.



Şekil 7: LSB kodlama ile veri gömme.

LSB ile veri gömme işlemini şekil 7'de görmekteyiz. Veri gömüldükten sonra verinin tekrar elde edilmesi için şekil 7'de yapılan işlemin tersi yapılır. 3 pikselin 9 ağırlıklı değerinden ilk 8 ağırlıklı değer okunur. Ve bu değerlerin en önemsiz bitleri alınarak 8 bit bir araya getirilir. Bir araya getirilen bu değerlikler decimal değerliği alınarak Ascii karakter kod karşılığı bulunur. Şekil 8'de gizli verinin elde edilmesi yer almaktadır.

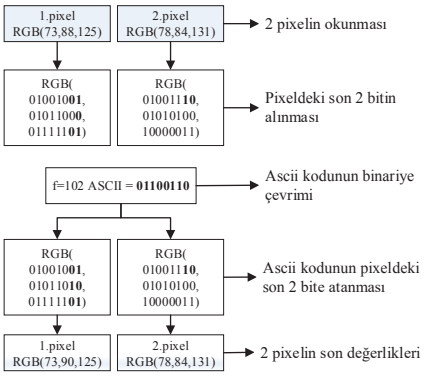


Şekil8: LSB gizli verinin elde edilmesi.

2LSB Kodlama Tekniği

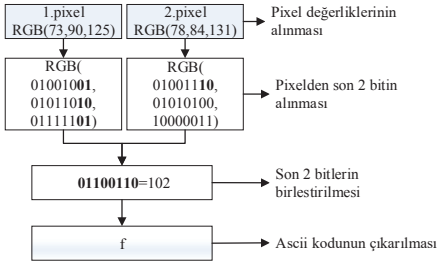
2LSB yöntemi, LSB yöntemine göre 2 kat veri gizleme kapasitesine sahiptir. 2 bit LSB yöntemi maskeleme, filtreleme vb gibi pek çok algoritmalar ile pek çok yönteme göre oluşabilecek tespitlere karşı daha dayanıklıdır (Sivaram vd., 2013). 2LSB biti ile bir görüntü içerisine gizlenen verinin fark edilmesi neredeyse imkansızdır. Fakat steganaliz yöntemleri ile gizli bilginin varlığına ulaşmak LSB'ye göre daha kolaydır (Ker, 2007).

2LSB bit kodlama tekniğinde en önemsiz 2 bit kullanılır. Ve gizlenecek olan veri son 2 bite gömülür. LSB yönteminde en önemsiz bit alırken burada son 2 bit alınmaktadır. LSB yönteminde 3 piksel içerisindeki 8 ağırlıklı renkten 8 bite yerleştirilirken, 2 bit LSB yönteminde ise 2 piksel içerisinde bulunan 4 ağırlıklı renkten 8 bite yerleştirilir. 2 pikselin okunması ve Ascii karakter kodunun yerleştirilmesi işlemi şekil 9'da bu durum ifade edilmektedir.



Şekil 9: 2LSB bitine gömme

Gömü işleminden sonra verinin çıkarılması için şekil 9'da anlatılan işlemlerin tersi yapılmaktadır. Bu durum şekil 10'da gösterilmektedir.

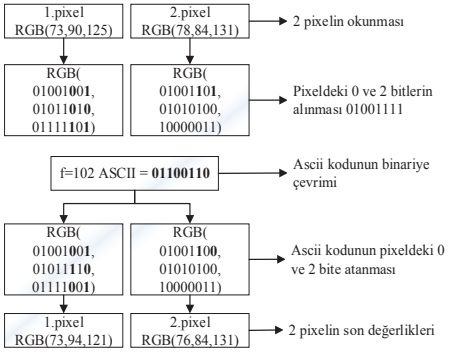


Şekil 10: 2LSB gizli veririn elde edilmesi.

Önerilen Yaklaşım

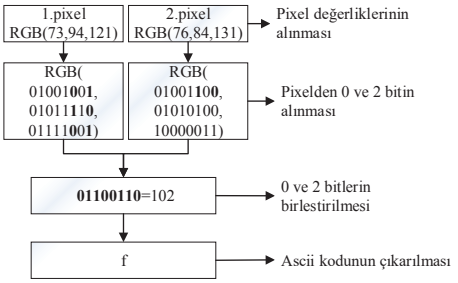
0. ve 2. bite kodlama tekniği LSB veri gömme tekniğine benzer şekilde işlenmektedir. LSB tekniğinde son bit olan en az ağırlıklı değerin kullanılmasıyla gerçekleşir. Bu teknik LSB kodlama tekniği ile 2 LSB kodlama tekniğinin harmanlanmış şeklidir. Burada görüntüde yer alan bir piksel içerisindeki renk ağırlıkları binary hale getirilir. Daha sonra gizlenecek olan binary halindeki verinin sırasıyla gömü yapılacak görüntüdeki renk değerliğinin 0. ve 2. bitine yerleştirilerek gerçekleşir. Yani gizli verinin ilk iki biti gizlenecek olan görüntü içerisindeki piksel değerliğinin 0 ve 2 bitine yerleştirilir.

Şekil 9'da görüldüğü gibi öncelikle görüntü resmindeki 2 piksel değeri okunmakta. Bu piksel değerlikleri binary'e çevrilmekte. Daha sonra gömü verisi olan bir ascii karakter kodunun decimal karşılığı olan sayı elde edilip bu decimal değerde binary'e çevrilmekte. Binary'e çevrilen bu değerin ilk 2 biti olan 01 verisi gömü verisindeki ilk pikselin r ağırlıklı kodunda yer alan son 3 bitteki 0. ve 2. bite yerleştirilmektedir. Bitlerin yerleşmesinden sonra piksel değerliklerindeki decimal değerlikleri bir sonraki aşamada yer almaktadır.



Şekil 11: 0. ve 2. LSB bite kodlama tekniği ile veri gömme

0. ve 2. bite kodlama tekniğinde verinin gömülmesi işlemi yukarıdaki gibi anlatılmıştır. Verinin elde edilmesi sırasında ise bu işlemin tersi bir durum söz konusu olacaktır. Bu durum Şekil 10'da gösterilmiştir. Buna göre görüntü verisi içerisindeki piksel değerliği okunur. Okunan piksel değerliği içerisinde yer alan decimal değerliklerin binary'e dönüşümü yapılır. Binary değerliğin en az ağırlıklı olan 0. ve 2. bitleri alınır. Piksel değerlikleri içerisindeki binary değerlikleri 8 bit olunca bu 8 bit değerin decimal değerliği hesaplanır. Ve bu decimal değerliğin ascii karakter kod karşılığı tespit edilir.



Şekil 12: 0. ve 2. kodlama ile verinin elde edilmesi.

Veri gizleme kodlama tekniklerinin yanında bizim geliştirmiş olduğumuz kodlama tekniğinin gerçeklenmesi, işlem algoritması (Procedurel kod) şeklinde aşağıda yer almaktadır.

```
Procedure goruntuye_veriyi_gizle
Görüntü ← resim(x,y)
gizlenecek_veri←metin
veri_gizleme_teknigini seç
while (gizlenecek_veri karakteri kadar tekrar et)
   karakter ← gizlenecek_verin'in son karakteri
   asciikodu ← karakter'in ascii kod karşılığını bul
   toplambinary ← toplambinary  + asciikodu'nu
    binary'e cevir
do
while(resim(x,y) her pixele veri gömene kadar devam et)
     rgb ← resim(x,y)
     while(rgb(r) mod 2<8)
        rgb(r) ← rgb(r)/2
     do
     while(rgb(g) mod 2 <8)
        rgb(g) ← rgb(g)/2
     do
     while(rgb(b) mod 2 <8)
        rgb(b) ← rgb(b)/2
     do
     gomubiti ← left(toplambinary,2)
     if(rgb(b) gömme işlemi yapıldıysa) then
        rgb(r) göme işlemini yap //bir sonraki işlem
     if (gomubiti="00") then
        if (rgb(r) >= 4) then
           rgb(r) ← rgb(r) - 4
        if (rgb(r) mod 2 = 1) then
          rgb(r)  ← rgb(r)  - 1
     if (gomubiti="01")  then
        if (rgb(r) >= 4) then
           rgb(r)  ← rgb(r) - 4
        if (rgb(r) mod 2 =0) then
          rgb(r)  ← rgb(r) + 1
     if (gomubiti="10") then
        if (rgb(r)  <  4) then
          rgb(r)   ← rgb(r)  + 4
```

```
      if (rgb(r)  mod 2=1) then
          rgb(r)  ← rgb(r)  - 1
  if (gomubiti=”11”) then
       if (rgb(r)  < 4) then
         rgb(r)  ← rgb(r) + 4;
       if (rgb(r)  mod 2=0)
         rgb(r)  ← rgb(r) +1;
   if(rgb(r) gömü tamamlandıysa) then
      rgb(g) gömme işlemini gerçekleştir.
   if(rgb(g)  gömü tamamlandıysa) then
      rgb(b) gömme işlemini gerçekleştir.
do
end procedure
```

Yukarıda belirtildiği üzere piksellerin binary'e çevrilerek değil aldığı decimal değerlikler düşünülerek bir algoritma yapılmıştır. Veri gömme algoritması yukarıda gösterildiği gibidir. Gömülü verinin imge içerisinden çıkarılabilmesi için ise aşağıdaki gibi bir algoritma tasarlanmıştır.

```
Procedure goruntuden_veriyi_cikar
görüntü ← resim(x,y)
veri_gizleme_teknigini seç
while(resim(x,y) her pixel okunana kadar)
rgb ← resim(x,y)
while(rgb(r) mod 2<8)
rgb(r) ← rgb(r)/2
do
while(rgb(g) mod 2 <8)
rgb(g) ← rgb(g)/2
do
while(rgb(b) mod 2 <8)
rgb(b) ← rgb(b)/2
do
if (rgb(r)= 0 or rgb(r)= 2) then
bitler ← bitler+"00"
if (rgb(r) = 1 veya rgb(r)= 3) then
bitler ← bitler+ "01"
if (rgb(r) = 4 veya rgb(r) = 6) then
bitler ← bitler+"10"
if (rgb(r) = 7 veya rgb(r)= 5) then
bitler ←bitler +"11"
// rgb(r) için yapılan bitler işlemi rgb(g) ve rgb(b) içinde
yapılacaktır.
   if (bitler.lenght=8) then
decimaldeger=Decimal(bitler)
//bitlerin decimal değerliğini bul
karakter←Ascii(decimaldeger)
gizlibilgi←gizlibilgi+karakter
do
//Bütün pikseller okunduğunda programı sonlandır.
End procedure
```

Görüntü Kalite Değerlendirme Yöntemleri

Dijital görüntüler üzerinde yapılan değişiklikler sonrasında bozulmalar meydana gelir. Bu bozulmalar resminde görsel farklılıklara yol açar. Stenografik uygulamalarda da veri gizlendikten sonra resimde çok küçükte olsa bozulmalar yani değişiklikler meydana gelecektir. Bu değişiklikler insan gözü ile görünmese dahi dijital ortamda yapılacak olan analizlerle saptanabilir.

Temelde kalite ölçümlerini yapmak için iki farklı yaklaşım vardır. Orijinal ve bozulmuş görüntüleri birbirinden ayıklamak için insan görü sistemi (Human VisionSystem-HVS) kullanılır. Bu görü sistemi sayesinde farklılıklar ortaya çıkarılır (Masry vd., 2006). İkinci yaklaşımda ise yapısal bozulma kalite ölçümlerine dayanmaktadır (Ong, 2004)

Literatürde bu tür değişiklikleri saptamak için pek çok algoritma yer almaktadır. Bunlardan en sık kullanılan yapıları çalışmalarımızda uygulayarak resim üzerindeki değişikliklerin saptanması ya da saldırılara karşı ne kadar sağlıklı olduğunu bulmaya yardımcı olacaktır. Bunlar;

a) MSE (Mean Square Error)

Bir görüntü üzerinde farklı tip işlemler yapıldıktan sonra orijinal görüntü ile işlem yapılmış görüntüyü karşılaştırmak için kullanılır. Görüntüde oluşabilecek farklılıkları karşılaştırmak için kullanılan karesel ortalama hata tahminidir. Karesel hata tahmini için kullanılan matematiksel fonksiyon şu şekildedir;

$$\mathrm{MSE} = \frac{1}{MN}\sum_{y=1}^{M}\sum_{x=1}^{N}[I(x,y) - I^{'}(x,y)]^2 \qquad (1)$$

M=Görüntünün yüksekliği.
N=Görüntünün genişliği.
X=Koordinat düzlemindeki yatay değer.
Y=Koordinat düzlemindeki dikey değer.
I(x,y)=orijinal resim.
I'(x,y)=işlem yapılmış resim.

b) RMSE (Root Mean Square Error)

Görüntü üzerindeki bozulmaların karekökünü ifade eder. Yani MSE'nin karekökü'dür.

c) PSNR (Peak Signal to Noise Ratio)

Dijital görüntülerde görüntüler arasındaki benzerliği ortaya çıkarabilmek için PSNR kullanılmaktadır. Gizli bilgi gömüldükten sonra stego objesi üzerindeki bozulmaları PSNR ile saptanır (Qi ve Qi, 2007). Bu hesaplama için kullanılan denklem aşağıda verilmiştir.

$$PSNR = 10Log_{10}\frac{MAX_f^2}{MSE} \quad (2)$$

c) SSIM (Structural Similarity)

İmge görüntülerindeki yapısal benzerliğin ölçümü için kullanılan yöntemlerden biri de Structual Similarity (SSIM), ve diğer kalite ölçümleri karşılaştırıldığında kabul edilebilir hesaplama karmaşıklığı ile doğru bir oran verir. Pek çok kalite değerlendirme yönteminden en basiti SSIM algoritmasıdır (Wang vd., 2004; Sheikh vd., 2006).

Uygulama ve Başarım

Bu makalede literatürde en sık kullanılan Airplane, Baboon, Barbara, Lenna, Lighthouse, Peppers, Tiffany resimleriyle çalışılmıştır. Kullanılan resimlerin boyutları 128x128 pikseldir. 4 farklı stenografi tekniği kullanılmıştır. Ve bununla beraber geliştirmiş olduğumuz başka bir stenografi tekniği incelenmiştir. Kullanılan stenografi tekniklerinde resim içerisine gizlenebilecek maksimum gömü gerçekleştirilmiştir. Yani bütün piksellere veri gömülmüştür.

Veri gizleme ve çıkarma için kullanılan uygulama c# ortamında yapılmıştır. Görüntülerdeki bozulmaları görmek için kullanılan görüntü kalite değerlendirme yöntemleri MSE, RMSE ve PSNR için C#, SSIM için ise Matlab programından faydalanılmıştır.

Yapılan veri gizleme uygulamalarında orijinal görüntü ile veri gizlenmiş stego objesi arasındaki bozulmanın en az olduğu teknik LSB tekniği olduğu görülmüştür. Kullanılan görüntü kalite değerlendirme yöntemlerinde; PSNR değerliği en yüksek olan teknik LSB tekniğidir. MSE'den az hata biti değeri ve SSIM'den yüksek benzerlik oranı yine LSB tekniğinde görülmektedir. Bu da veri gizleme teknikleri arasında görüntü üzerindeki en az bozulmanın LSB tekniği ile gerçekleştiğini göstermektedir. Ancak gizlenebilecek olan veri miktarına göre diğer tekniklerle karşılaştırıldığında LSB tekniğinde gizlenen veri miktarı en düşük seviyededir. Gizlenecek veri miktarının az olması gereken durumlarda LSB tekniğini tercih etmek daha sağlıklı olacaktır. Burada bozulmanın diğer tekniklere göre en fazla olduğu teknik ise RGB kodlama tekniği olmuştur. Ancak RGB kodlama tekniğinde gizlenebilecek olan veri miktarı diğer tekniklere göre çok daha fazla olduğu görülmüştür. Benzerlik oranlarındaki değerler ise diğer tekniklere oranla başarımı daha düşüktür. Kullanılan veri gizleme tekniklerine genel olarak imge içerisine gizli bilgi yerleştirildiğinde görüntü üzerindeki bozulmaları gözle fark edebilmek mümkün değildir.

2 Bit LSB yönteminde LSB yöntemine oranla bozulma miktarı daha fazladır. Ancak 2Bit LSB yöntemi ile gizlenebilecek veri miktarının LSB yöntemindeki gizlenebilecek veri miktarının 2 katı kadar veri gizlenebildiği görülmektedir. 2 Bit LSB yöntemi ile geliştirmiş olduğumuz 0 ve 2 bite kodlama tekniğindeki veri gömme miktarları aynı olduğu gözlenmektedir. Ancak bozulma miktarları arasında nisbi fark olduğu gözlenmektedir. 2Bit LSB kodlamada son iki bitin almış olduğu decimal değerlik 0 bit için 1, 1 bit için ise 2 olması sebebiyle toplam 3 decimal değere sahip iken; 0. ve 2. bitte ise bu durum 0. bit için 1, 2. bit için ise 4 değere sahiptir. Yani toplam decimal değerliği 5'tir. Bu da 2Bit LSB yöntemiyle kıyaslandığında bozulma miktarı olarak çok fazla kıyas yapılabilecek bir değer olarak görünmemektedir. PSNR, MSE, RMSE değerliklerinin bir birlerine yakın değerlikler olduğu görülmektedir. Bu değerler ne kadar az olsa da bozulmaların en aza indirgenmesi ve bilginin varlığının gizlenmesi en önemli etkendir.

Yapılan uygulama ile ilgili olarak elde edilen PSNR, MSE, RMSE, Gömü miktarı, SSIM değerlikleri aşağıdaki Tablo 2'de gösterilmektedir.

Sonuçlar ve Tartışma

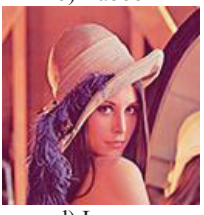
Görüntülerin sayısallaştırılması ve bu görüntülerin depolanması sağlık, bankacılık, ulaşım vb. pek çok alanda yoğun şekilde kullanılmaktadır. Bu dokumanlar modern tarayıcılarla taranan ve yüksek düzeyde gizliliğe sahip olan belgeler olabilir. Bu belgeler medikal görüntüler, finans sektöründeki finansal tablolar, yada kuruma ait bilgileri içerebilir. Bu görüntülerin güvenirlik, gizlilik ve bütünlüğün önemli olması sebebiyle araştırmalara konu olmuştur (Vellasques vd., 2011). Stenografide verinin gizliliği çok önemlidir. Ayrıca gizlenecek verinin miktarı da önem arz etmektedir. Bu çalışmada literatürde en çok bilinen LSB veri gizleme tekniğine göre 2 kat daha fazla veri gizlenebilmesi önemli bir faktördür. Veri gizlenirken veri bitlerinin sıralı olmaması bu noktada verinin tekrardan elde edilmesini de güçleştirmektedir. Veri gömmeye farklı bir bakış getirerek önceki çalışmalar uygulanmıştır. Bu sebeple stenografik yaklaşımlara yardımcı olduğu düşünülmektedir. Öte yandan bozulma miktarı LSB'ye göre fazla olduğu görülmektedir. Bu bozulmayı en aza indirgemek için optimizasyon yapılabilir. Kullanılacak olan optimizasyon algoritmaları ile bozulmalar en asgari düzeye indirilebilir. Böylelikle veri gizleme miktarında artış gerçekleşirken bozulma da en az düzeye indirilmiş olacaktır. Yapılan uygulamalarda görüntülerin her pikseline veri gizlenmiştir. Ve burada etken bozulma miktarı olmaktadır. Çalışmada kullanılan görüntüler literatürde en fazla kullanılan görüntüler olup Tablo1 görülmektedir.

Tablo1. Çalışmada kullanılan görüntüler.


a) Airplane

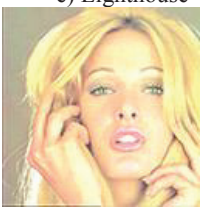

b) Baboon


c) Barbara


d) Lenna


e) Lighthouse


f) Peppers


g) Tiffany

Tablo2. Veri Gizleme Uygulamalarının Görüntü Kalite Değerlikleri

	RESİM ADI	PSNR(db)	MSE	RMSE	SSIM	GÖMÜ MİKTARI
LSB 2 bit	baboon	38,55684576	6,565002441	2,562226071	0,9995	12287
	barbara	39,90356783	6,648498535	2,578468254	0,9993	12287
	lenna	39,89930389	6,655029297	2,579734346	0,9986	12287
	lighthouse	39,94032313	6,592468262	2,567580235	0,9987	12287
	peppers	39,85630154	6,721252441	2,592537838	0,9897	12287
	airplane	39,89031154	6,668823242	2,582406483	0,9994	12287
	tiffany	39,52135854	7,260131836	2,694463181	1	12287
R Kodlama	baboon	28,64542887	64,32452393	8,020257098	0,9974	16384
	barbara	30,18050679	62,37774658	7,897958381	0,9957	16384
	lenna	30,12662347	63,15649414	7,947106023	0,9939	16384
	lighthouse	30,11957392	63,25909424	7,95355859	0,9954	16384
	peppers	30,02871396	64,59649658	8,037194572	0,9706	16384
	airplane	29,97751382	65,36254883	8,084710807	0,998	16384
	tiffany	29,70785208	69,54968262	8,339645233	0,9997	16384
RGB Kodlama	baboon	28,3116776	69,46270752	8,334429046	0,9973	16384
	barbara	29,78787827	68,27984619	8,263161997	0,9956	16384
	lenna	29,74724815	68,92163086	8,301905255	0,9939	16384
	lighthouse	29,7272298	69,24005127	8,321060706	0,995	16384
	peppers	29,72621924	69,25616455	8,322028872	0,9704	16384
	airplane	29,76964334	68,56713867	8,280527681	0,9978	16384
	tiffany	27,53997621	114,5731201	10,70388341	0,9996	16384
LSB Kodlama	baboon	45,05646855	1,469848633	1,212373141	0,9999	6143
	barbara	46,42860199	1,479858398	1,216494307	0,9999	6143
	lenna	46,4248421	1,481140137	1,217021009	0,9996	6143
	lighthouse	46,42001273	1,482788086	1,217697863	0,9997	6143
	peppers	46,46891138	1,466186523	1,210861893	0,9973	6143
	airplane	46,41161884	1,485656738	1,218875194	0,9999	6143
	tiffany	46,38671146	1,49420166	1,222375417	1	6143
0 ve 2 Bite Kodlama	baboon	33,01552797	23,51617432	4,849347824	0,9988	12282
	barbara	34,43072954	23,44268799	4,841764966	0,9981	12282
	lenna	34,34986013	23,88330078	4,887054407	0,9971	12282
	lighthouse	34,4173398	23,51507568	4,849234546	0,9975	12282
	peppers	34,40812872	23,56500244	4,854379717	0,9822	12282
	airplane	34,42059876	23,49743652	4,847415448	0,9988	12282
	tiffany	34,11556558	25,20715332	5,020672596	0,9999	12282

Kaynaklar

Akar, F., Ertürk, İ., Yalman, Y., Çetin, Ö., (2014). "Veri Gizleme", ISBN 6053331414.

Akar, F., Selçuk H.V., (2004). "A New RGB Weighted Encoding Technique for Efficient Information Hiding in Images", Journal of Naval Science and Engineering, 2, 21–36.

Anguraj, S., Shantharajah, S.P., Murugan, R.A., Balaji, E., Maneesh, R., Prasath, S., (2011). "A Fusion of A-B MAP Cipherand ASET Algorithms for the Enhanced Security and Robustness in Audio Steganography", IEEE-International Conference on Recent Trends in Information Technology(ICRTIT).

Behnia, S., Ahadpour, S., Ayubi, P., (2014). "Design and implementation of coupled chaotic maps in watermarking", Applied Soft Computing, 21 481–490.

Blakley, G., (1979). "Safeguarding cryptographic keys", National Conf. on AFIPS, 48, 313-317.

Charudhary, A., Vasavada, J., (2012). "A hash based approach for secure keyless image steganography in lossless rgb images", First Int. Workshop on Cyber Crime, 941-944. IEEE.

Ching-Yu Y., (2007). "Color İmage Steganography Based On Module Substitutions", Intelligent Information Hiding and Multimedia Signal Processing, 2007. IIHMSP 2007. Third International Conference, 118 – 121.

Coşkun, I., Akar, F., Çetin, Ö., (2013). "A new digital image steganography algorithm based on visible wavelength", Turkish Journal of Electrical Eng. & Computer Sci. 548 – 564.

Doğan, F., Güzeldereli, E.A., Çetin, Ö., (2013). "Medikal Görüntüler içerisine tıbbi bilgilerin gömülmesi için yeni bir yaklaşım", SAU J., 17, 2, 277-286.

Erçelebi, E., Subaşı, A., (2006). "Robust Multi Bit and High Quality Audio Watermarking Using Pseudo-Random Sequences", Computers and Electrical Eng., 525–536.

Fridrich, J., Goljan, M., (2002). "Practical Steganalysis of Digital Images – State of the Art", Security and Watermarking Multimedia Contents IV SPIE, 4675, 1–13.

Hayati, P., Potdar, V., ve Chang, E., (2007). "A Survey of Steganographic and Steganalytic Tools for the Digital Forensic Investigator", in Workshop of Information Hiding and Digital Watermarking to be held in conjunction with IFIPTM, Moncton, New Brunswick, Canada.

Ker, A.D., (2007). "Steganalysis of Embedding in Two Least-Significant Bits", IEEE Transactions on Information Forensics and Security, 2, 1.

Matam, B.R., Lowe, D., (2009). "Exploiting sensitivity of nonorthogonal joint diagonalisation as a security mechanism in steganography", Digital Signal Processing, 2009 16th International Conference, 1 – 7.

Masry, M., Hemami, S.S., Sermadevi, Y., (2006). "A Scalable Wavelet-Based Video Distortion Metric and Applications", IEEE Trans. On Circuits Syst. Video Technol., 16, 2, 260-273.

Neeta, D., Snehal, K., Jacobs, D., (2006). "Implementation of LSB steganography and it sevaluation for various bits", IEEE 1st Int. Conference on Digital Information Management, 173-178, India.

Ong, E.P., Lin, W., Lu, Z., Yao, S., Etoh., M., (2004). "Visual Distortion Assessment With Emphasis on Spatially Transitional Regions", IEEE Trans. Circuits Syst. Video Technol., 14, 4, 559-566.

Qi, X., Qi, J., (2007). "A robust content-based digital image watermarking scheme", Signal Processing 87, 1264–1280.

Rai, S., Dubey, R., A., (2012) "Novel Keyless Algorithm for Steganography", IEEE-Engineering and Systems (SCES), 1 – 4.

Sethi, N., Sharma, D., (2012). "A new cryptology approach for image encryption", IEEE Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE Int. Conference, 905 – 908.

Shahadi, H.I., Jidin, R., Way, W.H., (2014). "A Novel and High capacity Audio Steganography Algorithm based on Adaptive Data Embedding Positions", Research J. of Applied Sci., Eng. and Tech., 7, 11, 2311-2323.

Shamir, A., (1979). "How to share a secret, Communication ACM", 22, 612-613.

Sheikh, H.R., Sabir, M.F., Bovik, A.C., (2006). "A Statistical Evaluation of Recent Full Reference Image Quality Assessment Algorithms", IEEE Transactions on Image Processing, 15, 11, 3441-3452.

Singh, M., Singh, S.B. ve Singh L.S.S., (2007). "Hiding encrypted message in the features of images", IJCSNS Int. Journal of Computer Science and Network Security, 7, 4.

Sivaram, M., Devi, B.D., Steffi, J.A., (2012). "Stenography of Two LSB Bits", In. J. of Communications and Eng., 1, 1.

Vellasques, E., Sabouring, R., Granger, E., (2011). "A high throughput system for intelligent watermarking of bi-tonal images", Applied Soft Computing 11,5215–5229.

Wang, Z., Bovik, A.C., Sheikh, H.R., Simoncelli, E.P., (2004). "Image Quality Assessment: From Error Visibility to Structural Similarity", IEEE Transactions on Image Processing, 13, 4, 600-612.

A new steganography approach for digital images

Extended abstract

In today's technology it is vitally important and necessary to protect the data from outsiders. For this reason, there are many methods developed and implemented to protect the data. One of these methods is stenography. It is aimed to convey the data safely by using stenographic techniques to hide the data in images. The main idea in here is to hide the existence of the data and the changes in images by minimizing the distortion of the image. By means of making changes in digital images, it is possible to hide lots of data in images. However these changes should not be noticed. If it is considered that the internet is used almost every single area of our life, it can be seen that we are all in digital images. With the help of stenographic techniques, it is possible to hide the data in dozens of digital images from social media, social network and websites. Besides it is nearly out of question to notice the hidden data with this technique. In this article, most commonly used data hiding methods of stenography namely LSB coding, 2LSB coding, RGB coding and R coding are compared to each other. By analyzing these methods a new data coding is developed. Newly developed hiding in the 0 and 2 bit method and previous methods are compared. As newly developed method is less known than the other methods, accessing the hidden data would be harder. Data hiding applications are made with newly developed method and previous methods and with the analyses of PSNR (Peak Signal to Noise Ratio), MSE (Mean Squared Error), SSIM (Structural Similarity) the rates of distortion in the picture is revealed. By taking the results into the consideration, the advantages of hiding data methods compared to each other and stated in this article.

Keywords: *informaiton security,stenography, LSB, Hiding 0 and 2 bit.*