SAÜ Fen Bil Der 19. Cilt, 1. Sayı, s. 1-6, 2015

# 24 bit renkli hareketli resimler (video) üzerinde geliştirilen sırörtme yöntemi

Yasemin Yıldız[1*], Ahmet T. Özcerit[2]

*08.01.2014 Geliş/Received, 18.04.2014 Kabul/Accepted*

**ÖZ**

Gelişen teknolojiyle birlikte sayısal olarak iletilmek istenen verilerin (ses, görüntü, video vb.) ortam güvenliğinin azalması nedeniyle koruma ihtiyacı ortaya çıkmıştır. Güvenlik ihtiyaçlarının giderek artmasıyla veriyi şifreleme ve veriyi taşıyıcı bir dosyaya gizleme alanında yapılan çalışmalar hız kazanmıştır. Şifreleme mesajın içeriğinin korunmasıyla ilgilenirken, sırörtme (steganography) mesajın varlığının gizlenmesi ile ilgilenmektedir. Bu çalışmada ise AVI formatındaki video dosyalarının üzerine şifrelenen mesaj klasik veri gömme tekniği olan LSB'den farklı olarak RGB ağırlık tabanlı veri gizleme ile gerçekleştirilmiştir. Algoritmalar, Matlab hazır fonksiyonları yerine C# programlama dilinde gerçekleştirilmiştir. Bu kodlama tekniğiyle veri gömme kapasitesi nispi olarak oldukça artmıştır.

**Anahtar Kelimeler:** steganography, sırörtme, RGB kodlama, veri gizleme, histogram

# 24-bit color moving pictures (video) on the method developed steganography

**ABSTRACT**

Since communication channels are insecure, techniques for information hiding (steganography) have nowadays become increasingly more sophisticated and widespread. Crytptography and steganography have devised technologies for needs of data security. While cryptography is used to encrypt the message, steganography is used to hide the mesasage. In this study, an encrypted message has been embedded into an AVI video file based on RGB weight based algorithm in contrast to classical LSB algortihm. The algorithms are implemented in C# language other than Matlab libraraies. This technique has considerably increased relative data embedding capacity.

**Keywords**: steganography, RGB method, kriptology, digital video, histogram

* Sorumlu Yazar / Corresponding Author
1 Kaman Teknik ve Endüstri Meslek Lisesi, Kırşehir -yasemintiryaki86@hotmail.com
2 Sakarya Üniversitesi Teknoloji Fakültesi, Bilgisayar Mühendisliği, Sakarya – aozcerit@sakarya.edu.tr

## 1. GİRİŞ (INTRODUCTION)

İnsanoğlunun içinde bulunduğu ve iletişimin olmadığı hemen hemen hiçbir durum yoktur. İnsan varsa iletişim mutlaka vardır. İletişim sadece günlük iletileri kapsamak zorunda değildir. Kimi zaman bir şirketin özel bilgileri, kimi zaman bir devletin sırları, kimi zamansa bir eylemin ayrıntıları diğer kullanıcıya iletilmek istenebilir. İletişimde verinin gizliliği arttıkça güvenliği de o doğrultuda azalmaktadır. Yetkisiz kişilerden gelebilecek saldırılar artabilir. Tüm bu güvensizliklerin giderilmesi çalışmalarının temeli antik çağlara kadar dayanmaktadır. Çağlar değiştikçe gelişen ve değişen teknolojiyle birlikte güvenlik için kullanılan tekniklerde de önemli farklılıklar kendini göstermektedir. Her yöntemde amaç mesajın üçüncü kişilerin eline geçmeden ilgili noktalara ulaştırmak olsa da şekil ve metotlar konusunda ayrılıklar yaşanmaktadır. Bu çalışmada, gizli verilerin saldırılardan korunarak iletişimin gerçekleştirilmesi için sırörtme algoritmaları geliştirilmiştir.

Sayısal medyada iletişimin güvenliği için sayısal damgalama (watermarking) ve sırörtme (steganography) teknikleri geliştirilmiştir. Geliştirilen bu iki teknik amaç bakımından benzerlik gösterse de aralarında bazı farklar bulunmaktadır. Sayısal damgalama herkes tarafından bilinen bir medya dosyasının (film, müzik parçası vb.) korunması için kullanılırken, sırörtme yöntemi ise bilinmeyen bir dosyanın içerisinde gizli verinin ilgili yerlere iletilmesini amaçlar. Damgalamada damgalama yapıldığını herkes görebilir (örneğin televizyon kanallarının logoları), fakat sırörtme de verinin varlığından kimsenin haberi yoktur.

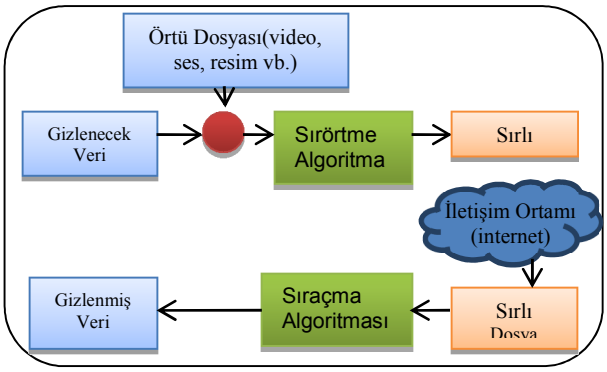
Sırörtme (steganography) kullanım alanları açısından üçe ayrılmaktadır:

- Metin (text) steganografi,
- Görüntü (image) steganografi,
- Ses (audio) steganografi,

Gizli haberleşme teknikleri ilk olarak resim dosyaları üzerine uygulanmış fakat resim dosyalarının gizli mesajları sınırlaması ve bu sınırı aşabilecek veriler için gömme işlemi yapılamaması gibi sebeplerden dolayı araştırmacılar video dosyaları üzerine yoğunlaşmıştır. Video dosyaları çok sayıda resmin peşi sıra sürekli olarak akmasıyla ve aynı zamanda görüntünün yanı sıra ses dosyalarının akışıyla da oluşur. Bu sebepten dolayı hem resim hem de ses dosyasına veri gömme teknikleri video içerisine veri gömmede kullanılabilir. Video içerisine veri gömmek için dönüşüm boyutu yöntemleri (Discrete Cosine Transform–DCT, Discrete Wavelenght Transform-DWT) kullanılır.

Sırörtme'de videonun kullanılmasının temel nedeni videonun gizlenecek veriyi sınırlamamasıdır. Yani mesaj ne kadar uzun olursa olsun ona uygun uzunlukta bir videonun seçilmesi ile veri güvenli bir şekilde gömülebilir. Örneğin, saniyede 25 resim geçebilen (25 fps-frame per seconds) 10 saniyelik bir videoya normal tekbir resim üzerine gömülebilecek mesajın 250 katı daha uzun veri gömülebilir.

Videolar üzerinde yapılan ilk veri gömme denemeleri ham videolar üzerinde olmuştur. Bu çalışmada da temel olarak ham videolar hedeflenmiştir.




Şekil 1. Steganografik sistem (Steganographic system)

Şekil 1'de gösterildiği üzere bir veri gizleme işlemi yapılması için öncellikle taşıyıcı bir dosyanın bulunması gerekir. Gizlenecek verinin boyutuna uygun olarak seçilen dosya ile birlikte gizlenecek veri bir gömme algoritmasına tabi tutulur. Gömme işlemi sonucunda oluşan dosya sırlı dosyadır. Bu dosya internet gibi bir iletişim ortamında alıcı noktaya ulaşır. Alıcı sırlı videoya bir çıkarma algoritması uygular ve orijinal veri geri elde edilmiş olur.

## 2. SAYISAL GÖRÜNTÜ, PİKSEL VE SAYISAL VİDEO KAVRAMLARI (DIGITAL IMAGE, PIXEL AND DIGITAL VIDEO CONCEPTS)

Sayısal görüntüyü oluşturan en küçük yapı taşına piksel denir. Piksel İngilizce "Picture cell" resim hücresi anlamına gelen kavramın kısaltılmasıyla oluşmuştur. Bir piksel ilgili resmin tüm renk özelliklerini taşır. Bu sebeple sayısal görüntünün temel yapı taşı denilmektedir. Bir görüntüyü oluşturan piksel sayısı ne kadar fazla ise görüntü gerçek rengine o kadar yakın olur. Piksel sayısı azaldıkça bulanık, donuk, rengi bozuk görüntüler oluşur. Bir görüntüdeki kaç piksel olduğu bilgisi ise çözünürlüğü ifade eder. Çözünürlük bir görüntüdeki yatay ve dikey olarak toplam kaç pikselin olduğunu veren değerdir. Bir görüntüdeki piksel sayısı fazla ise görüntü o kadar net olacağı daha önce belirtilmişti. Bu ifadeden yararlanarak çözünürlük ne kadar fazla ise görüntü gerçek rengine o

kadar yakındır denilebilir. Örneğin bir görüntünün yatayda 640, dikeyde 480 pikseli var ise bu görüntü 640 x 480 çözünürlüğe sahiptir denir.

Sayısal bir videonun oluşması için, bir ışık kaynağına, bir nesneye ve nesnenin ışığı yansıtmasına gerek vardır. Tüm bu şartlar oluştuğunda önce görüntü ve ardından sayısal video oluşur.

Bir videonun bellekte kapladığı alanı hesaplamak için:

Video boyutu x Çerçeve sayısı x Renk yoğunluğu x video süresi (1)

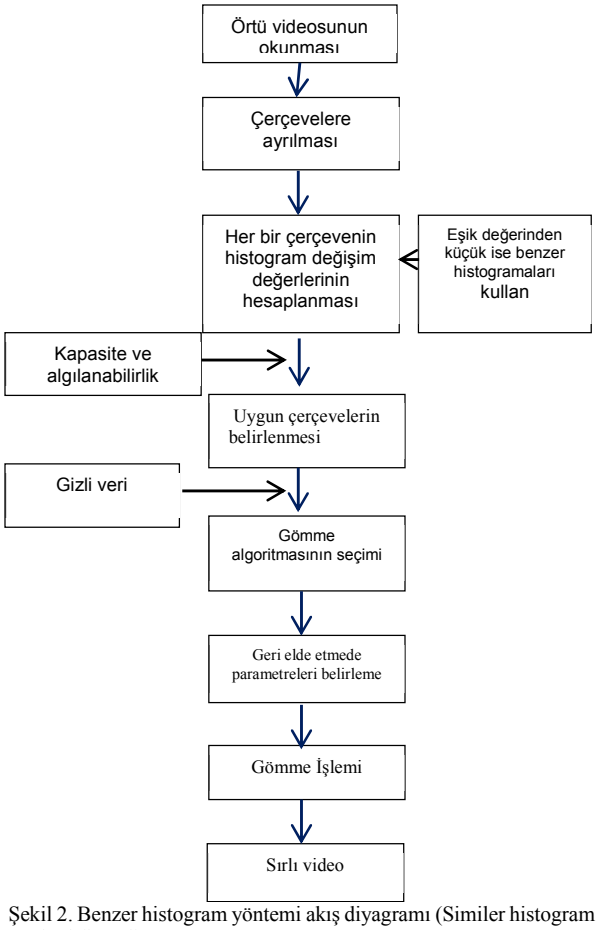
Yukarıdaki denklemden elde edilen sonuca göre ise videonun bellekte kapladığı alan bulunur.

## 3. SONUÇLAR VE TARTIŞMA (RESULTS AND DISCUSSION)

Bu çalışmada insan göz sisteminin görme özelliklerinden faydalanılarak C# programlama dilinde algoritmalar tasarlanmıştır. Önceki çalışmalarda veri gizleme ve elde etme işlemleri Matlab tabanlı hazır fonksiyonlarla gerçekleştirilirken, bu çalışmada algoritmalar bir programlama dili ile en temele seviyeden başlayarak tasarlanmıştır.

Gizlenecek olan verinin video içerisinde uygun olan alanlara gömülebilmesi için klasik tekniklerden farklı olarak histogramlar yöntemi kullanılmıştır. Bu yöntemle video içerisindeki hareketli ya da hareketsiz, renk yoğunluğunun fazla ya da az olduğu alanların tespitinde kullanılır.

Histogramlar yönteminde, ardı sıra gelen video çerçevelerinin her bir pikselinin ayrı ayrı histogram değerleri hesaplanır ve olay bu değerler üzerinde yorumlanır. Bu yöntemde öncelikle içerisine veri gömülebilecek piksellere sahip olan çerçeveler belirlenir. Elde edilen bu çerçevelerde bulunan piksellerin histogram değerleri bulunur. Histogram, bir videoyu oluşturan her bir hareketsiz görüntüyü (resim) oluşturan piksellerinin sahip oldukları renk bileşenlerinin koyuluk bilgilerine göre dağılımlarını gösteren değerler dizisidir. Genel olarak 24-bit renkli resimler için histogram 256 elemanlı pozitif tam sayılar dizisidir başka bir ifadeyle resmi oluşturan her bir pikselin 0 ile 255 arasında bir renk koyuluk değerine sahiptir. Geliştirilmiş olan histogramlar yönteminde, öncelikle video kendisini oluşturan hareketsiz görüntülere ayrılıyor. Bunların her biri genel olarak çerçeve (frame) olarak adlandırılıyor. Videoyu oluşturan çerçevelerin her bir pikseli için o pikselin renk tonunu oluşturan renk bileşenleri (R,G,B) için ayrı ayrı bulunduktan sonra bulunan bu değerin ortalaması alınır. Örneğin; n. pikselin R=255, G=24, B=45 bulunmuş olsun bu n. pikselin histogramı, (R+G+B)/3 'den bulunur. Ardışık çerçevelerde de bu işlem gerçekleştirildikten sonra birbirini takip eden her bir çerçevenin aynı pikseli için bulunan histogramlar arasındaki fark hesaplanır. Böylece değerlendirilecek olan tek bir değer elde etmiş olunur. Örneğin; birinci çerçevedeki üçüncü pikselin histogramı 156 değerinde, bir sonraki çerçeve olan ikinci çerçevenin yine aynı pikselinin (üçüncü piksel) histogramı 147 değerindedir. Bu iki histogram arasındaki farkın mutlak değeri alınır ve değerlendirme yapmak için tek bir değer elde edilmiş olunur. Elde edilen bu değer ne kadar az ise resim çerçeveleri arasındaki fark o kadar azdır, ne kadar fazla ise de resimler arasındaki renk ve ton o kadar birbirinden farklıdır denilir. Böylece hangi çerçevenin hangi pikseline veri gömüldüğünde insan göz sisteminin bu değişimi algılamasının en az olacağını yorumlayabiliriz. Eşik değeri ardışık çerçeveler arasında bir değişim veya benzerlik algılanmasında kullanılan, maksimum alabileceği değer histogramın maksimum alabileceği değerle aynıdır ve maksimum 255 değerini alabilir. Eşik değer kullanıcı tanımlı bir algılama kıstasıdır. Çalışmada geliştirilen veri gizleme programında bu eşik değeri algılanabilirlik – kapasite parametresi ile kullanıcı tarafından ayarlanabilmektedir. Bununla kullanıcıya bir esneklik sağlamak amaçlanmıştır. Eşik değerinin yüksek seçilmesi ile çerçeve geçişlerindeki algılama hassasiyetin arttırılmasına karşılık bölümlenebilecek çerçeve sayısında düşme olur. Çerçeve sayısının azalması ise gömülebilecek veri uzunluğunun azalması anlamına gelmektedir. Eşik değerinin düşük seçilmesi durumunda ise hassasiyet azalacak fakat bölümlenebilecek çerçeve sayısı artacaktır. Dolayısıyla gömülebilecek veri uzunluğu da artacaktır. Bu bilgiler ışığında kullanıcı tarafından girilecek bir eşik değer ile ardışık çerçevelerin histogram farkları karşılaştırılarak veri gizlenebilecek video çerçeveleri ve pikselleri belirlenir. Eşik değerin üzerinde kalan pikselleri seçilirse, ardışıl video çerçevelerinin renk bakımından karışık bir yapıya sahip olduğu anlaşılır ki bu Farklı Histogramlar yöntemi olarak adlandırılır. Eşik değerin altında kalan bileşenlerin seçilmesi durumunda ise ardışıl video çerçevelerinin renk bakımından tekdüze olduğu anlaşılır ki bu da Benzer Histogramlar yöntemi olarak adlandırılır.

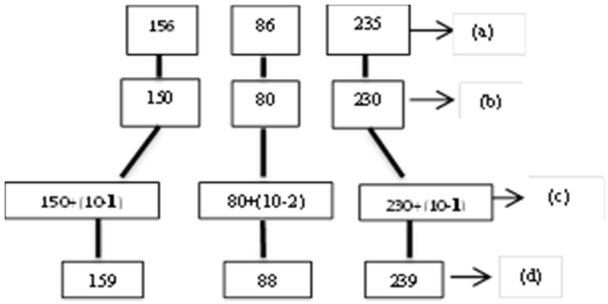



Şekil 2. Benzer histogram yöntemi akış diyagramı (Similer histogram method flow diagram)

Şekil 2 'de benzer histogramlar yönteminin akış diyagramı görülmektedir.

Veri gömme tekniklerinde en temel amaç, görüntünün en az bozulmayla maksimum veri gömme kapasitesinin elde edilmesidir. Bu amaçla RGB ağırlıklı kodlama tekniği kullanılmıştır [1].

RGB değerleri için; R=156, G=86, B=235 rengine sahip olan piksele "y" harfini gömmek istersek; Öncelikle "y" harfini ASCII kod değerine çevirmemiz gereklidir. "y" harfinin ASCII kodu '121'dir. R=156, G=86, B=235 gömülen bilginin yeniden elde edilmesi aşamasında sorun yaşamamak için son rakamlar sıfırlanır. Buna göre elimizde R=150, G=80, B=230 değerleri oluşur. Bir sonraki aşama ise "y" harfinin ASCII kodunun her bir rakamı '10' sayısından çıkarılır (10-1=9, 10-2=8, 10-1=9). Elde edilen bu rakamlar her bir RGB değerlerinin son basamağına yerleştirilir. Bu yüzden RGB'nin rakamlarına bakıldığında anlamlı bir değişikliğin olduğu anlaşılmaması için, gizlenecek bilginin ASCII kodunun her bir rakamı '10' sayısından çıkarılır. Son aşamada ise R=150+9=159, G=80+8=88, B=230+9=239 değerleri elde edilir. Böylelikle gizlenecek olan veri örtü dosyasının uygun pikseline gömülmüş olur. Gizli verinin çıkarılması evresinde ise yapılan işlemlerin sağlaması yapılır. Yani pikselin RGB değerleri alınır (159, 88, 239). Son basamaklarındaki sayıları 10'dan çıkarılır. (10-9=1, 10-8=2, 10-9=1). Böylece "y" harfinin tekrar ASCII kod karşılığını bulmuş oluruz.



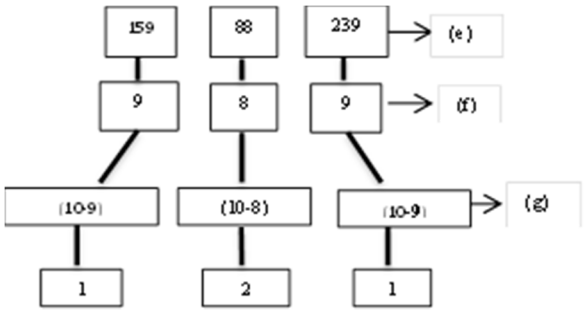

a) orijinal piksel ağırlığı,

b) RGB son rakamlarının sıfırlanması,

c) "y" kodunun gömülmesi,

d) Elde edilen yeni RGB ağırlıklı piksel

Şekil 3. Bir piksel içine ASCII kodunun gömülmesi (Embedding of ASCII code in to a pixel)




e) Kodlu RGB ağırlıklı,

f) RGB son rakamlarının alınması,

g) "y" gömülü karakterin elde edilmesi.

Şekil 4. Bir piksel içinden ASCII kodunun çıkarılması (Removing the ASCII code for a pixel)

## 4. SONUÇLAR (CONCLUSIONS)

Çalışmanın bu bölümünde önerilen sırörtme tekniklerinin bozulan piksel sayıları ve algılanabilirlik gibi parametrelere bağlı başarımları değerlendirilecektir. Çalışmada kullanılan video 100 x 100 boyutlarında ve çerçeve sayısı 6'dır.

Deneysel çalışmaların değerlendirilmesi aşamasında, sırlı videoların istatiksel kalitelerini ölçmek için Tepe Sinyal Gürültü Oranı (Peak Signal to Noise Ratio-

PSNR) ölçütü kullanılmıştır. PSNR, orijinal görüntü ile sırlı görüntü arasındaki benzerlik kalitesini hesaplar. Hesaplama sonucunda PSNR tek bir değer üretir. Bu değerin yüksek olması kalitenin de yüksek olduğu anlamına gelir. Aslında PSNR değeri, insan görme sistemi ile birebir uyuşan sonuç vermemektedir. Çünkü insanların renkleri ve tonları algılama davranışı tamamen birbirlerinden farklıdır. Bu durum göz önüne alınarak bir başka görsel kalite değerlendirme kıstası olan görsel ölçüm yöntemi de geliştirilen tekniklerin başarım değerlendirmesinde kullanılmıştır.

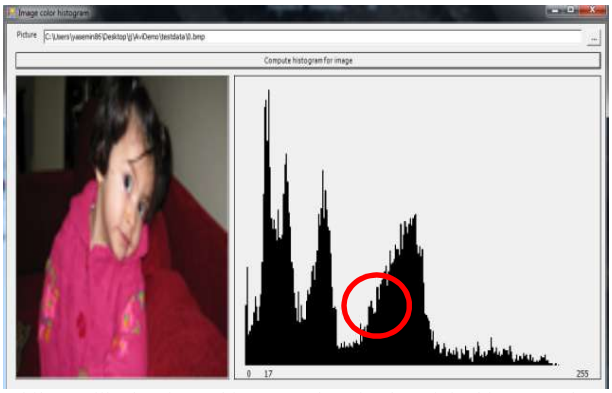
İki görüntü arasındaki PSNR değerini hesaplamak için öncelikle Ortalama Kare Hatası (Mean Squared Eror-MSE) değeri hesaplanmalıdır [10]. MSE değerinin hesaplanması için Denklem 1 kullanılabilir. MSE değerinin hesaplanmasının ardından Denklem 2'ye göre PSNR hesaplanır [9].

$$MSE = \frac{\sum_{M,N}[I(i,j)-K(i,j)]^2}{MxN} \quad (1)$$

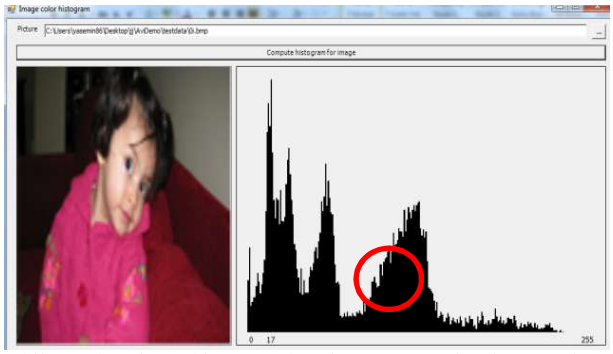
Denklem 1'de kullanılan I ve K birbiriyle kıyaslanan görüntülerdir. I veri gömülmeden önceki yani orijinal görüntüdür. K ise veri gömüldükten sonraki orijinal görüntüdür. M x N ile temsil edilen ise videonun görüntü boyutlarıdır.

$$PSNR = 10\log_{10}\left(\frac{MAX^2}{MSE}\right) \quad (2)$$

Denklem 2'de kullanılan MAX görüntüye ait bir pikselin kaç bit ile ifade edildiğini gösterir. Örneğin bir pikseli ifade etmek için 8 bit kullanılıyorsa o zaman MAX 255'tir. Genellikle de işlemlerde sabitliği sağlamak için 255 değeri kullanılır.




Şekil 5. Orijinal resim ve histogram değeri (The original image and the histogram value)




Şekil 6. Sırlı resim ve histogram değeri (Steganography picture and the histogram value)

Şekil 5 de orijinal resim ve Histogram değeri verilirken Şekil 6 'da gizli veri gömülmüş video çerçevesinin Histogram değeri verilmiştir. RGB ağırlıklı kodlama tekniğiyle klasik LSB kodlama tekniğinden daha az kayıp yani bozulan piksel sayısı olmuştur denilebilir. Görüntüler içerisinde daire içerisine alınmış alanların dışındaki piksellerde herhangi bir bozulma görünmemiştir. Bu Tablo 1'de elde edilen MSE ve PSNR değerleri verilmiştir.

Tablo 1. Elde edilen sırlı görüntüler için hesaplanan görüntü kalite ölçütleri (The resulting image quality metrics calculated for glazed images)

| Video boyutu (bayt) | Veri boyutu (bayt) | MSE | PSNR |
|---|---|---|---|
| 90000 | 12.711 | 3.08796 | 43,234077 |
| 90000 | 16.384 | 10.2063 | 38.04212 |
| 240000 | 20.455 | 14.244 | 36.011 |

Tablo 1'de görüldüğü üzere örtü dosyasının boyutu arttıkça içerisine gömülebilecek veri uzunluğu da artmaktadır. Gömülen veri uzunluğu arttıkça da bozuşan piksel sayısında artmalar olmuştur. Fakat bu artış diğer gömme algoritmalarına oranla çok küçüktür. Bu da RGB algoritmasının üstünlüğünü göstermektedir.

## KAYNAKLAR (REFERENCES)

[1] Çetin Ö., "Hareketli Görüntü Uygulamaları için Sırörtme Yaklaşımı ile Veri Gömme Algoritması Tasarımı", Sakarya Ün. Fen Bil. Ens., Dok. Tezi, 2008

[2] F. Akar, H.S. Varol, "A New Rgb Wighted Encoding Technique For Efficient İnformatin Hiding In Images" Journal Of Naval Science And Engineering Number 2 Volume 2 July 2004.

[3] Yerlikaya T., Buluş E., Arda D., "Asimetrik Kripto Sistemler Ve Uygulamaları", II. Mühendislik Bilimleri Genç Araştırmacılar Kongresi, İstanbul, Mbgak 2005.
[4] Krenn J. R. , "Steganography And Steganalysist," ( Erişim Tarihi 2011).
[5] Jonathan, K. S., Hartung F., Girid, B., "Digital Watermarking Of Text, Image, And Video Documents Comput. & Graphics", Vol. 22, No. 6, Pp. 687±695, Elsevier Science, 1999.
[6] Netravalı, A.N., Haskell, B. G. ,"Digital Pictures: Representation, Compression, And Standards(2nd Ed)," Plenum Press, New York, Ny, 1995.
[7] Amin M. F., Mohammad R., Akbarzadeh T., Farshad V.A., "A New Genetic Algorithm Approach For Scure Jpeg Stagenography" , 2006.
[8] Shali M., "Steganography İn Mms" , 2007.
[9] Gruhl, D., Bender, W., Lu A., "Echo Hiding" , Isbn 3-540-61996-8, 1996.
[10] Nedeljko C., Tapık S., "Incresing The Cappacity Of Lsb Based Audio Steganography" (Erişim Tarihi 2010).