Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı, S. 73-80, Ağustos 2020

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue, pp. 73-80, August 2020

Research Article

Cebirsel Şifrelenmiş LSB Yöntemi

Ali Karaduran[1*], Metin Turan[2]

[1] İstanbul Ticaret Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, İstanbul, Türkiye (ORCID: 0000-0000-0000-0000)
[2] İstanbul Ticaret Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, İstanbul, Türkiye (ORCID: 0000-0000-0000-0000)

(Bu yayın 26-27 Haziran 2020 tarihinde HORA-2020 kongresinde sözlü olarak sunulmuştur.)

(**DOI:** 10.31590/ejosat.779070)

ATIF/REFERENCE: Karaduran, A. & Turan M. (2020). Cebirsel Şifrelenmiş LSB Yöntemi. *Avrupa Bilim ve Teknoloji Dergisi*, (Special Issue), 73-80.

Öz

Teknolojinin gelişmesi ile birlikte verilerin elektronik ortamda güvenli bir biçimde transfer edilmesi önem kazanmıştır. Bu amaçla birçok yöntem önerilmiş ve kullanılmaktadır. Bu çalışmada, stenografi bilim dalının en az ağırlıklı bit şifreleme tekniği olarak bilinen LSB algoritmasının veri güvenliğini cebirsel ifadeler ile iyileştirmek, belli oranda daha fazla sıkıştırma sağlarken, resim üzerinde oluşan değişim hata oranını da çok artırmamak amaçlanmıştır. Geliştirilen algoritmada mesajın 24 bit renkli resimlere şifrelenmesi sağlanmıştır. Mesajda yer alan her karakter, şifrelenmek istenen resmin 2 pikseline kodlanır. Modelin başarımını ölçmek üzere (orijinal resim ile şifreli resmin değişim oranı) MSE ve PSNR metrikleri kullanılmış, LSB algoritması ile önerilen çalışma yaygın olarak kullanılan bazı model resimler üzerinde farklı uzunlukta mesajlar için karşılaştırılmışlardır. Elde edilen sonuçlara göre, çalışmada önerilen algoritmanın sıkıştırma oranı %33 daha iyi olmasına rağmen, yapılan sınamalarda elde edilen değerlerin ortalamasına göre beklendiği üzere MSE hata oranı %29 artmış ve PSNR %2.5 azalmıştır. Her ne kadar metrik değerleri negatif gözükse de, orijinal resimdeki bu değişimler çok ufak ve gözle algılanabilir olmaktan uzaktır. Kazanılan sıkıştırma oranı ve ayrıca verinin gizlenme güvenliği göz önünde bulundurulduğunda, güvenliğin önemli olduğu uygulamalara hitap ettiği düşünülmelidir.

Anahtar Kelimeler: Stenografi, Kriptoloji, Metin Şifreleme, En Az Ağırlıklı Bit

Algebraically Encrypted LSB Method

Abstract

With the development of technology, the security of data becomes important. There are many methods that ensure the security of digital data with the developing technology. In this study, it is aimed to improve the data security of LSB algorithm which is known as the least weighted bit encryption technique of the steganography discipline by providing algebraic expressions, while increasing the compression rate some ratio, not to increase the error rate of change on the picture. With this developed algorithm, the message is encrypted to 24-bit color images. Each character in the message is encoded to the 2 pixels of the picture to be encrypted. MSE and PSNR metrics were used to measure the performance of the model (the rate of change of the original picture and the encrypted picture). The proposed study with the LSB algorithm was compared for messages of different lengths on some commonly used model pictures. According to the results obtained, although the compression rate of the algorithm proposed in the study was 33% better, the MSE error rate increased by 29% and PSNR decreased by 2.5% as expected compared to the average of the values obtained in the tests. Although the metric values seem negative, these changes in the original image are very small and far from perceptible. Considering the compression rate gained and also the security of data hiding, it should be considered that it addresses applications where security is important.

Keywords: Steganography, Cryptology, Text Encryption, LSB

1. Giriş

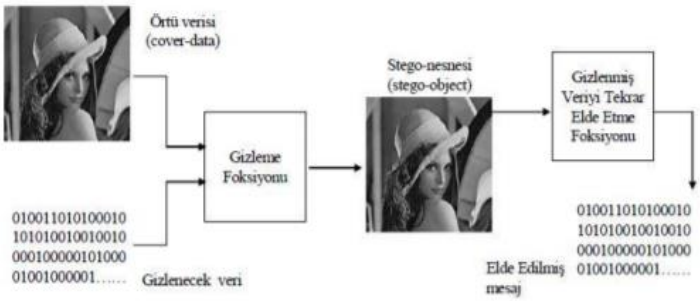
Teknolojinin gelişmesiyle günlük hayatta veriler elektronik ortamda saklandığından dolayı verilerin güvenliği sağlanamamaktadır. Elektronik ortamda saklanan verinin karşı tarafa gönderilirken verinin korunması ve güvenliğin olması önemli bir hususdur [1]. Gün geçtikçe alınan önlemlere rağmen değişik tehdit yöntemleri çıkmaktadır. Bu tehditlere karşı birçok teknik geliştirilmiştir. Bu tekniklerden bilinen en etkin yollarından biri kriptolojidir [2]. Kriptoloji verinin bir algoritma ile biçim değiştirerek (şifrelenerek) alıcıya gönderilmesi işlemidir. Alıcı bu biçim değiştirmiş veriyi nasıl orijinal hale getireceğine dair yeterli bilgiye

sahiptir ve en önemlisi biçim değiştirmiş veri orijinal haline tekrar dönüştürülebilir. Kriptolojinin uygulama alanlarından biri de steganografidir [3]. Steganografi, mesajın dijital verinin içinde kodlanması bilimidir. Steganografi' de verinin gizlenmiş olduğundan haberiniz yoktur, veri esasen dijital bir nesnedir (ses, resim, video). Çoğunlukla resimler üzerine uygulanır ve genel akış şeması Şekil 1'de görülmektedir.

Gizlenecek mesaj düz metin, şifrelenmiş metin ya da bitler halinde kaydedilebilir. Görüntü dosyalarında gizlenecek mesajlar metin dosyası veya herhangi bir resim içerisine şifrelenmiş başka bir resim dosyası da olabilir.

Tarihte steganografi, hem şifreleme yapıldığı zamandan itibaren hem de öncesinde kullanılmıştır. Eski Yunanistan'da mesajlar tahtalara yazılıp üzerine mum kaplanarak cisim kullanılmamış tablete benzetilirdi. Mesajın okunabilmesi için mumum eritilmesi gerekirdi. Benzer bir uygulamada, 1960'lı yıllarda mor ötesi boya ile yazı yazılabilen sprey ve kalemlerdir. Bu kalemlerin yazdığı yazılar, sadece bir mor ötesi ışıkla görülebilmekteydi.

Steganografinin mantığı resim dosyasının önemli olmayan bitlerine, şifrelenecek mesajın kodlanması ile insanın fark edemeyeceği yeni bir görüntünün oluşturulmasıdır. Mesajın gizlenmesi için çeşitli yöntem ve teknikler bulunmaktadır.

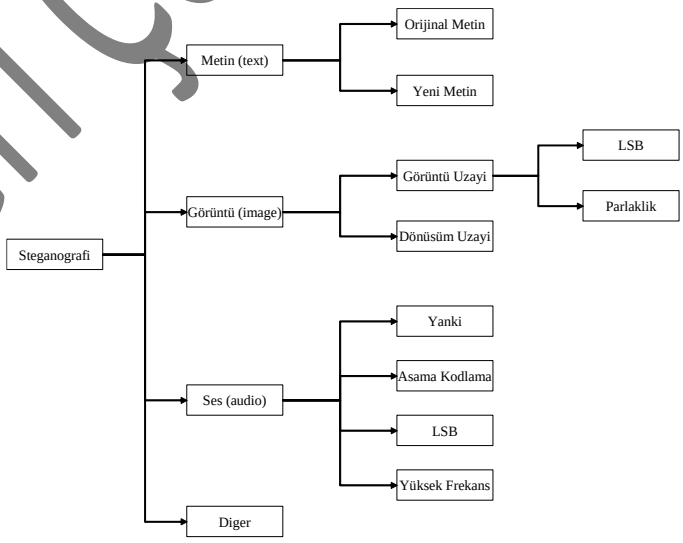


Şekil 1. Stenografinin uygulanması

Steganografinin amacı bilginin var olduğunu saklamaktır. Bu yüzden steganografi kriptolojinin bir parçası olarak görünebilir. Kriptoloji ve steganografi beraber kullanıldığında güvenlik düzeyi artmaktadır. İlk olarak mesaj kriptoloji ile şifrelenir. Daha sonra şifrelenmiş mesaj, veri gizleme işlemi yapılarak dosyaya şifrelenir [4].

Teknolojinin hızlı gelişimi ile verilerimizi korumak gerekli bir hal almıştır. Bu yüzden günümüzde dijital nesneler üzerinde steganografi çalışmaları yapılmakta ve bu uygulama sıklıkla kullanılmaktadır.

Steganografi kendi içerisinde Dilbilim Steganografi ve Teknik Steganografi olmak üzere ikiye ayrılmaktadır. Dilbilim Steganografide metin (text) taşıyıcı veridir. Teknik Steganografinin ise birçok alt metni vardır. Bunlar; görünmez mürekkep, gizli yerler, microdot'lar, ve bilgisayar tabanlı yöntemler gibi başlıklar altında toplanabilmektedir. Bilgisayar tabanlı yöntemler metin, ses, görüntü, resim dosyalarını kullanarak veri gizleme yöntemleridir. Bu Steganografinin veri gizleme yöntemlerinin yapısı Şekil 2' de görünmektedir. Görüntü steganografisinde kullanılan yöntemler ise imge uzayı ve dönüşüm uzayı tabanlı yöntemlerdir. İmge uzayında kullanılan yöntem LSB(Least Significant Bit)' dir. Dönüşüm uzayı tabanlı yöntemler imge verisini frekans uzayına dönüştürüp saklama işlemini dönüşüm uzayında gerçekleştirirler [5].



Şekil 2. Steganografi veri gizleme yöntemleri

2000'li yıllardan sonra, LSB ve Bit Plane Complexity Segmantation (BPCS) yöntemiyle, dönüştürme tekniğiyle ve permütasyon tekniği ile resim içerisine veri çalışmaları gerçekleştirilmiştir [6].

C. Koçak (2015) Erciyes üniversitesinde yayınlanan makalesinde kriptoloji ve steganografi üzerine çalışma yapmıştır. Bu çalışma kapsamında 2bit LSB yöntemi kullanılmıştır. RGB değerlerinden R ve G değerleri kullanılmıştır. Bu yöntemde 4 bit değiştirerek veri gizleme işlemi gerçekleştirilmiştir [7].

Y. Yıldız, A. T. Özcerit (2015) Sakarya Üniversitesinde yayınlanan makalesinde Steganografi üzerine çalışma yapmıştır. Bu çalışma kapsamında 24 bit Renkli hareketli videoların RGB değerlerinde cebirsel işlemler yaptıktan sonra yeni oluşan Red Green Blue değerlerine kaydetmektedir. Çalışmada gizlenen veri uzunluğu arttıkça piksel sayısında bozulmalarda arttığı görülmüştür. Fakat bu artış diğer veri gizleme algoritmalarına göre çok küçüktür [8].

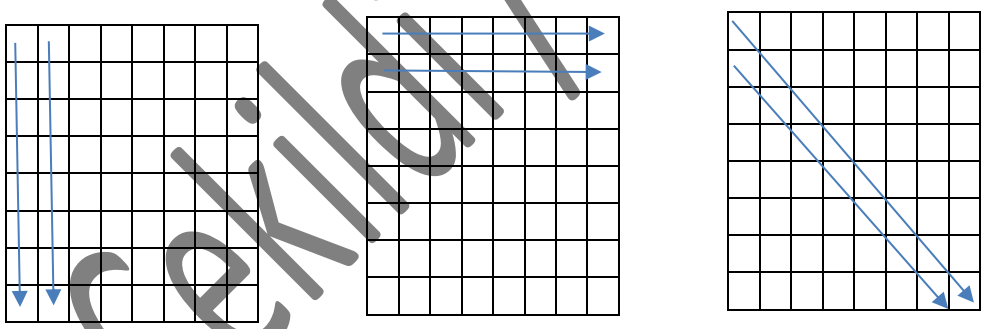
Bu çalışmada yazılan metni gizliliğini ve güvenliğini artırmak için metinde yer alan her bir karakteri Resmin 2 pikselinin RGB değerlerinde cebirsel şifreleme yapmaktadır. Bu işlem her bir karakter için uygulanmaktadır ve resmin hangi piksel değerinde kalındıysa o pikselden devam etmektedir. Verinin gizliliğini artırmak için Cebirsel LSB yönteminin geliştirilmesi ve geliştirilen Cebirsel LSB yöntem ile LSB yönteminin karşılaştırılması yapılmıştır.

1.1. Least Significant Bit (LSB)

En Önemsiz Bite ekleme yöntemi (LSB) yaygın olarak kullanılan ve uygulaması basit bir steganografi yöntemdir. Gizli mesajın bitlerinin örtü imgenin piksellerin en önemsiz bitiyle yer değiştirilmesidir. Resmin satır veya sütunlarına mesajın bitleri gizlenebilir bu durumda mesajın geri elde edilmesi daha kolay olacaktır. LSB yönteminin temelinde olan piksellere birçok teknik uygulanabilir. Bu yöntemlere örnek olarak ayrık logaritma fonksiyonu ve Laplacian kenar bulma algoritması verilebilir [9].

Sayısal değeri düşük olan bit üzerinde yapılacak değişimin, resim üzerindeki etkisi göz ile fark edilecek kadar belli olmayacaktır. LSB yöntemi ile genellikle yüksek kalitedeki görsel dosyalarda, yüksek miktarda veri gizleme işlemi yapılmaktadır. Fakat uygulamasının yaygınlığı ve iyi bilinmesinden dolayı bu yöntem saldırılara karşı dayanıksızdır [10].

Veri görüntü içerisinde satır, sütün veya köşegen sıralı olarak resmin piksellerine gizlenebilmektedir [11]. Bu yöntemler Şekil 3'te görülmektedir. Şeklin b şıkkında satıra veri gizleme işlemi ilk satırdan itibaren soldan sağa doğru ilerlemektedir. Şeklin a şıkkında sütuna veri gizleme işlemi de benzer biçimde ilk sütün' dan itibaren yukarıdan aşağıya doğru ilerlemektedir. Şeklin c şıkkında ise, köşegen uygulamasında veri gizleme işlemi görülmektedir. Projede önerilen LSB yönteminde veri gizleme işlemi satır sıralı soldan sağa doğru olacak şekilde uygulanmıştır.



(a) Sütun yöntemi (b) Satır yöntemi (c) Köşegen yöntemi

Şekil 3. LSB yönteminin resim üzerinde piksellere uygulanma yöntemleri

24 –bit renkli resimde LSB yönteminin uygulanması çok basittir. Her piksel 3 bayt ile temsil edilmektedir. Bu durum, bir pikselin rengini belirleyen 3 ana renk olan R(Kırmızı) , G(Yeşil), B(Mavi) 'den oluşmasındandır. Buna pikselin RGB değeri denmektedir. Bu durumda her baytın son bitini değiştirmek suretiyle bir pikselde 3 bitlik bilgi saklanabilir. Gizlenmek istenen mesaj, saklama işleminden önce sıkıştırılırsa, çok daha fazla sayıda bilgi resmin içine gizlenebilir. Örneğin, bir resmin orijinal halinin 3 pikseline ait RGB değerleri aşağıdaki gibi olsun.

1. piksel : 10010101 00001101 11001001 (149,13,201)
2. piksel : 10010110 00001111 11001010 (150,15,202)
3. piksel : 10011111 00010000 11001011 (159,16,234)

Yukarıdaki verilen 3 pikselin içine 'a' karakterini gizlediğimizi düşünürsek. 'a' karakterinin ASCII kodu olan 97'ye eşdeğer bit dizisi "01100001" olacaktır. Bu 8 bit toplamda 8 bayt veri üzerine gizlendiğinde oluşan yeni piksel değerleri aşağıdaki yer almaktadır. Buradaki örnekte orijinal değerlerden sadece 4 bitte değişiklik olmuştur (koyu yazılmış olanlar).

1. piksel : 1001010**0** 00001101 11001001 (149,12,201)
2. piksel : 10010110 0000111**0** 11001010 (151,14,203)

3. piksel : 10011110 00010001 11001011 (159,16,234)

Sonuç olarak elde edilen yeni renk tonları çok ufak değişimlere uğradığından, bu değişikliğin göz ile tespiti mümkün olmayacaktır. LSB yönteminin çıkış noktası, en az ağırlıklı bite uygulanmak üzere olsa da, en az ağırlıklı farklı sayıda bite uygulanacak çeşitli yöntemlerde önerilmiştir [12]. Önerilen Cebirsel Şifreleme modelinde eklenen rakam değerleri olduğundan, en fazla 9 değeri alabilmekte, bu sebeple en az ağırlıklı 4 bit üzerinde çalışmaktadır.

1.2. Least Significant Bit (LSB) Algoritmsının Geliştirilmesi

Bu çalışmada, LSB yönteminin saldırılara karşı dayanıksız olmasından dolayı, yöntemin güvenliğini artırmayı amaçlayan bir matematiksel kodlama yöntemi önerilmiştir. Önerilen yöntemde, mesajın 1 karakteri resmin 2 pikselinin RGB değerlerine gizlenmektedir. Mesaj, görüntü içerisinde satırlar bazında yazılmaktadır. Resmin toplam piksel sayısının yarısı kadar karakter şifrelenebilmektedir. Geliştirilen bu yöntem, basit LSB yöntemine göre veri gizlemede daha fazla veri saklama olanağı tanımasının yanı sıra, yöntemi bilmeyenler tarafından anlaşılabilmesi ve çözülebilmesi geleneksel LSB yöntemlerine göre oldukça zordur. Ayrıca şifrelenmiş görüntüler üzerinde uygulanan kalite metriklerinin değerlerine göre, yöntemin görsel kalitede önemsenecek bozulmalara yol açmadığını da görülmektedir.

1.3. Cebirsel Şifreleme Yöntemi

Önerilen şifreleme yöntemi, basit cebirsel işlemlerden sonra elde edilen toplam değerlerin piksellere dağıtılmasına dayanmaktadır. Hem cebirsel işlem hem de farklı piksellere dağılan rakamlardan dolayı yöntem daha güvenilirdir.

Öncelikle, mesajın her bir karakterinin ASCII kod değerinin basamak değerlerinin 3 farklı toplamı elde edilir. Bu toplamlar daha sonra sırasıyla piksellerdeki renk baytlarına dağıtılırlar. Böylece piksel bazında tahmin edilebilirlik ortadan kalktığı gibi, cebirsel yöntemin getirdiği daha fazla bir güvenlik söz konusu olmaktadır. Bu cebirsel ifadeler daha sonra kullanılarak, orijinal basamak değerlerinin kolayca tekrardan elde edilmesi mümkündür.

Teori:

3 basamaklı bir sayının (karakterin ASCII değeri) yüzler basamağını x, onlar basamağını y ve birler basamağını z ile gösterelim. Bu durumda 3 cebirsel toplam yazılarak elde edilecek değerlerden tekrar orjinal değere ulaşmak mümkündür.

xy = x+y (1. Toplam) yz = y+z (2. Toplam) xyz = x+y+z (3. Toplam)

Olmak üzere, x değeri; xyz-yz cebirsel farkından, z değeri; xyz-xy cebirsel farkından ve nihai olarak y değeri; xyz-(x+z) cebirsel farkından tekrar elde edilebilir.

Örnek:

Basit bir "ab" mesajının, çalışmada önerilen yöntemle şifreleme ve çözme algoritmalarının nasıl uygulandığı aşağıda örneklenmiştir.

(a karakteri için)

097 ➔ xy=yüzler basamak değeri + onlar basamak değeri (0 + 9) = 09

yz=onlar basamak değeri + birler basamak değeri (9 + 7) =16

xyz=yüzler basamak değeri + onlar basamak değeri + birler basamak değeri (0 + 9 + 7)=16

(b karakteri için)

098 ➔ xy=yüzler basamak değeri + onlar basamak değeri (0 + 9) = 09

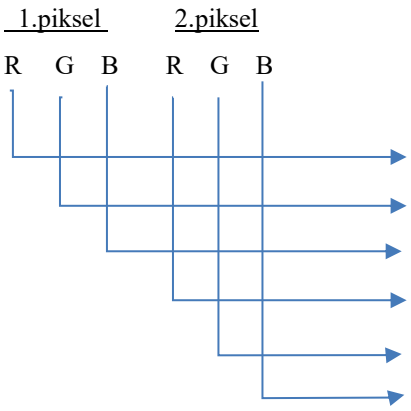
yz=onlar basamak değeri + birler basamak değeri (9 + 8) =17

xyz=yüzler basamak değeri + onlar basamak değeri + birler basamak değeri (0 + 9 + 8)=17

Elde edilen bu toplamlar, daha sonra ilgili resimde yer alan piksellerin RGB baytlarına aşağıdaki gibi kodlanır. Her renk değeri 0 ile 255 arası bir yoğunluk değeriyle belirlendiğinden, yöntemde her renk değerine mod 10 uygulanır ve sıfırlanan birler basamak değerine şifrelenecek mesaja ait toplam değerlerin rakamları (sıfır ile başlasa bile iki basamak olarak düşünülürek) sırasıyla yerleştirilir. İşlemin nasıl uygulandığı aşağıda örneklenmiştir.

Orijinal resime ait ilk satır ilk 4 piksel değerinin aşağıdaki gibi olduğunu varsayalım.

1. piksel			2. piksel			3. piksel			4. piksel			…….
R	G	B	R	G	B	R	G	B	R	G	B	…..
135	197	63	215	167	133	234	97	145	253	155	28	……



1. piksel R değeri mod 10 değeri alınır. (130)
1. piksel G değeri mod 10 değeri alınır. (190)
1. piksel B değeri mod 10 değeri alınır. (60)
2. piksel R değeri mod 10 değeri alınır. (210)
2. piksel G değeri mod 10 değeri alınır. (160)
2. piksel B değeri mod 10 değeri alınır. (130)

Daha sonra, gizlenecek mesajın 'a' karakteri cebirsel toplamlarının rakamları mod işlemine tabi tutulmuş bu sayısal değerlere eklenir.

130 + xy'nin onlar basamağı= 130 + 0 =130

190 + xy'nin birler basamağı= 190 + 9 =199

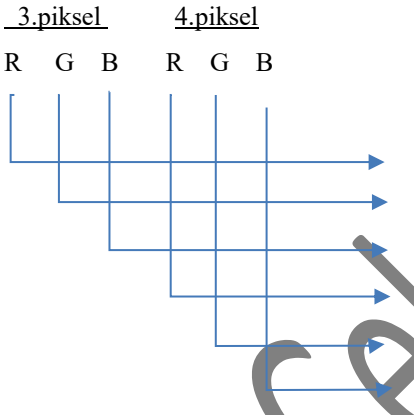
60 + yz'nin onlar basamağı= 60 + 1 =61

210 + yz'nin birler basamağı= 210 + 6 =216

160 + yz'nin onlar basamağı= 160 + 1 =161

130 + yz'nin birler basamağı= 130 + 6 =136

Benzer işlem gizlenecek mesajın 'b' karakteri için uygulanacak olursa aşağıdaki değerler elde edilecektir.



3. piksel R değeri mod 10 değeri alınır. (230)
3. piksel G değeri mod 10 değeri alınır (90)
3. piksel B değeri mod 10 değeri alınır (140)
4. piksel R değeri mod 10 değeri alınır (250)
4. piksel G değeri mod 10 değeri alınır (150)
4. piksel B değeri mod 10 değeri alınır (20)

230 + xy'nin onlar basamağı= 230 + 0 =230

90 + xy'nin birler basamağı= 90 + 9 =99

140 + yz'nin onlar basamağı= 140 + 1 =141

250 + yz'nin birler basamağı= 250 + 7 =247 (>255, onluk basamak 1 eksiltilir → 246 olur)

150 + yz'nin onlar basamağı= 150 + 1 =151

20 + yz'nin birler basamağı= 20 + 7 =27

Resim üzerinde 'ab' mesajı şifrelenmiş piksel değerleri artık aşağıdaki gibi olacaktır.

1. piksel			2. piksel			3. piksel			4. piksel			…….
R	G	B	R	G	B	R	G	B	R	G	B	…..
130	199	61	216	161	136	230	99	141	247	151	27	……

Yeni piksel değerlerinden görüleceği üzere, renk kodlarının sayısal değerlerinin değişimi sınırlı olduğundan, gözle görünür bir biçimde resim üzerinde bir fark yaratmayacaktır. Şifreleme işleminin çözülme algoritması ise aşağıdaki gibidir.

1.4. Cebirsel Şifreleme Çözme Yöntemi

Şifreleme yapılan piksellerin R G ve B değerlerinin mod 10 değeri alınır böylelikle piksele hangi sayının eklendiği bulunur. Bulunan bu sayılar ağırlıklandırılarak (1.piksel R*10) + (1.piksel G) işleminin sonucu x+y değeri bulunur. Daha sonra (1.piksel B *10) + (2.piksel R) işleminin sonucu ise y+z değeri bulunur ve en sonunda (2.piksel G *10) + (2.piksel B) işleminin sonucu ise x+y+z değeri elde edilir.

Teoride verilen 3 bilinmeyenli 3 farklı denklem kullanılarak, x, y ve z değerleri bulunur. Nihai olarak, (x*100)+(y*10)+(z) cebirsel işlemi bize mesajdaki orijinal karakterin ASCIII değerini verecektir. Bu değer ile orijinal karakter tablodan artık bulunabilir. Bu işlem mesaj uzunluğunda metin elde edilene kadar devam uygulanır. Bu algoritmayı sadece ilk mesaj karakteri 'a' için uygularsak;

130%10=0 ve 199%10=9 değerlerinin ağırlıklı toplamı (0*10+9) xy'yi verir, yani 9'dur.

61%10=1 ve 216%10=6 değerlerinin ağırlıklı toplamı (1*10+6) yz'yi verir, yani 16'dır.

161%10=1 ve 136%10=6 değerlerinin ağırlıklı toplamı (1*10+6) xyz'yi verir, yani 16'dır.

Buradan x, y ve z değişkenleri (basamak rakamları) bulunur.

x=xyz-yz cebirsel işleminden, 16-16=0 olarak bulunur.

z=xyz-xy cebirsel işleminden, 16-9=7 olarak bulunur.

y=xyz-(x+y) cebirsel işleminden, 16-(0+7)=9 olarak bulunur.

Karakterin ASCII değeri ise, ağırlıklar kullanılarak (x*100)+(y*10)+(z) cebirsel işleminden 97 olarak bulunur. ASCII tablosunda 97 değeri 'a' karakterine karşılık gelmektedir.

2. Görüntü Kalite Tespiti

LSB ve önerilen cebirsel şifreleme modeli tarafından şifrelenmiş resimler, orijinal resimler ile karşılaştırılmıştır. Görüntü kalitesi metrikleri olarak PSNR ve MSE kullanılmıştır. Bu yöntemler için Matlab fonksiyonları uygulanmıştır.

2.1. Ortalama Karesel Hata (Mean-Squared Error-MSE)

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 [13]. Bu metriğin hesaplanması basittir ancak insanın kalite algısına uygun değildir. Ortalama karesel hata ne kadar küçükse, aslına o kadar yakındır. Matlab uygulamasında "immse" komutu ile hesaplanır. MSE performans değerini ölçer, her zaman pozitif değerlidir ve MSE değeri sıfıra yakın olan tahminleyicilerin daha iyi bir performans gösterdiğini söylenmektedir.

$$\text{MSE} = \frac{1}{n}\sum_{i=1}^{n}(y_i - \tilde{y}_i)^2 \tag{2.1}$$

2.2. Tepe Sinyali Gürültü Oranı (Peak Signal to Noise Ratio -pSNR)

Dijital görüntülerde görüntüler arasındaki benzerliği ortaya çıkarabilmek için PSNR kullanılmaktadır. Metin resme şifrelendikten sonra görüntü üzerindeki bozulmalar PSNR değeri ile anlaşılır. PSNR değerinin yüksek olması resmin kalitesini ve görüntü üzerindeki bozulmaların daha az olduğunu göstermektedir [14]. Metnin içindeki gizlenmiş görüntünün bozulmalarını hesaplayan PSNR değeri 2.2'deki formül ile bulunmaktadır. PSNR değerini dB cinsinden hesaplamaktadır. PSNR değeri Matlab uygulamasında "psnr" komutu ile hesaplanır.

$$\text{PSNR} = 10*\log_{10}\left(\frac{MAX_I^2}{MSE}\right) \text{ (dB)} \tag{2.2}$$

3. Araştırma Sonuçları ve Tartışma

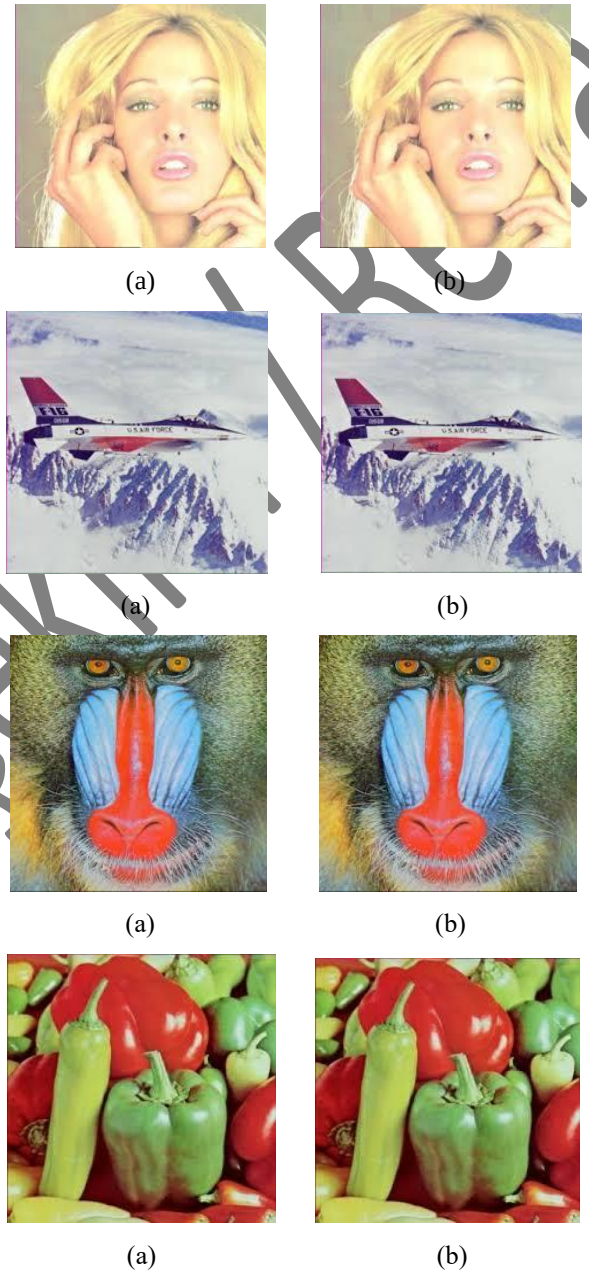
Steganografi' de verinin gizliği önemlidir. LSB algoritmasında mesajın 1 karakteri resmin 8 baytına kopyalanmaktadır. Önerilen cebirsel şifreleme yaklaşımında ise 1 karakter resmin 2 pikseline (yani toplam 6 bayta) eklenmektedir. Böylelikle veri güvenliğinin artırılmasının yanı sıra, yaklaşık %33 oranında (8 / 6 ≅ %33) veri sıkıştırma da sağlanmaktadır.

Veri gizleme işlemi resmin piksellerine satır öncelikli uygulanmıştır. Piksellerin renk değerlerine, cebirsel işlem sonucunun rakamları en ağırlıklıdan başlayarak sırasıyla yerleştirilir. Örneğin cebirsel toplam 18 ise, ilk piksele 1 sonraki piksele 8 eklenir. Doğal

olarak en büyük rakam 9 olabileceğinden dolayı her renk baytının en az ağırlıklı son 4 biti değiştirilebilir. Fakat öncesinde renk değerinin son rakamı mod işlemi ile atıldığından, sonuç olarak normal şartlarda değişim olmamaktadır. Sadece eğer renk değeri >250 ise bu durumda eklenecek yeni rakam değeri ASCII kod sınırını aşmasına neden olmaktadır ki, bu durum renk değerinin onlar basamağının bir eksiltilmesi şeklinde uygulanmıştır. Renk değerinin son rakamı çıkartılarak, yerine cebirsel ifadenin yeni rakamı eklendiğinden MSE hatalarının çok olmaması beklenmektedir. Fakat bahsedildiği üzere renk değeri çok canlı olan resimlerde, modelde hata oranı büyüme eğilimindedir. Yapılan denemelerde benzer sonuçlar elde edilmiştir. Veri güvenliği ve sıkıştırmadan kaynaklı MSE hata oranının artması kabul edilebilir düzeydedir. Elde edilen şifrelenmiş resimler orijinallerinden çıplak gözle fark edilebilir değillerdir.

Genel olarak sınamalarda kullanılan 24 bitlik Tiffany, Peppers, Airplane, Baboon resimlerine 25, 251 ve 2070 karakter uzunluğunda hem LSB, hem de cebirsel LSB yöntemi uygulanarak veri gizleme işlemi yapılmıştır. Orijinal resimler ve cebirsel şifrelenmiş resimler Şekil 4' de görünmektedir. Her iki yöntemle şifrelenen resimlerin kalite karşılaştırılması, MSE ve PSNR metrik değerleri, Tablo 1 ve Tablo 2 'de verilmiştir.

25 karakter şifrelenmiş olan resimlerde LSB yönteminin MSE metrik değeri, Cebirsel LSB yöntemi ile şifrelenmiş olanlarla hemen hemen aynı bulunmuştur. Bununla birlikte, beklendiği üzere, karakter sayısı artıkça cebirsel yöntemin MSE değeri artmaktadır. Yapılan sınamalarda elde edilen değerlerin ortalamasına göre MSE hata oranı %29 artmış ve PSNR %2.5 azalmıştır. Her ne kadar metrik değerleri cebirsel MSB için negatif gözükse de, orijinal resimdeki bu değişimler çok ufak ve gözle algılanabilir olmaktan uzaktır.



Şekil 4. Çalışmada kullanılan görüntüler (a) Orijinal Resim (b) Stego Resim

Tablo 1. LSB yönteminin uygulanmasının görüntü kalite değerlikleri

Resim Adı	Karakter Uzunluk	MSE	PSNR(db)
Airplane	25	2,13	44,88
Baboon	25	2,36	44,43
Tiffany	25	0,98	48,26
Peppers	25	1,41	46,66
Airplane	251	2,13	44,88
Baboon	251	2,36	44,43
Tiffany	251	0,98	48,24
Peppers	251	1,40	46,71
Airplane	2070	2,13	44,87
Baboon	2070	2,35	44,45
Tiffany	2070	0,98	48,26
Peppers	2070	1,41	46,67

Tablo 2. Cebirsel Şifrelenmiş LSB yönteminin uygulanmasının görüntü kalite değerlikleri

Resim Adı	Karakter Uzunluk	MSE	PSNR(db)
Airplane	25	2,14	44,85
Baboon	25	2,36	44,43
Tiffany	25	0,99	48,22
Peppers	25	1,43	46,62
Airplane	251	2,26	44,61
Baboon	251	2,47	44,24
Tiffany	251	1,66	45,95
Peppers	251	2,07	45,01
Airplane	2070	3,17	43,15
Baboon	2070	3,65	42,53
Tiffany	2070	1,95	45,25
Peppers	2070	2,44	44,29

4. Sonuç

Çalışmada C# programlama dili kullanılmıştır. Resmin piksellerine veri gizleme işlemleri yapıldıktan sonra, MSE ve PSNR metrik değerlerinin hesaplanması için Matlab programı kullanılmıştır.

25, 251 ve 2070 karakterlik veriler kullanılarak LSB ve Cebirsel LSB yöntemleri ile şifrelenen veriler görüntülerin içerisine satır olarak gizlenmiştir. Karakter sayısı arttıkça cebirsel LSB yöntemi ile şifrelenmiş resimlerdeki MSE metrik değeri arttığı görülmüştür. Metrik değerleri cebirsel LSB yöntemi için olumsuz görünsede orijinal resimlerdeki bu değişimler çok ufak ve gözle algılanamamaktadır. Kazanılan sıkıştırma oranı ve ayrıca verinin gizlenme güvenliği göz önünde bulundurulduğunda, bu yöntemin güvenliğin önemli olduğu uygulamalara hitap ettiği düşünülmelidir.

Kaynakça

[1] F. Özbilgin, F. Durmuş, S. Karagöl, Yazılı metni şifreleyip LSB yöntemi ile gizleme, Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 2018

[2] H. K. Sevindir, N. Sayın, Dalgacık Dönüşümü Tabanlı Görsel Kriptoloji, Afyon Kocatepe Üniversitesi Fen ve Mühendislik Bilimleri Dergisi, 2018

[3] A. Şahin, E. Buluş, M. T. Sakallı, 24-bit renkli resimler üzerinde en önemsiz bite ekleme yöntemini kullanarak bilgi gizleme, Trakya Üniversitesi, 2005

[4] M. Aydoğan, Adli bilişimde görüntü üzerine kriptografi uygulamaları, Fırat Üniversitesi Yüksek Lisans Tezi, 2014

[5] Ö. Kurtuldu, İmge kareleri kullanan yeni bir steganografi yöntemi, Journal of Naval Science and Engineering, 2009

[6] M. Bilgin, Steganografi, Akademik Bilişim 2013 – XV. Akademik Bilişim Konferansı Bildirileri, 2013

[7] C. Koçak, Kriptografi ve stenografi yöntemlerini birlikte kullanarak yüksek güvenlikli veri gizleme, Erciyes Üniversitesi Fen bilimleri Enstitüsü dergisi, 2015

[8] Y. Yıldız, A. T. Özcerit, 24 bit renkli hareketli resimler (video) üzerinde geliştirilen sır örtme yöntemi, Sakarya Üniversitesi Fen Bilimleri dergisi, 2015

[9] C. Olcay, N. Saran, İmge içine Bilgi gizlemede kullanılan LSB Yöntemlerinin karşılaştırılması, Çankaya University Journal of Science and Engineering, 2013

[10] T. Tuncer, E. Avcı, Yerel ikili örüntü tabanlı veri gizleme algoritması: LBP-LSB, Türkiye Bilişim vakfı bilgisayar bilimleri ve mühendislik dergisi, 2017

[11] E. Güvenoğlu, Resim şifreleme amacıyla dinamik S kutusu tasarımı için bir yöntem, El-Cezeri Fen ve Mühendislik dergisi, 2016

[12] F. Doğan, R. Daş, İ. Türkoğlu, İmgeler için farklı bir veri gizleme yaklaşımı, Dicle Üniversitesi Mühendislik Dergisi, 2016

[13] T. Tuncer, E. Avcı, Göktürk alfabesi tabanlı görsel sır paylaşımı metodu ile veri gizleme uygulaması, Gazi Üniversitesi Mühendislik ve Mimarlık Dergisi, 2016

[14] Ü. Kaş, E. Tanyıldızı, Euler Renk ve hareket büyütme yöntemlerinin performans analizi, Afyon Kocatepe Üniversitesi Fen ve Mühendislik Bilimleri dergisi, 2017.