Koçak, Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 31(2):115-123

Erciyes University Journal of the Institute of Science and Technology
Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi
ISSN 1012-2354
Cilt (Volume): 31 , Sayı (Issue): 2, Mayıs/May -2015
http://fbe.erciyes.edu.tr/

Kriptografi ve stenografi yöntemlerini birlikte kullanarak yüksek güvenlikli veri gizleme

Cemal KOÇAK
Gazi Üniversitesi Teknoloji Fakültesi Bilgisayar Mühendisliği

Anahtar Kelimeler: Yüksek kapasiteli veri gizleme, Kriptografi, Steganografi, PSNR, SSIM

ÖZET

İletişimin gizliliğinde ve güvenli mesaj iletiminde kullanılan iki önemli teknik Kriptografi ve Steganografidir. Bu iki yöntemin birlikte kullanılması veri güvenliğini artırmaktadır. Kriptografide gizli bir mesaj şifrelenir, Steganografide ise mesaj, görüntü veya ses dosyaları içine yerleştirilir. Bu çalışmada Kriptografi ve Stenografi birleştirilerek hibrit bir model sunulmakta ve bu model için ise bir ara yüz tasarımı gerçekleştirilmektedir. Kriptografide, kullanıcının belirleyeceği anahtar kelime ile şifrelenecek metin bir matris oluşturularak şifrelenmiştir. Şifreli metnin resim içine gizlenmesi aşamasında güvenlik katmanı olarak ikinci şifre girilmesi sağlanmıştır. Şifrelenecek metin gerçek renkli RGB görüntü içine sadece "Kırmızı" ve "Yeşil" kanallarının en az değerlikli 2 biti değiştirilerek gizlenmiştir. Toplamda 4 bit değiştirilerek resme saklanabilecek şifreli metin boyutunda artış sağlanmıştır. Çalışmada kullanılan taşıyıcı resimler 24 bit/pixsel renk seviyeli olarak belirlenmiştir. Bu çalışmada stego görüntülerin kaliteleri Tepe Sinyal-Gürültü Oranı (Peak Signal-to-Noise Ratio-PSNR) ve Yapısal Benzerlik Endeksi (SSIM) ölçüm kriterlerine göre değerlendirilmiştir.

High-capacity data hiding scheme together using cryptography and steganography

Key Words: High-Capacity Data Hiding Scheme, Cryptography, Steganography, PSNR, SSIM..

ABSTRACT

Cryptography and steganography are the two significant techniques used in security of communication and in safe message transfer. These two methods are applied together to improve data reliability. In cryptography, a secret message is encrypted, and in Steganography the message is placed into image, or voice files. In this study, a hybrid model is proposed by combining, cryptography and steganography and an interface is designed for proposed model. In cryptography, the text to be encrypted with a keyword determined by user is encoded by creating a matrix. While hiding an encrypted text into the picture, a second password is required to increase security. The text to be encrypted in true color RGB image are hidden by changing the least significant 2 bits of "red" and "green" channels. Size of the encrypted secret message has been increased by changing 4 bits in totally. The carrier pictures utilized in this study have been determined as 24 bit/pixel color scale. In this study, quality of the stego images has been evaluated according to the quality measurement criteria of Peak Signal-to-Noise Ratio (PSNR-dB) and Structural Similarity Index (SSIM)

*Sorumlu Yazar (Corresponding author) e-posta: ccckocak@gazi.edu.tr

1. Giriş

Kriptografi, kimlik doğrulama, veri kaynağı doğrulama, veri bütünlüğü, gizlilik konuları gibi bilgi güvenliği ile ilgili matematiksel teknik çalışmaların bütünüdür. Kriptografi Yunancada gizli anlamına gelen kryptos ve yazı anlamına gelen graphein'den türetilmiştir. Kriptoloji ise şifre bilimidir ve bilgi güvenliğini sağlar. Burada şifrelenecek mesaja düz metin, dönüşüm sonrasında elde edilen mesaja şifreli metin, dönüştürme sürecinde kodlama işlemine şifreleme, tersi işleme de şifre çözme denir. Şifreleme ve şifre çözme için aynı gizli anahtar kullanılmalıdır [1 - 3]. Kriptografi yönteminde Advanced Encryption Standard (AES) metodu en çok kullanılan yöntemdir. AES; standart Rijndael algoritması olarak bilinen, güvenlik ve hız açısından yüksek verimliliğe sahip simetrik anahtar blok şifrelemedir [1, 4 - 10]

Mesajın içeriğini saklamak olan kriptolojinin bir parçası olarak Stenografi, bir nesnenin içine bir verinin gizlenmesi olarak tanımlanabilir. Stenografi kelimesi Yunanca steganos ve grafi kelimelerinden türetilmiş Türkçe karşılığı olarak gizlenmiş yazı, kaplanmış yazı anlamına gelmektedir. İçerisinde gizli veri bulunduran taşıyıcıya stego adı verilir. Stenografi de amaç, bir mesajın varlığını saklamak ve bir örtülü kanal (covert channel) oluşturmaktır [1, 2, 11].

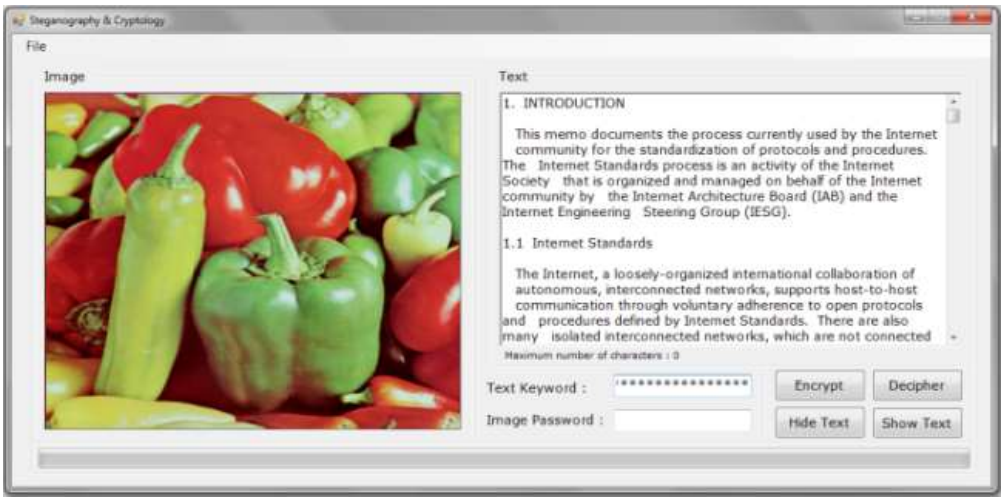
Daha önceki çalışmalarda stenografik metotlardan pratik ve yaygın olanı En Az Değerlikli Bit'lerde (Least Significant Bit - LSB) mesajın gizlenmesidir ve LSB ekleme yöntemi olarak bilinir. Bu metotta her piksele gizli bir mesaj yerleştirmek için sabit K-LSB kullanılır. Bu yöntemde, resmi oluşturan her pikselin her byte'ın en önemsiz biti olan son biti değiştirilerek o bitin yerine gizlenmesini istediğimiz verinin bitleri sırasıyla verinin başlangıcından itibaren birer birer yerleştirilmektedir. Bu şekilde büyük boyutlu verilerin sınırlı boyutta resim üzerine gizlenmesi mümkün hale gelir. Son zamanlarda, gizli veriyi gömmek için iki veya daha fazla LSB kullanımını öneren birçok LSB yöntemleri önerilmiştir [4 - 9].

Kriptografi ile Stenografinin birlikte kullanıldığı çalışmada [1] şifreleme için DES algoritması, stenografi için 3 bit LSB yöntemi, bir başka çalışmada gelişmiş şifreleme standardı (Advanced Encryption Standard-AES) algoritması, mesajı resim içine gizlemek için piksel değeri farklılıkları (Pixel Value Differencing - PVD) ile K-LSB yöntemleri kullanılmıştır [12]. Yapılan [1] çalışmada resim kalitesini belirleyecek herhangi bir karşılaştırma yapılmamıştır. AES algoritması kullanılarak 128-bit şifreleme kullanılan çalışmada [12] Kırmızı, Yeşil, Mavi (Red Green Blue - RGB) kanallarına farklı değerlerde daha az veri gizlenerek 38,25 dB - 43,96 dB Sinyal Gürültü Oranı (Peak Signal-to-Noise Ratio - PSNR) elde edilmiştir. Bir dizi içine, sıkıştırılmış ya da sıkıştırılmamış ses, resim, video veya metin gömmek için insan görme sistemi karakteristiklerinden parlaklık ve karşıtlık (kontrast) özelliklerine bağlı olarak LSB'lerin sayısını belirlemeye yönelik çalışmada [6] farklı gri seviyelerin piksel değerlerine uyabilen LSB'lerin sayısı hesaplanmıştır. Gizli veri olarak resim kullanılan bu çalışmada ise 33 dB – 43 dB PSNR değerleri elde edilmiştir. Rastgele üretilen 16 karakterli şifreleme algoritması kullanılan çalışmada [13], gizlenen resim boyutları verilmiş fakat performans değerlendirilmesi yapılmamıştır. Ortalama 775.220-bit veri gizlenen bir başka çalışmada ise 39,12 dB PSNR sonucu elde edilmiştir [14]

Bu çalışmada Kriptografi ve stenografi birlikte kullanılarak, gizli veriler için yüksek güvenlikli uygulama gerçekleştirilmiştir. Kriptografi için Advanced Encryption Standard (AES), Stenografi için K-bit en az-değerli 2 bit (LSB) değiştirme metodu kullanılmıştır. 2 bit LSB algoritması için RGB kanallarından R ve G kanalları kullanılmıştır. 2-bit LSB yöntemi ile toplamda 4-bit değiştirilerek gizli veri kapasitesi arttırılmış böylece daha fazla veri gizlenmesi ve daha az bozulmalar sağlanmıştır. Çalışmanın sonraki bölümlerinde sırasıyla şu konular ele alınmaktadır: Bölüm 2'de sırasıyla önerilen yöntem ve tasarlanan arayüz tanıtımı hakkında bilgiler verilmektedir. Bölüm 3'te sonuçların karşılaştırmalı analizi, son olarak çalışmadan elde edilen sonuçların değerlendirilmesi yer almaktadır.

2. Önerilen Yöntem

Kriptografi ve Stenografi yöntemlerini birleştirerek veri güvenliğini ve gizliliği arttıran hibrit modelin ara yüz tasarımı şekil 1'de gösterilmektedir. Bu çalışma Visual Studio.Net platformu kullanılarak gerçekleştirilmiştir.



Şekil 1. Şifrelenecek metin ve stego resim

Bu çalışmada mesaj, "Simetrik Anahtar Şifreleme" metodu kullanılarak şifrelenmiştir. Simetrik anahtarlamada metni şifrelemek için bir anahtara ihtiyaç vardır ve aynı anahtar kullanılarak şifreli metnin şifresi çözülmektedir. Çalışmada kullanılan anahtar, kullanıcının belirleyeceği herhangi bir sayı, alfabede yer alan harfler ya da özel karakterler olabilir. Kullanıcının belirlediği 16 karakterli anahtara bağlı olarak şifrelenecek metnin her bir karakteri başka bir karaktere dönüştürülür. Bu dönüşüm işlemi, karakterlerin sayı değerleri (ASCII) üzerinde yapılan işlemler vasıtasıyla olur. Metnin her karakterinin kodu (ASCII) ile anahtar kelimenin sıradaki karakter kodu (ASCII) XOR işlemine tabi tutularak şifrelenmiş metin oluşturulur. Bu sistem aşağıdaki gibi kısaca ifade edilebilir:

$$c_i=p_i \oplus k_i \quad (1)$$

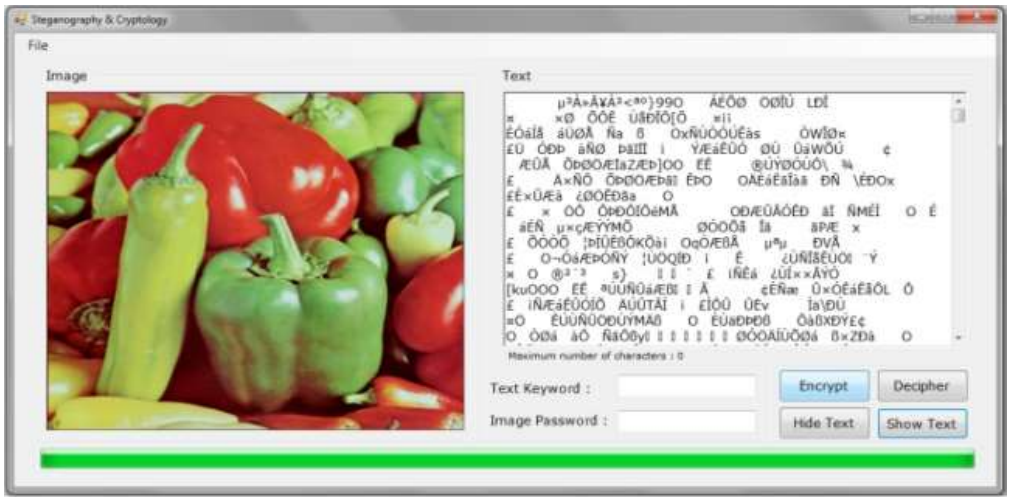
pi = i. düz metnin binary (ikili) karşılığı
ki = i. anahtar kelimenin binary (ikili) karşılığı
ci = i. şifreli metnin binary (ikili) karşılığı
⊕= exclusive-or (XOR) işlemi.

Şifrelenecek metinin her bir karakterinin ASCII binary karşılığı elde edilir. Aynı şekilde anahtar kelimenin de her bir karakterinin ASCII binary karşılığı çıkarılır. Formul 1'deki ifadeye göre sıra ile karakterlerin binary değerleri XOR işlemine tabi tutulur. Elde edilen değer, şifrelenmiş karakterin (ci) binary karşılığıdır. ASCII kod tablosunda elde edilen bu değer şifrelenmiş metnin bir karakterini oluşturmaktadır. Şifreleme işlemi bu şekilde sıra ile devam etmektedir. Şifre çözme işlemi, aynı anahtar kullanılarak formül 2'de gösterilen eşitliğe göre XOR işlemi gerçekleştirilir.

$$p_i=ci \oplus k_i \quad (2)$$

Bütün bu işlemleri basit bir örnek ile açıklamak gerekirse;
p= "a" , k="z" olsun;
"a" ASCII değeri 97=(1100001)2
"z" ASCII değeri 122=(1111010)2
c = (p XOR k) = (0011011)2 = decimal 27 karakter 'ESC'
Şifreli "a" karakterini elde etmek için;
c = (0011011)2
k = (1111010)2
p= (c XOR k) = (1100001)2 = decimal 97 ASCII karşılığı "a" karakteri elde edilir.

Karakterleri şifrelerken XOR işleminin seçilmesinin birkaç nedeni vardır. Şifrelenmiş karakter tekrar XOR işlemi kullanılarak orjinal karakterin elde edilebilmesi nedenlerden biridir. Diğer bir neden ise şifrelerken taşma olmamasıdır. Yani bir karakterin ASCII değeri ile başka bir karakterin ASCII değeri XOR işlemi sonucunda yine 0-255 arası bir sayı, yani başka bir karakterin ASCII değeri elde edilir. Şekil 2'de maksimum 128 bitlik bir anahtar kelime kullanılarak şifrelenmiş metin görülmektedir.



Şekil 2. Şifrelenmiş metin

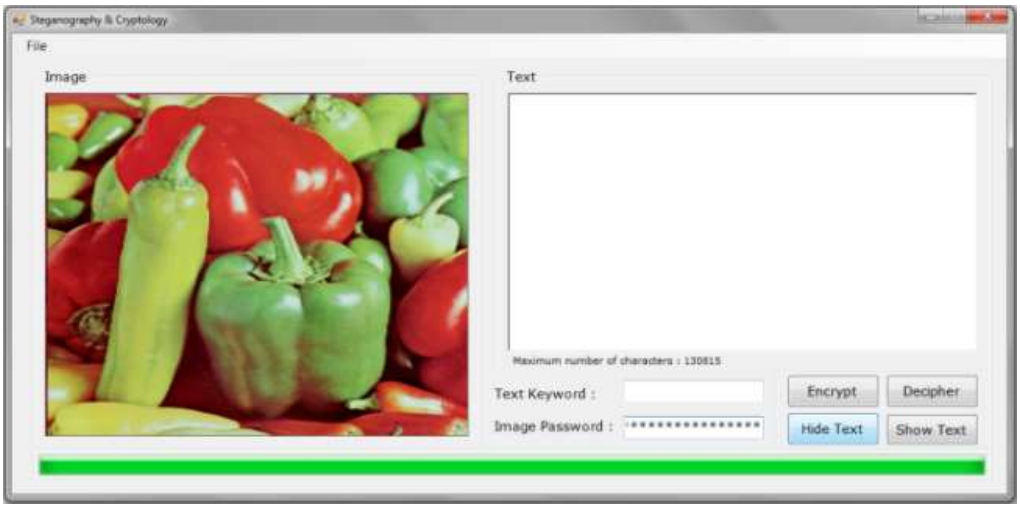
Stenografide en fazla kullanılan tekniklerden biri K-bit LSB değiştirme yöntemidir. Bu teknik kullanılarak her baytın sadece son 2 veya daha fazla bit değerinde değiştirme yapılabilmektedir. Bu çalışmada RGB kanallarından sadece R ve G kanalının en az değerlikli 2 biti kullanılarak değiştirme işlemi yapılmıştır. Kullanılan bu yöntemde; resmi oluşturan Kırmızı ve Yeşil renklere ait her pikselin her byte'nın en önemsiz son 2-biti değiştirilerek o bitin yerine gizlenmesini istediğimiz şifrelenmiş verinin bitleri verinin başlangıcından itibaren sıra ile birer birer yerleştirilmektedir. Daha sonra kullanıcının belirleyeceği maksimum 16 karakterli (128-bit) bir şifre ile örtü resim içine şifrelenmiş verinin gizlenmesi işlemi sonlandırılmaktadır. Böylece anahtar kelime ile şifrelenmiş metin, güvenliği arttırmak amacıyla başka bir şifre kullanılarak resim içine gizlenmiştir.

Çalışmada 24-bitlik renkli resimler kullanılmıştır. 24-bitlik bir görüntü dosyasının her bir pikseline 16 milyon (24 bit = 16.777.215 renk) renk tanımlaması yapılabilir. Bu nedenle R ve G kanalının en az değerlikli 2-bit üzerinde yapılan değişiklikler, gözümüz tarafından algılanamayacak kadar önemsizdir.

Resimler farklı formatlarda olabileceğinden gizleme kapasiteleri de değişmektedir. Toplamda 4-bit değişim ile gizlenebilecek maksimum veri boyutunu formül 3'ü kullanarak bulabiliriz.

MaxBytes=[{image (height(…)*width(…)*2*2}/8] (3)

24 bit 512*512 pixel boyutunda bir resim içine LSB (3bit) kullanılarak en fazla **786432** bit bilgi yerleştirilebilir. Önerilen ve kullanılan LSB (RG-4bit) yöntemi ile aynı resim içine 1048576 bit yerleştirilebilmektedir. Aradaki fark **262144 bit** (32768 bayt) olmaktadır. Şekil 3'de maksimum 128 bitlik şifre kullanılarak şifrelenmiş metinin örtü resim içine gizlenmesi gösterilmiştir.



Şekil 3. Şifreli metnin resme gömülmesi

3. Sonuçların Karşılaştırmalı Analizi

Microsoft bitmap formatında boyutu 512x512 piksel, 768 kb, 24 bit/piksel renkli resimler, deneysel çalışmalarda kullanılmıştır ve bunlardan iki tanesi Şekil 4'de gösterilmiştir.

(a) (b)

Şekil 4. Örtü resimler (a) Lena.(b) Peppers

Çalışmanın sonuçlarının karşılaştırılmasında öncelikle görüntü işleme araştırmalarında yaygın olarak kullanılan Tepe Sinyal-Gürültü Oranı (Peak Signal-to-Noise Ratio - PSNR) adı verilen bir ölçme kullanılarak test edilmiştir. PSNR ölçü birimi desibel (dB)'dir.

Büyük PSNR değerleri daha iyi sinyal yenileme anlamına gelir. Görüntü kalitesini anlamak için kullanılan diğer bir ölçü Yapısal benzerlik endeksi (Structural Similarity Index-SSIM) dir.

SSIM, bir görüntünün algılanan görsel kalitesine ne kadar yaklaştığını gösterir. SSIM indeksi [0,1] değerleri alır ve kalite arttıkça artar [15, 16]. Çalışmada kullanılan şifrelenmiş veri içeren iki resim Şekil 5'te gösterilmiştir.

Resimlerde şifreli veri değerleri ve elde edilen ortalama PSNR sonuçları da belirtilmiştir.

(a) (b)

Şekil 5. (a) Lena (1046519 bit, PSNR 29,885 dB), (b) Peppers (1046275 bit, PSNR 27,963 dB)

Tablo 1'de, kullanılan test resimleri ve en fazla gizlenebilecek şifreli veri boyutlarına karşılık R ve G kanalı için elde edilen PSNR ve SSIM değerleri verilmiştir.

Tablo 2'de örtü resmi Lena için 50.000 – 500.000 bit değerleri arasında gizlenen şifreli veri değerlerine karşılık "R" ve "G" kanallarından elde edilen PSNR (dB) ve SSIM sonuçları verilmiştir.

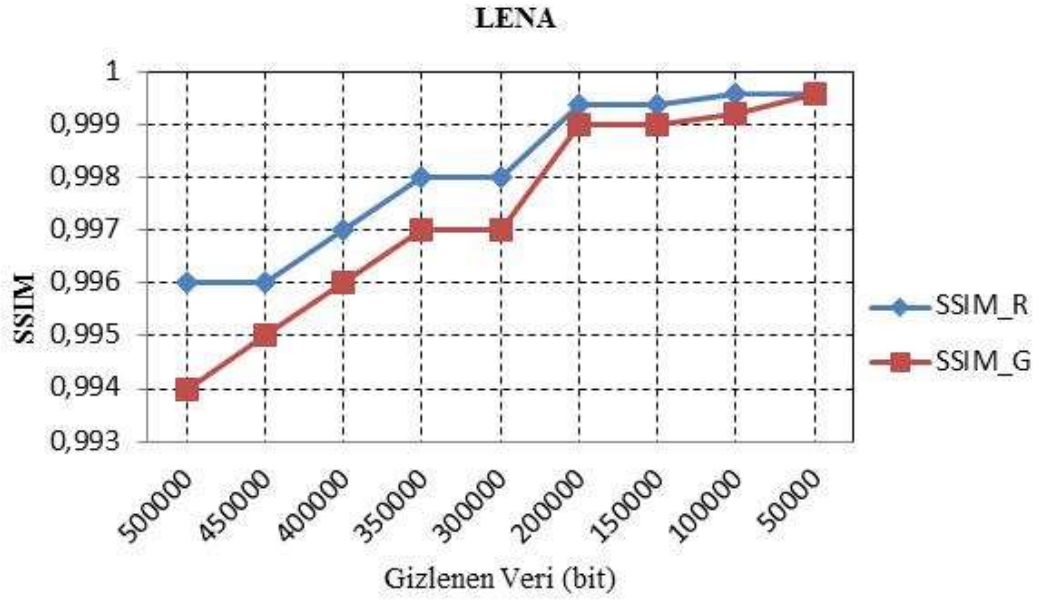
Tablo 1. Test resimleri için PSNR (dB), SSIM değerleri

Test resmi	Gizli veri (bit)	PSNR (dB)		SSIM	
		R	G	R	G
Lena	1.046.519	31,099	28,670	0,989	0,984
Tiffany	1.046.520	31,498	26,751	0,976	0,942
Peppers	1.046.519	28,762	27,163	0,979	0,988
Baboon	1.046.275	24,377	23,281	0,961	0,933
Airplane	1.046.517	30,534	26,376	0,985	0,972
House	1.046.520	27,664	26,165	0,978	0,967

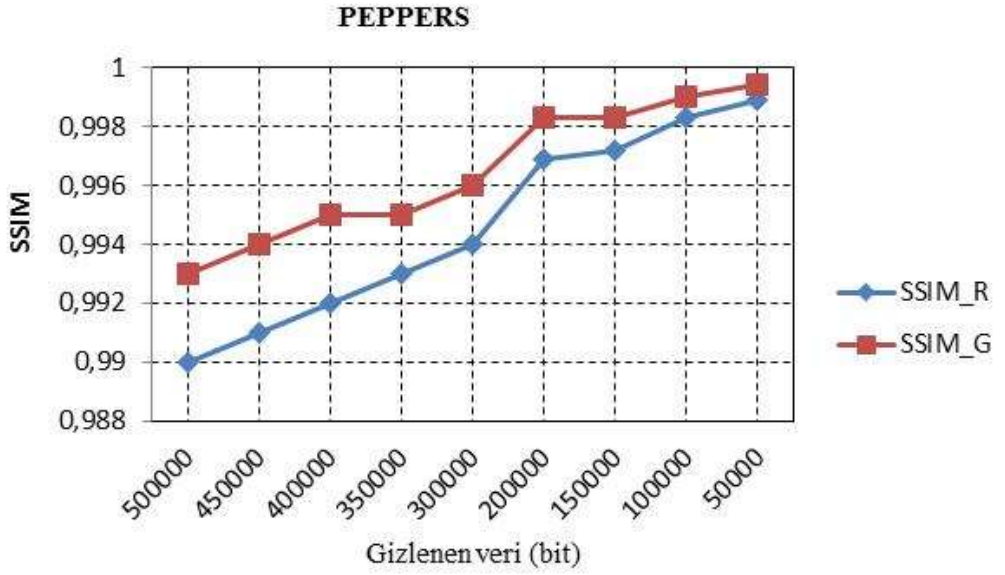
Tablo 2. Lena PSNR (dB), SSIM değerleri

LENA				
Gizlenen veri (bit)	**PSNR_R (dB)**	**PSNR_G (dB)**	**SSIM_R**	**SSIM_G**
50.000	50,5	47,99	0,9996	0,9996
100.000	47,46	44,75	0,9996	0,9992
150.000	44,89	42,17	0,9994	0,999
200.000	44,9	42.15	0,9994	0,999
300.000	39,89	37,2	0,998	0,997
350.000	39,05	36,1	0,998	0,997
400.000	37,91	34,91	0,997	0,996
450.000	36,97	34,02	0,996	0,995
500.000	36,19	33,36	0,996	0,994

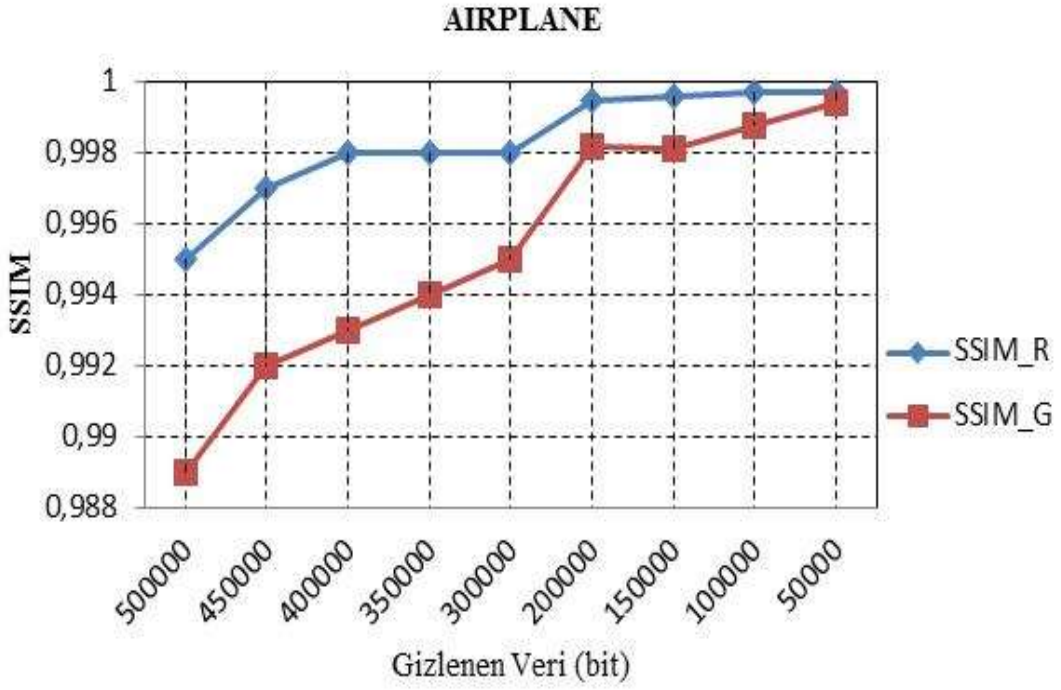
Şekil 6, 7 ve 8'de sırasıyla Lena, Peppers ve Airplane örtü resimlerine 50.000-500.000 bit veri miktarlarında gömülen şifreli metinlere karşılık R ve G değerlerinin SSIM ölçümleri grafik olarak gösterilmiştir. Grafiklerden SSIM değerlerinin çok iyi sonuçlar verdiği anlaşılmaktadır. Gizlenen veri miktarının 500.000 bit olmasına rağmen benzerlik değerlerinin 0,99 olması (1'e yakın) orijinal resmin fazla bozulmadığını göstermektedir.



Şekil 6. Lena SSIM değerleri



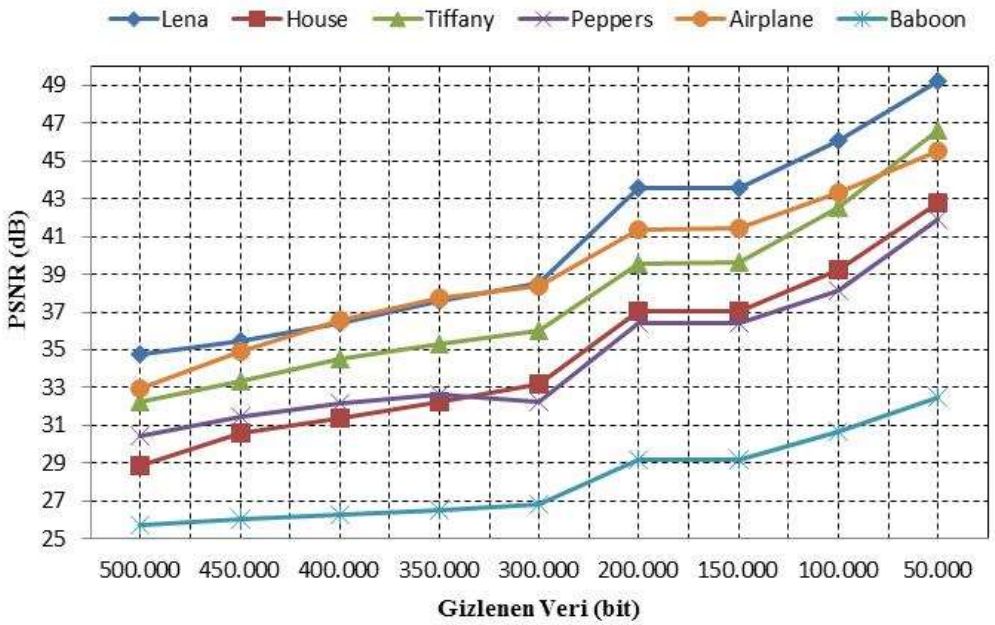
Şekil 7. Peppers SSIM değerleri



Şekil 8. Airplane SSIM değerleri

Şekil 9'da ise aynı veri miktarlarında gömülen şifreli metinlere karşılık elde edilen R ve G kanallarının ortalama PSNR (dB) değerleri karşılaştırılmıştır. Bu sonuçlardan da görüleceği gibi gizlenen veri değerlerindeki azalmaya bağlı olarak PSNR değerleri de artmakta ve resimdeki bozulmalar azalmaktadır. Ortalama 277778 bit şifreli veri gizlenen stego resimlerin ortalama PSNR (dB) değeri 35,82 dB'dir.

Stenografide ana hedeflerden biri görüntü resme gizlenecek verinin kapasitesini arttırmak ve PSNR değerini yükseltmektir. Bununla birlikte "yüksek kapasite" ve "yüksek PSNR" arasında bir denge sağlamak gerekir. Bu kriterlere göre daha önce yapılan çalışmalardan elde edilen karşılaştırmalı sonuçlar Tablo 3'de gösterilmiştir.



Şekil 9.Stego resimlerin PSNR (dB) değerleri

Tablo 3'de gösterildiği gibi örneğin, satır 1 [17] için, maksimum kapasite 145.787 bit değerinde PSNR 42.26 dB iken yapılan çalışmada 43,624 dB elde edilmiştir. Aynı şekilde, yapılan diğer çalışmalara [18-19] göre de daha iyi PSNR değerleri ve daha iyi benzerlik performansı elde edilmiştir. Son yapılan çalışmaya [20] göre karşılaştırma yapıldığında, elde edilen PSNR 33,136 dB ve SSIM 0,9935 değerleri çalışmada kullanılan yöntemin daha iyi sonuç verdiğini göstermektedir.

Maksimum 1046519 bit şifreli verinin gizlenmesinden elde edilen PSNR değeri 29,885 dB ve SSIM değeri 0.986 göz önüne alındığında, yapılan çalışmanın görüntü kalitesinde fazla bozulma yapmadığı anlaşılmaktadır. Bu durumda, PSNR değeri satır 4'de [20] yapılan çalışmaya göre biraz düşük olmasına rağmen kapasite açısından %58 daha fazla veri gizlenmiş ve iyi bir SSIM elde edilmiştir. Karşılaştırmalar, çalışmada kullanılan yöntemin daha iyi sonuç verdiğini göstermektedir. Aynı zamanda çok fazla bozulma olmadan şifreli veri kapasitesinde artış sağlanmıştır.

Tablo 3. Diğer çalışmalar ile karşılaştırma.

Stenografi Çalışmalar	Test Resmi	Gizlenen Veri (bit)	PSNR (dB)	Yapılan çalışmada	
				PSNR (dB)	SSIM
1. Mandal ve Das [17]	Lena	145787	42,26	43,624	0,9997
2. Lin ve diğerleri [18]	Barbara	53248	27,03	31,982	0,9933
3. Swain ve Lenka [19]	Lena	20032	53,78	54,676	0,9996
4. Wafaa ve diğerleri [20]	Lena	609129	32,87	33,136	0,9935
Yapılan çalışmada	Lena	1046519	29,885	29,885	0,986

4. Sonuçlar

Önerilen hibrit model sayesinde kullanıcının belirleyeceği 128 bitlik (16 karakterli) bir şifre kullanılarak veri şifreleme daha sonra örtü resim içine yine kullanıcının belirleyeceği 128 bitlik (16 karakterli) başka bir şifre kullanılarak veri gizlenmiştir. Bu sayede gerçekleştirilen model ile verilere yüksek güvenlik özelliği sağlanmıştır.

Elde edilen sonuçların performansı PSNR (dB) ve SSIM görüntü kalite ölçütlerine göre değerlendirilmiştir. Çalışmada gerçek görüntü ile stego görüntü arasındaki bozulmalar PSNR (dB), benzerlikler ise SSIM sonuçlarına göre değerlendirilmiştir. Örtü resimlerin kırmızı (R) ve yeşil (G) kanallarına veri gizleme yapıldığı için kalite ölçütlerinden (PSNR ve SSIM) elde edilen değerler bu kanallar için verilmiştir. Deneysel çalışmalarda, resimlere ortalama 1.046.478 bit şifreli veri gizlemesi yapılmıştır.

Elde edilen değerlerin PSNR (dB) ortalaması: R_kanal 28,989 dB ve G_kanal 26,401 dB, SSIM ortalaması: R_kanal 0,978 ve G_kanal 0,964 dB. Tablo 2'de gösterilen Lena görüntü içine gizlenen şifreli veri büyüklüklerinden PSNR (dB) ortalaması: R_kanal 41,97 dB ve G_kanal 38,81 dB, SSIM ortalaması: R_kanal 0,998 ve G_kanal 0,997 dB sonuçları elde edilmiştir. Çalışmada kullanılan yöntemin, orijinal resim ile stego-resimler arasında benzerlikler (SSIM) ve bozulmalar (PSNR dB) açısından, çok iyi bir görüntü kalitesi elde ettiğini göstermiştir. Aynı zamanda gerçekleştirilen bu yöntem ile resme gizlenen bilginin kapasitesi de artırılmıştır.

Teşekkür

Deneysel çalışmadaki desteklerinden dolayı Doç. Dr. Recep DEMİRCİ ve Sercan ALTAŞ'a teşekkür ederim.

Kaynaklar

1. D. Seth, L. Ramanathan, A. Pandey, Security Enhancement: Combining Cryptography and Steganography, International Journal of Computer Applications Vo. 9 No 11, November 2010.
2. S. Narayana, G. Prasad, Two New Approaches For Secured Image Steganography Using Cryptographic Techniques And Type Conversions, Signal & Image Processing : An International Journal (SIPIJ) Vol.1, No.2, December 2010.
3. R. Nivedhitha, T. Meyyappan, M. Phil., Image Security Using Steganography And Cryptographic Techniques, International Journal of Engineering Trends and Technology- Vol. 3 No 3, 2012.
4. C. K. Chan and L. M. Chen, Hiding data in images by simple LSB substitution, Pattern Recognition., Vol. 37, No 3, pp. 469–474, 2004.
5. L. Der-Chyuan, L. Jiang-Lung, Steganographic Method for Secure Communications, Computers & Security Vol. 21, No 5, pp 449-460, 2002.
6. W.N. Lie, L.C. Chang, Data hiding in images with adaptive numbers of least significant bits based on the human visual system, Proceedings of the 1999 International Conference on Image Processing, Vol. 1, pp. 286-290, December 1999.
7. Y.K. Lee, L. H. Chen, High capacity steganographic model, IEEE Proceedings-Vision, Image and Signal Processing, Vol. 147, No 3, pp. 288-294 June 2000.
8. C. H. Yang, C. Y. Weng, S. J. Wang, H. M. Sun, Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems, IEEE Information Transactions On Forensics And Security, Vol. 3, No. 3, September 2008.
9. H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, Image steganographic scheme based on pixel-value differencing and LSB replacement methods, Proc. Inst. Elect. Eng., Vis. Image Signal Process. Vol. 152, No 5, pp. 611–615, 2005.
10. D. K. Sarmah, N. Bajpai, Proposed System for data hiding using Cryptography and Steganography, International Journal of Computer Science and Security, Vol 4 No 5, 2010.
11. S. Usha, G. A. Sathish Kumal, K. Boopathybagan., A Secure Triple Level Encryption Method Using Cryptography and Steganography, 2011 International Conference on Computer Science and Network Technology, IEEE December 24-26, 2011
12. S. Phad Vitthal, S. Bhosale Rajkumar, R. Panhalkar Archana, A Novel Security Scheme for Secret Data using Cryptography and Steganography, I. J. Computer Network and Information Security, pp. 36-42, 2012.
13. J. Nath, A. Nath, Advanced Steganography Algorithm using Encrypted secret message, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011.
14. H. Yang, X. Sun, G. Sun., A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution, Radio Engıneerıng, Vol. 18, No 4, December 2009.
15. F. Lussona, K. Baileya, M. Leeneya, K. Curran., A novel approach to digital watermarking, exploiting color spaces, Signal Processing, Volume 93, No 5, pp. 1268–1294, May 2013.

16. C. Yen-Yu, C. Ying-Wen, Y. Wen-Chien, Design a deblocking filter with three separate modes in DCT-based coding, Journal of Visual Communication and Image Representation, Volume 19, No 4, pp. 231-244, May 2008.
17. J.K. Mandal, D. Das, Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain, International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, pp. 83-93, July 2012.
18. G-S. Lin, Y-T. Chang, W-N. Lie, A Framework of Enhancing Image Steganography With Picture Quality Optimization and Anti-Steganalysis Based on Simulated Annealing Algorithm, IEEE Trans Multimedia, Vol. 12, No. 5, pp. 345–57, 2010.
19. G. Swain, S. K. Lenka, LSB Array Based Image Steganography Technique By Exploring The Four Least Significant Bits, Global Trends in Information Systems and Software Applications Communications in Computer and Information Science, In: P. V. Krishna, M. R. Babu, E. Ariwa, Editors, Springer Berlin Heidelberg, Vol. 270, pp 479- 488, 2012.
20. M. A. Wafaa, S. R. M. Abdul, K. P. Al-Sakib, Mix column transform based on irreducible polynomial mathematics for color image steganography: A novel approach, Computers and Electrical Engineering, Vol. 40, No. 4, pp. 1390–1404, May 2014.