Düşük Bozulma Oranlı Steganografik Veri İletim Modeli

Low Distortion Rate Steganographic Data Transmission Model

Refik Samet
Bilgisayar Mühendisliği Bölümü
Ankara Üniversitesi
Ankara, Türkiye
samet@eng.ankara.edu.tr

Timuçin Köroğlu
Bilgisayar Programcılığı Programı
Pamukkale Üniversitesi
Denizli, Türkiye
tkoroglu@pau.edu.tr

Öz **- Steganografide veriler farklı yöntemlerle gizlenmektedir. Yapılan çalışmalarda temel hedef, örtü resminin minimum düzeyde bozulmaya sahip olmasıdır. Önerilen modelde küçük miktarlı verinin büyük miktarlı veriyi temsil ederek iletilmesi temel alınmıştır. Örtü resmi içerisine temsili veri gizlenerek çok düşük resim bozulma oranlarıyla büyük veriler dolaylı taşınmaktadır. Bu model, belli sürelerde değiştirilen ve önem değeri yüksek verilerin güvenli iletiminde kullanılmalıdır. Örtü resmine gizlenen küçük miktardaki veri, sunucu tarafında büyük miktardaki verinin çözümlenmesinde kullanılmıştır. Böylece steganografinin temel yapı taşlarından sezdirmezlik prensibinin üst düzeylere çıkması sağlanmıştır. Elde edilen sonuçlar, önerilen modelin yaklaşık %10 ile %40 aralığında daha güvenli olduğunu göstermiştir**.

Anahtar Sözcükler — Steganografi, Veri güvenliği, Örtü Resmi, Örtü Nesnesi, Veri Gizleme

Abstract **- In steganography, the data is hidden in different ways. The main objective of the studies is to have a minimum distortion of the cover image. The proposed model is based on the transmission of small amounts of data representing large amounts of data. By hiding the representative data in the cover image, large data is carried indirectly with very low image distortion rates. This model should be used for the safe transmission of data of high importance and which have been modified at certain times. Small amounts of data hidden in the cover image were used to analyze large amounts of data on the server side. Thus, the principle of imperceptibility, which is one of the basic building blocks of steganography, has been increased. The results showed that the proposed model is safer in the range of about 10% to 40%.**

Keywords — ***Steganography, Data security, Cover Image, Cover Object, Data Hiding***

I. GİRİŞ

İnternetin son yıllarda artan gücü ile birlikte toplum hızla dijitalleşmekte ve kişisel veriler hızla siber ortamlara aktarılmaktadır. Bununla birlikte yeteri kadar güvenli olmayan ağlar, kişisel verilerimizin güvenliği konusunda potansiyel bir tehlikeyi açığa çıkarmaktadır.

Bilgi güvenliğini sağlamanın iki yolu vardır. Bunlar kriptoloji (şifreleme) ve veri gizleme (steganografi)'dir [1].

Kriptoloji, iki ya da daha çok tarafın arasında gerçekleştirilen veri iletişiminde, verinin başkalaştırılmasını esas alan ve bu işlemleri matematiksel yöntemlere dayandıran tekniklerin ve uygulamaların bütünüdür [2]. Kriptolojide gizli olmayan bilgiye düz metin (plaintext), gizli metne şifreli metin (ciphertext) ismi verilir. Düz metinden şifreli metne çevirme işlemine şifreleme (encryption), şifreli metni düz metne çevirme işlemine şifre çözme (decyption) adı verilir [3].

Steganografi, verinin üçüncü şahıslar tarafından incelenmesini ve ele geçirilmesini engellemek amacıyla veriyi bir örtü (cover) üzerine gizleyen ve bu şekilde iletilmesini hedefleyen veri gizleme bilim dalıdır [4]. Örtü nesnesi metin, ses, resim ya da video olabilir. Örtü nesnesinin veri gizlenmiş haline stego nesnesi adı verilir [5].

Steganografi'de veriler uzaysal (spatial) ya da frekans (transform) uzayı alanlarına gizlenirler. Uzaysal alanlarda veri gizleme işlemi, örtü nesnesi piksellerinin gizlenecek veriye göre değiştirilmesi ile gerçekleştirilir. Frekans uzayı alanında matematiksel yöntemler kullanılarak veri gizlenir [6].

Sezilmezlik, dayanıklılık ve kapasite steganografinin üç temel karakteristiğidir. Steganografi'nin başarısı örtü nesnesi üzerine gizlenmiş verinin sezilememesine bağlıdır.

Steganografinin kriptolojiye karşı en büyük üstünlüğü sezilemez oluşudur. Kripto edilerek anlaşılamaz duruma getirilmiş şifreli veriler üçüncü şahısların dikkatini çekmektedir. Buna karşılık steganografik yöntemler ile iletilmek istenen veri üçüncü şahısların dikkatlerini çekmeden örtü nesnesine gizlenmekte ve güvenli bir şekilde alıcı tarafına ulaştırılmaktadır [7].

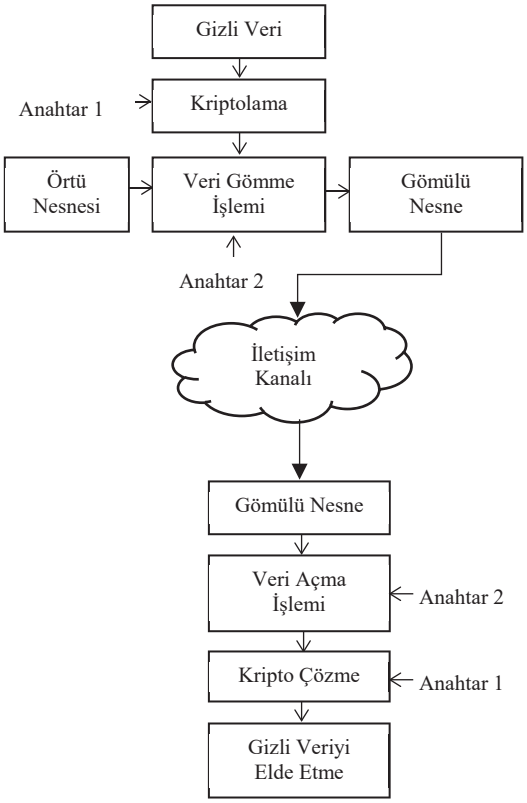
II. ÖNERİLEN MODEL

Kadhim, I. J vd. steganografi veri gizleme biliminde, verinin örtü nesnesi üzerine gizlenirken örtü nesnesinde bozulmalar olacağını ve bozulma oranının azaltılmasının, steganografinin sezilmezlik özelliğinin korunması açısından önemli olduğunu vurgulamıştır. Kadhim, I. J vd. steganografide kullanılan temel adımları Şekil 1'deki gibi özetlemiştir [8].

Önerilen model, istemci-sunucu mimarisine dayalı olup her iki tarafta veri iletişimi, steganografi biliminin temel esasları çerçevesinde gerçekleştirilmektedir. Modelde örtü nesnesi olarak resim kullanılacaktır.

Klasik steganografik yöntemlerde veri, örtü nesnesi üzerine gizlendiğinde örtü nesnesinde çeşitli oranlarda bozulmalar meydana gelmektedir. Önerilen modelde ise gizlenen veri miktarı arttıkça örtü resmindeki bozulma oranı azalmaktadır. Böylece yüksek veri gizleme buna karşılık düşük bozulma miktarı ile sezilmezlik prensibi en üst düzeyde uygulanmıştır. Önerilen modelde, istemci-sunucu mimarisinde belli sürelerde değiştirilen ve önem değeri yüksek verilerin steganografik teknikler kullanılarak güvenli bir şekilde nasıl iletilebileceği üzerinde durulacaktır.

978-1-7281-3964-7/19/$31.00 ©2019 IEEE

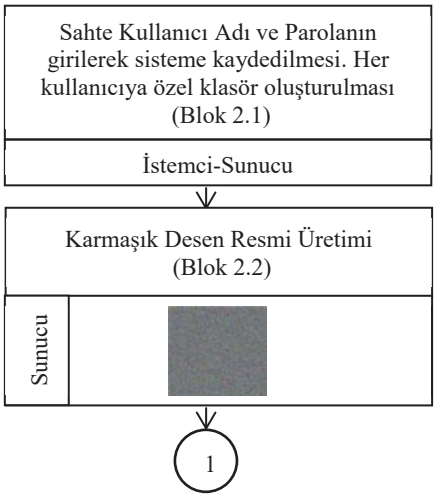


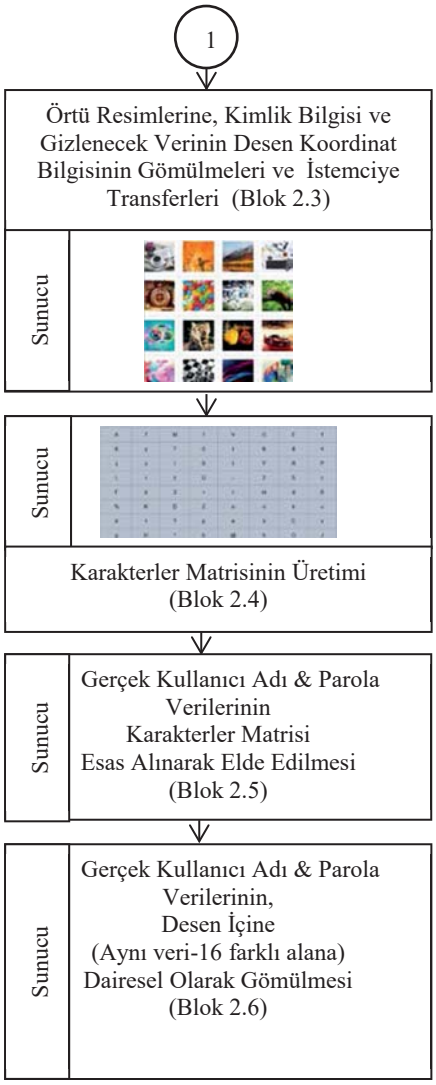
Şekil 1. Steganografi biliminde temel aşamalar

A. Modelin İşleyişi

Model iki temel aşamada incelenmelidir. Bunlar sisteme kayıt olma ve sisteme giriş yapma süreçleridir.

1) Sisteme Kayıt Olma Süreci: Sisteme kayıt olma süreci, kullanıcı tarafından bir kez gerçekleştirilen bir işlemdir. Bu sürecin ilk aşamasında, bir web arayüzü aracılığıyla kullanıcıdan sahte kullanıcı adı ve parola bilgilerinin istemci tarafında girilerek sunucu veritabanına kaydedilmesi istenmektedir. Sisteme kaydedilen bu bilgiler gerçekte örtü resmini seçme işlemi yapan ve üçüncü şahısları gerçek kullanıcı adı ve paroladan gizleyen bir sosyal mühendislik kalkanıdır. Sisteme kayıt olma sürecinin genel akış şeması Şekil 2'de görülmektedir.





Şekil 2. Kayıt olma süreci genel akış şeması

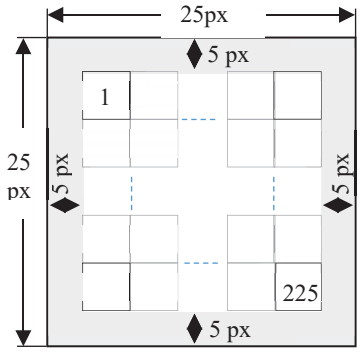
a) Sahte Kullanıcı adı ve parola (Blok 2.1): Bu aşamada, kullanıcı tarafından girilen sahte kullanıcı adı ve parola bilgileri sisteme kaydedilmekte ve bu bilgiler esas alınarak klasör ismi türetilmektedir. Böylece her kullanıcı için üretilen isme sahip ayrı bir klasör, sunucu tarafında oluşturulacaktır. Bu klasör içerisine, her kullanıcı için rassal olarak üretilen desen resmi ve istemci tarafından gönderilen örtü resimleri saklanacaktır.

b) Karmaşık desen resmi üretimi (Blok 2.2): Sisteme giriş için yetkilendirilme denetimi, desen resmi içine gizlenecek gerçek kullanıcı adı ve parola vasıtasıyla gerçekleştirilecektir. Bu amaçla kullanıcıların sisteme kayıt olma sürecinde karmaşık desen resmi sistem tarafından rassal piksel değerleri ile sunucu tarafında üretilmekte ve ilgili kullanıcının klasöründe saklanmaktadır. Model için geliştirilen uygulamada karmaşık desen resmi 16x16 boyutlarında parçalanacaktır. Bu boyut farklı uygulamalarda ihtiyaca göre değiştirilebilir. Toplamda 256 parça olan alanlardan rassal olarak 16 tanesi seçilerek gerçek kullanıcı adı ve parola verileri bu alanlara gizlenecektir. Desen resminin 16 bölümüne veri saklanması, model uygulamasında 16 adet örtü resmi kullanıldığı içindir. 16 adet örtü resmi içine desen parçalarının başlangıç koordinatları

gizlenmekte ve istemciden sunucuya gönderilen örtü resmine göre ilgili parçadan veri okunmaktadır. Desen resminin alanları şu şekilde karakterize edilmiştir: 512x512 piksel boyutundaki desen resmi her yönden 56 piksellik iç kenar boşluklarına sahiptir. Veri gömülecek alan [512-(2*56)] x [512-(2*56)] = 400 x 400 piksellik kare biçiminde bir alandır. Bu durumda 16x16'lık alanın her biri (400/16)x(400/16)=25 x 25 piksellik alanlardan oluşmaktadır.

c) Örtü resimlerine veri gizlenmesi(Blok 2.3): Desen resmindeki 25x25'lik alanlar gerçek kullanıcı adı ve parolanın gizleneceği alanlardır. Veri gizlenecek bu alanlar her yönden 5 piksellik iç kenar boşluklarına sahiptir. Bu durumda veri gizlenecek alan (25-2x5) x (25-2x5) = 15 x 15'lik kare biçiminde bir alandır. Bu alanların satır/sütun koordinatları 4'er bit veri ile temsil edilmekte ve başlangıç koordinat değerleri sıfırdan başlamaktadır. Toplamda gizlenecek veri miktarı toplam kapasitesi 15x15=225 bittir. Örtü resminin içerisinde bu alanların koordinatları saklanacaktır. Alanlardan bir tanesinin gösterimi Şekil 3'de verilmiştir.

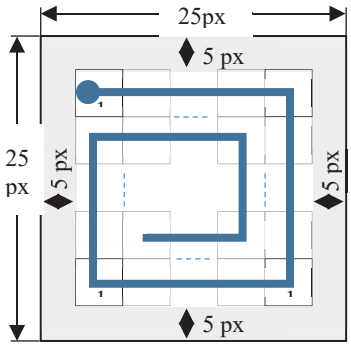
Önerilen modelde, örtü resimlerinin içerisine 4 bitlik resim kimliği ve desen resminin 256 mantıksal parçasından gerçek kullanıcı adı ve parolanın saklanacağı 16 adet parçanın, 8 bitlik başlangıç koordinat verileri saklanmaktadır. Model uygulamasında 16 adet örtü resmi kullanılmaktadır. Resimler 512x512 piksel boyutlarında "png" formatındadır.



Şekil 3. Karmaşık desen resmi mantıksal alanları gösterimi

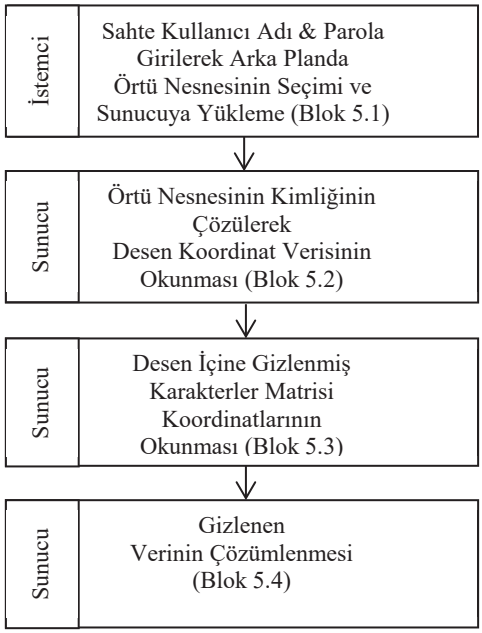
d) Karakterler matrisi ve koordinat verisinin elde edilmesi (Blok 2.4 ve Blok 2.5) : Yetkilendirilme için kullanılacak sekizer karakterli gerçek kullanıcı adı ve parola sistem tarafından üretilmektedir. Üretilen kullanıcı adı ve parola saf 8 bitlik ASCII karakterleri olarak saklanmamaktadır. Modelde her bir karakterin farklı bir veriye dönüşümü sağlanmıştır. Bu amaçla her kullanıcı için rassal olarak ayrı bir karakterler matrisi üretilmektedir. Karakterler matrisi 8 x 8 boyutunda olup her bir hücresinde farklı bir karakter saklamaktadır. Üretilen kullanıcı adı ve parola, karakterler matrisinin satır ve sütunu ile eşleştirilerek, karakterler matrisinin koordinat değerlerini gösterecek biçimde elde edilmektedir. Koordinat verileri 6 bit uzunluğundadır. Böylece 128 bit uzunluğundaki gerçek kullanıcı adı ve parola 96 bit uzunluğuna düşmektedir.

*e) Gerçek kullanıcı adı ve parolanın desen içine dairesel gizlenmesi (Blok 2.6) :*Önerilen modelde veri saklama karmaşıklığını arttırma amacıyla karakterler matrisi koordinat adreslerine dönüştürülen gerçek kullanıcı adı ve parola, desen resmi içinde dairesel olarak saklanacaktır.



Şekil 4. 25x25 lik alana verinin dairesel olarak gömülmesi

2) Sisteme giriş yapma süreci : Sisteme giriş yapma sürecinin genel işleyişi Şekil 5'te görülmektedir.



Şekil 5. Sisteme giriş yapma süreci genel işleyişi

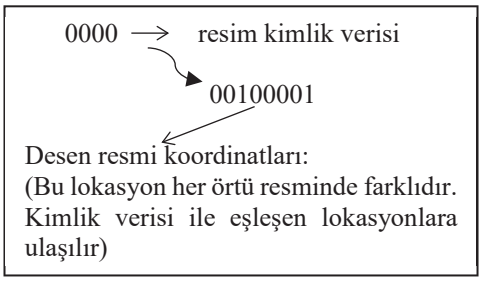
a) Sahte kullanıcı adı ve parola verisi ile örtü nesnesi seçimi (Blok 5.1) : İstemci tarafında, kullanıcı adı ve parola için oluşturulan metin kutularına, örtü resmini seçmesi ve ters sosyal mühendislik uygulaması için sahte kullanıcı adı ve parola girilecektir. Ters sosyal mühendislik uygulanmasında DiGraph algoritması kullanılacaktır [9]. Girilen sahte kullanıcı adı ve parolanın her karakteri geliştirilen sistem tarafından ASCII kodlarına çevrilmektedir. Bu kodlar bir sonraki aşamada Min-Max fonksiyonu ile normalizasyon işleminden geçirilmektedir. Min-Max fonksiyonu ASCII kodlarını [0-1] aralığına çekmektedir. [0-1] aralığına çekilen her değer 4 ile çarpılmakta ve sekizer adet [0-3] aralığında satır-sütun verilerini veren değerler elde edilmektedir. Bu işlemleri yapmak için kullanılan Min-Max fonksiyonu [10] aşağıda verilmektedir.

$$X = \frac{X_i - X_{min}}{X_{max} - X_{min}} \quad (1)$$

Sonraki aşamada sistem rassal olarak indis verisi üretmekte ve [0-3] aralığındaki sekizer adet iki grup sayıdan birer tanesini seçmektedir. Bu sayılar 4x4 boyutlarında örtü

resimlerinden hangisinin seçileceğini gösteren satır ve sütun değerlerini vermektedir.

b) Desen koordinat verisinin okunması (Blok 5.2): İstemci tarafında girilen sahte kullanıcı adı ve parola ile seçilen örtü resmi, sunucu tarafına gönderilecektir. Örtü resmi içinde resim kimlik bilgisi saklıdır. Resim kimlik bilgisi 16 adet örtü resmini temsil eden 0-15 aralığında 4 bitlik bir sayıdır. 4x4 boyutlarındaki matrisin 0. satır ve 0. sütunundaki ilk örtü resmi için '0000', 0. satır ve 1. sütundaki ikinci örtü resmi için '0001' değerini içerir. Diğer resimler sırasıyla "1111" değerine kadar sıradaki sayı ile temsil edilir. Her örtü resmi içinde 8 bitlik desen resmi koordinat verisini saklar. Ancak bu koordinat verileri her örtü resminin farklı bir lokasyonunda saklanmıştır. Her örtü resmi kimlik bilgisi ile eşleşen lokasyonlara ulaşılır. Böylece bu lokasyonlarda asıl kullanıcı adı ve parolanın gizlendiği desen resminin koordinat verilerine ulaşılır. Bu durum Şekil 6'da gösterilmiştir.



Şekil 6. Örtü resmi kimlik bilgisi işlevi

c) Gerçek kullanıcı adı ve parolayı temsil eden karakterler matrisi koordinat verisinin okunması ve çözümlenmesi (Blok 5.3 ve Blok 5.4): Desen koordinat verisinin örtü resmi içinden okunması ile sunucu tarafında tutulan karmaşık desen resmi içerisine gizlenen 96 bitlik gerçek kullanıcı adı ve parolayı temsil eden veri, dairesel olarak okunmakta ve sunucuda çözümlenmektedir. Çözümlenen gerçek kullanıcı adı ve parola ile sisteme giriş yetkilendirilmesi yapılmaktadır.

III. DENEYSEL SONUÇLAR VE ANALİZ

Gömülü resim ile orijinal resim arasındaki bozulma oranını tespit edebilmek amacıyla PSNR ve MSE ölçütleri kullanılmıştır.

$$PSNR(f,g) = 10\log 10(\frac{255^2}{MSE(f,g)}) \quad (2)$$

$$MSE(f,g) = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(f_{ij} - g_{ij})^2 \quad (3)$$

formüllerde, f orijinal ve g ise test resmini ifade etmektedir.

Elshare, S. ve El-Emam, N. N geliştirdikleri "Düzenlenmiş Çok Seviyeli Steganografi" modeli ile Baboon ve Barbara isimli örtü resimlerine farklı miktarlarda veri gizlemişlerdir. Modelin etkinliğini kanıtlamak amacıyla Ou, B. ve diğerleri ile Li, J tarafından geliştirilen modellerin örtü resimleri üzerinde yaptığı bozulma miktarı kıyaslanmıştır [11]. Tablo 1'de, Elshare, S. ve El-Emam, N. N ile Ou, B. vd. , Li, J'nin yaptıkları ölçümler listelenmektedir. Bu çizelgeye, önerilen modelin dolaylı olarak taşıyabileceği veri miktarı ve örtü resmi PSNR ölçümleri eklenmiştir. Çizelgeden görüleceği üzere önerilen modelde PSNR oranları her iki örtü resmi için diğer modellere göre oldukça yüksektir.

TABLO I. ÖNERİLEN MODEL İLE DİĞER MODELLERİN PSNR ORANLARININ GÖSTERİMİ

Resim Büyüklüğü 512x512		Baboon					Barbara				
Gömülü bit x 104		2	2.8	3.6	4.4	5.6	2	5	7	10	12.5
PSNR(dB) Ou, B., ve diğerleri (2015)		56.8	54.9	53.3	51.9	49.8	62	57	55.1	53	51.1
PSNR(dB) Li, J., (2013)		57.1	55.2	53.3	51.9	49.9	59.8	55.8	54.1	52.5	51.1
PSNR(dB) Elshare, S ve El-Emam, N		59.2	56.1	54.9	53.2	53.4	63.2	59.6	58.5	55.9	54.8
ÖNERİLEN YÖNTEM	Direk Gömülü Bit	12	11	11	11	12	11	10	10	10	10
	Dolaylı Taşıma Kapasitesi (Bit)	225	600	600	600	225	600	1600	1600	1600	1600
	PSNR(dB)	69.25	69.25	69.25	69.25	69,25	69.25	69.83	69.83	69.83	69.83

IV. SONUÇ

İnternet ortamında belli aralıklarla değiştirilen çok önemli verilerin iletiminde çok katmanlı steganografik bir model önerilmiştir. Steganografik veri iletim modelleri birbirleri ile yüksek kapasite düşük resim bozulma oranına göre kıyaslanmakta ve değerlendirilmektedir. Bu anlamda önerilen model mevcut modellerden daha iyi sonuçlar vermiştir. Bunun sebebi: önerilen modelde, örtü resmi üzerinde gizli verinin kendisinin değil desen resmi üzerindeki asıl verinin koordinatının taşınmasıdır. Resim kimliği ve koordinat verisinin toplam uzunluğu 12 bitlik bir veridir. Desen resmi üzerindeki gerçek veri ise 96 bittir. Uygulamada 96 bit veri dolaylı olarak taşınmıştır. Farklı uygulamalarda desen resmi daha az parçalara bölünerek daha yüksek miktarlarda veri dolaylı olarak taşınabilir. Önerilen yöntem büyük verinin küçük veri ile temsili ve taşınması ilkesi üzerine kuruludur. Tablo 1'de verilen mevcut modeller, Baboon isimli örtü resminde 49,8 dB - 59,2 dB aralığında, Barbara isimli örtü resminde 51,1 dB - 63,2 dB aralığında PSNR değerlerine sahiptir. Önerilen modelde, Baboon isimli örtü resminde tüm veri miktarlarında 69,25 dB, Barbara isimli örtü resminde 69,25 dB - 69,83 dB aralıklarında PSNR değerleri ölçülmüştür.

Model uygulamasında bir kullanıcı adı ve parolanın güvenli bir şekilde düşük PSNR değerleri ile nasıl taşınabileceği örneklendirilmiştir. Önerilen model ile önem değeri yüksek daha farklı veriler taşınabilir. Desen resmi ihtiyaç duyulan uygulamaya göre daha az/daha fazla parçalara bölünebilir. Örtü resmi sayısı ve boyutları da değiştirilebilir.

Önerilen modelin dezavantajı sürekli güncellenen verilerin iletimi için uygun olmamasıdır. Bunun sebebi, desen resminin ve çoklu örtü resimlerinin ağ üzerinden

istemci bilgisayarına sıklıkla transferinin, ağ trafiğini olumsuz etkileyecek olmasıdır. Bu yüzden belli süre aralıklarında güncellenen veri iletiminde kullanımı daha etkili olacaktır.

Gelecekte, önerilen modelin geliştirilerek anlık yüklenen verileri de taşıyabilecek duruma getirilmesi güvenli ve düşük bozulmalı veri iletiminde önemli bir boşluğu dolduracaktır.

KAYNAKLAR

[1] Tuncer, T., & Avcı, E. (2017). Renkli İmgelerde Kimlik Doğrulaması ve Saldırı Tespiti için Görsel Sır Paylaşım Tabanlı Yeni Bir Kırılgan Damgalama Algoritması. International Journal of Innovative Engineering Applications 1, 1(2017), 1-8

[2] Yalman, Y., Ertürk İ., Çetin, Ö. (2014) Veri Gizleme Kitabı, 13, Beta Basım Yayın.

[3] Klima, R., Klima, R. E., Sigmon, N., & Sigmon, N. P. (2018). Cryptology: Classical and Modern. CRC Press.

[4] Li, P., & Lu, A. (2018). LSB-based Steganography Using Reflected Gray Code for Color Quantum Images. International Journal of Theoretical Physics, 57(5), 1516-1548.

[5] Jung, K. H. (2018). A survey of interpolation-based reversible data hiding methods. Multimedia Tools and Applications, 77(7), 7795-7810.

[6] Subhedar, M. S., & Mankar, V. H. (2018). Curvelet transform and cover selection for secure steganography. Multimedia Tools and Applications, 77(7), 8115-8138.

[7] Bai, J., Chang, C. C., Nguyen, T. S., Zhu, C., & Liu, Y. (2017). A high payload steganographic algorithm based on edge detection. Displays, 46, 42- 51.

[8] Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. Neurocomputing, 335, 299-326.

[9] Por, L. Y., Ku, C. S., Islam, A., & Ang, T. F. (2017). Graphical password: prevent shoulder-surfing attack using digraph substitution rules. Frontiers of Computer Science, 11(6), 1098-1108.

[10] Jain, A., Nandakumar, K., & Ross, A. (2005). Score normalization in multimodal biometric systems. Pattern recognition, 38(12), 2270-2285.

[11] Elshare, S., & El-Emam, N. N. (2018). Modified Multi-Level Steganography to Enhance Data Security. International Journal of Communication Networks and Information Security, 10(3), 509.