EJONS International Journal on Mathematic, Engineering and Natural Sciences | ISSN 2602 - 4136

Article Arrival Date: 29.03.2021 | Article Type: Research Article | Article Published Date: 20.06.2022

SHAMIR SIR PAYLAŞIM ALGORİTMASININ GÖRÜNTÜ STEGANOGRAFİSİNDE UYGULANMASI

APPLICATION OF SHAMIR SECRET SHARING ALGORITHM IN IMAGE STEGANOGRAPHY

Zekeriya KAYA*

Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü, Bilişim Sistemleri Mühendisliği, Kocaeli / Türkiye

ORCID: 0000-0003-3764-403X

Doç. Dr. Serdar SOLAK

Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü, Bilişim Sistemleri Mühendisliği, Kocaeli / Türkiye

ORCID: 0000-0003-1081-1598

ÖZET

İnternet kullanımının artmasıyla doğru orantılı olarak bilgi akışında artış yaşanmıştır. Bu durum sonucunda bilginin, siber saldırılara ve güvenlik zafiyetlerine karşı korunma ihtiyacı doğmuştur. Bilgi güvenliği ve gizliliğini sağlamak için kullanılan yöntemler arasında steganografi ve sır paylaşım algoritmaları bulunmaktadır. Steganografi, karşı tarafa iletilecek gizli bilgiyi, çaktırmadan metin, ses, görüntü ve video gibi ortama saklamayı amaçlamaktadır. Aynı zamanda gizli bilginin korunmasını arttırmak amacıyla sır paylaşım algoritmaları kullanılmaktadır. Sır paylaşım algoritmaları sayesinde sır bilginin güvenliği için bilgiyi saklama veya bir kişide bulundurma koşulu ortadan kalkmıştır. (k,n) eşik sır paylaşım algoritmalarında gizlenen bilgi n adet paya dağıtılır ve k adet payın bir araya getirilmesi ile sır bilgi yeniden elde edilir. Bu makalede gizli bilginin güvenliğini sağlamak amacıyla, görüntü steganografisinde yaygın kullanılan LSB ve Shamir sır paylaşım algoritması beraber kullanılmıştır. Örtü görüntü, Shamir' in polinomsal tabanlı sır paylaşım algoritması ile istenilen sayıda anlamsız pay görüntülere bölünmüştür. Bu sayede veri iletimi sırasında araya giren kötü niyetli kişiler, k adet payı bir araya getiremediği sürece gizli veriyi elde edememektedirler. Sonuç olarak tercih edilen yöntemlerin birlikte kullanımı ile gizli bilginin güvenliği artmaktadır. Yapılan deneysel çalışmalar sonucunda veri güvenliğini arttırmak için veri gizleme tekniklerinin tek başına kullanılması yerine, şifreleme ve sır paylaşım algoritmaları ile beraber kullanılmasının uygun olacağı gözlemlenmiştir.

Anahtar Kelimeler – Bilgi Güvenliği, Görüntü Steganografisi, LSB, Shamir Sır Paylaşım Algoritması, Veri Gizleme

ABSTRACT

There has been an increase in the flow of information in direct proportion to the increase in the use of the Internet. As a result of this situation, the need to protect information against cyber attacks and security vulnerabilities has arisen. Steganography and secret sharing algorithms are among the methods used to ensure information security and confidentiality. Steganography aims to hide the confidential information to be transmitted to the other party in the media such as text, sound, image and video without being hidden. At the same time, secret sharing algorithms are used to increase the protection of confidential information. Thanks to the secret sharing algorithms, the condition of keeping the information or keeping it in one person has been removed for the security of the confidential information. The information hidden in (k, n) threshold secret sharing algorithms is

distributed to n shares, and the secret information is obtained by bringing together k shares. In this article, LSB and Shamir secret sharing algorithm, which is widely used in image steganography, are used together to ensure the security of confidential information. The cover image is divided into the desired number of meaningless share images by Shamir's polynomial-based secret sharing algorithm. In this way, malicious persons intervening during data transmission cannot obtain confidential data unless they can bring together k shares. As a result, the security of confidential information increases with the combined use of preferred methods. As a result of the experimental studies, it has been observed that instead of using data hiding techniques alone to increase data security, it would be appropriate to use them together with encryption and secret sharing algorithms.

Keywords – Information Security, Image Steganography, LSB, Shamir Secret Sharing Algorithm, Data Hiding

1. GİRİŞ

Günümüzde, tablet, telefon ve bilgisayar gibi cihazların artması, ağ üzerinden veri iletişiminin yaygın kullanılması sayısal veri üretimini arttırmıştır. Bu sayısal verinin uçtan uca iletimi sırasında güvenliğini sağlamak günümüzde önem kazanmıştır. Verilerin güvenliğini sağlamak için, şifreleme, veri gizleme ve sır paylaşım algoritmaları gibi yöntemler kullanılmaktadır [1]. Veri gizleme veya steganografi, farklı örtü dosya türleri içinde çeşitli verileri çaktırmadan gizleyip güvenilir iletişim sağlamaya denilmektedir [2]. Steganografi, gizli bilgiyi bir ortama saklamayı amaçlar. Steganografi, kelime olarak gizlenmiş yazı anlamını taşımaktadır. İletilmesi istenilen gizli bilginin saklanması ve üçüncü şahısların eline geçmesini engellemek için örtü nesnesi olarak sayısal resim, metin, ses ya da video dosyası kullanılabilir [3-6]. Günümüzde, çok sayıda veri gizleme yöntemi bulunmasına karşın, en yaygın yöntem, en düşük anlamlı bit (Least Significant Bit - LSB) yöntemidir [3]. Bu veri gizleme yöntemlerinin dışında gizli bilginin korunması için Sır Paylaşım Algoritmaları kullanılmakta olup en önemlilerinden birisi Shamir ve Blakley'in (1979) birlikte önerdiği sır paylaşım algoritmasıdır [4]. Shamir sır paylaşım algoritması, (k,n) eşik sır paylaşım algoritması olarak da bilinmektedir. Bir (k,n) algoritmasında gizli bilgi, temel olarak bir bütün halinde bir yerde olmaktansa, n adet paylara ayrılmaktadır. Burada, k adet pay bir araya getirilerek hem gizli veri elde edilir hem de bu bilginin güvenliği sağlanmış olur.

Makale çalışmasında, LSB veri gizleme yöntemi ve Shamir sır paylaşım algoritması kullanılarak hibrit bir güvenlik algoritmasının uygulanması anlatılmaktadır.

Makalenin ikinci bölümünde LSB, Shamir'in Sır Paylaşım Algoritması ve Maple (t,n) eşik değer uygulaması sunulmaktadır. Üçüncü bölümde, önerilen uygulama, bulgular hakkında detaylar vermektedir. Dördüncü bölümde ise yöntem ile ilgili sonuçlar analiz edilmektedir.

2. MATERYAL VE YÖNTEM

2.1. Görüntü Steganografisinde LSB Yöntemi

Steganografinin temelde iki prensibi vardır. Biri, sayısala çevrilmiş resim veya ses dosyalarının, sahip oldukları fonksiyonlarını kaybetmeksizin değiştirilebilmeleridir. Diğeri ise insanın, görüntü ya da ses kalitesinde oluşabilecek ufak değişiklikleri fark edememesidir. Buradaki amaç; anlamsız bilgiler taşıyan nesnelerdeki bilgileri, istenilen bilgilerle yer değiştirmektir. Resim dosyalarının içeriğine baktığımızda; veri gizleme için bitlerden oluşan herhangi bir pikselin en az anlam taşıyan bitleri üzerinde yapacağımız bir değişim resimde renk değişikliğine sebep olsa da görsel olarak algılanabilir bir seviyede olmayacaktır.

En önemsiz bite yapılan veri gizleme yöntemi olan LSB, basit ve gerçeklemesinin kolay olmasından

dolayı yaygın olarak kullanılmaktadır. Yöntemde görüntüyü oluşturan piksellere ait sayısal değerler ve gizlenecek olan veri ikili sayı sistemine çevrilmektedir. Gizlenecek olan verinin her bir biti ilgili piksel değerinin en düşük anlamlı bitinde saklanmaktadır [7-14]. Örnek bir görüntüye ait bazı piksel değerlerinin ikili karşılığı aşağıda sunulmaktadır.

11101000 11101000 11101001 10011010

11111010 11101001 11111110 11111101

Bu piksel değerlerine A (65) karakteri saklanmak istendiğinde, bu karaktere ait ikili sayı sistemindeki karşılığı (01000001) bitleri ile ifade edilmektedir. Bu bilgi, yukarıda verilen piksel değerlerine gizlendiğinde aşağıda sunulduğu gibi değişmektedir. Koyu renkli olan bitler, sırasıyla A karakterini temsil eden bitlerdir [8].

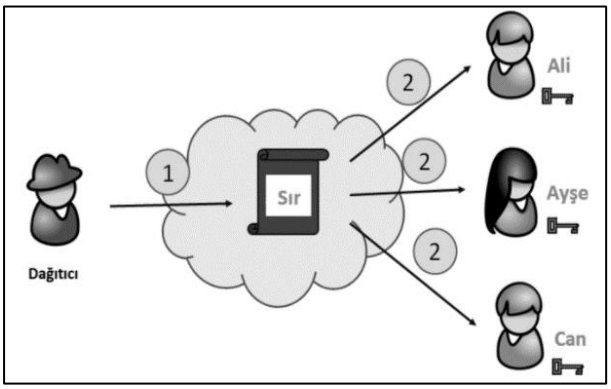
11101000 11101001 11101000 10011010

11111010 11101000 11111110 11111101

Pikseldeki değişimler en düşük anlamlı bitlere sırayla yapıldığında görüntü içine gizlenmiş bilgi, kötü niyetli üçüncü şahıslar tarafından kolaylıkla elde edilebilmektedir. Bu durumu engellemek için rastgele veya bir anahtar kullanılarak değişim yapılabilir. Çalışmada, LSB yönteminin steganaliz ataklarına karşı dayanıklılığını arttırmak ve karakter kayıplarını gidermek için sır paylaşım algoritması ile birlikte kullanımı sağlanacaktır.

2.2. Shamir 'in Sır Paylaşım Algoritması

Sır paylaşım algoritmaları, herhangi bir anahtarı, herhangi bir grup içerisinde belirli paylara dağıtmak amacıyla geliştirilmiş sistemlerdir. En çok bilinen Shamir isimli sır paylaşım algoritması, Shamir ve George Blakley tarafından 1979'da birbirinden bağımsız olarak bulunmuştur. Shamir, İnterpolasyon yöntemi kullanırken Blakley, Hiper Düzlemlerin Kesişimi 'ni, McElice ve Sarwate ise Reed Solomon Kodları 'nı kullanmıştır. Sır paylaşım, bir sırrı bir grup üye arasında, her birine bir parça verecek şekilde dağıtma metodudur.



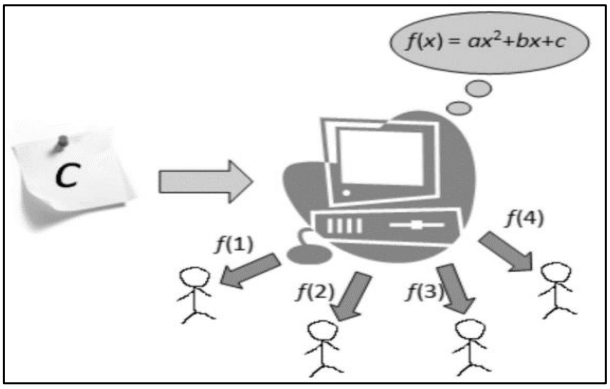
Şekil 1. Sır paylaşım şeması

Anahtar n parçaya bölünür;

- Anahtarı yeniden oluşturabilmek için t tanesine ihtiyaç bulunmaktadır.
- t-1 parça, anahtar ile ilgili bilgiye sahip değildir. Şartın sağlanma durumuna "mükemmel sistem" denir.
- Tek bir parçanın anahtardan daha uzun olma imkanı yoktur. Parçanın anahtara eşit olma durumu ise "ideal sistem" olarak tanımlanır.

Sır paylaşım algoritmasının çalışma prensibi polinom açılımına dayanmaktadır [15-18]. 2 boyutlu x-y düzlemindeki t noktaları (x_1,y_1) ,…, (x_t,y_t) için her biri birbirinden farklı x 'ler olacak şekilde, sadece bir tane t-1 dereceli bir q(x) polinomu bulunur. Her i için $q(x_i)=y_i$ olur. Bilginin P adet parçaya bölünmesi durumunda rastgele bir t-1 dereceli $q(x)=a_0+a_1x+\ldots+a_{t-1}x_{t-1}$ polinomu seçilip $a_0=P$ şeklinde açıldığında;

$P_1=q(1),\ldots,P_i=1(i),\ldots P_n=q(n)$ elde edilir.



Şekil 2. Polinomun paylara bölünmesi

İnterpolasyonda bulunan q(x) değerlerinin katsayılarını bulmak ve P=q(0)'ın hesaplanabilmesi, P_i parçalarının herhangi bir alt kümesi olan t değeri ile sağlanır. P 'nin hesaplanması için bu değerlerin t-1 tanesi yeterli değildir. Modüler aritmetik kullanılarak daha kesin ifadeler elde edilebilir. Asal sayı olan m 'nin modu alınarak elde edilen tamsayılar kümesi interpolasyonun hesaplanmasını sağlar. Tamsayı olan P bilgisinin verilmesi durumunda, m>n ve m>P olacak şekilde bir asal m sayısı seçilir. q(x) 'teki $a_0,a_1,\ldots,a_{t-1}$ katsayıları rastgele [0,m] aralığından seçilir ve $P_1,\ldots,P_n$ değerleri de mod m 'ye göre hesaplanır.

2.3. Maple'da (t,n) Eşik Değer Uygulaması

Maple, cebirsel hesaplama programı olup 1980 yılında Maplesoft tarafından geliştirilmiştir. Kompleks matematiksel hesaplamalar için kullanılır. Shamir 'in eşik değer şeması yaklaşımına göre, Mod 23, t=3 ve $K=a_0=a(0)=9$ olacak şekilde, rastgele $a_1=7$ ve $a_2=11$ seçildiğini varsayalım. f(x) fonksiyonu $f(x)=9+7x+11x^2$ olarak verildiği durumda bu verilerle 5 pay oluşturulup f(x) polinomu yok edildiğinde P_0, P_1, P_2, P_3, P_4 olmak üzere 5 kişiden 2., 3. ve 4. kişilerin payları ile anahtar yeniden oluşturulmaya çalışılırsa işlem sıralaması aşağıdaki gibi olur.

Maple'de polinomun 5 parçaya bölünüp 3 parçanın birleşimi ile tekrar elde edilmesi	
Girdiler	**Çıktılar**
f := x -> (9 + 7*x + 11*x^2) mod 23	f := x -> (9 + 7*x + 11*x^2) mod 23
n := 4	n := 4
X := [seq(i, i = 1 .. 5)]	X := [1, 2, 3, 4, 5]
Y := map(f, [1, 2, 3, 4, 5])	Y := [4, 21, 14, 6, 20]
L := array(n .. n, 0 .. n)	L:=array(4..4,0..4,[(4,0)=(?)[4,0],(4,1)=(?)[4,1],(4,2)=(?)[4,2],(4,3)=(?)[4,3],(4,4)=(?)[4,4]])
for k from 2 to n do L[n, k] := 1;od;	L[4, 2] := 1 L[4, 3] := 1 L[4, 4] := 1
for k from 2 to n do for i from 2 to n do if i<>k then L[n,k]:=(L[n,k]*(x-X[i+1]))/((X[k+1]-X[i+1]));fi;od; L[n,k]:=unapply(Expand(L[n,k])mod	L[4, 2] := x -> 12*x^2 + 7*x + 10 L[4, 3] := x -> 22*x^2 + 8*x + 8 L[4, 4] := x -> 12*x^2 + 8*x + 6
F := 0:for k from 2 to n do F := F + Y[k + 1]*L[n, k](x):od:Fmod23:	11*x^2 + 7*x + 9
F := unapply(F mod 23, x)	9
F(0)	

Tablo 1. Maple 'de yapılan işlemler

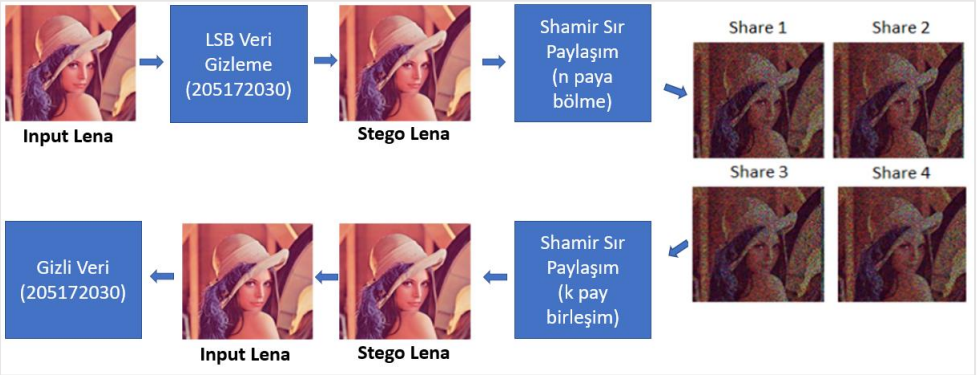
İşlem Sıralaması

- Payların bu fonksiyonda aldığı değerler ve fonksiyon hesaplanır.
- Paylar için L(x) değerleri bulunur.
- Bulunan L değerlerinin toplanması durumunda orijinal polinom elde edilir.
- Anahtar $K=a_0=a(0)$ olup f(0) fonksiyonu ile çağırılacağı için anahtar değerin orijinal polinomdaki değerinin f(0)=9 olması beklenir.
- Eldeki 3 parça ile 5 parçaya ayrılmış bir polinomun Shamir interpolasyon ile yeniden oluşturulabildiği görülmektedir.

3. ÖNERİLEN ÇALIŞMA VE BULGULAR

3.1. LSB Görüntü Steganografisi ve Shamir Sır Paylaşım Algoritmasının Birlikte Kullanımı

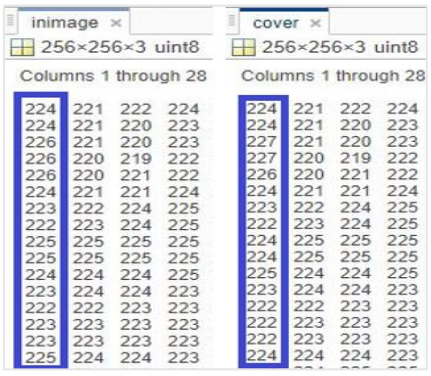
Çalışmada, örtü görüntü olarak kullanılan Lena (256*256) görüntüsüne istenen veri gizlenerek stego Lena görüntüsü elde edilmiştir. Shamir'in sır paylaşım algoritması kullanılarak bu görüntü n adet paya bölünmüştür. k adet payın bir araya getirilmesi ile tekrar stego Lena görüntüsü elde edilmiş ve orijinal görüntü ile karşılaştırılarak gizlenen veri elde edilmiştir. Şekil 3'te çalışmada kullanılan algoritmanın blok şeması bulunmaktadır.



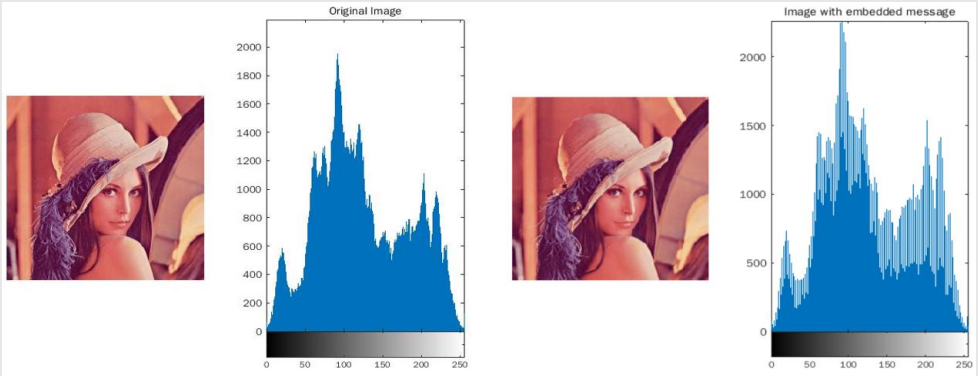
Şekil 3. Çalışmada kullanılan algoritmaya ait blok şeması

Lena orijinal görüntüsüne LSB yöntemiyle veri gizlemek için Matlab uygulamasında bir algoritma oluşturulmuştur. Bu algoritmada import edilen ilgili resme .txt içerisine girilen veri gizlenmektedir. Orijinal ve stego resimlerin piksel karşılaştırması yapılarak resme gizlenen bilginin bir kısmına ait görüntü Şekil 4'de sunulmaktadır.

00110010 - (50) - 2 00110000 - (48) – 0



Şekil 4: Orijinal ve Stego Görüntülerin Piksel Karşılaştırması



Şekil 5: Orijinal ve Stego Görüntülerin Histogram Karşılaştırması

Şekil 5'te orijinal Lena ve stego Lena görüntülerine ait karşılaştırma sunulmaktadır. Orijinal Lena örtü görüntüsüne maksimum kapasitede veri gizlenerek stego görüntü elde edildikten sonra tepe sinyal gürültü oranı (PSNR): 53.649943 olduğundan görüntüde gözle görünür değişiklik olmadığı gözlemlenmiştir. Ayrıca, Şekil 6'da sunulduğu üzere Matlab kullanılarak "Encryptgui" adı verilen kullanıcı arayüzü tasarlanmıştır. Bu arayüz sayesinde, stego Lena görüntüsü (n) parçaya bölünmesi ve (k) parça ile görüntünün tekrar elde edilmesi sağlanmaktadır. Şekil 7'de oluşturulan pay görüntüler yer almaktadır.

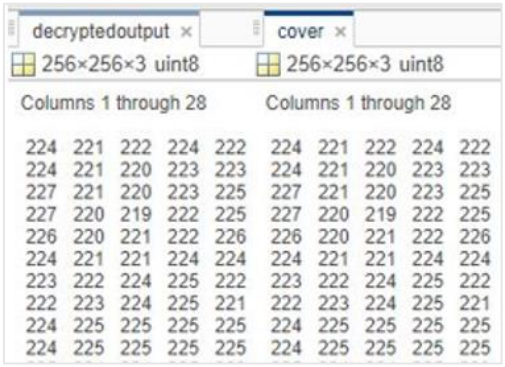
Şekil 6: Stego Görüntünün Paylara Bölünmesi

Şekil7: Oluşturulan pay görüntüler

Şekil 8'de sunulan ve "Decryptgui" adı verilen uygulama ile "Encryptgui" uygulamasında belirtilen k parça görüntünün arayüze eklenerek stego Lena görüntüsü elde edilmektedir.

Şekil 8: k Parça Pay ile Stego Görüntünün Elde Edilmesi

Şekil 9'da sunulan stego Lena görüntüsü ve k parçanın birleşimi ile oluşan görüntünün piksel değerlerine bakıldığında parçalanmış resmin tekrar elde edildiği kanıtlanmıştır.



Şekil 9: Birleşik Görüntü ile Stego Görüntünün Piksel Karşılaştırması

Görüntü kalitesi metrikleri arasında en yaygın kullanılan tepe sinyal gürültü oranı (PSNR) değeridir. Steganografide yöntemin kabul edilebilir olması için PSNR değerinin 30'un üzerinde olması gerekmektedir. Bu değerin 30'un altında olması hali, resimdeki bozulmanın bir insan tarafından anlaşılabilir hale gelmesidir. PSNR değeri hesaplanırken Denklem 1 kullanılır.

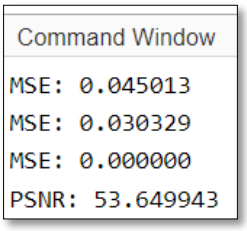
$$PSNR = 10 * \log_{10}\left(\frac{max^2}{MSE}\right) \qquad (1)$$

Denklem 1'de max olarak ifade edilen kısım değişkenin alabileceği maksimum değeri ifade eder. Bu değer sekiz bitlik bir resim için 255'tir.

MSE ise ortalama hata kare anlamına gelmektedir. Denklem 2'deki eşitlik ile hesaplanır.

$$MSE = \frac{1}{m*n}\sum_{0}^{m-1}\sum_{0}^{n-1}\left(X'_{i,j} - X''_{i,j}\right)^2 \qquad (2)$$

Şekil 10 'da orijinal Lena ve stego Lena görüntülerinin MSE ve PSNR değerleri gösterilmiştir.



Şekil 10: PSNR ve MSE Değerleri

4. SONUÇLAR

Sosyal medya kullanımının artması ve teknolojinin günden güne ilerlemesi ile bilginin erişilebilirliği artmış ve bu durum üçüncü kişiler tarafından elde edilmesini istemediğimiz paylaşımlara da erişimi kolaylaştırmıştır. Kullanılan haberleşme uygulamaları veri güvenliğine ne kadar önem verip dikkat etse de dijital ortamda şifreleme algoritmasının kırılması veya veri kaynağına erişim imkansız değildir. Bu nedenle veri güvenliği için steganografi ile bizim için önemli olan veriler, başka bir örtü veri içerisine gizlenip asıl verinin varlığı gizlenir. Burada amaç, gizli veriye erişmeye çalışan üçüncü kişilerin karşısına asıl veri yerine bir görüntü vb. çıkararak yanıltılması ve şüphe oluşturmadan asıl verinin karşı tarafa iletilmesini sağlamaktır. Sır paylaşım ise bir sırrı bir grup üye arasında, her birine bir parça verecek şekilde dağıtma ve istenilen sayıda parçanın bir araya gelmesi ile sırrın yeniden elde edilmesini amaçlar. Geliştirilen sistemde; LSB yöntemi ile gizlenecek veri gönderilecek görüntü içerisine saklanmış ve Shamir sır paylaşım algoritması ile paylara bölünerek daha güvenli bir uygulama geliştirilmiştir. Paylar 3. şahıslar tarafından ele geçirilmiş olsa dahi k sayıda elde edilmediği sürece stego görüntü elde edilemez. k sayıda parça birleştirilmesi durumunda ise orijinal görüntü ile kıyaslama yapamayacakları için gizli veriye erişim imkânsız hale gelecektir.

İleriki çalışmalarda, kriptoloji yöntemlerinden faydalanarak gizlenecek verinin şifrelenmesi ayrıca pay görüntülerinin de şifrelenerek gönderilmesi planlanmaktadır.

KAYNAKÇA

[1] Sahu, A. K., & Swain, G. (2018). An improved data hiding technique using bit differencing and LSB matching. Internetworking Indonesia Journal, 10(1), 17-21.

[2] Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., & Jung, K. H. (2018). Image steganography in spatial domain: A survey. Signal Processing: Image Communication, 65, 46-66.

[3] Solak, S., "High embedding capacity data hiding technique based on EMSD and LSB substitution algorithms", IEEE Access, 8: 166513-166524, (2020).

[4] Ruchi, R., & Ghanekar, U. (2019, April). A Brief Review on Image Steganography Techniques. In Proceedings of the International Conference on Advances in Electronics, Electrical & Computational Intelligence (ICAEEC).

[5] Jin, X., Su, L., & Huang, J. (2021). A Reversible Data Hiding Algorithm Based on Secret Sharing. Journal of Information Hiding and Privacy Protection, 3(2), 69.

[6] Muhammad, Y. I., Kaiiali, M., Habbal, A., Wazan, A. S., & Sani Ilyasu, A. (2016). A secure data outsourcing scheme based on Asmuth–Bloom secret sharing. Enterprise Information Systems, 10(9), 1001-1023.

[7] Solak, S., Altınışık, U., "The least significant two-bit substitution algorithm for image steganography", International Journal of Computer (IJC), 31(1): 150-156, (2018).

[8] Sarosh, P., Parah, S. A., & Bhat, G. M. (2021). Utilization of secret sharing technology for secure communication: a state-of-the-art review. Multimedia Tools and Applications, 80(1), 517-541.

[9] Solak, S., & Altınışık, U. (2019). Image steganography based on LSB substitution and encryption method: adaptive LSB+ 3. Journal of Electronic Imaging, 28(4), 043025.

[10] Konyar, M. Z., & Solak, S. (2021). Efficient data hiding method for videos based on adaptive inverted LSB332 and secure frame selection with enhanced Vigenere cipher. Journal of Information Security and Applications, 63, 103037.

[11] Solak, S., & Altınışık, U. Image Steganography-Based GUI Design to Hide Agricultural Data. Gazi University Journal of Science, 34(3), 748-763.

[12] Sahu, A. K., & Sahu, M. (2020). Digital image steganography and steganalysis: A journey of the past three decades. Open Computer Science, 10(1), 296-342.

[13] Konyar, M. Z., & Öztürk, S. (2020). Reed solomon coding-based medical image data hiding method against salt and pepper noise. Symmetry, 12(6), 899.

[14] Sahu, A. K., & Sahu, M. (2016). Digital image steganography techniques in spatial domain: a study. International Journal of Pharmacy & Technology, 8(4), 5205-5217.

[15] Shamir, A. (1979). How to Share a Secret. Communications of the ACM, 22, 612-613.

[16] Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. Cryptography, 2(1), 1.

[17] Pang, L. J., & Wang, Y. M. (2005). A new (t, n) multi-secret sharing scheme based on Shamir's secret sharing. Applied Mathematics and Computation, 167(2), 840-848.

[18] Yang, C. C., Chang, T. Y., & Hwang, M. S. (2004). A (t, n) multi-secret sharing scheme. Applied Mathematics and Computation, 151(2), 483-490.