HORA 2019
www.horacongress.com

International Congress on Human-Computer Interaction, Optimization and Robotic Applications
July 5-7, 2019, Urgup, Nevşehir, Turkey

SETSCI
Conference Proceedings
www.set-science.com
4(5): 178-183, 2019

Hiding Data into an Image by Using Cryptography and Steganography

Coskun BALKESEN[1*] and Hasan Erdinc KOCER [2]

[1]*Information Technologies Engineering Dept., Natural and Applied Science Institute, Selcuk University, Turkey*
[2]*Electrical and Electronics Engineering Dept., Technology Faculty, Selcuk University, Turkey*
[*]*(c.balkesen@gmail.com)*

Abstract **–** Today, with the widespread use of communication technologies, the need for securing the information has increased. This study has been conducted to contribute to the security of information by taking advantage of two important areas of security, such as cryptography and steganography techniques. A major sub-branch of cryptography and data hiding, which is a password generation unit, has been handled with steganography subjects. It can be seen that data encryption and data hiding are mostly using in providing information security. In this study, a complementary application was developed by using cryptography and steganography methods together. Thus, a new effective method for data security has been introduced and the implementation is coded in Visual C # programming language. With the application of the data, a mathematical model determined for encryption. In addition to these, a special cryptographic USB (Universal Serial Bus) dongle is developed and defined for authorized persons. The techniques developed for encrypting and hiding the data were examined on the images with various resolution and format. As a result of implementation, use of mathematical model developed for ciphering and cloaking of the text increased the data security.

Keywords – Cryptography, Data Encryption, Data Hiding, Steganography, USB Dongle

I. INTRODUCTION

Information is a very important phenomenon for human beings. Information, which has become a storage and sharing, especially through the discovery of the writing, has become a tool used throughout history to generate income of civilizations, to win wars and to shape the development of civilizations. Competitions and rivalries in the progress of civilizations have shown that security of information is an inevitable necessity. Although this situation results in their understanding of data encryption / decryption and data hiding in other words, it has become modern and transferred to computer environment in parallel with the developments in information technologies. Especially with the developments in the internet world, which brings many people together on a common platform, regardless of time and space, it is possible for people who do not have access to information to access information between two users communicating with each other over the network. In the face of this situation, the encryption and concealment of data has become popular and has improved day by day.

Cryptography and steganography are two important methods of data hiding. The term cryptology is derived from the Greek words 'kryptos' (hidden) and 'logos' (word) ([2]). In this context, cryptology is a mathematical science that deals with the concealment and discovery of information ([13]). The main purpose of cryptology is to conceal the meaning of certain words, to ensure the safety of words, to protect the confidentiality ([9]).

The science of cryptology is divided into two subsystems. These are: Cryptography and cryptoanalysis ([16]). Cryptography is the process of making the data closed from the open state ([4]). In other words, cryptography is the meaninglessness of open text.

The term steganography is derived from the Greek words 'steganos' (hidden) and 'graphein' (writing) ([15]). Steganography is the art of sending a message or information to a destination by storing it in a suitable digital medium, in a way that no one but the target to be transmitted can notice. In steganography, a carrier object is needed to be used to hide dataThe carrier object to which information is hidden is called a cover object, and the object that is released after hiding is called a stego object ([11], [12], [14]). Steganography is not an encryption method, but it is a complement to encryption ([1]).

In the study [15], where cryptography and steganography were used together, the results of AES encryption algorithm were analyzed using 128, 192, and 256 bit keys. In addition, DES and AES encryption algorithms were applied on Steganography and an open text of 1.14 KB was encrypted separately with DES algorithm having 56 bit key value and AES encryption algorithms using 128 bit key. Embedded in the picture was carried out by LSB method.

In another study in which cryptography and steganography were used together [2], the patient's information on radiographic images used in the field of dentistry called OPT was encrypted with the cryptography method of the diagnoses and diagnoses to be used in the treatment. Then, an application has been developed to hide the encrypted data over OPT images and thus to avoid the problems of storage and loss. In the same application, in order to prevent counterfeiting, an application has been developed that hides the patient's identification number on the picture on the identity.

DOI: 10.36287/setsci.4.5.035

With the cryptography application developed in another study [7], the text to be encrypted with the keyword to be determined by the user is formed by creating a matrixIn the process of hiding the encrypted text into the image, a second password is provided as the security layer. In this study, RGB (Red Green Blue) channels were changed using only the least valued 2 bits of R and G channels. In this method, the bits of the data that are wanted to be hidden and encoded are placed in the last two bits of the byte values of the Red and Green color channels of the pixels forming the picture.

II. Materials and Method

In this study, it is aimed to hide high security data in the image by using cryptography and steganography methods together. The flow chart of the developed software are given in Figure 1.

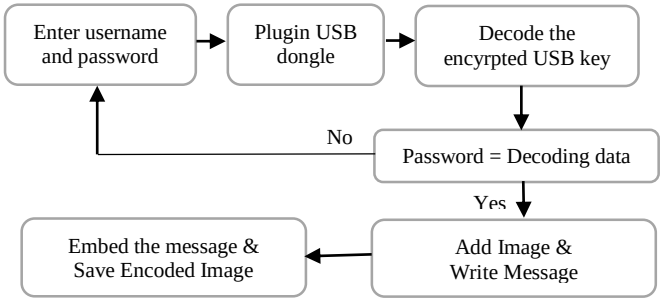


Fig 1. Flow chart of the system

A. *Management Side: Management Panel and USB Key Generation*

Access to the encryption and decryption screen is specific to users identified through the developed admin panel. Users registered in the database have a user name and password that allows them to access the encryption and decryption screen. Using the AES (256 bit) encryption algorithm from the management panel, the information of the user registered to the system database is encrypted and saved to the USB memory. In AES (256 bit) encryption, the number of loops is 14 and each loop consists of four layers: displacement of bytes, translation of rows, shuffling of columns, adding keys to the loop, respectively. User is prompted for user name and password for access to the encryption and decryption screen and The encrypted information on the USB memory device is decoded and compared with the information entered by the user. If the information on the USB memory does not match, access is blocked. This prevents users who are not registered to the database from accessing the software for encryption and decryption. This increases data security.

Figure 2 shows the management panel and Figure 3 shows the USB key generation process.

B. *User Side: Encryption / Hiding, Decrypting / Revealing*

The method evaluated and suggested during the cryptography phase of the study is AES (256 bit) encryption. AES (256 bit), which is used to decrypt the user-defined password in the USB key generation process, has also been used to decrypt the data to be hidden. Data hiding is usually done on 24-bit images. In 24-bit images, each pixel consists of three primary colors. These colors are red (R), green (G), blue (B). Pixel color is obtained by mixing these colors.

In 24-bit images, the pixel color value is called the RGB value of that pixel.

Since red, green and blue are each expressed as 8 bits, 3 bytes per pixel are used in 24-bit images. This means 16 million different colors for each pixel ([8]).

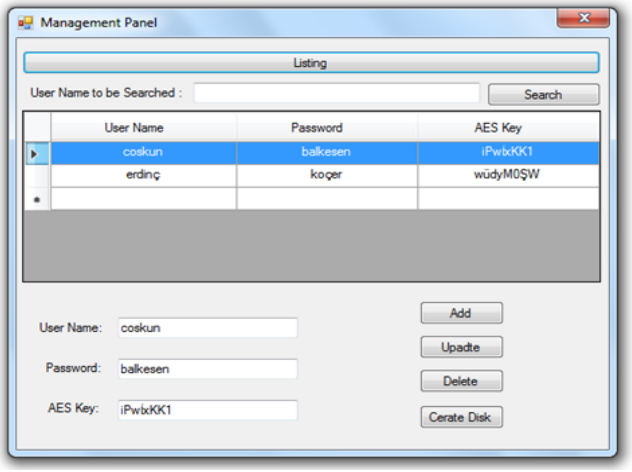


Fig 2. Management panel window

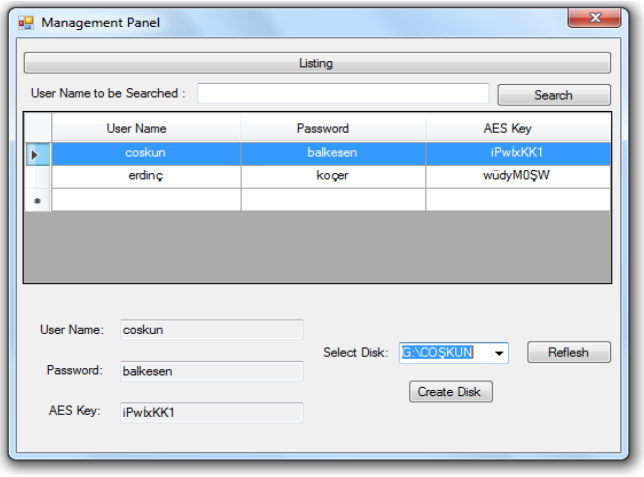


Fig 3. USB key generation process

In a 24-bit image (Figure 4), each color is expressed as binary codes that can range from 0 to 255. For example, the RGB code of a turquoise pixel, R = 48 = $(00110000)_2$, G = 214 = $(11010110)_2$, B = 200 = $(11001000)_2$ shaped ([10]).

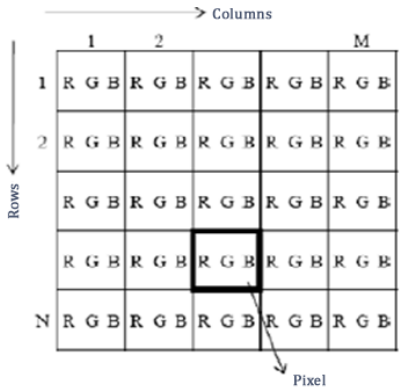


Fig 4. Structure of a 24-bit color digital image

The LSB method is called the Least Significant Bit Insertion Methods. In this method; the pixels on which the

data will be embedded are selected sequentially, not according to a particular algorithm. It is based on the placement of the next bit of data to be hidden in the last bit of each byte, ie the least significant bit of each selected pixel. When the data embedding is complete, it is not possible to know how many characters the text consists of during the embedding of the embedded data. A sign character is added to the end. The change in the pixel during the change process is 0 at best, ± 1 at worst. In this case, the difference between the cover object and the stego image cannot be perceived by the human ([10], [5]).

In the case of steganography (hiding), the proposed method is to perform LSB in reverse order. In the application where the data to be hidden may be rendered meaningless by the AES encryption algorithm, the data is hidden in the image by the reverse implementation of my LSB method. Pixels selected for data hiding are determined by the original mathematical model specified below.

bmp.width, width of picture,

k= vertical index of the selected pixel and starting value 0 on each line;

$$k = k + ((bmp.width)/3) \quad (1)$$

Table 1 shows an example of embedding an 8-bit letter "C 3 in a pixel of 144 pixels in 3 pixels.

Table 1. Embedding the 8 bit data

Data to Hide:	"C" letters (ASCII = 67= (01000011)$_2$)		
Original Picture Pixels	Color Channels		
	R	G	B
1.Pixel (indices 0)	00100111	11101001	11001000
2.Pixel (indices 48)	00100111	11001000	11101001
3.Pixel (indices 96)	11001000	00100111	11101001
Gizleme Sonrası Pixelleri	R	G	B
1.Pixel (indices 0)	00100110	11101001	11001001
2.Pixel (indices 48)	00100110	11001000	11101000
3.Pixel (indices 96)	11001000	00100111	11101000

The software developed given in Figure 5 shows the screen where the text can be hidden or directly hidden into the image. If the text is to be saved with encryption, the password must be entered in the if Encryption "section. In the same window, "Data Extraction" button is clicked to switch to the window where hidden data will be revealed. In reverse order of encryption and cloaking, confidential data is revealed.

III. Results

The measure of the change in the cover object is very important when evaluating a steganographic algorithm. the known measuring methods for determining the change rate of deterioration in cover or object: MSE (Mean Squared Error) and PSNR (Peak Signal to Noise Ratio). Histogram graph is also used to determine the durability.

MSE is a test based on average square error, which is frequently used to measure the difference between two sets of numbers. The average squared error is calculated with the formula (2), with the source image x in size M x N and the embedded image y with data.

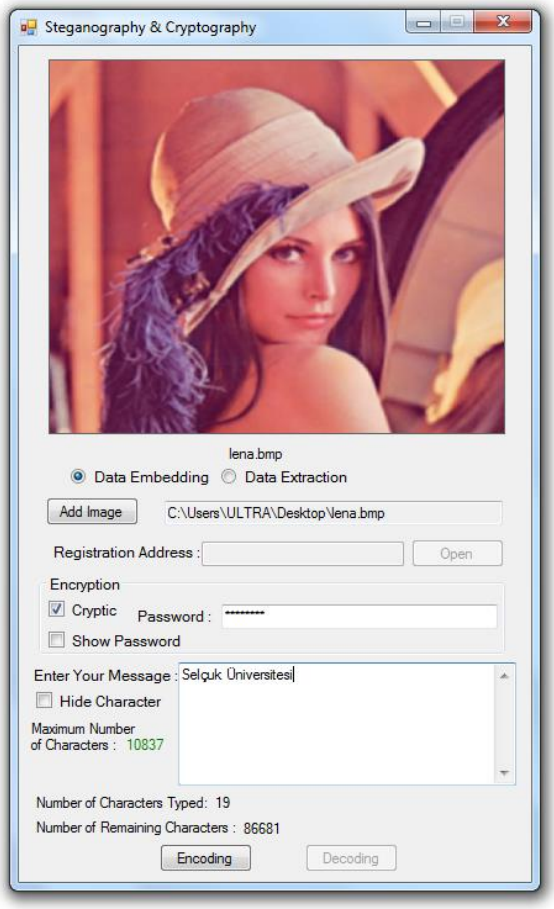


Fig 5. Data embedding and extraction window

$$MSE = \left(\frac{1}{M \times N}\right) \sum_{i=1}^{M} \sum_{j=1}^{N} (x_{ij} - y_{ij})^2 \quad (2)$$

An important factor that distorts the image quality is noise. An input image is taken as a reference for the calculation of the PSNR and an output image is compared to the input image to measure the noise level in the input image. The original images are distorted in a controlled manner, then the signal to noise ratios of the original and distorted images are compared. A higher PSNR means higher image quality. A low PSNR represents a high numerical difference between images ([3], [6]).

$$PSNR = 10 \times \log\left(\frac{255^2}{MSE}\right) (dB) \quad (3)$$

The developed method is coded with Visual Studio software in .NET Framework 4.7 environment with C # programming language. The different resolutions were tested on 4 images in color format and 12 images in 3 different image formats, hiding 275 characters for each image (Figure 6). MSE values of each color channel obtained as a result of the test are shown in Table 2, PSNR values are shown in Table 3 and histogram graphs are shown in Figure 7.

a)lena (512*512 pixel) b) grilena (512*512 pixel) c) meyve (630*428 pixel) d) tatil (1440*920 pixel)

Fig 6. Pictures used for testing

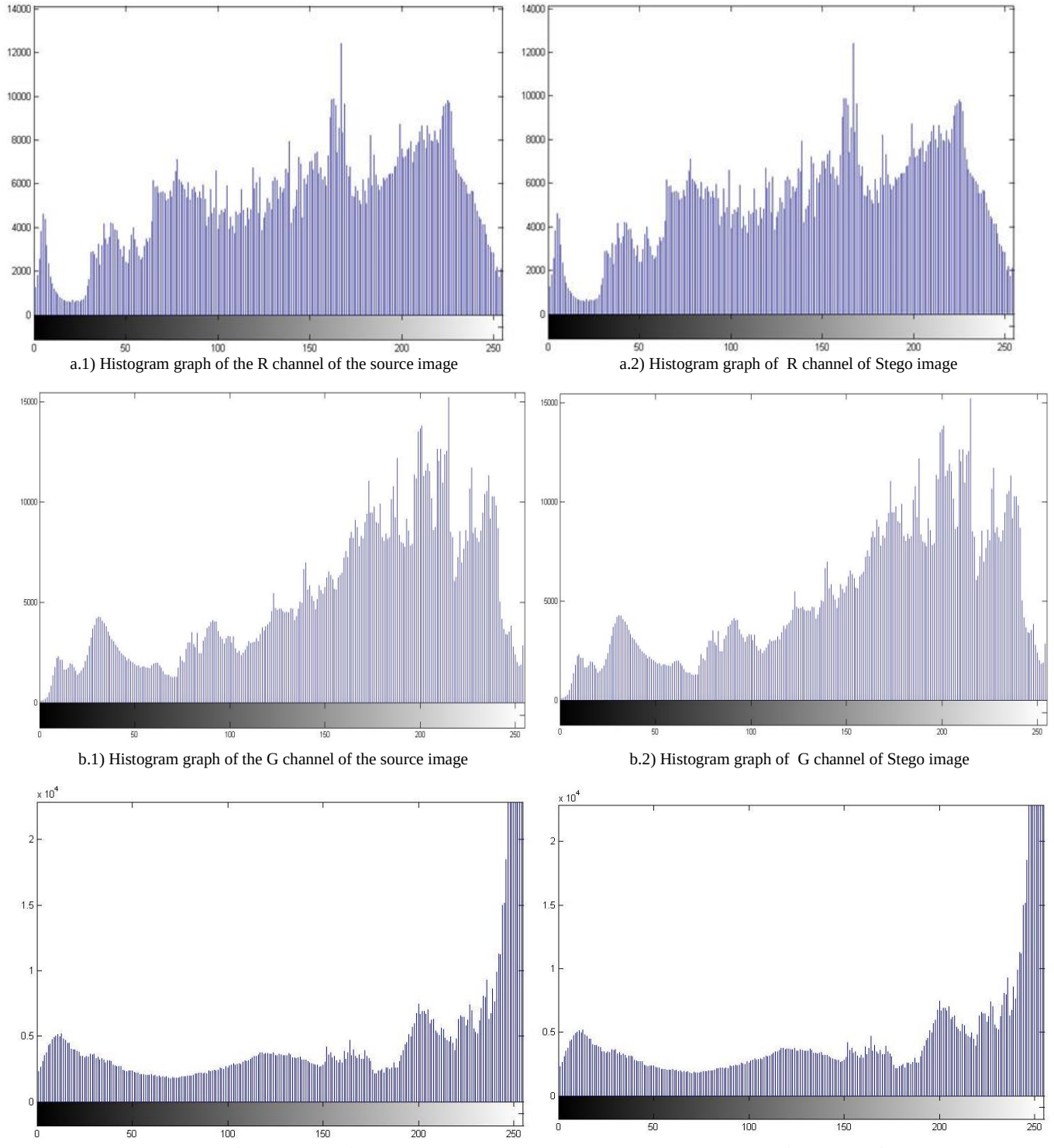
Table 2. MSE ratios between information hidden images and original image

Cover Object		Stego Object		MSE		
File Name	File Size (Bayt)	File Name	File Size (Bayt)	R	G	B
lena.jpg	70.243	lenajstg.png	512.495	0,0021781	0,0021362	0,0020751
		lenajstg.bmp	786.486	0,0021553	0,0021209	0,0020751
lena.png	882.334	lenapstg.png	553.945	0,0021324	0,0020751	0,0020675
		lenapstg.bmp	1.048.630	0,0021286	0,0021209	0,0020942
lena.bmp	786.486	lenabstg.png	511.628	0,0021629	0,0021133	0,0020599
		lenabstg.bmp	786.486	0,0021286	0,0021171	0,0020446
meyve.jpg	72.377	myvjstg.png	755.112	0,0022214	0,0021287	0,0020175
		myvjstg.bmp	809.830	0,0021992	0,0021139	0,0019433
meyve.png	1.525.333	myvpstg.png	850.304	0,0022288	0,0021102	0,0019915
		myvpstg.bmp	1.078.614	0,0022659	0,0021473	0,0019804
meyve.bmp	809.830	myvbstg.png	219.079	0,0023030	0,0020026	0,0021287
		myvbstg.bmp	809.830	0,0022734	0,0019730	0,0021213
tatil.jpg	149.217	tatiljstg.png	2.012.662	0,0004370	0,0004445	0,0004400
		tatiljstg.bmp	3.974.454	0,0004355	0,0004400	0,0004491
tatil.png	3.415.401	tatilpstg.png	2.152.276	0,0004355	0,0004310	0,0004498
		tatilpstg.bmp	5.299.254	0,0004362	0,0004445	0,0004483
tatil.bmp	3.974.454	tatilbstg.png	2.002.957	0,0004393	0,0004378	0,0004415
		tatilbstg.bmp	3.974.454	0,0004249	0,0004325	0,0004453
grilena.jpg	32.911	grilenajstg.png	237.133	0,0021324	0,0020103	0,0021934
		grilenajstg.bmp	786.486	0,0021896	0,0020866	0,0021934
grilena.png	385.253	grilenapstg.png	230.122	0,0021362	0,0020484	0,0021591
		grilenapstg.bmp	1.048.630	0,0021209	0,0020294	0,0021553
grilena.bmp	786.486	grilenabstg.png	109.863	0,0022125	0,0018348	0,0026359
		grilenabstg.bmp	786.486	0,0022163	0,0018692	0,0026397

Table 3. PSNR ratios between information hidden images and original image

Cover Object		Stego Object		PSNR		
File Name	File Size (Bayt)	File Name	File Size (Bayt)	R	G	B
lena.jpg	70.243	lenajstg.png	512.495	74,749841	74,834322	74,960213
		lenajstg.bmp	786.486	74,795718	74,865454	74,960213
lena.png	882.334	lenapstg.png	553.945	74,842084	74,960213	74,976209
		lenapstg.bmp	1.048.630	74,849860	74,865454	74,920479
lena.bmp	786.486	lenabstg.png	511.628	74,780372	74,881105	74,992265
		lenabstg.bmp	786.486	74,849860	74,873272	75,024554
meyve.jpg	72.377	myvjstg.png	755.112	74,664378	74,849527	75,082657
		myvjstg.bmp	809.830	74,708099	74,879898	75,245333
meyve.png	1.525.333	myvpstg.png	850.304	74,649902	74,887524	75,138903
		myvpstg.bmp	1.078.614	74,578234	74,811861	75,163234
meyve.bmp	809.830	myvbstg.png	219.079	74,507730	75,114709	74,849527
		myvbstg.bmp	809.830	74,564042	75,179530	74,864686
tatil.jpg	149.217	tatiljstg.png	2.012.662	81,725521	81,651153	81,695621
		tatiljstg.bmp	3.974.454	81,740548	81,695621	81,607137
tatil.png	3.415.401	tatilpstg.png	2.152.276	81,740548	81,785945	81,599844
		tatilpstg.bmp	5.299.254	81,733028	81,651153	81,614442
tatil.bmp	3.974.454	tatilbstg.png	2.002.957	81,703076	81,718026	81,680748
		tatilbstg.bmp	3.974.454	81,847222	81,770760	81,643786
grilena.jpg	32.911	grilenajstg.png	237.133	74,842084	75,098096	74,719524
		grilenajstg.bmp	786.486	74,727083	74,936329	74,719524

grilena.png	385.253	grilenapstg.png	230.122	74,834322	75,016459	74,788038
		grilenapstg.bmp	1.048.630	74,865454	75,057086	74,795718
grilena.bmp	786.486	grilenabstg.png	109.863	74,681922	75,494752	73,921422
		grilenabstg.bmp	786.486	74,674441	75,414242	73,915141



a.1) Histogram graph of the R channel of the source image

a.2) Histogram graph of R channel of Stego image

b.1) Histogram graph of the G channel of the source image

b.2) Histogram graph of G channel of Stego image

c.1) Histogram graph of the B channel of the source image

c.2) Histogram graph of B channel of Stego image

Fig 7. Source images and histograms of R channels of the hidden image

IV. DISCUSSION

When the findings in Table 3 and Table 4 are examined, it shows that the distortion is minimal when data with .bmp extension is used as source image and the resulting stego image is saved as .bmp. The fact that the MSE values are low and the PSNR values are high between the image selected as the cover object and the stego image prove this situation.

Another result obtained from the study is that if the selected source image is at high resolution, there is no difference between the source image and the stego image when the MSE value is low and the PSNR value is high. It is another conclusion that the proposed method is more

effective in applications where high resolution source images are used.

In addition, when the histogram graphs of the color channels of the cover object and the stego object shown in Figure 7 are examined, no difference between the graphs indicates that the proposed method is durable.

V. CONCLUSION

Steganography algorithms are frequently used in data security. At the center of these algorithms is the most insignificant bit embedding algorithm. The least significant burial method is the least destructive method on the covering object. However, the sequential embedding of this method increases the detectability of the data. In order to avoid this situation, original models and encryption techniques can be used. In the process of hiding with the original model, it will be more difficult to obtain the actual text, since it will be meaningless if the information is detected by decreasing the detectability of the information.

Access to encryption and decryption operations via a USB key application and connected to a hardware unit was another factor that increased security. Thus, access to the software is prevented for people who do not have a defined hardware.

Table 4 shows the advantages and disadvantages of the proposed method.

Table 4. Advantages and disadvantages of the proposed method

Advantages	Disadvantages
Not exactly noticeable with the eye.	Data security is compromised if the original mathematical method is solved.
It is easy to apply.	
It is safer because data hiding is performed with an original mathematical model and in a sequence different from the known methods.	
Hiding can be made by making the data encryption meaningless. This increases the security of data. Because the hidden data will be meaningless even if it is decoded.	
The security of the software is provided with the created USB key.	

ACKNOWLEDGMENT

This paper belongs to Coskun BALKESEN's master's thesis titled High Security Data Hiding In Image By Using Cryptography And Steganography Methods at the Department of Information Technologies of Selcuk University Institute of Natural & Applied Science.

REFERENCES

[1] Anderson, R., 1997, Information Hiding, Stretching the Limits of Steganography 39-48.

[2] Aydoğan, M., 2014, Adli Bilişimde Görüntü Üzerine Kriptografi Uygulamalari, Yüksek Lisans Tezi, *Fırat Üniversitesi*, Elazığ, 88.

[3] Boztoprak, H., 2016, Kenar Geişleri Kullanılarak Görüntüdeki Bulanıklığın Giderilmes, *SDU International Journal of Technological Science*, 8 (2), 28-36.

[4] Coşkun, A. ve Ülker, Ü., 2013, Ulusal Bilgi Güvenliğine Yönelik Bir Kriptografi Algoritması Geliştirilmesi ve Harf Frekans Analizine Karşı Güvenirlik Tespiti, *Bilişim Teknolojileri Dergisi*, 6 (2), 31-39.

[5] Demirci, B., 2016, Görüntü Steganografi Metotları ve Performanslarının Karşılaştırılması, Yüksek Lisans Tezi, *Selçuk Üniversitesi*, Konya, 83.

[6] Kılıçaslan, M., Tanyeri, U. ve Demirci, R., 2018, Renkli Görüntüler İçin Tek Boyutlu Histogram, 6, 1094-1107.

[7] Koçak, C., 2015, Kriptografi ve Stenografi Yöntemlerini Birlikte Kullanarak Yüksek Güvenlikli Veri Gizleme, *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 31 (2), 115-123.

[8] Morkel, T., Eloff, J. H. P. ve Olivier, M. S., 2005, An overview of image steganography. Proceedings of the ISSA 2005 New Knowledge Today Conference. Sandton**:** 1-11.

[9] Oppliger, R., 2005, Contemporary Cryptography *Norwood*, Artech House Publishers p. 1-3.

[10] Öztürk, E., Mesut, A. Ş. ve Mesut, A., 2011, LSB Ekleme Yönteminde Bilgi Gizleme İçin Tek Renk Kanal Kullanımının Güvenliğe Etkileri. IV.Ağ Ve Bilgi Güvenliği Ulusal Sempozyumu. Ankara, Ankara.

[11] Petitcolas, F. A. P., Anderson, R. J. ve Kuhn, M. G., 1999, Proceedings of the IEEE, Information Hiding—A Survey 1062-1078.

[12] Razavi, N., 2017, LSB Steganografi Yönteminde Yüksek Kapasiteli Veri Gizleme, Yüksek Lisans Tezi, *Gazi Üniversitesi*, Ankara.

[13] Soyalıç, S., 2005, Kriptografik Hash Fonksiyonlari ve Uygulamaları, Yüksek Lisans, *Erciyes Üniversitesi*, Kayseri, 92.

[14] Şahin, A., Buluş, E. ve SAKALLI, M. T., 2006, Gri Seviye Resimler Üzerinde Rasgele LSB Yöntemini ve Sayı Teorisini Kullanarak Bilgi Gizleme Ve Steganaliz, *Bilgi Teknolojileri Kongresi IV / Akademik Bilişim 2006*, Denizli.

[15] Yerlikaya, T., 2006, Yeni Şifreleme Algoritmalarının Analizi, Doktora Tezi, *Trakya Üniversitesi*, Tekirdağ, 139.

[16] Yılmaz, R., 2010, Kriptolojik Uygulamalarda Bazi İstatistik Testler, Yüksek Lisans Tezi, *Selçuk Üniversitesi*, Konya, 135.