Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı, S. 123-130, Eylül 2020

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue, pp. 123-130, September 2020

Research Article

Embedding Encrypted Data into an Image with a Random Pixel Layout Approach

Coşkun Balkesen[1*], Hasan Erdinç Koçer[2]

[1] Selçuk Üniversitesi, Teknoloji Fakültesi, Bilgisayar Mühendisliği Bölümü, Konya, Türkiye (ORCID: 0000-0002-8580-6825)
[2] Selçuk Üniversitesi, Teknoloji Fakültesi, Elektirk ve Elektronik Mühendisliği Bölümü, Konya, Türkiye (ORCID: 0000-0002-0799-2140)

(1st International Conference on Computer, Electrical and Electronic Sciences ICCEES 2020 – 8-10 October 2020)

(**DOI:** 10.31590/ejosat.802191)

ATIF/REFERENCE: Balkesen, C. & Koçer, H. E. (2020). Embedding Encrypted Data into an Image with a Random Pixel Layout Approach. *European Journal of Science and Technology*, (Special Issue), 123-130.

Abstract

With the recent developments in information and communication technologies, data is transferred to digital environments. However, it has become very important to protect the information in digital environments. This situation raises the need for information security. Cryptography and steganography are among the most effective areas in ensuring information security. This study was carried out in order to contribute to information security by using cryptography at the point of making data meaningless by encrypting, and steganography at the point of hiding meaningless data. In this study, random pixel layout approach is used to hide the encrypted data into a 24-bit image. The proposed technique was examined on images with different file types and resolutions. The Structural Similarity Index Measure (SSIM), Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) parameters were revealed to measure the effectiveness of the proposed approach. It has been observed from the application that this method increases the security level of embedding data process.

Keywords: Cryptography, Data encryption, Data hiding, Steganography, Random pixel.

Şifrelenmiş Verileri Rast Gele Piksel Yaklaşımı ile Bir Görüntüye Gömme

Öz

Bilgi ve iletişim teknolojilerindeki son gelişmeler ile veriler dijital ortamlara aktarılmaktadır. Bununla beraber dijital ortamlarda yer alan bilgilerin korunması oldukça önemli hale gelmiştir. Bu durum bilgi güvenliği ihtiyacını artırmaktadır. Bilgi güvenliğinin sağlanmasında en etkili alanlar arasında kriptografi ve steganografi yer almaktadır. Bu çalışma, verilerin şifrelenerek anlamsız hale getirilmesi noktasında kriptografi, anlamsız verilerin gizlenmesi noktasında ise steganografi kullanılarak bilgi güvenliğine katkı sağlamak amacıyla yapılmıştır. Bu çalışmada, şifrelenmiş verileri 24 bitlik bir görüntüye gizlemek için rastgele piksel düzeni yaklaşımı kullanılmıştır. Önerilen teknik, farklı dosya türleri ve çözünürlüklere sahip görüntüler üzerinde incelenmiştir. Önerilen yaklaşımın etkinliğini ölçmek için Yapısal Benzerlik İndeksi Ölçümü (SSIM), Ortalama Kare Hata (MSE) ve Pik Sinyal Gürültü Oranı (PSNR) parametreleri ortaya çıkarılmıştır. Uygulamadan bu yöntemin veri gömme işleminin güvenlik seviyesini artırdığı gözlemlenmiştir.

Anahtar Kelimeler: Kriptografi, Veri şifreleme, Veri gizleme, Steganografi, Rastgele piksel.

[*] Corresponding Author: Selçuk Üniversitesi, Teknoloji Fakültesi, Bilgisayar Mühendisliği Bölümü, Konya,, Türkiye, ORCID: 0000-0002-8580-6825, c.balkesen@gmail.com

1. Introduction

Information, every period of history is to confront human beings as a significant phenomenon. In fact, the reason for many important events in history that can cause the destiny of many civilizations to change and even the age to close and the era to open is actually knowledge. Since the discovery of the article, the security of the information that can be shared and stored has always been in question. Methods were applied to ensure the security of information in every period. Information has been transferred to the computer environment with the digitalization of information and technological developments. Parallel to these developments, modern approaches and methods have been developed to ensure the security of information in the computer environment. Internet networks have expanded considerably with the recent developments in the internet world. Thus, many people can gather on the same platform regardless of time and place. This situation threatens the security of information in digital environments. Encryption and hiding methods, which are very popular today, have been developed in order to eliminate the threats to information security by preventing unauthorized access to information.

Cryptology is a mathematical science that deals with hiding and revealing information (Soyalıç, 2005). It is known that the main purpose in cryptology is to hide the meaning of certain words, to ensure the security of words, to protect their privacy (Oppliger, 2005). Cryptology has two main sub-branches; Cryptography and Cryptoanalysis. Cryptography is about encryption. It is the process of making open data meaningless by encrypting it. Since the information encrypted with the cryptography process will be meaningless even if it is captured by third parties, the real information is protected and third parties are prevented from accessing real information. Cryptoanalysis is the process of deciphering encrypted information. It is the conversion of the information that is encrypted and made meaningless by the sender to open form. It is the reverse of the cryptography process.

There are different approaches to data encryption. Cryptography algorithms are examined under two main headings according to key usage patterns. These are symmetric (private key) and asymmetric (public key) encryption algorithms. The same key is used for data encryption and data decryption in symmetric encryption algorithms. AES (Advanced Encryption Standard) and DES (Data Encryption Standard) are examples of symmetric encryption algorithms. There are two different keys in asymmetric encryption algorithms. The keys used for decryption and encryption processes in asymmetric encryption algorithms are different. Hence, public and private key pairs are unique for each user. RSA (Ron Rivest, Adi Shamir, Leonard Adleman) and DSA (Digital Signature Algorithm) algorithms are commonly used asymmetric encryption algorithms in literature (Kodaz & Botsalı, 2010).

The AES method is the most used method in cryptography method. AES is known as the standard Rijndael algorithm. A symmetric key with high efficiency in terms of security and speed is block cipher (Chan & Cheng, 2004; Sarmah & Bajpai, 2010; Seth, Ramanathan, & Pandey, 2010). AES is of three types according to the key size used and named as "AES-128", "AES-192" and "AES-256".

Steganography is data hiding. It is defined as the art of sending a message or information to the destination in a way that no one but the recipient will notice. In the steganography process, the environment where the data will be hidden is needed. The carrier object that contains data is called a cover object. The cover object can be in different file types depending on the steganography area to be applied. The object that is revealed after the hiding process is called a stego object (Petitcolas, Anderson, & Kuhn, 1999). Although steganography is not an encryption method, it is a complementary element to encryption (Anderson, 1997).

Although there are various methods in the field of image steganography, LSB (Least Significant Bit) method, which minimizes the distortion in the image, is a prominent method. Because the data hidden in the picture should not be noticed. A noticeable deterioration in the picture endangers the security of the information it contains.

2. Material and Method

In the study, it was aimed to embed the encoded data in randomly selected pixels in the image by using cryptography and steganography methods together. AES was chosen as the encryption algorithm and LSB method was chosen for the embedding of the encrypted data. It is aimed to increase data security by randomly selecting the pixels to be used to hide the data in the image. The software belonging to the developed method was created through Visual Studio.Net. The algorithm steps for the software developed are included in Table 1.

Table 1. Algorithms Steps of the Software Developed

Step	Process
Step 1:	Get matte object (image)
Step 2:	Get the information to be hidden
Step 3:	Encrypt information with AES
Step 4:	Randomly select pixels to hide data
Step 5:	Embed data in R, G and B channels of selected pixels by LSB method
Step 6:	Encrypt pixel values for selected pixels
Step 7:	Embed pixel values selected according to the original mathematical model

2.1. AES-256 Encryption Algorithm

The AES-256 encryption algorithm uses a 256-bit long key. The number of turns depends on the key length and is 14. 128-bit data blocks are used for encryption of data (Stinson, 2006). In the AES-256 encryption algorithm, a 128-bit data block is converted into a 4×4 byte matrix. After this process, the following operations are performed in each cycle (Smith, 2010).

a) Replacement of bytes (Sub-Bytes transformation)
b) Translation of lines (Shift-Rows transformation)
c) Mixing columns (Mix-Columns transformation)
d) Adding a key to the loop (Add RoundKey transformation)

In AES encryption algorithm, the decryption process is done by replacing the rows in the encryption, shifting of bytes, shuffling of columns with inverse operations. The point to note here is that the key conversion is the inverse itself (Sakallı, 2006).

2.2. Structure of Digital Picture

The smallest significant unit of a digital image is a pixel. In 24-bit images, each pixel is the result of the combination of three primary colours. These colours are red (red, R), green (green, G), blue (blue, B). The resulting colour value is also the RGB value of the pixel. Each colour is expressed in 8 bits. In this case, it can be said that there are 16 million colour options for each pixel in 24-bit images (Morkel, Eloff, & Olivier, 2005).

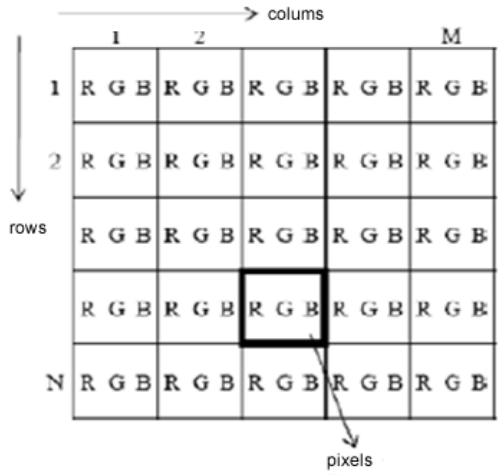


Figure 1. Structure of 24-bit colour digital picture

2.3. LSB Method

LSB method is the method of adding the least important bit. It occurs by replacing the least significant bit, which is the last bit of each byte of each pixel selected, with the least significant bit of the next character of the data to be hidden. In this case, the change in the colour channels of the pixels is ± 1 at worst and 0 at best. As a result of the concealing process, the difference between the cover object and the stego image is a degree that cannot be distinguished by the human eye. Table 2 contains an example of embedding the 8-bit letter "C" into 3 pixels in a 24-bit digital image.

Table 2. Sample Bit Embedding

Data to be hidden:	**"C" letter (ASCII = 67= (01000011)$_2$)**		
Original Picture	**Colour Channels**		
Pixels	R	G	B
1.Pixel	00100111	11101001	11001000
2.Pixel	00100111	11001000	11101001
3.Pixel	11001000	00100111	11101001
After Hiding Pixels	R	G	B
1.Pixel	0010011<u>0</u>	11101001	1100100<u>1</u>
2.Pixel	0010011<u>0</u>	11001000	1110100<u>0</u>
3.Pixel	11001000	00100111	1110100<u>0</u>

2.4. Developed Method

With the method developed in this study, the process of hiding data into the image is not directly hidden, but by encrypting with the AES-256 encryption method. Since AES-256 is a symmetric encryption algorithm, the same key is needed for data encryption and decryption. Key must be 256 bit 32 characters. While users create 8 characters of the 32-character key in accordance with the principles of password security, the other characters are completed by the software and the key is created. The ASCII binary equivalent of the next character of the encrypted data is obtained. The ASCII counterpart of the character is divided into bits and embedded in the image with the LSB method. The pixels to be embedded in data are randomly selected by software. In order to reach the correct data during the decoding of the hidden data, the pixel information selected in the data hiding stage is hidden in the image with the original mathematical model shown in the expression (1).

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

Here, bmp.width is a width of the picture, k is the vertical index of the selected pixel and the starting value of 0 in each row. Figure 2 shows the screen shot of the software developed.

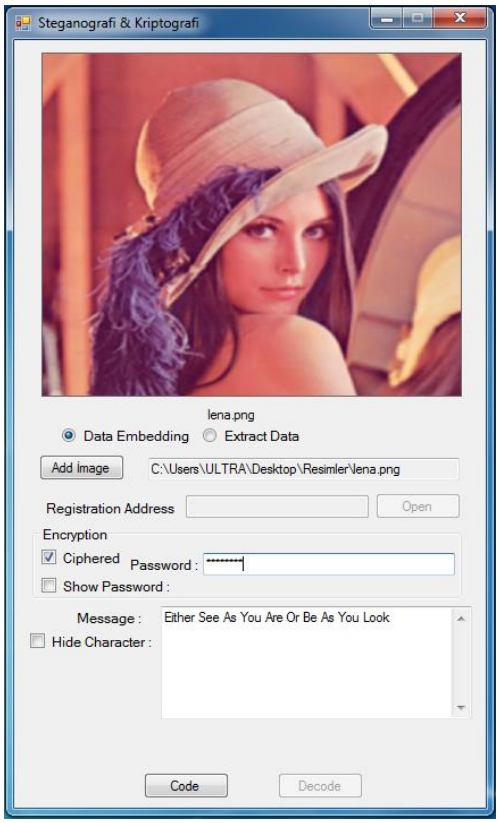


Figure 2. Image of the software developed

3. Results and Discussion

The difference between cover object and stego object is very important for evaluating a steganography application. It can be said that the less the change in the cover object, the higher the success of the said steganography algorithm. In particular, there should not be any visible change in the stego object obtained in image steganography.

The most known measurement methods for determining the change in the cover object, in other words the rate of distortion in image steganography applications are MSE (Mean Squared Error), PSNR (Peak Signal to Noise Ratio) and SSIM (Structural Similarity Index Measure).

MSE is used to measure between two strings of numbers. It is a test based on mean square error. Pixels in the images are treated as a matrix of size M x N. The mean square error is calculated by the formula (2) with the source picture x and the data embedded picture y.

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

Noise is one of the important factors that determine image quality. PSNR is used to reveal the quality difference between the original image and the compressed image. PSNR is a measurement showing the ratio of the maximum possible power of the original

image to the strength of the compression error on the original image. It can be expressed as the calculation of the highest signal to noise ratio among images (Karaca, 2007). It is measured in decibels. In the calculation of PSNR, the noise ratios of the cover object and the stego object are compared. Calculation of PSNR is given in equation (3).

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

SSIM is a method used for similarity between two images. The SSIM index acknowledges that one of the two images compared is of excellent quality. In this case, one of the two images acts as the quality image of the other. Since PSNR and MSE measurements do not exactly fit human eye perception, SSIM was designed as an alternative to them. The equations used for SSIM measurement are given below. Structural similarity index; μ_x, μ_y, σ_x, σ_y and σ_{xy} are calculated by the connection in the expression (7), namely local averages, standard deviations, cross covariances and I brightness (4), c contrast (5), s structure (6), respectively.

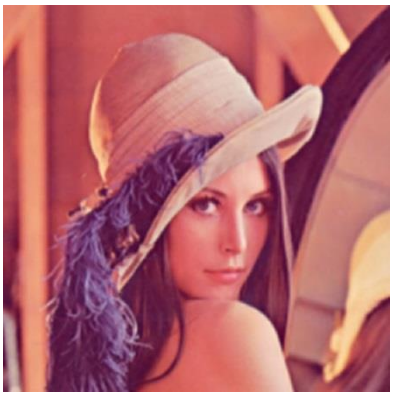
$$l(x,y)=\frac{2\mu_x\mu_y+c_1}{\mu_x^2+\mu_y^2+c_1} \tag{4}$$

$$c(x,y)=\frac{2\sigma_x\sigma_y+c_2}{\sigma_x^2+\sigma_y^2+c_2} \tag{5}$$

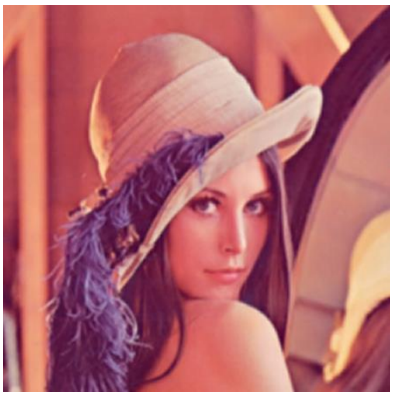
$$s(x,y)=\frac{\sigma_{xy}+c_3}{\sigma_x\sigma_y+c_3} \tag{6}$$

$$SSIM(x,y)=[\,l(x,y)\,]^{\alpha}+[\,c(x,y)\,]^{\beta}+s(x,y)^{\gamma} \tag{7}$$

With the help of the software developed for the determined method, the advice of Mevlana Celaleddin-I Rumi "Either See As You Are Or Be As You Look" has been embedded in five images with different resolutions. The images used as the cover object and the resulting stego images are shown in Figure 3. MSE, PSNR and SSIM measurements were made. MSE and PSNR values are given in Table 3, SSIM values are given in Table 4.

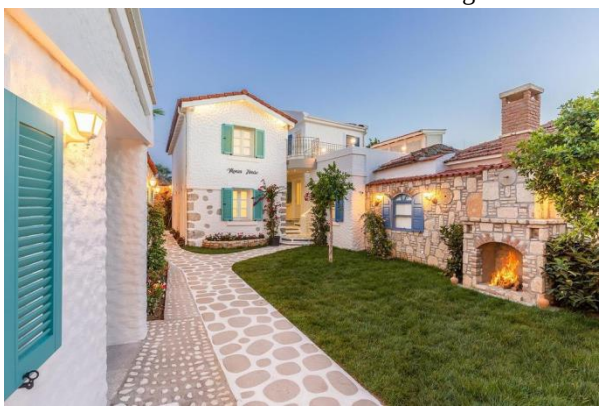


(a) lena

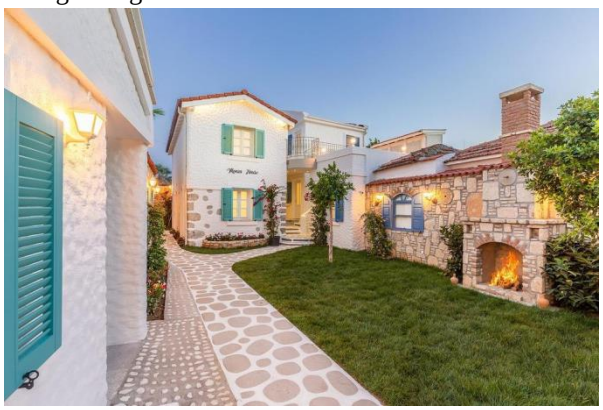


(b) stglena

Figure 3. Cover object and stego images



(c) house



(d) stghouse

(e) flowers

(f) stgflowers

(g) airplane

(h) stgairplane

(i) fruit

(j) stgfruit

Figure 3. Cover object and stego images

Table 3. MSE and PSNR Values Between Information Hidden Images and Original Image

Cover Object		**Stego Object**	**MSE**			**PSNR**		
File Name	**Resolution**	**File Name**	**R**	**G**	**B**	**R**	**G**	**B**
lena	512*512	stglena	0,0010452	0,0010529	0,0010643	77,860163	77,906932	77,93881
house	650*344	stghouse	0,0003973	0,0003782	0,0003483	82,711269	82,353588	82,139618
fruit	1440*600	stgfruit	0,0003299	0,0003391	0,000331	82,932524	82,827526	82,94698
flowers	690*450	stggrilena	0,0008921	0,0008986	0,000934	78,427335	78,595139	78,626668
airplane	2560*1600	stgplane	0,0000652	0,0000669	0,0000691	89,736023	89,876542	89,988328

Table 4. SSIM Values

Cover Object		Stego Object	SSIM
File Name	**Resolution**	**File Name**	
lena	512*512	stglena	0,9983
house	650*344	stghouse	0,9984
fruit	1440*600	stgfruit	0,9994
flowers	690*450	stgplane	0,9983
airplane	2560*1600	stgflowers	0,9996

When the data in Table 3 are examined, it is seen that MSE values are low and PSNR values are high. Low MSE and high PSNR value indicates minimal distortion in the picture. In addition, the fact that the SSIM values in Table 4 are very close to one is an indication that the difference between cover objects and stego objects is almost negligible. It is important for information security to embed data in the cover object in a way that causes the least disruption. The MSE, PSNR and SSIM values obtained support that the proposed method is effective at this point.

An important result obtained is that MSE, PSNR and SSIM values are related to resolution. As can be seen in Table 3 and Table 4, as a result of using images with high resolution as a cover object, MSE values were lower, PSNR values were higher and SSIM values were closer to one. Based on this, it is possible to say that the proposed method is more effective in high resolution images.

Table 5 includes the results of four different studies on Cryptography and Steganography and the results of the study made with the proposed method. In order to make the comparison healthy, data close to the amount of data hidden in other studies were hidden in the image named Lena at the same resolution. When the table is examined, it is seen that although the amount of data hidden in the study was high, the PSNR and SSIM values were high. This situation shows that the developed method gives better results.

Table 5. Comparison With Other Studies

Steganographic Studies	Test Picture	Hidden Data (bit)	PSNR (dB)	SSIM
1. Lin et al. (Lin, Chang, & Lie, 2010)	Barbara	53248	27,03	0,9933
2.Swain and Lenka (Swain & Lenka, 2012)	Lena	20032	53,78	0,9996
3.Doğan et al. (Doğan, Dağ, & Türkoğlu, 2016)	Lena	12282	34,34	0,9971
This study	Lena	42280	51,29	0,9800

4. Conclusions and Recommendations

Steganography and cryptography algorithms are frequently used algorithms to ensure data privacy and security. Using steganography algorithms alone causes the data to remain open. With the use of cryptography algorithms alone, data is encrypted and becomes meaningless, but the element to hide the information is needed. At this point, steganography and cryptography algorithms complement each other.

In the proposed model, the data is encrypted with AES 256 bit and a 32 character key. In order to minimize the deterioration, LSB method was used in image steganography application. However, in this method, the sequential selection of the pixels to be embedded in the data jeopardizes the data security and increases the detectability of the data. In order to avoid this situation, pixels are chosen randomly. In addition, original models were used to embed the pixel information used in encoding into the image to be used in the decoding phase. In the process of hiding the information with random pixel selection and original mathematical model, the detectability of the information is reduced, and it will be more difficult to obtain the real text as it will be meaningless if the information is detected with encryption.

Acknowledge

This report belongs to Coskun BALKESEN's thesis on "High Security Data Hiding in Images by Using Cryptography and Steganography Methods" in Selcuk University, Institute of Science and Technology Department.

References

Anderson, R. (1997). Stretching the Limits of Steganography. *Information Hiding, 1174*, 39-48.

Chan, C.-K., & Cheng, L. M. (2004). Hiding data in images by simple LSB substitution. *Pattern Recognition, 37*, 469-474.

Doğan, F., Dağ, R., & Türkoğlu, İ. (2016). İmgeler İçin Farklı Bir Veri Gizleme Yaklaşımı. *Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi, 7*(3), 501-514.

Karaca, N. (2007). *Alçak Çözünürlüklü Fotoğrafların Görüntülenmesi ve Bunların Optimizasyonu ile İlgili Bir Çalışma.* (Yüksek Lisans Tezi), Ege Üniversitesi, İzmir.

Kodaz, H., & Botsalı, F. M. (2010). Simetrik ve Asimetrik Şifreleme Algoritmalarının Karşılaştırılması. *Selçuk-Teknik Dergisi, 9*(1), 10-23.

Lin, G. S., Chang, Y. T., & Lie, W. N. (2010). A Framework of Enhancing Image Steganography With Picture Quality Optimization and Anti-Steganalysis Based on Simulated Annealing Algorithm. *IEEE Transactions on Multimedia, 12*(5), 345-357.

Morkel, T., Eloff, J. H. P., & Olivier, M. S. (2005). *An overview of image steganography*. Paper presented at the Proceedings of the ISSA 2005 New Knowledge Today Conference, Sandton.

Oppliger, R. (2005). *Contemporary Cryptography* Norwood: Artech House Publishers

Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). Information Hiding—A Survey. *Proceedings of the IEEE, 87*, 1062-1078.

Sakallı, M. T. (2006). *Modern Şifreleme Yöntemlerinin Gücünün İncelenmesi* (Doktora Tezi), Trakya Üniversitesi, Tekirdağ.

Sarmah, D. K., & Bajpai, N. (2010). Proposed System for Data Hiding Using Cryptography and Steganography. *International Journal of Computer Applications, 8*, 7-10.

Seth, D., Ramanathan, L., & Pandey, A. (2010). Security Enhancement: Combining Cryptography and Steganography. *International Journal of Computer Applications, 9*, 3-6.

Smith, D. (2010). *Multivariate Cryptography.* (Doktora Tezi), Indiana University, Bloomington.

Soyalıç, S. (2005). *Kriptografik Hash Fonksiyonlari ve Uygulamaları.* (Yüksek Lisans), Erciyes Üniversitesi, Kayseri.

Stinson, D. R. (2006). *Cryptography: Theory and Practice* (3 ed.). Boca Raton: CRC.

Swain, G., & Lenka, S. (2012). LSB Array Based Image Steganography Technique by Exploring the Four Least Significant Bits. *Communications in Computer and Information Science, 270*, 479-488.