IMPROVEMENT OF LSB BASED IMAGE STEGANOGRAPHY

[1]ÖZCAN ÇATALTAŞ, [2]KEMAL TÜTÜNCÜ

[1,2]Selcuk University Faculty of Technology Konya, Turkey
E-mail: [1]ozcancataltas@selcuk.edu.tr, [2]ktutuncu@selcuk.edu.tr

Abstract - Privacy is one of the most important issues in today's communication systems. In applications where the importance of your privacy is indispensable, the main aim is to send the information to desired target without being captured by the third persons or by bringing them in such a way that they cannot understand. Today, researchers have developed data hiding methods using a wide variety of digital media. At this point, it is important not only to hide data, but also to develop mechanisms to prevent third parties from identifying hidden data. In this study, a new method that combine chaos-based logistic map encryption with improved Least Significant Bit (LSB) insertion method of image steganography was proposed. The message to hidden is encrypted by one dimensional logistic map and then improved LSB method was used to form stego-image. Proposed method has been tested on 3 different images. Likewise, the classical LSB methods have also been tested on the same images. It has been seen that proposed method increased the resistance of stego-images against attacks due to encryption. Additionally, Peak Signal to Noise Ratio (PSNR) in the stego-images were increased up to 6.6% that means to decrease sense by the human observation. Thus, proposed method increased the resistance and visibility of the stego-images.

Keywords - Encryption, Image Steganography, LSB, Logistic Map, PSNR.

I. INTRODUCTION

With the increasing widespread use of information technologies, work and transactions are shifted to electronic environments and it becomes important to protect or secure the information stored, processed and transferred in these environments. In an environment where digital data communication occurs, there are many threats for the message sent such as unauthorized access, damage, destruction, modification and reproduction. Despite the precautions taken, reports for these threats are increasing day by day [1][2]. Various techniques have been developed to remove these threats in response to the emergence of these threats. Encryption techniques are among the first solutions.

Encryption makes it difficult to reach the original data by converting it into an unusable form. However, there are situations in which any crypto-analysis cannot be prevented. In addition, communication can be blocked by 3rd parties when it is understood that encrypted communication is made between the two sides in the electronic environment. This is the point where the methods of steganography take place. Steganography is a scientific discipline whose roots date back thousands of years [3].

The meaning of the word is hidden or obscure writing [4]. The most basic goal is to ensure the confidentiality of the communication. In steganography, a numerical data is stored in another numerical data without noticeable changes. For example, an encrypted text is stored in an image file, and the resulting image file is not physically and visually different from the original. Thus, those who monitor the communication between the two sides see a picture that is only transferred between them, but they are not aware that a hidden messaging actually takes place by this picture.

Digital images are the easiest to distribute and are files that can be met almost every page on the internet. The most commonly used environments for steganography applications are image files, although they vary according to the formats used. For this reason, studies on steganography and developed techniques are mainly in the frame of image steganography. It is possible to hide a text inside an image file as well as hide another image inside image files. Two files are involved in embedding (or concealing) a secret information [5]. The first file, called the cover image, is the image file that will hide the hidden information. The second file is the message with the information to be hidden. This message is also called stego. A message can be something else that can be stored as plain text, chipper text, other images, or bitmaps. As the result of the embedding process, the cover image that includes the embedded message is called "stego image". Information can be hidden in images using many different methods. These methods can be grouped under two headings, taking into account the data they use during embedding [6].

1. Spatial / Image Domain Technique
2. Frequency / Transform Domain Technique

The technique called Spatial Domain or Image Domain uses directly the pixels of the image file for embedding. An example of this technique is the Least Significant Bit Insertion (LSB) method, which is commonly used. The technique known as Frequency Domain or Transform Domain implements embedding in cover image, which is transformed in frequency domain. The algorithms for embedding data in JPEG format image files can be shown as

examples of the Transform Domain technique. These algorithms apply data embedding to the Discrete Cosine Transform (DCT) coefficients of JPEG [7].

II. RELATED WORK

In [8], a method combining Rivest-Shamir-Adleman (RSA) cryptology and LSB steganography was proposed. It's achieved a 5.8% increase in PSNR value compared to the standard LSB substitution technique.

In [9], two different LSB methods based on bit inversion was proposed. In the study, 6 different messages were embedded in 3 different images. As a result of the experiments carried out, the PSNR value was improved by 5.92% in first proposed method, by 15.8% in second proposed method

In [10], a new LSB steganography method was proposed for color images. According to this method, 2-2-4 message bits are embedded in the R-G-B channels, respectively. The new method was experimented on 2 different images and PSNR value was improved by 36.44% and 64.54%, respectively.

In [11], 1-2-4 LSB method were applied to embed data in grayscale and color images. The message is encrypted with the RSA algorithm to increase resistance against the attacks. The proposed method was tested on 4 different images and improved PSNR value up to 41.48% was obtained.

In [12], a new LSB steganography algorithm based on changing the embedding direction of message bits was proposed. The proposed method has been tested on 10 different images and a 1.32% improvement in PSNR value compared to the classical LSB method has been achieved.

In [13], a new steganographic method that combines LSB steganography with 8-Neighboring PVD (8nPVD) was proposed. The proposed new method was tested on 5 different images. The obtained method was compared in terms of capacity and PSNR value. The increase in PSNR was 2.38%.

III. MATERIALS AND METHODS

A. LSB Technique

The least significant bit embedding method is a widely used and simple method to apply [14]. In this method, the bits of the message to be hidden are placed one by one to least significant bit of each byte of pixels forming cover image [15].

In this embedding process, 4 out of 8 bits have changed. However, when the embedding is done in order, an image in which the message is hidden can be easily solved by third parties. Since the same random number is likely to be generated more than once, there is a possibility that the same group of pixels may be changed more than once in the random embedding process. In this case, character loss can be found when the hidden message is solved.

A simple example of this method is given in Fig 1.

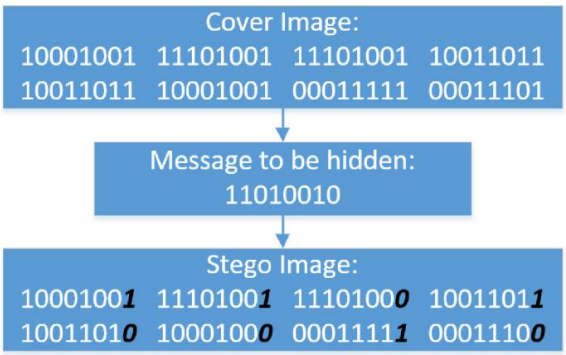


Fig. 1. An example of LSB steganography technique

B. Logistic Map

The use of chaotic signals for carrying information was first put forward in 1993 by Hayes et al [16]. Chaos-based encryption programs basically generate chaotic equations and generate a long random number sequence such as pseudo-random number generators and encrypt a plain image with this sequence [17]. One of the simplest and most studied nonlinear systems is the logistic map. This system was originally introduced in 1838 by Pierre Franois Verhulst as a demographic model. In 1947, Ulam and von Neumann worked on the logistic map as a random number generator [18].

In the encoding of images, logistic maps are used in place of S-boxes because they are sensitive to their initial conditions, behave like random number, and contain non-repetitive features. Chaos-based encryption programs basically encrypt the plain image with these random numbers by generating a long random number sequence as random number generators using chaotic maps [19].

The logistic map can be formulated as in (1).

$$x_{k+1} = \mu * x_k * (1 - x_k) \quad (1)$$

Where μ and x_0 are initial values. The map is in chaotic state when $3.57 < \mu \leq 4$ [20], and behaves like random.

C. Image Quality Measures

Image quality is a characteristic for an image that measures the apparent image debasement (regularly, contrasted with a perfect or ideal image). Imaging systems may present some amounts of artifacts or distortion in the image, so the quality assessment is an essential issue.

One of the most well-known and widely used measure of comparing two images is the Peak Signal to Noise Ratio (PSNR). PSNR is an engineering term for the proportion of the maximum possible power of original image to the power of the differences between original image and stego image. The unit of

PSNR is decibel (dB). A higher PSNR value means that the stego image is less distorted. The Peak Signal to Noise Ratio of two images can be expressed by (2).

$$PSNR = 20 * \log_{10} \frac{255}{\sqrt{MSE}} \quad (2)$$

Where MSE is an abbreviation of Mean Square Error and is the average of the difference between the original image and the stego image.

Another method used to evaluate image quality is Maximum Difference (MD). MD is the largest difference between each pixel of the original image and the stego image. Therefore, the lower MD value means that the difference between the two pictures can be less. The formula for MD is given in (3).

$$Maximum\ Difference = \max(|I(i,j) - S(i,j)|) \quad (3)$$

Average Difference (AD) is another method used in image quality assessment. It is equal to mean of the differences between original image and stego image. The closer the AD value is to 0, the more similar the two pictures are to each other. The formulation of AD is given in (4):

$$Average\ Difference = \sum_{i=1}^{m}\sum_{j=1}^{n} \frac{[I(i,j) - S(i,j)]}{m * n} \quad (4)$$

The Structural Similarity Index Measure (SSIM) is a perceptual metric that quantifies image quality degradation caused by processing such as data embedding or data compression. It is a full reference metric that requires two images from the same image capture: a reference image (cover image) and a processed image (stego image). SSIM has values between 0 and 1, and 0 means that the images are completely different from each other, whereas 1 means that the two images are identical. The formulation of SSIM is given in (5):

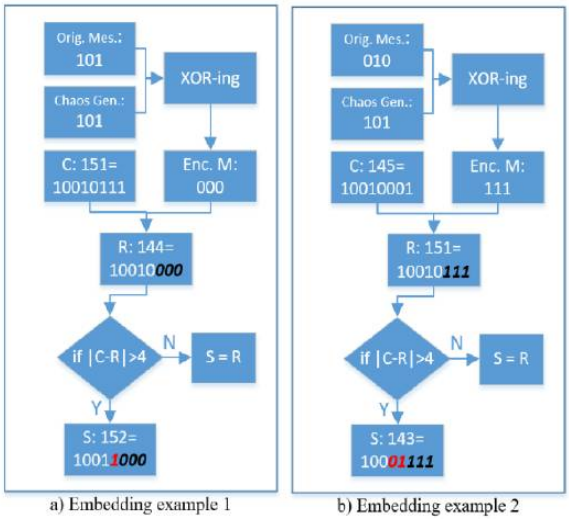
IV. THE PROPOSED ALGORITHM

A. Embedding Algorithm (n-LSB on 24bit RGB image)

- Using the logistic map, random numbers are produced up to the number of message bits to be embedded. The initial conditions x and u are used as keys in the communication.
- Since the chaos generator produces numbers between 0 and 1, these numbers are first multiplied by 10 until the integer is reached.
- Then, the least significant bits of these integers are taken and used as random numbers.
- The encrypted message bits are obtained by XOR-ing the random numbers with the original message bits.
- The least significant n bits of each pixel's R, G and B channels are sequentially replaced with the bits of the encrypted message.
- If the difference between the newly created R, G and B values and the original R, G and B values is more than $2^n/2$, then this difference is reduced by; Checking and modifying all consecutive bit starting from (n+1)th bit till the 8th bit (most significant bit) unless it has value of 1. When the bit with value of 1 is met then change it's value to 0 and stop the operation. If we have all 0s starting from (n+1)th bit to 8th bit then don't do any change on these consecutive bits.
- If the difference between the newly created R, G and B values and the original R, G and B values is less than $-2^n/2$, then this difference is increased by; Checking and modifying all consecutive bit starting from (n+1)th bit till the 8th bit (most significant bit) unless it has value of 0. When the bit with value of 0 is met then change it's value to 1 and stop the operation. If we have all 1s starting from (n+1)th bit to 8th bit then don't do any change on these consecutive bits.

When the embedding algorithm is checked, it's been seen that the main aim is to compensate the change in pixel value if it is higher than absolute value of $2^n/2$. When the change in pixel value is positive and above $2^n/2$ the proposed method tries to reduce this difference to $2^n/2$ that gives bigger PSNR value than classical n-LSB. When the change in pixel value is negative and less than $-2^n/2$ the proposed method tries to increase this difference up to $-2^n/2$ that also gives bigger PSNR value than classical n-LSB.

An example of the embedding algorithm for 3-LSB is shown in Fig 2.



a) Embedding example 1 b) Embedding example 2

B. Extraction Algorithm

- The least significant 3 bits of each pixel of R, G and B channels of the stego image is fetched in order.
- Random numbers are generated using a chaotic random number generator and initial values x and u. Since the chaos generator produces numbers between 0 and 1, these numbers are first multiplied by 10 until the integer is reached.
- Then, the least significant bits of these integers are taken and used as random numbers.

- The original message bits are obtained by XOR-ing the random numbers with the extracted message bits.

Proposed method increase complexity or resistance of stego-image against attack by employing logistic map random number generator and XOR-ing operation to encrypt the text message as expressed in embedding algorithm.It should be noted here that proposed method improves LSB by reducing the difference between cover and stego-image during the embedding process as follows: Let's check how proposed method works on 3-LSB. Assume that we have 111 (3 bits) encrypted data to embed into R channel whose last 3 bits is 000. For this case the change in cover image will be 7 (bigger than $2^3/2$). This will affect the visibility or sense of a human on the image. The proposed method will check the 4^{th} bit of cover image and if it is 1 then it will change it to 0 and then stop the operation. Changing 4^{th} bit value from 1 to 0 means reducing the value of related pixel -8. Total change of related pixel will be 7-8=-1 instead of 7 that means to increase PSNR ratio of stego-image.

As can be seen from embedding-extraction algorithms proposed method is not appropriate for 1-LSB. For 1-LSB, the change in last bit can be between -1 (from 1 to 0) and 1 (from 0 to 1). The proposed method will only apply encryption but never improve 1-LSB since only the change in last bit will never be bigger than $2^1/2$ or that is equal to 1. Briefly speaking proposed method only increases the resistance of 1-LSB due to encryption but keep degradation of 1-LSB same. Thus, proposed method should be applied to n-LSB where n is greater than 1.

V. EXPERIMENTAL STUDY

In this study, the classical 2-LSB (last two bits insertion) and 3-LSB (last three bits insertion) methods and proposed methods have been applied to 3 different images namely "Lena", "Cat" and "Bird". These images are shown in Fig. 3. The embedding capacities of each images for each algorithm are given in Table 1.

In order to see the effect of the messages in different sizes on the images, 3 text files in different sizes are used as the message. The names of these files are "Text1.txt", "Text2.txt" and "Text3.txt" and they have sizes of 2.71 kB, 5.82 kB and 10.48 kB, respectively.

The initial values of the chaos generator logistic map used in this study are x = 0.675 and u = 3.9762.

The classical 2-LSB and 3-LSB algorithms and proposed methods were applied to Image 1 (Lena), Image 2 (Cat) and Image 3 (Bird). The obtained results are given in Table 2. In addition, the stego image which is formed as a result of applying the proposed 3-LSB method is given in Fig. 4.

Methods	Capacity (Kilobyte)		
	Image 1-"Lena" 225x225	*Image 2-"Cat" 960x603*	*Image 3-"Bird" 1024x768*
2-bit LSB	37.07 Kb	423.98 Kb	576 Kb
Proposed 2-bit LSB	37.07 Kb	423.98 Kb	576 Kb
3-bit LSB	55.61 Kb	635.97 Kb	864 Kb
Proposed 3-bit LSB	55.61 Kb	635.97 Kb	864 Kb

Table I. Embedding capacity of each image in each algorithm

Fig. 3. The original cover images

Text File	IQM	Image 1, "Lena"				Image 2, "Cat"				Image 3, "Bird"			
		2-bit LSB	*Proposed 2-bit LSB*	*3-bit LSB*	*Proposed 3-bit LSB*	*2-bit LSB*	*Proposed 2-bit LSB*	*3-bit LSB*	*Proposed 3-bit LSB*	*2-bit LSB*	*Proposed 2-bit LSB*	*3-bit LSB*	*Proposed 3-bit LSB*
Text1.txt	PSNR	53,0082	55,2505	48,5549	51,397	63,7063	65,9110	59,1702	62,0850	65,0086	67,2403	60,5294	63,3893
	MD	3	2	7	4	3	2	7	4	3	2	7	4
	AD	3,1166E-	1,251E-4	0,0015	1,6461E-	1,1747E-	1,0461E-	3,4396E-	1,0096E-	6,4426E-	5,3123E-	4,0831E-	4,2244E-
	SSIM	0,9998	0,9999	0,9996	0,9998	0,999998	0,999999	0,9997	0,9998	0,999998	0,999999	0,9998	0,9999
Text2.txt	PSNR	49,7698	52,0307	45,2667	48,0838	60,5179	62,7353	56,1768	59,0674	61,8177	64,1084	57,2722	60,0947
	MD	3	2	7	4	3	2	7	4	3	2	7	4
	AD	2,4362e-4	4,1043E-	0,0031	6,0137E-	2,8465E-	1,8196E-	8,2132E-	1,6008E-	2,9105E-	1,2857E-	1,0808E-	3,5604E-
	SSIM	0,9995	0,9997	0,9988	0,9994	0,9997	0,9998	0,9993	0,9996	0,9999	0,9999	0,9997	0,9998
Text3.txt	PSNR	47,3333	49,5689	42,8823	45,7126	57,9943	60,1950	53,6387	56,5641	59,2513	61,5088	54,9938	57,8292
	MD	3	2	7	4	3	2	7	4	3	2	7	4
	AD	5,27E-05	4,8285E-	8,3182E-	4,4774E-	5,2861E-	3,2918E-	0,0016	6,7928E-	1,4355E-	9,4378E-	2,0684E-	1,1557E-
	SSIM	0,999	0,9994	0,9977	0,9988	0,9996	0,9997	0,9988	0,9994	0,9998	0,9999	0,9995	0,9997

Table II. Embedding results

CONCLUSION

In this paper, a new image steganography algorithm that consists of combination of improved LSB insertion and one dimensional logistic based (chaos theory) encryption is proposed. Traditional n-LSB algorithm is improved by compensating the change in pixel value if it is higher than absolute value of $2^n/2$. Thus, the degradation ratio between cover and stego-images were reduced. Proposed method has been tested on 3 different images together with classical 2-LSB and 3-LSB methods. 3 text files of different lengths were used as the message and these messages were encrypted with a logistic based chaos generator before being embedded. The results obtained from proposed method and classical methods were evaluated according to the PSNR, MD, AD and SSIM criterions. The improvements in PSNR value for each image and each text file are given in Table 3. As can be seen from Table 3, the proposed method has PSNR values 6.6% that is higher than conventional n-LSB steganography methods. Additionally, SSIM values of proposed method were almost same or higher than classical n-LSB methods as can be seen from Table 2. All these results showed that proposed method increases the resistance of the stego-mages without causing noticeable degradation to the cover image.

REFERENCES

[1] Canbek, G., Sağıroğlu, Ş., "Bilgi ve Bilgisayar Güvenliği Casus Yazılımlar ve Korunma Yöntemleri", Grafiker, Ankara, 1-50 (2006)

[2] Sağıroğlu, Ş., Alkan, M., "Her Yönüyle Elektronik İmza (e-İmza)",Grafiker,Ankara,3,5,33 (2005).

[3] Caldwell, 2nd Lt. J., "Steganography", CROSSTALK The Journal of Defense Software Engineering, 25-27 (2003).

[4] Internet: Cummins, J., Diskin, P., Lau, S., Parlett, R., " Steganography and Digital Watermarking", 2004.

[5] Hartung F., Kutter M., "Multimedia watermarking techniques," Proc. of the IEEE,vol. 87, pp. 1079–1107, July 1999

[6] Heredotus, "The Histories", First Published in Greek 430 B.C.E., Translated by Selincourt A., Penguin Classics, Hammondsworth, 1971.

[7] Johnson N.F., Duric Z., Jajodia S., "Information Hiding: Steganography and Watermarking - Attacks and Countermeasures", Kluwer Academic Publishers, ISBN: 0-79237-204-2, 2000.

[8] X. Zhou,W. Gong, W. Fu, L. Jin, "An Improved Method for LSB Based Color Image steganography Combined with Cryptography", ICIS 2016, June 26-29, 2016, Okayama, Japan, IEEE

[9] N. Akhtar, S. Khan, P. Johri, "An Improved Inverted LSB Image Steganography", Interational Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014, IEEE

[10] A. Singh, H. Singh, "An Improved LSB based Image Steganography Technique for RGB Images", IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2015

[11] S. Goyal, M. Ramaiya, D. Dubey, "Improved Detection of 1-2-4 LSB Steganography and RSA Cryptography in Color and Grayscale Images", International Conference on Computational Intelligence and Communication Networks, 2015,IEEE

[12] S. Sugathan, "An Improved LSB Embedding Technique for Image Steganography", 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), 2016,IEEE

[13] M. Kalita, T. Tuithung, "A Novel Steganographic Method Using 8-Neighboring PVD (8nPVD) and LSB Substitution", The 23rd International Conference on Systems,Signals and Image Processing, 23-25 May 2016, Slovakia, IEEE

[14] E.M. Esin, E. Guvenoglu, "Resim İçine Yazi Gizlenmesi Amaciyla Kullanilan Lsb Ekleme Yönteminin Shuffle Algoritmasiyla İyileşitirilmesi", , Türkiye Bilişim Vakfı Bilgisayar Bilimleri Dergisi, sayı 2, sayfa 73-79, 2006.

[15] M.M. Amin, M. Salleh, S. Ibrahim, Katmin, "Information hiding using steganography", 4th National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia, p.21–25.

[16] S. Hayes,C. Grebogi, E. Ott, "Communicating with chaos.", Phys Rev Lett 1993;70(20):3031–4.

[17] A.N. Pisarchik, N.J. Flores-Carmona, M. Carpio-Valadez, "Encryption and decryption of images with chaotic map lattices.", Chaos: Interdiscipl J Nonlinear Sci2006;16(3):033118.

[18] S.M. Ulam, J. Neumann, "On combination of stochastic and deterministic processes.", Bull Am Math Soc 1947;53:1120.

[19] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps.", Int J Bifurcat Chaos 1998;8:1259–84.

[20] R. Bose, A. Banerjee, "Implementing Symmetric Cryptography Using Chaos Function", Indian Institute of Technology.

★★★