

A New Robust Audio Signal Steganography Based On Multiple Chaotic Algorithms With Edge Detection Technique

Amir Houshang Arab Avval¹, Shahram Mohanna²

¹Department of electrical and electronic engineering of Sistan and Baluchestan university, Zahedan, Iran
amirhoushang.arab@gmail.com

²Department of electrical and electronic engineering of Sistan and Baluchestan university, Zahedan, Iran
mohana@hamoon.usb.ac.ir

Abstract

This paper proposes a novel robust blind steganography scheme for embedding audio signal into edge of color image based on a chaotic map and LSB method, which is different from some existing works. In this paper, we employed the LSB substitution technique and chaos as a fundamental stage and we also take advantage of edge detection technique. The present paper improved security by using of chaotic maps. Chaotic maps are used for two important applications in our scheme: selecting of random location in edge pixels for embedding and extraction and selecting of random bit location in LSB of pixel byte. The suggested scheme is robust, secure and flexible. In the extraction procedure, the stego can be extracted from the stego image without the requirement of the original host color image or the original stego image. Experimental results show that the proposed audio steganography scheme has stronger robustness against attack, Because The chaotic map was implemented to increase both the number of keys (control parameters) and complexities involved in the algorithm. The size of key space for initial conditions and control parameters were computed about 10^{28} .

Keywords: *Steganography, Security, Robustness, Chaos, logistic Map, Edge detection.*

1. Introduction

Electronic communication is increasingly susceptible to eavesdropping and malicious interventions. The issues of security and privacy have traditionally been approached using tools from cryptography. Messages can be appended with a message authentication code (hash) and encrypted so that only the rightful recipient can read them and verify their integrity and authenticity. Modern cryptography is a mature field based on rigorous mathematical foundations and decades of development. Steganography is the act of covert communications, which means that only the sender and receiver are aware of the secret communication. To achieve this, the secret message is hidden within benign-looking communications known as cover texts or cover

Works [1]. Steganography techniques can be broadly classified into two categories: Spatial [2] and Transform [3] domain methods. The first steganalytic methods focused on the most common type of hiding called Least Significant Bit embedding [4, 5] in bitmap and GIF images. Later, main effort had been directed to the most common image format JPEG [6, 7] and audio files [8]. Exact methods for detecting hidden messages prompted mainly research in steganography for multimedia files [9, 10]. The advantage of using LSB method is that it is easy to embedding the message bits directly into the low significant bits [11, 12]. The weakness of the method is that it is very sensitive to any kind of filtering or manipulation of the stego images [13, 14].

In most spatial domain schemes, steganography signal is embedded in the LSB (least significant bit) of the pixels in host image in which the robustness against attacks is weak i.e. stego can be detected easily [15]. But we have used the chaotic map and also embedding in four low significant bits, so it is very robust and secure. Two main requirements for an acceptable watermarking and steganography technique are imperceptibility [16] and robustness [17]. Imperceptibility refers to perceptual quality of the data being protected. Robust steganography embeds information data within the image with an insensible form for human visual system, but in a way that protects from attacks such as common image processing operations. Image scrambling is one of the most prevailing encryption algorithms these years [18], [19], [20].

At the late years the chaotic maps have been used to increase the digital security of watermarking and steganography [21]. The first chaotic system was discovered by Edward Lorenz in 1963[22]. Other chaotic systems have been established by many different research areas, such as physics, mathematics, and engineering. The idea of using chaotic signals in different layers of communication systems attracted the attention of researchers [23-28]. The most important specification of chaos is that it is sensitive to the primary conditions. In a way that the primary different but so similar conditions are

selected and then the system output will be so different, so, it is possible to produce a pseudo-random string [29]. Chaotic maps in steganography are used for two goals: to find the embedding location in the edges and the bit location through LSB method. Some changes are needed in the maps in any of the said processes. Chaos signal seems like noise but it is completely firm. It means that using the primary values and the map function, it is possible to reproduce the signal value again. Piecewise nonlinear chaos and logistic chaos map began as an attempt to find chaos in the sense of extreme sensitivity to changes in initial conditions. Chaotic functions such as Markov Maps, Bernoulli Maps, Skew Tent Map, and Logistic Map have been widely used to generate watermark sequences [30], [31]. This paper mainly focuses on the application of the piecewise nonlinear chaotic map [32] in encryption schemes of stego signal. The chaotic maps are employed to enhance the security and the best extraction, as well as determining the location of LSB significant for the stego embedding.

The article is organized as; section 2 describes the chaotic maps for scrambling processes. The details of Steganography embedding and extraction are presented in section 3. Some simulation results are discussed in section 4 and the document is concluded in Section.

2. APPLIED CHAOTIC MAPS

2.1 Logistic map

Robert May said in an effective paper in 1976 that even simple nonlinear maps could have very complicated dynamics [33]. This point is made clear by logistic map. Logistic map is defined in mathematical language as follows:

$$X_{n+1} = r \times X_n \times (1 - X_n) \quad (1)$$

This map is an equation to define the population growth rate. x_n show the population number in n^{th} generation and r shows the growth rate which is both positive values. Usually they take into consideration the r parameter which is $0 \leq r \leq 4$ so x will be normalized to the values $0 \leq x \leq 1$.

2.2 Selecting location by Piecewise nonlinear chaotic map

2.2.1 Using the chaotic map to identify the embedding and extraction location of stego audio in host image

In steganography procedure the binary bits are embedded and extracted with no specific order in the pixels of the edge of the host image to increase the safety. To find the location of these pixels, the edges of the image are stored in a one dimension array and the following relation which is the famous formula for modularity calculations is used to find the chaotic locations.

$$EdgeLoc = [X_{n+1} \times 10^{+14}] \bmod M \quad (2)$$

In this relation, EdgeLoc is identified the location of the pixel in which the binary content will be saved.

2.2.2 Using the Chaotic map to identify the bit location in identified pixel

When the pixel location is identified by the relation (2), the bit location must be defined in LBS. For more safety we don't choose a constant place for it and it is calculated by the chaotic map which is a number from 1 to 4 and is calculated as follows:

$$BitLoc = ([X_{n+1} \times 10^{+14}] \bmod 4) + 1 \quad (3)$$

3. STEGO EMBEDDING AND EXTRACTION

3.1 Stego embedding

3.1.1 Embedding process

Figure1 shows the total diagram block of the embedding algorithm. For better description of the embedding algorithm, we divide the algorithm into two parts to describe the embedding process better. The semi-code of the process is as follows:

3.1.1.1 Algorithm 1, General process of Embedding

- Agreement with the destination to select the host image from a database of the ready colored images.
- Getting the red, blue and green channels from the input image.
- Finding the image edges according to the agreement with the destination on the edge finding algorithm type (sobel, prewit, Roberts, log, zerocross, canny).
- Receiving the sound file and dividing it into three equal parts according to the input file size.
- Embedding any part of the audio file on red, green and blue channels respectively each in an independent manner and according to the algorithm 3-2.
- Combining the red, green and blue channels to create the final file to send to the destination.

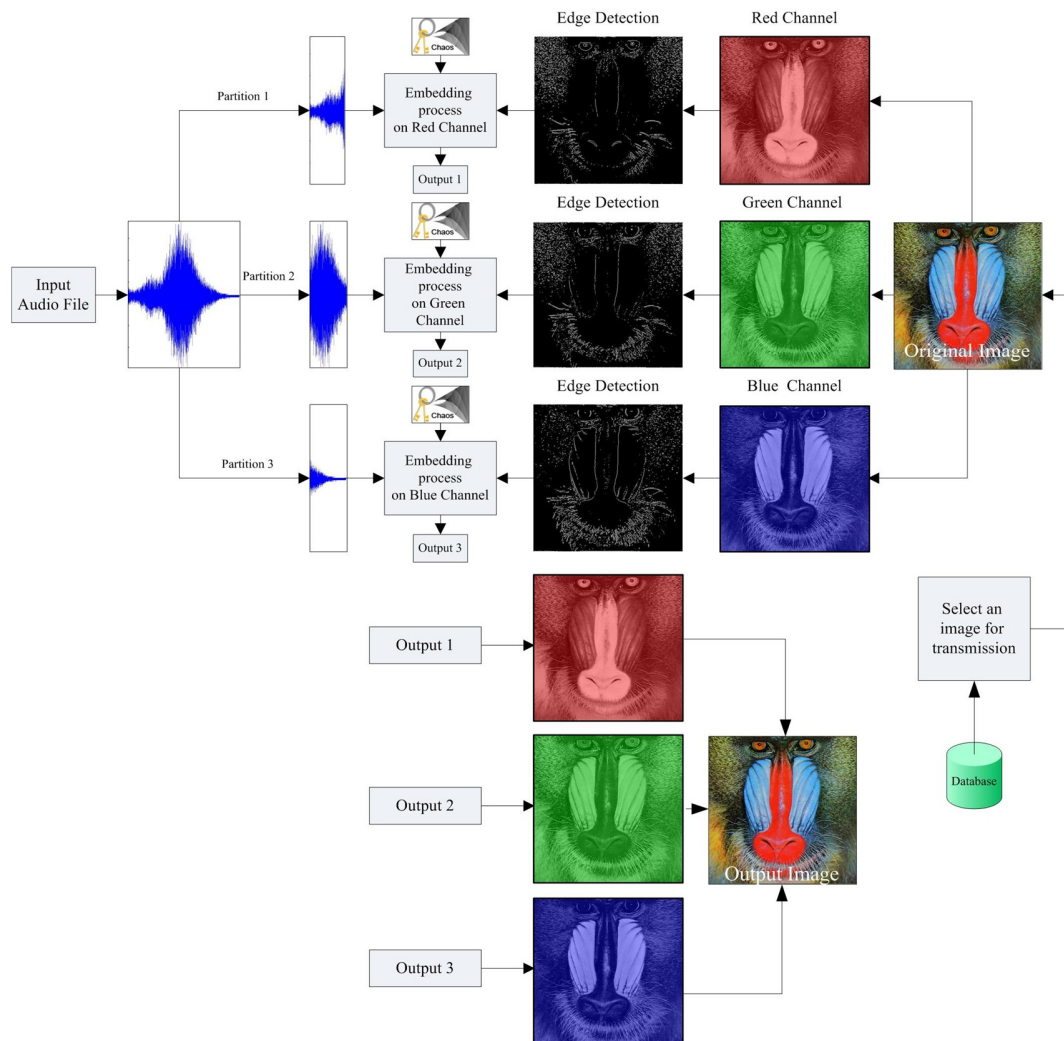


Figure. 1 Flowcahrt of Embedding process

3.1.1.2 Algorithm 2 the specialized process of chaotic embedding for the fifth step of the algorithm 1

- Agreement on the keys μ_2 , X_2 , μ_1 , X_1 . These keys are the primary conditions and the control parameters of logistic chaotic map. X_1 , X_2 are a number in $(0, 1)$ and μ_1 and μ_2 are a number between 3.6 and 4.

The coordinates of the rows and the columns of the image edges are stored in a 2D array named Edges. This array holds two rows and ES columns. ES shows the length of the array.

- The contents of input audio file are stored in a one dimensional array of AS size.

- Getting the edge pixel place using the logistic map and the X_1 and μ_1 password keys and the calculated number will be from 1 to ES.
- Calculating the bit location using the logistic map and the X_2 and μ_2 passwords and the calculated number will be 1 to 4.
- Embedding of one bit of the audio file in the calculated location from the fourth step and in the bit number of BitLoc which is calculated in fifth step.
- Repeat the fourth to sixth steps until all bits are embedded.

The flowchart of the algorithm is shown in figure 2.

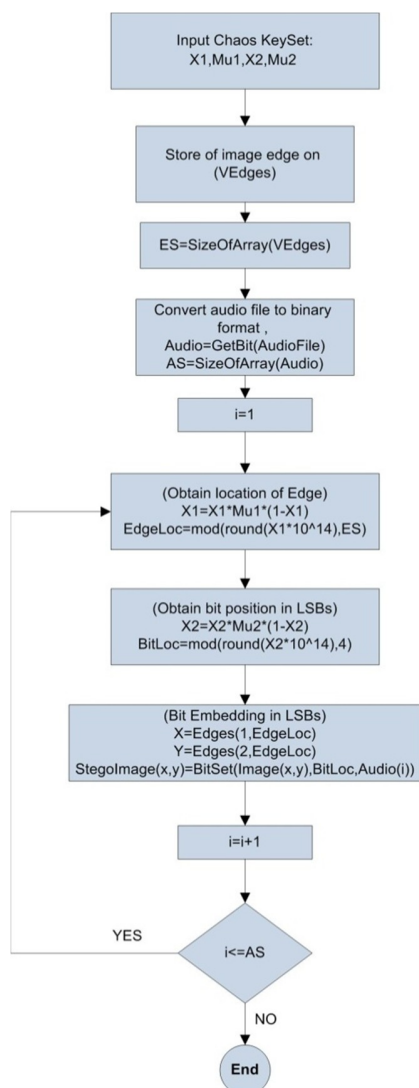


Figure. 2 the specialized process of chaotic embedding

3.2 Stego Extraction

3.2.1 Extraction process

Figure 3 shows the total block diagram of the extraction algorithm. For better description of the extraction algorithm, it is divided into two parts to

- Agreement on the keys μ_2 , X_2 , μ_1 , X_1 . These keys are the primary conditions and the control parameters of logistic chaotic map. X_1 , X_2 are a number in (0, 1) and μ_1 and μ_2 are a number between 33.6 and 4.
- The coordinates of the rows and the columns of the image edges are stored in a 2D array named

Edges. This array holds two rows and ES columns. ES shows the length of the array.

- Making the destination aware of the file size which could be extracted in AS length. This variable is of the keys of the problem.
- Getting the edge pixel place using the logistic map and the X_1 and μ_1 password keys and the calculated number will be from 1 to ES.

show the extraction process better. The semi- code of the process is shown as follows:

3.2.1.1 Algorithm, the general process of extraction

- Agreement with the source on selection of the image from a database of the ready colored images.
- Calculating the red, blue and green channels from the embedded original images from the database. On this image no embedding had taken place.
- Finding the original image edges according to the agreement with the source on the edge finding algorithm type (sobel, prewit, Roberts, log, zerocross, canny).
- Receiving the stego image from the source.
- Calculation the red, green and blue channels from stego image.

Extraction of three parts of the audio file from red, green and blue channels respectively in independent manner and according to the algorithm 3.4 receiving the input edges of the original picture and the embedded edges of steganography.

- Combination of the three parts of audio file calculated from red, green and blue channels for getting the final audio file.

Algorithm 4 the specialized process of chaotic extraction for the fifth step of the algorithm 3-3

- Calculating the bit location using the logistic map and the X_2 and μ_2 passwords and the calculated number will be 1 to 4.
- Extraction of one bit of the audio file from the calculated location from the fourth step and from

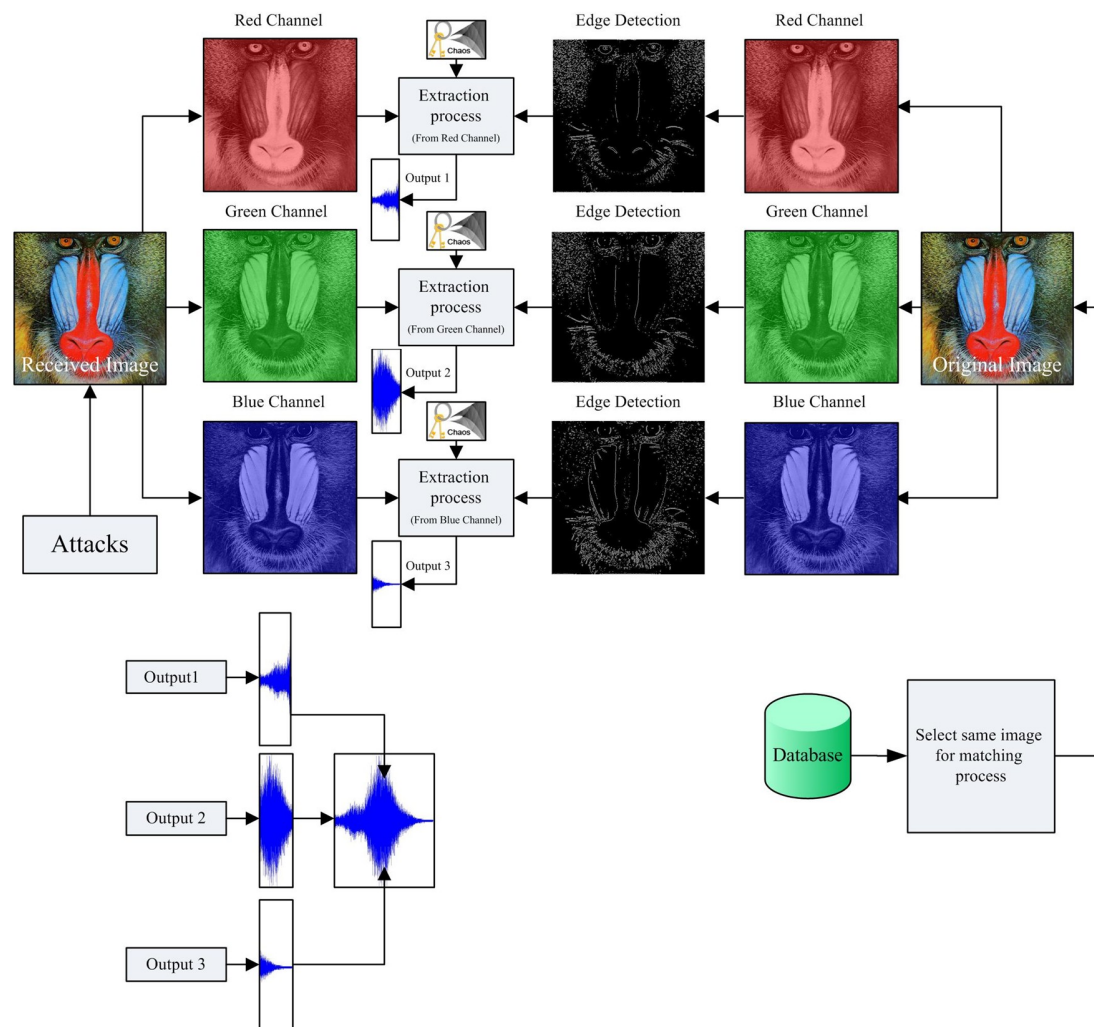


Figure. 3 Flowcahrt of Extraction process

the bit number of BitLoc which is calculated in fifth step.

- Repeat the fourth to sixth steps until all bits are extracted.

The flowchart of the algorithm is shown in figure 4.

4. EXPERIMENTAL RESULTS

This section will present and discuss the experimental results of our proposed scheme. Steganography techniques must satisfy the following properties.

4.1 Evaluation of the effectiveness

To demonstrate the effectiveness of the proposed algorithm, MATLAB simulations are performed by using:

4.1.1 Original image or cover

This image is predicted for embedding of the audio file. In the image processing algorithms, a series of standard images is used. These images are found in almost all image processing algorithms. The goal of using these images is to compare the different algorithms with the constant images.

Figure 5 shows the used images in proposed algorithm which includes the four famous Boat, Airplane, Peppers and Baboon images. The size of the images is considered 1024×1024.

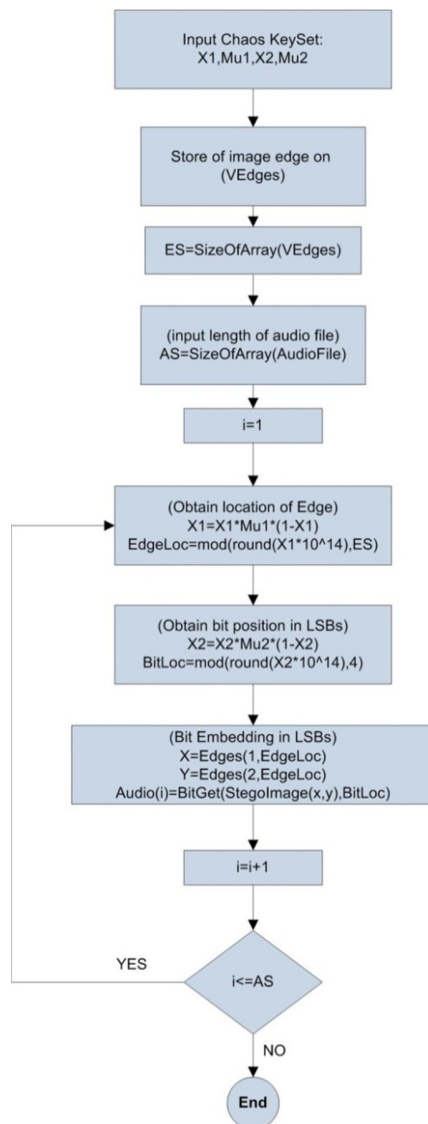


Figure. 4 the specialized process of chaotic extraction

4.1.2 Stego Audio

Stego audio which is embedded into a cover image is a audio file which is in form of binary. Figure 6 shows the cover stego in the used algorithm. Table 1 shows the complete characteristics of the audio file.

4.2 Embedding effectiveness

According to the said definition, the efficiency of a stego system is the output probability of a embedding system, to show the efficiency of the proposed algorithms, the standard 1024x1024 images and the stego audio specifications are used as shown in (Fig 5) used for the proposed algorithm in table 1. Figure 7 shows the results of the proposed algorithm. As it can be seen, the embedding and extraction is done with any possible error.

In this image the histogram of the Original image and the resulted one from steganography is shows. Also the extraction operation is showed by the chaotic map right key and wrong key.

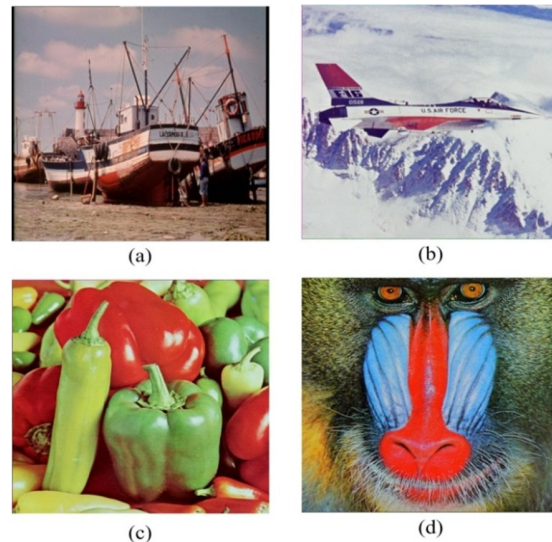


Figure. 5 Standardimages a) Boat b) Airplane c) Peppers d) Baboon

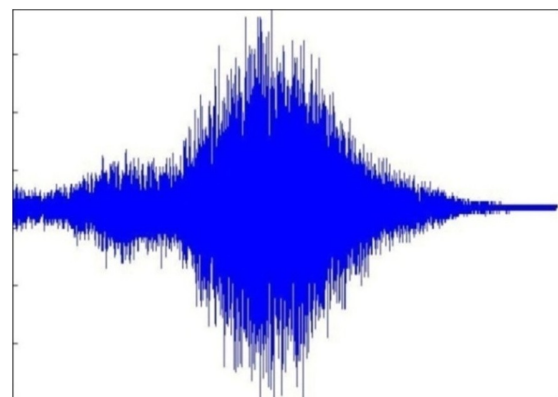


Figure. 6 Fixed audio file

Table1: the audio file specifications in proposed method

Specifications	Values
File Name	Sample.wav
File Size	26.6KB
Sampling rate	11025 HZ
The numberof bits	8
Format	Native

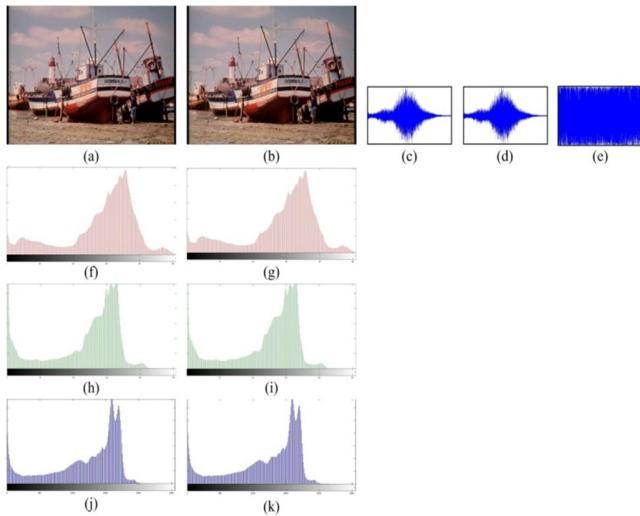


Figure. 7 a) original image Boat, b) the resulted image from steganography, c) original audio file, d) extracted audio file by the right key, e) extracted audio file by the wrong key, f, g, h) red, green and blue channels histograms of the original image, i, j, k) red, green and blue channels histograms of the image resulted from steganography

4.2.1 Fidelity

The next specification is the fidelity which studies the conception similarities between the original version and the steganography version. According to the figure 8 the stego in the steganography image is not understandable and this is what we aim. The presented histograms are also not understandable. But for evaluation of the efficiency of the proposed algorithms in this specification, a numeral factor must be presented and most of the researchers use the Peak Signal-Noise Ratio (PSNR) as it is defined here:

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} (dB) \quad (4)$$

In the above relation, MSE is the mean square of the error in statistics which is defined as follows:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (H_{i,j} - H'_{i,j})^2 \quad (5)$$

In this relation $H_{i,j}$ is the main pixel value in location (i, j) and the $H'_{i,j}$ points to the pixel value of steganography image in the same location. M and N are the rows and columns number of the image. Table (2) shows the results of the factor in the stego images.

4.2.2 Robustness

Robustness is the extraction ability of steganography against the common operations of signal processing and sometimes these operations are called attacks. As these operations take place from attackers to remove stego, the study of them is very emphasized by the researchers. To study the resistance of the proposed algorithms, the salt and pepper noise attack is used.

Salt and Pepper Noise: This noise is often could be seen in the image. This noise shows itself in random black and white pixels in the gray scale images and

white& red in colored images [34]. In this study, to study the reliability the extracted stego from the bit error rate is used as follows:

$$BER = \frac{B}{M \times N} \times 100 \quad (6)$$

In this relation B shows the extracted bit error rate and $M \times N$ points to the cover stego size. Table (2) shows the PSNR of the Original image and the attack against the noise. The bit error rate is calculated in percentage according to the relation, table (3). Figure (8) shows the noised and stego images of any image.

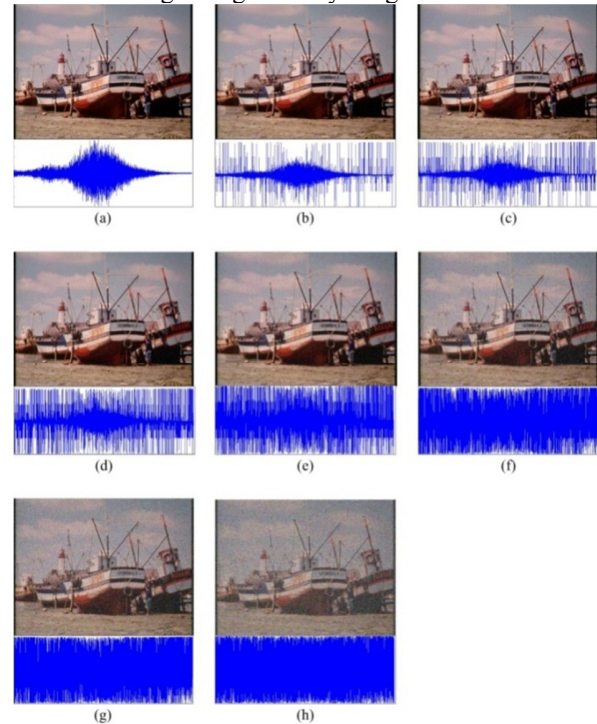


Figure. 8 the results after attacks to the Salt and Pepper noise (a) Noise 0%, (b) Noise 1%, (c) Noise 2%, (d) Noise 5%, (e) Noise 10%, (f) Noise 20%, (g) Noise 30%, and (h) Noise 50%.

4.3 Edge detection algorithms of the image

These algorithms receive the gray scale image as the input and return a black and white binary image of the same size. In this image, the binary output of the one bits are for presentation of the found edges in the input image and the one bit include the non-edge parts of the image. The common methods of edge detection in image are: Sobel method, Prewitt method, Roberts method, Laplacian of Gaussian method (LOG, Zero Cross method, Canny method. Fig 9 shows the edge detection algorithms of the image.

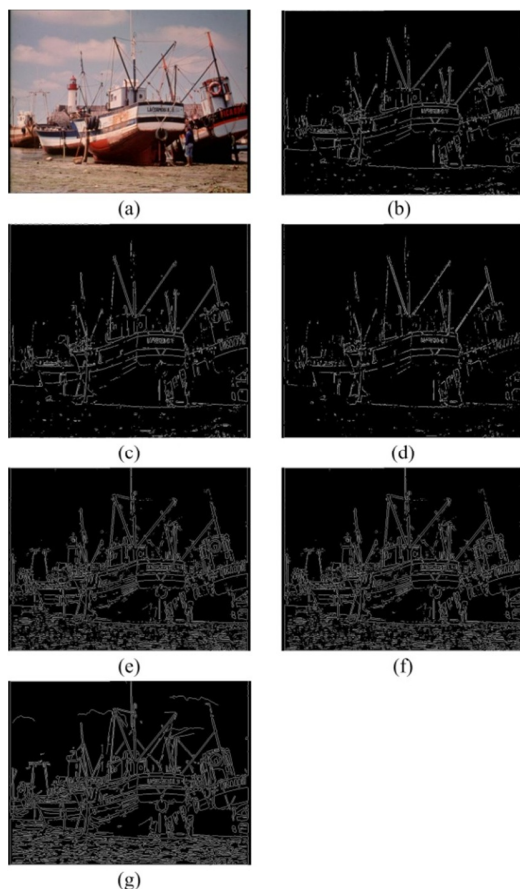


Figure. 9 Edge detection algorithms of the image a) Boat original image b) sobel edge detection c) sobel edge detection d) Prewitt edge detection e) Roberts edge detection e) Roberts edge detection f) log edge detection g) ZeroCross edge detection h) Canny edge detection

4.4 Key Space

Key is one of the most important aspects of encryption systems. Selection of a small key space leads to failure of the algorithm and impermissible embedding or extraction on the steganography system. The key space size depends on the encryption keys in decryptions present in the encryption systems. To study the key space in proposed algorithm, first we study the input variables in chaotic maps. The chaotic maps are sensitive to the inputs. It means that they are sensitive to the primary conditions and the control parameters so these variables are used as key in map.

For making the key space clearer, refer to the two branching diagram of logistic chaotic map in chapter four. Embedding and extraction stages get two key spaces. One key is as the key for identification of embedding of stego and the other key points to the favored bit location. The size of key space for initial conditions and control parameters is computed about 10^{28} .

Table 2: Simulation Results of PSNR Under Salt and Peppers Noise

Attacks	Baboon	Peppers	Airplane	Boat
Without attack	56.68	60.66	60.62	59.43
Noise 1%,	46.73	47.12	46.88	47.28
Noise 2%,	42.24	42.53	42.28	42.70
Noise 5%,	38.15	38.39	38.11	38.55
Noise 10%,	34.84	35.00	34.75	35.19
Noise 20%,	31.85	32.06	31.80	32.25
Noise 30%,	29.84	30.04	29.79	30.23
Noise 50%,	28.20	28.48	28.22	28.67

Table 3: Simulation Results of BER under Salt and Peppers Noise

Attacks	Baboon	Peppers	Airplane	Boat
Without attack	0	0	0	0
Noise 1%,	0.49	0.48	0.52	0.49
Noise 2%,	1.48	1.55	1.48	1.40
Noise 5%,	3.88	4.00	3.82	3.84
Noise 10%,	8.45	8.46	8.36	8.49
Noise 20%,	16.66	17.16	16.55	16.74
Noise 30%,	26.67	26.69	26.45	26.70
Noise 50%,	38.33	38.53	38.22	38.28

5. Conclusions

In this work, a new robust audio signal steganographic technique based on chaotic map has been proposed. Through using the LSB technique, the audio information is embedded into the Edge of the color image. In this scheme, The noise is added to the color image according to the defined algorithm and then the best audio signal detection can be successfully extracted from the host images subject to noise attacks. We improved the number of keys (control parameters) and complexities involved in this algorithm with multiple chaotic map. The size of key space for initial conditions and control parameters were computed about 10^{28} . Experimental results have shown that this proposed algorithm not only attains higher invisibility and fidelity of steganography, but also has stronger robustness in the operation of noise attack.

References

- [1] Cox JJ, Matthew LM, Jeffrey AB, et al. Digital Watermarking and Steganography. Second edition, Burlington, MA: Morgan Kaufmann Publishers (Elsevier); 2007..
- [2] H. Wei, M. Yuan, J. Zhao, Z. Kou, Research and Realization of Digital Watermark for Picture Protecting, First International Workshop on Education Technology and Computer Science, IEEE, Vol. 1, 2009, pp.968-970.
- [3] X. Li, A New Measure of Image Scrambling Degree Based on Grey Level Difference and Information Entropy, 2008 International Conference on Computational Intelligence and Security, Vol. 1, 2008, pp.350-354 .
- [4] A. Westfield and A. Pfitzmann. Attacks on steganographic systems. In A. Pfitzmann, editor, Information Hiding, 3rd International Workshop, IH'99, Dresden, Germany, September 29–October 1, 1999, volume 1768 of LNCS, pages 61–75. Springer-Verlag, New York, 2000.
- [5] J. Fridrich, M. Goljan, and R. Du. Reliable detection of LSB steganography in grayscale and color images. In J. Dittmann, K. Nahrstedt, and P. Wöhlmayer, editors, Proceedings of the ACM, Special Session on Multimedia Security and Watermarking, Ottawa, Canada, October 5, 2001, pages 27–30, 2001.
- [6] H. Farid and L. Siwei. Detecting hidden messages using higher-order statistics and support vector machines. In F. A. P. Petitcolas, editor, Information Hiding, 5th International Workshop, IW 2002, Noordwijkerhout, The Netherlands, October 7–9, 2002, volume 2578 of LNCS, pages 340–354. Springer-Verlag, New York, 2002.
- [7] J. Fridrich, M. Goljan, and D. Hoge. Steganalysis of JPEG images: Breaking the F5 algorithm. In 5th International Workshop on Information Hiding, Noordwijkerhout, The Netherlands, October 7–9, 2002, volume 2578 of LNCS, pages 310–323. Springer, New York, 2002.
- [8] A. Westfeld. Detecting low embedding rates. In F. A. P. Petitcolas, editor, Information Hiding, 5th International Workshop, IH 2002, Noordwijkerhout, The Netherlands, October 7–9, 2002, volume 2578 of LNCS, pages 324–339. Springer-Verlag, Berlin, 2002.
- [9] J. Fridrich, M. Goljan, and D. Soukal. Perturbed quantization steganography using wet paper codes. In J. Dittman and J. Fridrich, editors, Proceedings ACM Multimedia and Security Workshop, Magdeburg, Germany, September 20–21, 2004, pages 4–15. ACM Press, New York, 2004.
- [10] A. Westfeld. High capacity despite better steganalysis (F5—a steganographic algorithm). In I. S. Moskowitz, editor, Information Hiding, 4th International Workshop, volume 2137 of LNCS, pages 289–302. Springer-Verlag, New York, 2001.
- [11] S. Dumitrescu, X. Wu, and Z. Wang, “Detection of LSB steganography via sample pair analysis,” *IEEE Transactions on Signal Processing* **51**, pp. 1995–2007, July 2003
- [12] H. Özer, I. Avcıbas, B. Sankur, and N. Memon, “Steganalysis of audio based on audio quality metrics,” *Proceedings*
- [13] Johnson, N.F. & Jajodia, S., “Exploring Steganography: Seeing the Unseen”, *Computer Journal*, February 1998
- [14] Johnson, N.F. & Jajodia, S., “Steganalysis of Images Created Using Current Steganography Software”, *Proceedings of the 2nd Information Hiding Workshop*, April 1998.
- [15] A. Tefas, A. Nikolaidis, N. Nikolaidis, V. Solachidis S. sekeridou, I. Pitas, Markov chaotic sequences for correlation based watermarking schemes, chaos, solitons& fractals 17 (2003) 567-573.
- [16] Singh, N., Sinha, A. Digital image watermarking using gyrator transform and chaotic maps ,*Optik*, 121 (15), pp. 1427-1437 (2010).
- [17] Ma, N., Zhang, Q., Wei, X. Novel image watermarking algorithm based on DWT and chaos theory , *Journal of Information and Computational Science*, 7 (7), pp. 1613-1620 (2010).
- [18] Zhang, X.-C., Zhang, C.-J., Jia, J. Digital image watermarking by double encryption with chaos and arnold , *GuangdianGongcheng/OptoElectronic Engineering*, 36 (8), pp. 116-122(2009).
- [19] Peng, H., Jiang, T. Application of chaotic map in the color image watermarking , *Wuhan LigongDaxueXuebao (JiaotongKexue Yu Gongcheng Ban)/Journal of Wuhan University of Technology (Transportation Science and Engineering)*, 33 (4), pp. 776-778(2009).
- [20] A. Peres, Quantum Theory: Concepts and Methods 24.
- [21] Zhao Dawei, Chen Guanrong, “A Chaos-Based Robust Wavelet-Domain Watermarking Algorithm ”, *Chaos, Solitons and Fractals*22(2004) 47-54
- [22] JA.Logan, JC.Allen' Nonlinear Dynamics and chaos in insect population, *Annual Review of Entomology*, 37(1), 1992, pp. 455-477
- [23] V.S. Miller, Use of elliptic curves in cryptography. *Advances in cryptology CRYPTO 85* 1986, pp.417-426.
- [24] W.B. Pennebaker and J. L. Mitchell, *JPEG Still Image Data Compression* Standaard. Chapman & Hall, New York, 1993.
- [25] T. Acharya and P. Tsai, *JPEG2000 Standard for Image Compression: Concepts, Algorithms and VLSI Architectures*, Wiley, Hoboken, NJ,2004.
- [26] T.S. Huang, G. I.Yang, and G. Y .Tang, A Fast Two-Dimensional Median Filtering Algorithm, *IEEE Trans. Acoustics, Speech, and Signal processing*, ASSP-27, 1, 1979, pp.13-18.
- [27] R. C. Gonzalez, R. E. Woods, *Digital Image Processing*, Addisonwesley, Reading, MA, 1992.
- [28] W.K. Pratt, *Digital Image Processing*, 2nd ed., Wiley, New York, 1991.
- [29] DeyunPeng, Jiazhen Wang, Peixin Yan, Sumin Yang, Jianli Hu, “A secure dual digital watermarking technique based on wavelet transform and chaos system”, *International Society for Optical Engineering*,2005
- [30] M. Falcioni, L. Palatella, S. Pigolotti, Properties making a chaotic system a good pseudo random number generator, *Phys. Rev. E* 72 (2005) 016220-10. IMAGE ENCRYPTION BASED ON JACOBIAN ELLIPTIC MAPS 7
- [31] C.M. Gonzalez, H.A. Larrondoa, O.A. Rosso, Intensive statistical complexity measure of pseudorandom number generators, *PhysicaA* 354 (2005) 133-138.
- [32] A. Rosenfeld, A. C. Kak, *Digital Picture Processing*, 2nd ed., Vol. 1, Academic Press, 1982.
- [33] S. H. Strogatz “Nonlinear Dynamics and Chaos: With Applications To Physics, Biology, Chemistry, And Engineering”, *Westview Press*, 1996.
- [34] R. C. Gonzalez, R. E. Woods, *Digital Image Processing*, Addison-wesley, Reading, MA, 1992.

Amir Houshang Arab Avval obtained his BSC and degrees in electrical engineering from university of Najaf Abad, Iran in 1995 and he obtained his MSC inUniversity of Sistan and Baluchestan, Iran in 2013.His areas of research include signal and image processing.

Shahram Mohanna received his BSc and MSc degrees in electrical engineering from the University of Sistan and Baluchestan, Iran and the University of Shiraz, Iran in 1990 and 1994,respectively. He then joined the University of Sistan and Baluchestan,Iran.In 2005, he obtained his PhD degree in communication engineering from the University of Manchester, England. As an assistant professor at the University of Sistan and Baluchestan, his areas of research include signal processing and applied electromagnetic. Dr. Mohanna published several journal papers and attended a number of international conferences.