VOL. 13, NO. 23, DECEMBER 2018 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

MULTIMEDIA STEGANOGRAPHY BASED ON MODIFIED LSB TECHNIQUE

Hussien Y. Radhi
Department of Computer Engineering, College of Engineering, University of Diyala, Diyala, Iraq
E-Mail: hussien.yossif19820@gmail.com

ABSTRACT

Multimedia steganography is one of the most important technologies to secure different kinds of data in today networked environment. It can embed large amounts of data safely inside multimedia files in objective to deviate the attention of attackers of existing data. In addition, the data encryption techniques can be added with steganography technologies to strength data protection. In this paper, we proposed a method to hide image and text files inside a video using LSB technique and chaotic systems. Two keys are used to secure data such that first key employed to select specific frames form video and the second key to select columns inside selected frame images to embed data. Three image quality measures are used to compute the quality of Stego images in our experiments including MSE, PSNR and SSIM. Experimental results show that the proposed method is secure enough to prevent attackers from stealing encrypted images and text files.

Keywords: steganography, cryptography, chaos, PSNR, SSIM.

INTRODUCTION

Steganography is an art of hiding different kinds of information such as texts, sounds and images in another different digital media. So, only the transmitter and receiver know the existence of hidden information [1,2,3,4]. inside cover digital media such as video. It is different from cryptography science in terms that the attacker does not suspect there is hidden information inside digital cover while the encryption converts plain information into another apparent scrambled information. In other words, the cryptography and steganography are different complementary sciences. They aim to achieve full protection of data, computers, networks, operating systems, databases and communication channels by providing concealment, confidentiality, integrity and authentication as security services. For example, the concealment security service hides information inside video in specific locations of selected frames such that replaces the eighth bit of the pixel's using proposed multi-border equation [5,6,7,8]. The selection of concealment cover is based on the amount of information to be hidden, efficiency, security and the quality of steganography process.

In general, the steganography technique should have four important characteristics to be effective [9,10,11,12]. First, confidentiality is very important characteristic that enable both sender and receiver to communicate safely and privately. Second, information quality is the process to keep digital carrier quality have always high quality without any noise and distortion. Third, capacity is one of the most relevant properties of steganography that implies how much information can hide inside the digital media carrier. Lastly, the accuracy represents how much accurate and reliable the extraction of information from digital medium. Video is a signal consisting of a series of fixed size images. It can be converted into a large number of images to be used partially or totally to hide large amounts of information [13,14,15]. Video files give more flexibility and security to the process of hiding information and they are more resistant to the attacks because the concealment of information inside them is more complex than image. Also, there is exist an audio file with video that contains a large number of unused pixels up to four bits to hide the information. Hence, it is not easy to know the hidden data inside the video as easily as the image [16,17]. The process of video based steganography is accomplished using least significant bit (LSB) technique. LSB hide bits inside the eighth bit of image pixel (i.e. least significant bit of on the left). This replacement technology of less important bits is used for redundant pixels in the cover images of the high quality video. This technique is considered the easiest one among concealment techniques but it can be considered very important in terms of not generating distortions in the cover file. For instance, we can use LSB technique to hide data in video such that data is hidden in the spatial domain. Also, the transmitted information were compressed and encrypted before hiding for more security [18,19,20,21]. Peak Signal to Noise Ratio (PSNR) is an important tool to compute the quality of the steganography process. Also, undetectable is another important tool for detection capability of the hidden data and to determine how difficult it is to observe the presence of steganography process [22,23].The rest of paper is organized as follows. First,related work is explained. Then, cryptographic analysis is illustrated and then proposed method is explained. Simulation results and conclusions are presented in the last paper.

RELATED WORK

Some researchers proposed to combine both encryption and steganography to provide a high degree of security to transmitted information [22,23]. In this method, different kinds of data were encrypted and hidden in the random frames of video. For example, particular text was hidden in a bitmap image so that the data is hidden in the matching bits between the image and the data to give good results in terms of speed and resistance to the attacks. Odai

[24] proposeda new steganography algorithm which is called different size image segmentations. In this algorithm, the author used the theory of modified least significant bits where the information is hidden randomly way to obtain more security. Seifedine*et al.* [25] proposed a new algorithm that relies on embedding text inside an image using a secure key. It characterized by the small size of the resulting image as well as high speed concealment process. Orooba *et al.* [26] use LSB technique to develop a new method to hide information in a cover image so that data is hidden in certain bits of the image. Manisha *etal.* [27] used genetic algorithm as a tool to provide the key that used to complete the process of hiding information within an audio file. Anush *et al.* [28] proposed a technique of concealing frames of video in another video by using wavelet modulation. It works based on the principle of replacing the less important bits of a video are by the data frames. Parinita *et al.* [29] proposed to hide data in video using discrete wavelet packet transform (DWPT). The data is encrypted before hiding in the video to obtain more security against attacks. Kamesh *et al.* [30] proposed a method to hide large amounts of data within the video using Discrete Wavelet Transform (DWT) at high frequencies.

CRYPTOGRAPHY PROCESS

The cryptography of the input data is the first step in this research. Two chaotic systems are used to generate private key. The set of Chen systems are:

$$\begin{aligned} \dot{x}_2 &= a\,(y - x) \\ \dot{y}_2 &= (c - a)x - xz + cy \\ \dot{z}_2 &= xy - b\,z \end{aligned} \quad (1)$$

In addition, the equations of Lorenz system are [8]

$$\begin{aligned} \dot{x}_2 &= a\,(y - x) \\ \dot{y}_2 &= (b - z)x - y \\ \dot{z}_2 &= xy - c\,z \end{aligned} \quad (2)$$

For this work generate new key according to proposed key schedule.

$$\begin{aligned} x_3 &= \text{bitxor}(x_1, y_2) \\ y_3 &= \text{bitxor}(y_1, z_2) \\ z_3 &= \text{bitxor}(z_1, x_2) \end{aligned} \quad (3)$$

From this step obtain a new key and makes the work more strong. The $(x_3, y_3, z_3)$are used to generate the new random numbers sequences and then rearrange these numbers in descending order.

PROPOSED METHOD

We explain in this section our proposed method to hide an image and text inside special video as shown in block diagram below in Figure-1.

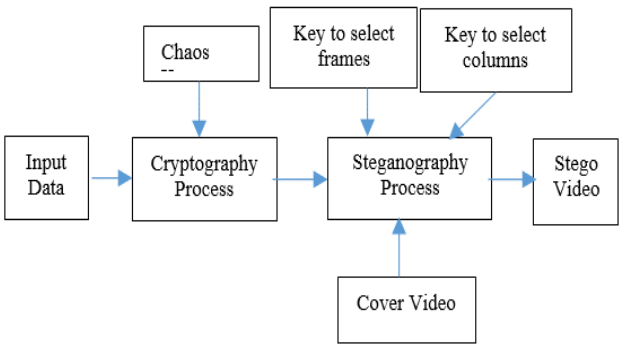


Figure-1. Block diagram of proposed method.

Encryption is the main tool to give more strength and safety to the protected data. Hence, it is applied to the image and text before steganography process in aim to be transmitted encrypted and hidden inside video. In this research, Lorenz and Chen chaos systems are used to perform the process of encrypting images and texts to eventually embed strongly scrambled data inside cover video. A 30-second video was used to hide the encrypted data. Audio is separated from video to hide part of the transmitted data. The video is converted to a set of frames as illustrated in Figure-2 and a special key is used to select specific frames to hide data in a way difficult to predict by attacker.

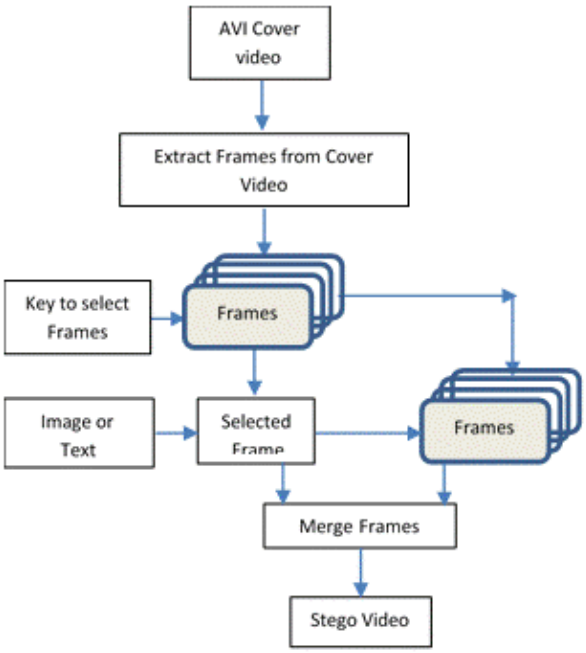


Figure-2. Another representation of proposed method.

LSB steganography technique is used in this research as an easy tool of information hiding to provide high degree of security. It can be regarded as an efficient method for information security in this paper because this algorithm used a special key to select certain columns of images to hide data randomly.

Our proposed approach to protect image or text at transmitter side is illustrated as follows:

a) Convert encrypted image or text to be secured into a binary system in the form of a matrix consisting of one column and a large set of rows. The image or text is encrypted using two chaotic key based systems.
b) This matrix is divided into specific parts so that some parts are hidden into the pre-selected images and the remaining parts are hidden in the audio file using LSB steganography technique. The first key used to select the columns for each image has a big role in increasing the security of the proposed system since it selects images and their columns randomly every time secure any bit of data.
c) Then these cover images are combined with each other to obtain the Stego video that carries the encrypted data. At this point the video is ready to be sent through the channel and on the other side it can retrieve encrypted hidden image or text within the video file.

Our proposed approach to retrieve protected image or text at receiver side is illustrated as follows:

a) The video is converted back into a group of images using the same first key that used to select images where the image or text is hidden.
b) Then use the second key to know the columns of each image in aim to ultimately integrate image or text parts from pre-selected images and the audio file into single whole image or text file.
c) Lastly the original encrypted image or text file is retrieved from video. It then decrypted the same chaos keys used in the transmitter.

STEGONGRAPHY ANALYSIS

Mean Square Error (MSE) is one of the most used measures to quantify the quality of quality of resultant image by measuring the difference between pixels of Stego and original images. Its mathematical equation [31]:

$$MSE = \frac{1}{M * N}\sum_{1}^{M}\sum_{1}^{N}(O_{ij} - g_{ij})^2 \quad (4)$$

Where M and N represent the number of rows and columns of the input images.

Peak Signal-to-Noise Ratio (PSNR) is another metric to calculate the quality of the Stego image. It compares the Stego and original images to obtain image quality in decibels and the higher the PSNR is the better the Stego image quality. PSNR is computed using the following equation [17]:

$$PSNR = 10\ log_{10}\frac{R^2}{MSE} \quad (5)$$

Where R^2 is the maximum images pixels values, for example, in gray scale image with 8 bits the maximum value is 255.Structural Similarity Measure (SSIM) is an innovative measure to quantify quality of compared images that introduced recently. The equation of this measure as follows:

$$SSIM\ (x,y) == \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (6)$$

Where x and y are windows of images X and Y and the explanation of the statistical parameters of this model can be found in reference [16].

$$MISSIM\ (X,Y) = \frac{1}{n}\sum_{i=1}^{n} SSIM\ (x_i, y_i) \quad (7)$$

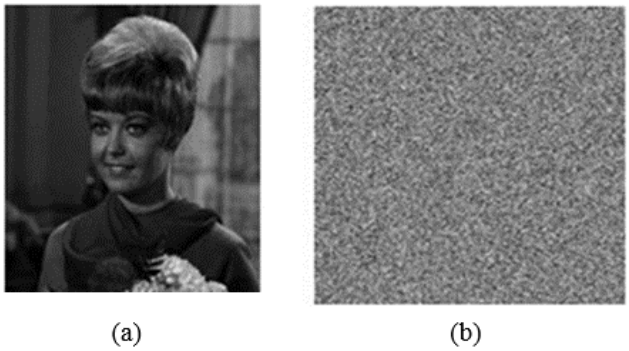
Mean SSIM is between two images X and Y over (n) windows.Table-1 below shows the values of these explained measures for certain frames of tested video.

Table-1. Values of MSE, PSNR and SSIM for video.

Frame No.	MSE	PSNR (db)	SSIM
1	0.013	76.46	0.530
2	0.012	76.73	0.601
3	0.012	77.32	0.67
4	0.012	77.56	0.605
5	0.012	77.64	0.65
6	0.012	77.32	0.525
7	0.013	77.46	0.615
8	0.024	77.73	0.540
9	0.021	77.32	0.550
10	0.015	77.56	0.675
11	0.012	75.42	0.642
12	0.010	75.61	0.580

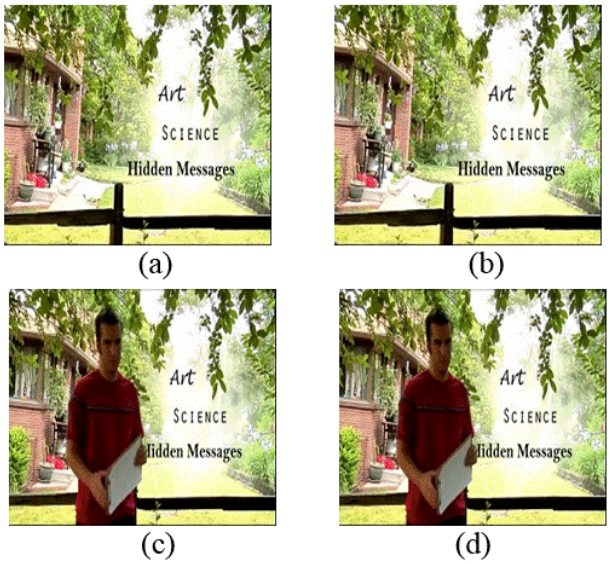
SIMULATION RESULTS

Several experiments have been conducted to prove the possibility of our proposed approach to secure multimedia contents. We can notice from figure 3 below that the encrypted image is totally different from original image. This means that even attacker found embedded image inside video than it is difficult to him decrypt this image to obtain original one. Hence, encryption is one the most significant tools to confuse and diffuse attacker from getting original image or text. Figure-4 is presented to show some frames of video before and after steganography process.



(a) (b)

Figure-3. Original and encrypted images.



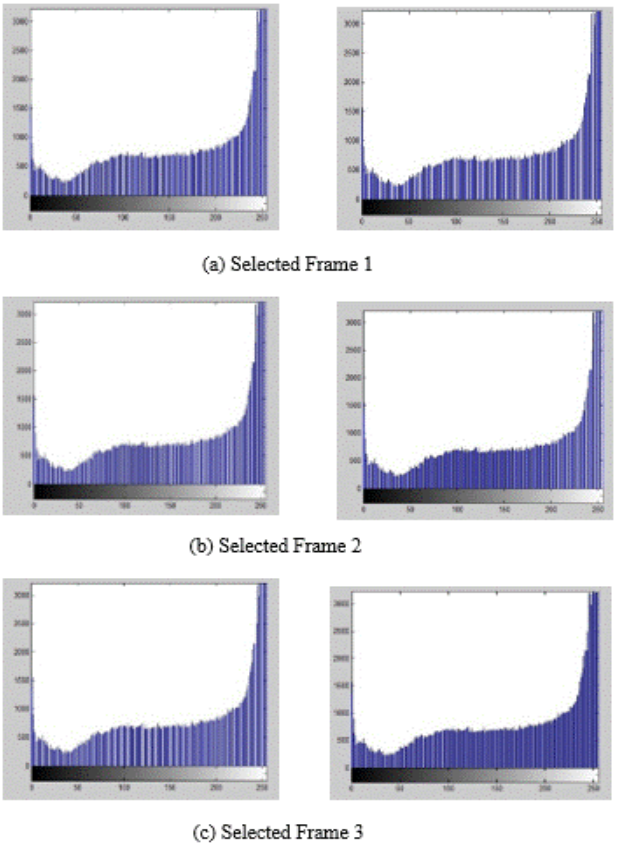
(a) (b) (c) (d)

Figure-4. Examples of frame images before (a,c) and after (b, d) steganography process.

Another way to illustrate the effect of steganography on the frames by showing the histogram of them. The following Figure-5 illustrate the histogram of some frames for the original and Stego frames in aim to prove that these histograms have no difference before and after information hiding process. These results indicate that the steganography process does not affect image quality and there is no any indication of hidden information inside frames of video.

CONCLUSIONS

We have proposed a new approach for multimedia steganography using modified LSB technique. Two security tools are used in this research including cryptography and steganography. The image or text data is encrypted using combined chaotic systems. Then the encrypted data is divided into parts and some of these parts are hidden inside pre-selected frames of video and remaining parts in the audio part of the video using a second key. It obvious from the results that the image can be recovered without any distortion in the cover and data.Also, the quality measures prove the strength of steganography and show that the proposed system is good and can be strong against attacks. As future work, will apply steganography and watermarking algorithms on the satellite images [32].



(a) Selected Frame 1

(b) Selected Frame 2

(c) Selected Frame 3

Figure-5. Histograms of some selected frame images before and after steganography process.

REFERENCES

[1] Mstafa R. J., Elleithy K. M. and Abdelfattah E. 2017. Video steganography techniques: Taxonomy, challenges and future directions. In Systems, Applications and Technology Conference (LISAT), 2017 IEEE Long Island (pp. 1-6). IEEE.

[2] Abboud A. J. and Jassim S. A. 2010. Image Quality Guided Approach for Adaptive Modelling of Biometric Intra-Class Variations. In Mobile Multimedia/Image Processing, Security, and Applications 2010, SPIE, 7708: 77080 L.

[3] Abboud A. J. and Jassim S. A. 2012. Incremental fusion of partial biometric information. In Mobile Multimedia/Image Processing, Security, and Applications 2012, SPIE, 8406: 84060K.

[4] Al-Assam H., Abboud A., Sellahewa H. and Jassim S. 2012.Exploiting Relative Entropy and Quality Analysis in Cumulative Partial Biometric Fusion.

In Transactions on Data Hiding and Multimedia Security, III: 1-18. Springer, Berlin, Heidelberg.

[5] Chobitkar Ashwini, Ubarhande Kiran, Dafale Ram B. N. An Approach to Video Steganography Using LSB Method. Satellite Conference ICSTSD 2016 International Conference on Science and Technology for Sustainable Development, Kuala Lumpur, MALAYSIA.

[6] Abboud A. J. and Jassim S. A. 2012.Biometric Templates Selection and Update Using Quality Measures. In Mobile Multimedia/Image Processing, Security, and Applications 2012, SPIE, 8406: 840609.

[7] Abboud A. J., Sellahewa H. and Jassim S. A. 2009. Quality Based Approach for Adaptive Face Recognition. In Mobile Multimedia/Image Processing, Security, and Applications 2009, SPIE, 7351: 73510N.

[8] Al-Assam H., Abboud A., and Jassim S. 2011. Hidden Assumption of Face Recognition Evaluation under Different Quality Conditions. In IEEE International Conference on Information Society (i-Society). pp. 27-32.

[9] Shinde M. P. V. and Rehman D. T. B. 2015. A Survey: Video Steganography techniques. Internati onal Journal of Engineering Research and General Science. 1(1).

[10] Jassim A. J., Al-Assam H., Abboud A. J. and Sellahewa H. 2010.Analysis of Relative Entropy, Accuracy and Quality of Face Biometric. In Proceedings of the Workshop on Pattern Recognition for IT.

[11] Al-Assam H., Abboud A. and Jassim S. 2011. Exploiting Samples Quality in Evaluating and Improving Performance of Biometric Systems. International Journal of Digital Society (IJDS). 2(2): 462-468.

[12] Abboud A. J. 2015. Multifactor Authentication for Software Protection. 8(4): 479-492.

[13] Pal Souma; Kumar Samir; Mahto Supriya and Togarwar Shilpa. 2016. Various Methods of Video Steganography. International Journal of Information Research and Review.

[14] Abboud A. J. 2011. Quality Aware Adaptive Biometric Systems. Ph.D. Thesis, UK, University of Buckingham, British Library, EthOS.

[15] Abboud A. 2015. Protecting Documents Using Visual Cryptography. International Journal of Engineering Research and General Science. 3(2): 464-470.

[16] Nasreen S. M., Jalewal G., and Sutradhar S. 2015. A Study on Video Steganographic Techniques. International Journal of Computational Engineering Research. p. 5.

[17] Abboud A. J. and Saleh O. S. Sustainable IT: A Realisation Survey among Academic Institutions of Iraq. International Journal of Enhanced Research in Science Technology and Engineering. 3(2): 25-31.

[18] K. Karthika, K. Sivakumar. 2017. Secure Video Sharing Using Video Steganography and Compression Technique. SSRG International Journal of Computer Science and Engineering - (ICCREST'17) - Special Issue. March 2017.

[19] Albu-Rghaif Ali N., Jassim Abbood K. and Abboud Ali J. 2018. A Data Structure Encryption Algorithm based on Circular Queue to Enhance Data Security. 2018 1st IEEE International Scientific Conference of Engineering Sciences - 3rdScientific Conference of Engineering Science (ISCES). pp. 24-29.

[20] Katre B. 2017. Dynamic Key based LSB Technique for Steganography. International Journal of Computer Applications. 167(13).

[21] Singh K. U. 2014. Video steganography: text hiding in video by LSB substitution. Int. Journal of Engineering Research and Applications. p. 4.

[22] Thakur A., Singh H. and Sharda S. 2015. Transferring Different Techniques of Image and Video Steganography: A Review. International Journal of Electronics and Electrical Engineering. 2(2).

[23] Farhan L.; Alzubaidi L.; Abdulsalam M.; Abboud Ali J.; Hammoudeh M.; Kharel R.2018. An efficient data packet scheduling scheme for Internet of Things networks. 2018 1st IEEE International Scientific Conference of Engineering Sciences - 3rd Scientific Conference of Engineering Science (ISCES). pp. 1-6.

[24] Al-Shatanawi O. M. and El Emam N. N. 2015. A new image steganography algorithm based on MLSB method with random pixels selection. International

Journal of Network Security & Its Applications. 7(2): 37.

[25] Kadry S. and Nasr S. 2013. New Generating Technique for Image Steganography. Lecture Notes on Software Engineering. 1(2): 190.

[26] Al-Farraji Orooba I. I.; Hoyer-Klick Carsten. 2017. Global New Technique of Steganography Based on Locations of Lsb. International Journal of Information Research and Review. 04(01): 3549-3553.

[27] Rana M. and Tanwar R. 2014. Genetic Algorithm in Audio Steganography. arXiv preprint arXiv:1407.2729.

[28] Kolakalur A., Kagalidis I. and Vuksanovic B. 2016. Wavelet Based Color Video Steganography. International Journal of Engineering and Technology. 8(3): 165.

[29] Sahu P. and Sinha S. 2017. Discrete Wavelet Packet Transform Based Video Steganography. International Journal of Information Research and Review. 04(01): 3549-3553.

[30] Kamesh S., Devi K. D., Raviteja S.N.V.P.2017. Dwt Based Data Hiding Using Video Steganography. International Journal of Engineering Sciences and Research Technology ISSN: 2277-9655.

[31] Kamdar N. P., Kamdar D. G., and Khandhar D. N.2013. Performance evaluation of lsb based steganography for optimization of psnr and mse. Journal of information, knowledge and research in electronics and communication engineering. 2(2): 505-509.

[32] Abboud A. J., Albu-Rghaif A. N. , Jassim A. K.,2018. Balancing compression and encryption of satellite imagery. International Journal of Electrical and Computer Engineering. 8(5): 3568-3586.