Improving the Security of Steganography in Video Using Genetic Algorithm

ZAHRAA JASIM JABER[1], MOHANAD J. ALTALQANI[2]

[1]E-mail: zahraaj.altalakany@uokufa.edu.iq [2] E-mail: mohanad.altalqani@uokufa.edu.iq

[1]Department of Computer Science, Faculty of Computer Science and Mathematics, University of Kufa, Najaf, Iraq

[2]Department of Basic Science, College of Dentistry, Kufa University, Najaf, Iraq

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract:

There has been a great development in information technology and methods of sending it via the Internet, but these developments expose the information transferred to violations of its security. To maintain information security, steganography and encryption are used. Hiding technology in multimedia, such as audio, video, text or pictures, provides an ability to protect information. Digital video is one of the most common data embedding media for its high ability to hide sensitive data. Where many methods have been proposed to hide the data in the video to prevent it from being seen by unauthorized persons. This paper proposes a new approach to hiding data in video by using two bitand and bitor processes without using the well-known LSB algorithm in the hiding method. In addition, confidential information is first encrypted using a genetic algorithm by which the encryption key is generated, which increases the strength of the proposed work. The experimental results showed that the used method is effective and safe as it provides a PSNR of 63, which makes the embedding capacity high.

Keyword: LSB, Hidden image, Genetic algorithm, Video steganography, Data embedding.

1. Introduction

Lately, the rapid advancement in communications technology leads to raising the need for information security. People exchange information directly using communications technology like a local area network, or the Internet [1].

" Security Threat" is one of the major problems related to transfer information over the internet. Secret information should be well secured in order to transfer it; therefore, information security became very significant and very important factor to complete the transfer successfully without hacking it [2]. Information security refers to the protection of data from a hacker or unauthorized users, it provides high security to prevent data modification. There are many techniques used for this purpose such as Cryptography, Information hiding (Steganography and digital watermarking) to improve the security features in information transfers over the internet.[3]

In encryption, the information is converted to unreadable form. Only the authorized user can retrieve the information using a secret key provided by the channel. This encrypted information raises the suspicion of a hacker for existence the secret information and trying to decipher the code to obtain the information. To avoid this problem, information hiding has become more important which aims at hiding the existence of secret information .[4]

Information hiding techniques are classified into two sections: steganography and watermarking. Characteristics of the information hiding techniques comprise (a) imperceptibility, (b) survivability, (c) capacity, and (d) security [5, 6].

Steganography is a system for hiding information. It aims to hide secret information into a digital cover file (image, audio, video, etc.) without being suspicious. On the other hand, Steganalysis technique aims to detect the existence of secret data that hidden in the cover files. A Steganographic

system considered broken if the attacker was able to reveal a presence or read the concealed message [7, 8].

In, this paper, we use both encryption and steganography techniques to increase the security of the transmitted data. The confidential data is encrypted using one of the artificial intelligence algorithms through which the encryption key is generated. Then this encrypted data is hidden inside the video randomly. The use of the genetic algorithm in generating the encryption key increases the power of the work, as it is not possible to decode the code by unauthorized persons even if they know the presence of the message inside the video.

2. Related work

Gupta et al. Proposed robust video steganography based on frequency domain. The embedding position is the redundant coefficient. Applied DWT on the video file. Then, using LSB process the hidden data embedded in the lowest plane. In this approach, to increase the robustness of the design, redundancy is used. In addition, a key used to improve the embedding and extraction operations is used to increase the layer of the security [9].

Alia used a method of embedding confidential information directly into the video. The masking method was based on matching the confidential information bits with the video frame bits. This match is used to randomly generate the hide key. [10].

Mstafa et al. Suggested method for embedding data within the video. The method relies on first encrypting confidential data using Arnold's cat map in order to increase security. Then the embedding method is based on Shi-Tomasi's algorithm, which detects the corner points in video frames. After determining the corner points in the tire, the confidential data is embedded in these points using the LSBs algorithm. The ratios of the PSNR measurements were 60.7 dB [11].

Nyo used two hiding and encryption techniques together to protect the transmitted data. Arnold scrambling and discrete wavelet transform (DWT) technology was used for confidential information (picture) first, then reference values are calculated from confidential information using a secret key. This key is encrypted with Twisted Exchange algorithm. The information is then hidden in the video using the least significant bit (LSB) algorithm. The experimental results showed that the value of the PSNR scale reached 30 dB [12].

3. Proposed Method

The proposed method consists of two parts the first part embedding (encryption and hidden):

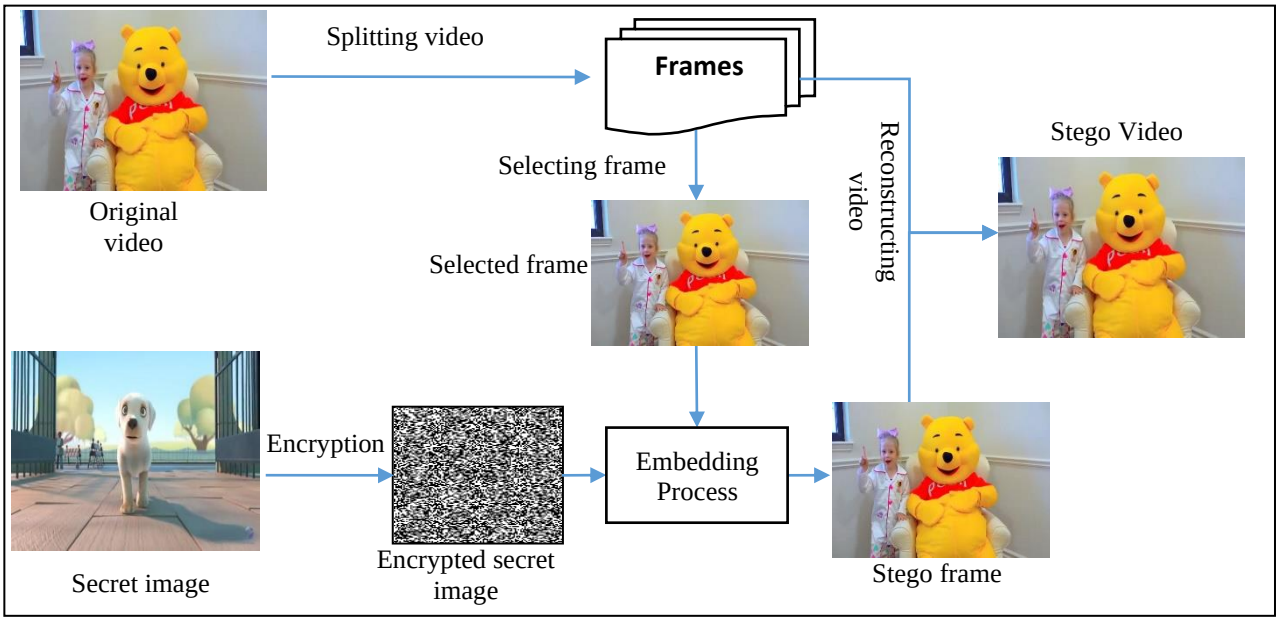
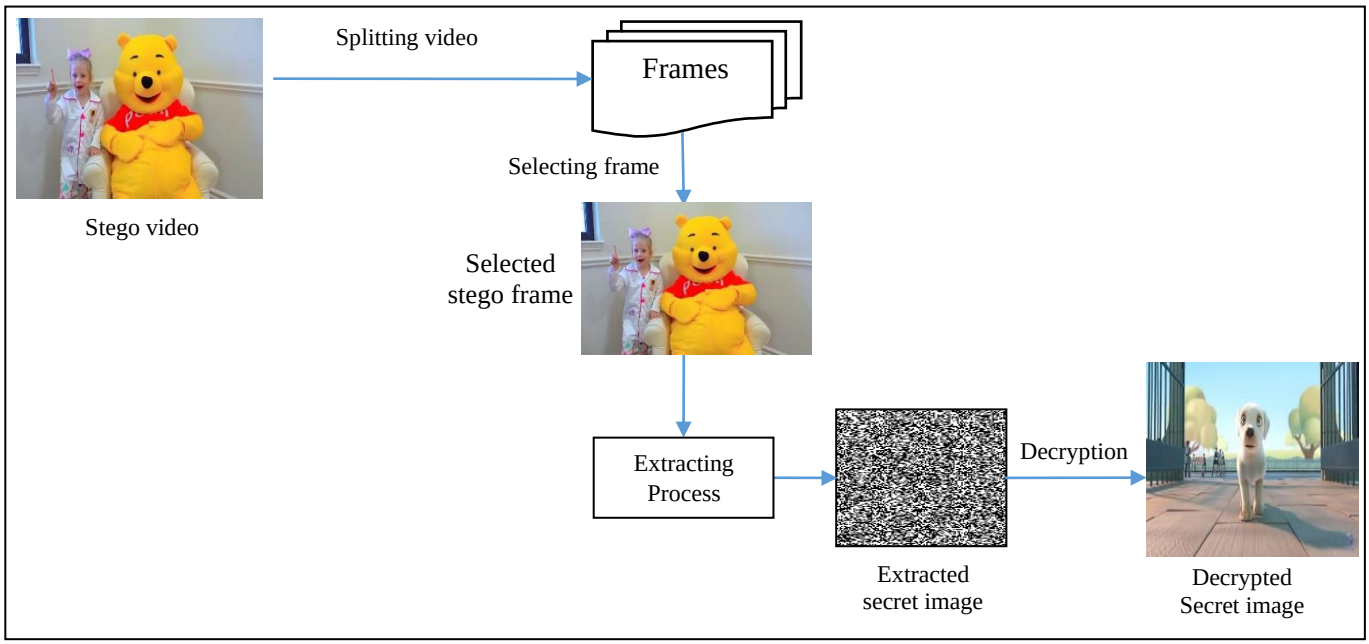


Fig 1. Steps of embedding method.



The second part extraction:

Fig 2. Steps of extraction method.

3.1 Encryption Image

Encrypting the secret message (image) requires a key and an algorithm to encrypt it. The key is generated using a genetic algorithm.

3.1.1 Genetic Algorithm

John Holland as effective ways to solve research and optimization problems presents genetic algorithms (GAs). Genetic algorithms are powerful and randomized research methods that rely on a great deal of implicit parallelism. The theory of natural genetics and evolution of genes is the basis of the work of the genetic algorithm. Following the Darwin concept of evolution, the genetic algorithm begins by preparing a set of potential coded solutions called chromosomes. Each solution contains the fitness value, based on the values of fitness are chosen from the parents to reproduce (survival of the fittest). Genetic factors are applied to the current generation to build the new generation such as selection (build a mating pool based on natural selection), crossover (Information between parents is exchanged) and mutation (A little change occurs in a parent) on chosen parents. Thus, as the number of generations increases, the quality of the population enhanced. This process continues until a determined criterion reached or the solutions reaches certain improved values [13, 14].

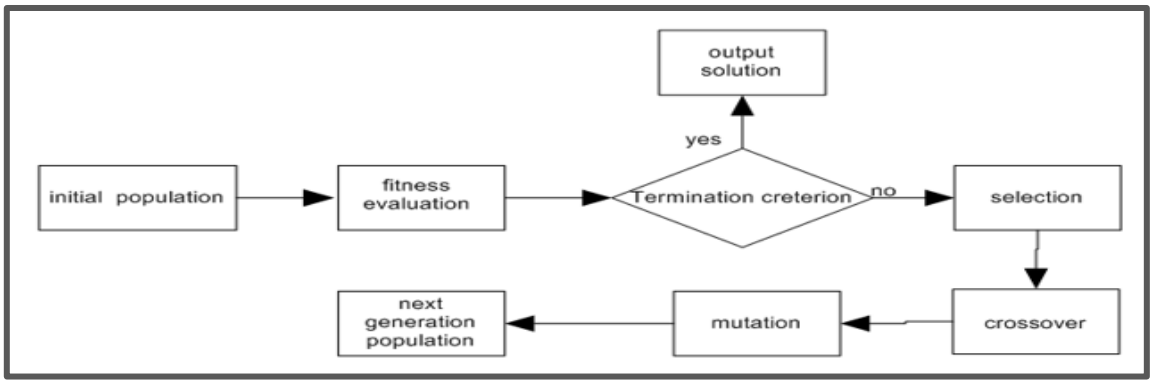


Fig 3. Steps of Genetic Algorithm.

Algorithm 1: Genetic algorithm

Input: Random binary matrix.

Output: optimal binary matrix.

Begin:

1- Generate initial population(chromosomes), where size of population based on n
2- Select part of population randomly
3- Compute fitness function to each chromosome then select part of chromosomes based on fitness function (select best chromosomes).
4- WHILE stop condition (fitness function of children worse than parents) is false DO
5- Select two chromosomes to Perform one-point crossover and generate two new children.
6- Compute fitness function to parents and children and select the chromosomes with the best fitness function.
7- Perform mutation operator (rate 0.01) on chromosomes.
8- Compute fitness function to children generate from step7, compare it with parent, and select best chromosome.

End

- The best chromosomes chosen as the seed in the key generation, where the binary chromosomes converted into a numerical value.
- ***Secret Image Encryption***: The secret image is encrypted using the following steps:

Input: Color or gray-scale image.
Output: Encryption image.
Begin:
1. Read gray scale image.
2. Generate the key using the seed (best binary chromosomes) using the following equation:

For i=1 to N
For j=1 to M

$$Key = (\mathbf{seed}^2 \times \mathbf{j}^2) + (\mathbf{seed}^2 \times \mathbf{i}^2) \bmod 255$$

end
end

3. Encrypting the image by making bitand operation between the key generated and origin image.
4. Encrypting the image by making bitor operation between the key generated and result from step 3.

3.2 Hidden encryption image inside Video

This part represents the non-sequential hiding of confidential data within the video.

3.2.1 Embedding Process: This process done as in the following steps:

Input: Origin video.
Output: Stego video.
Begin:
1. Selecting video.
2. Splitting the video into frames.

3. Select even frames.
4. Embedding the secret image in even frame using bitand & bitor operation.
5. Reconstructing the stego video by combining the stego frame with other frames of video.

End

***Embedding consists of several steps, including:**

1. Selecting the video (cover) that consists of several frames. The frames are separated from each other.
2. The confidential message is converted into binary and this binary data is contained within the video frames.
3. Choose marital frames only. Each frame is a color image consisting of three layers. The embedding is only one layer of each frame. In the first frame, the inclusion is in the red layer. In the second frame, the inclusion is in the green layer. In the third frame, the inclusion is in the blue layer. And so on for the rest of the frames.
4. The inclusion done using two cases.
   If bit of secret image is '0' using bitand between pixel of frame and 254.
   If bit of secret image is '1' using bitor between pixel of frame and 1.
5. Combining embedding frames with odd frames for video and video display in an integrated manner.

3.2.2 Extracting Secret Image Process

This process consists of two activities namely secret image extracting and secret image decryption. The following steps listed for doing the extracting process:

Input: Stego video.
Output: Secret image.
Begin:
1. Selecting the stego video.
2. Splitting the video into frames.
3. Selecting the stego frame (even frames).
4. Extracting the secret message from the selected stego frames and decryption image.

End

***Extraction consists of several steps, including:**

1. Choose video after embedding. The frames are separated from each other.
2. Choose the marital frames in which the message is included and specify the class for all the frames.
3. Extracting bits by making a mode between the frame pixel and the digital value '2'.
4. Converting the extracted bits into digital values in the form of a two-dimensional image.
5. Decryption the image with the same key used in encryption.

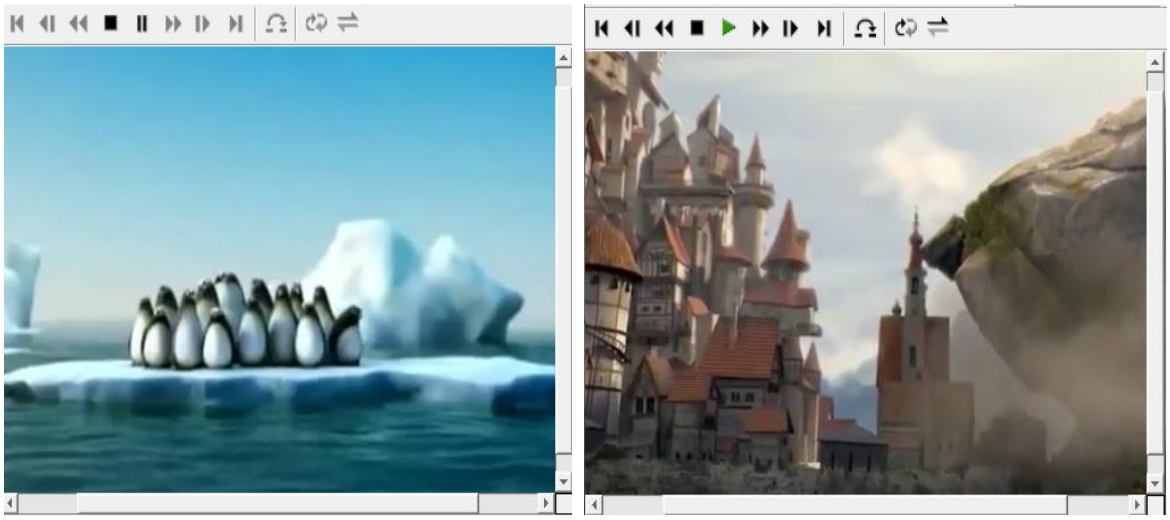
4. Experimental results

In this section, we will explain the results. It includes two parts, one of which includes encrypting the secret message and the other part includes hiding it inside the video.

A **B** **C** **D**

Fig. 5: (A, C) represent the origin image. (B, D) represent the encryption image.

We will include the encoded image (B) in the first video and image (D) in the second video. Then find the proportions of the PSNR and MSE measures to find out the amount of change in the video after the embedding. The encoded image size (128 * 128) can be of different other sizes.



Video1 **Video2**

Fig. 6: Screenshot taken for the video1 and video2.

Table1. Values of PSNR and MSE for stego video.

Test video1 (358×640)	
PSNR	**63.56**
MSE	**0.083**
Test video2 (360×640)	
PSNR	**60.87**
MSE	**0.091**

The method of embedding in non-sequential frames in addition to one layer in each frame increases the power of embedding and lack of knowledge by unauthorized persons. Because concealment in this way reduces the change in the shape of the frame, so we notice that the frame before and after embedding itself. The scale value also exceeded half the ideal value.

It is possible to use a video filmed by the sender himself and embedding in the suggested manner so that unauthorized persons cannot apply the scale between the video before and after the embedding.

5. Conclusion

In this paper, a method proposed that uses encryption and steganography techniques to provide greater protection for data sent over insecure channels. The encryption method based on the genetic algorithm gave good results, which increased the strength of the encryption, as unauthorized people could not know the key without knowing the random seeds that generated using this algorithm. The embedding of even and single-layer frames also makes the video look natural and uninterrupted. The experimental results of this method showed that the inclusion was of high quality and the metric values were close to the ideal value. This indicates that this method fulfills the lack of feeling of the inclusion in the video.

[1] S. Chikouche, & N. Chikouche (2017, October). An improved approach for lsb-based image steganography using AES algorithm. In 2017 5th International Conference on Electrical Engineering-Boumerdes (ICEE-B) (pp. 1-6). IEEE.

[2] A. Qadir, & N. Varol, (2019, June). A Review Paper on Cryptography. In 2019 7th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.
[3] A. Arya, & S. Soni, (2018). A literature review on various recent steganography techniques. *International Journal on Future Revolution in Computer Science & Communication Engineering*, *4*(1), 143-149.
[4] koduri, N. "Information security through image steganography using least significant bit algorithm," Master Thesis, Information Security and Computer Forensics University of East London, 2011.
[5] M Kavitha, Z. H. Mahmoud, Kakarla Hari Kishore, AM Petrov, Aleksandr Lekomtsev, Pavel Iliushin, Angelina Olegovna Zekiy, Mohammad Salmani. Application of Steinberg Model for Vibration Lifetime Evaluation of Sn-Ag-Cu-Based Solder Joints in Power Semiconductors. IEEE Transactions on Components, Packaging and Manufacturing Technology. 2021; 11(3):444-450
[6] M. Bilal , S. Imtiaz , W. Abdul , S. Ghouzali , and S. Asif, "Chaos based Zero-steganography algorithm," *Multimedia tools and applications*, vol. 72, No. 2, pp. 1073-1092, 2014.
[7] W. Luo, F. Huang, & J. Huang, "Edge adaptive image steganography based on LSB matching revisited," *IEEE transactions on information forensics and security*, vol. 5, No. 2, pp. 201-214, 2010.
[8] Mstafa, R. J., Younis, Y. M., Hussein, H. I., & Atto, M. (2020). A New Video Steganography Scheme Based on Shi-Tomasi Corner Detector. *IEEE Access*, *8*, 161825-161837.
[9] Gupta, Shivani, Gargi Kalia, and Preeti Sondhi. "Video Steganography Using Discrete Wavelet Transform and Artificial Intelligence." International Journal of Trend in Scientific Research and Development 3.4 (2019).
[10] Alia, M. A., Maria, K. A., Alsarayreh, M. A., Maria, E. A., & Almanasra, S. (2019, April). An Improved Video Steganography: Using Random Key-Dependent. In 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT) (pp. 234-237). IEEE.
[11] Mstafa, R. J., Younis, Y. M., Hussein, H. I., & Atto, M. (2020). A New Video Steganography Scheme Based on Shi-Tomasi Corner Detector. *IEEE Access*, *8*, 161825-161837.
[12] Nyo, H. L., & Oo, A. W. (2019). Secure Data Transmission of Video Steganography Using Arnold Scrambling and DWT. *International Journal of Computer Network & Information Security*, *11*(6).
[13] Mirjalili, S. (2019). Genetic algorithm. In *Evolutionary algorithms and neural networks* (pp. 43-55). Springer, Cham.
[14] Bandyopadhyay, S. and Sankar, K. .Classification and learning using genetic algorithms: applications in bioinformatics and web intelligence. Springer Science & Business Media, 2007.