



Combining A Cryptography and Steganography Techniques – Based Securing Transmitted Video Through Unsecure Channel

Hawra'a Razzak Radhi¹

Majid Jabbar Jawad²

1. Computer Sciences Department, College of Sciences for Girls, University of Babylon, Babylon, Iraq.

hawraa.radhi@student.uobabylon.edu.iq

2. Computer Sciences Department, College of Sciences for Girls, University of Babylon, Babylon, Iraq

wsci.majid.jabbar@uobabylon.edu.iq

Article Information

Submission date: 22/ 10/ 2020

Acceptance date: 8 / 11/ 2020

Publication date: 31 / 12/ 2020

Abstract

The Internet has become one of the important means used to transfer information via e-mail, social media, and others. It has become important to protect this information and find the best and most secure way to transfer and it to protect it from piracy attempts and common attacks on the Internet. In this paper, the encryption and steganography techniques are used to secure a transmitted through unsecure network. In this paper, we proposed a method for encryption images using second-order equations, then the encrypted image is embedded in the vide. The image is embedded according to the equations rather than embedding it sequentially in order to increase the security layer. The experimental results suggest that the approach proposed is achieves a high embedding ability. In addition, encryption and non-sequential selection of frames and locations for bit hiding increases the safety and robustness of the proposed system when compared to other methods of hiding information.

Keywords: Steganography, Cryptography, Video Steganography

1. Introduction

A unique means of protection mechanisms is being implemented by the growth of modern communication technologies. All individuals need the confidentiality and security of their communication data. When exchanging data through an open network, information security is a major issue of concern. As the amount of data being transmitted through the Internet increases day by day, network security is becoming more important. Cryptography and steganography are the two main techniques used to provide protection. [1].

A cryptography is used for ciphering information or data to achieve confidentiality of the information in a way that an unauthorized third party cannot understand its meaning [2].

A steganography is used for hiding content of information within any multimedia content such as image, audio, video. To increase the confidentiality of transmitted data, the cryptography and steganography techniques may be combined.[3].

2. Related works

This section reviews in brief some of the previously proposed methods related video Steganography:

Singh et al. [4] Hidden data can be a text file, an image, or an audio file. Diamond-encoding scheme used to mask a text file or image in a video frame. The authors note that the diamond encoding scheme has a high capacity / image quality ratio. The DCT used to cover hidden audio files in video frames. Using DCT, there are no noticeable changes to the frames; however, they are statistically observable

Ziabari [5] Steganography concealed a file within some another file. These types of files are suitable for the encryption due to high redundancy and large size of the video file. In this paper, the authors implement a new algorithm mainly for encrypted the data for video files by using encryption techniques. The proposed algorithm divides and encrypts the secret data using motion vectors and to check the data changes in each vector.

Gupta et al. [6] 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.

Nikam et al. [7] presented with the help of the Internet, data can be transferred from one place to another with high speed. It is very risky to transfer the data over the internet for security purpose. The various steganography techniques are used curity of the concealed data. to prevent and maintain the information from an unauthorized person from extracting the critical information. Steganography technique mainly used for hiding the secret data including image, text, video, and audio. This type of secret information will be hidden in audio, image, text and video files. Video steganography referred to as hiding secret information in the video file.

3. The Proposed method of video steganography

The suggested method of video steganography consists of two processes namely embedding and extracting. The details of the above processes are listed as follows:

3.2 Embedding secret image process

Before the embedding process is done, the hidden data will be encrypted and then hide it in the host video. Figure 1 illustrates the block diagram of the embedding process.

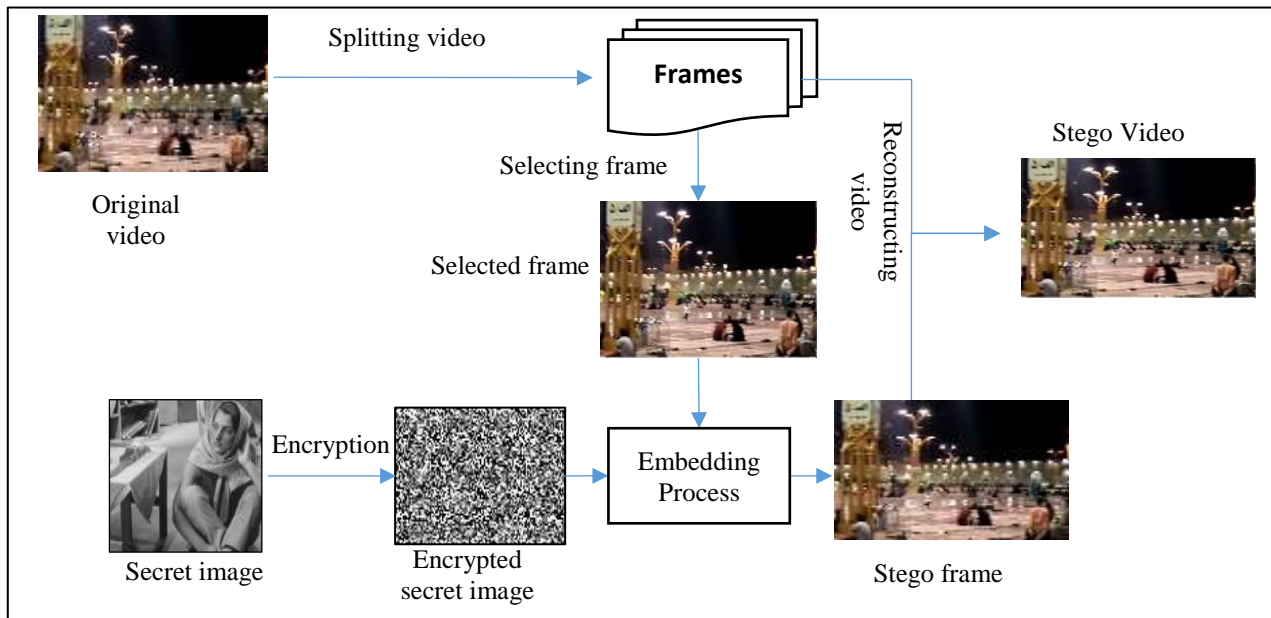


Fig. 1: Embedding Process

- **Secret Image Encryption:** The secret image is encrypted using the following steps:

Step One: Read gray scale image.

Step Two: Generating a random seed represented by a certain value determined by the sender

Step Three: Generate the encryption key based on the random seed and use the f equation below:

```

For i=1 to N
  For j=1 to M
    Key = (seed2 × j2) + (seed2 × i2) mod 255
  end
end

```

Step Four: Encrypting the image by making a Xor between the key generated

Figure 2 shows an example of the original and the encrypted secret image.

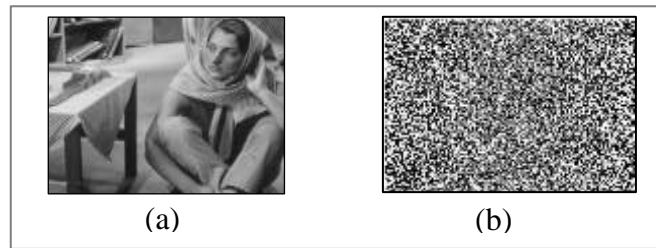


Fig. 2 (a) Original secret image **(b)** Encrypted secret image

The encrypted secret image is ready for embedding in the selected frame of video.

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

- Step 1: Selecting video file as a host.
- Step 2: Splitting the video into frames.
- Step 3: Select one frame.
- Step 4: Embedding the secret image in the selected frame using LSB method.
- Step 5: Reconstructing the stego video by combining the stego frame with other frames of video.

3.1 Extracting Secret Image Process

This process consists of two activities namely secret image extracting and secret image decryption. Figure 3 illustrates the block diagram of the extracting process. The following steps listed for doing the extracting process:

- Step 1: Selecting the stego video file.
- Step 2: Splitting the video into frames.
- Step 3: Selecting the stego frame.
- Step 4: Extracting the secret message from the selected stego frame

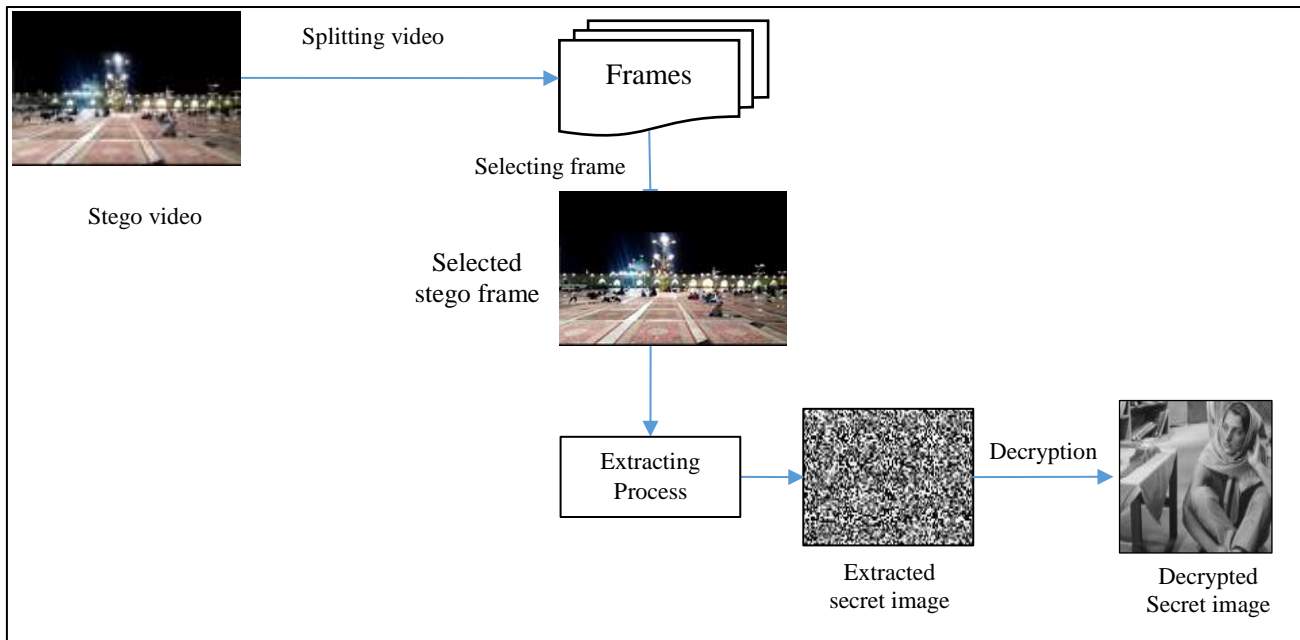


Fig 3: Extracting process

- **Secret Image Decryption**

The following steps perform the decryption process:

Step One: Read encryption image.
Step Two: Generating a random seed represented by a certain value determined by the receiver.
Step Three: Generate the decryption key based on the random seed and use the equation below:
 For i=1 to N
 For j=1 to M
 $Key = (seed^2 \times j^2) + (seed^2 \times i^2) \bmod 255$
 end
 end
Step Four: decrypting the image by making a Xor between the key generated

Figure 4 shows an example of the encrypted secret image and the decrypted secret image.

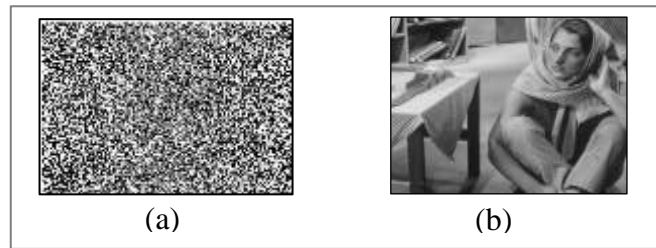


Fig. 4 (a) Encryption secret image (b) decrypted secret image

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) Encryption gray-scale image:













Fig. 5 (A) Origin image (B) encryption image.

b) Hiding the encryption image in video

The video consists of a group of frames, each frame representing a color image with equal dimensions for each frame.

The duration of this video is 10 seconds. It consists of 309 frames. Dimensions of each frame 720×1280 . Image A we hidden inside the frames for this video. The dimensions of the image were 512×512

The seed was individual, so it hidden in the individual, frames and in the even positions of each frame. Table 1 explains the values of PSNR and MSE after embedding operation.

Frame #	Original Frame	Stego Frame	MSE	PSNR
1			0.0834	58.9195
3			0.0834	58.9182
27			0.0835	58.9146
29			0.0835	58.9161
53			0.0834	58.9182



55			0.0545	60.7692
Average			0.079	59.226

Table 1: Frames before and after hiding operation with PSNR and MSE values

5. Conclusions and suggestions for future works

In this paper, a steganography method is proposed for securing a video channel for transmitting a secret image through unsecure network. A proposed method is used the spatial domain of video frame as a cover for embedding a secret image. In addition, a cryptography method is used for encrypting a secret image before embedding it in order to add more than one security layer. The experimental results show that the embedding method don't make significant distortion in the video where the average value of MSE values is less than **0.08** and the average value of PSNR values is more than **55 db** which means that the proposed method is satisfied the imperceptibility requirement.

The suggestions for future works can be listed as follows:

1. Studying the ability of applying the proposed method in another media such as image.
2. Studying the ability of embedding the secret image in the frequency domain rather spatial domain.
3. Studying the ability of applying the proposed method in the digital watermarking applications.

Conflict of Interests.

There are non-conflicts of interest .

References

- [1] Chikouche, Sofyane Ladgham, and Nouredine Chikouche. "An improved approach for lsb-based image steganography using AES algorithm." 2017 5th International Conference on Electrical Engineering-Boumerdes (ICEE-B). IEEE, 2017..
- [2] Qadir, Abdalbasit Mohammed, and Nurhayat Varol. "A Review Paper on Cryptography." 2019 7th International Symposium on Digital Forensics and Security (ISDFS). IEEE, 2019.
- [3] Arya, Anupriya, and Sarita Soni. "A literature review on various recent steganography techniques." International Journal on Future Revolution in Computer Science & Communication Engineering 4.1 (2018): 143-149.
- [4] Singh, Rajiv, et al. "Wavelets and Intelligent Multimedia Applications: An Introduction." Intelligent Wavelet Based Techniques for Advanced Multimedia Applications. Springer, Cham, 2020. 1-12.
- [5] Ziabari, S. Mohammadi. "Video-Steganography in the compressed area." Research Gate (2017): 1-17..
- [6] 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).
- [7] Choudry, Kedar Nath, and Aakash Wanjari. "A survey paper on video steganography." International Journal of Computer Science and Information Technologies 6.3 (2015): 2335-2338.

الخلاصة

أصبح الإنترنت من أهم الوسائل المستخدمة في نقل المعلومات عبر البريد الإلكتروني ووسائل التواصل الاجتماعي وغيرها. لقد أصبح من المهم حماية هذه المعلومات وإيجاد أفضل الطرق وأكثرها أماناً لنقلها وحمايتها من محاولات القرصنة والهجمات الشائعة على الإنترنت. في هذا البحث ، يتم استخدام تقنيات التشفير وإخفاء المعلومات لتأمين الإرسال عبر شبكة غير آمنة. في هذا البحث ، اقترحنا طريقة لتشفير الصور باستخدام معادلات من الدرجة الثانية ، ثم يتم تضمين الصورة المشفرة في الفيديو . يتم تضمين الصورة وفقاً للمعادلات بدلاً من تضمينها بالتتابع لزيادة طبقة الأمان. أظهرت النتائج التجريبية أن الطريقة المقترحة تحقق قدرة تضمين عالية. بالإضافة إلى ذلك ، يزيد التشفير والاختيار غير المتسلسل للإطارات والمواقع لإخفاء البتات من سلامة ومثانة النظام المقترح عند مقارنته بالطرق الأخرى لإخفاء المعلومات.

الكلمات الدالة: تقنية الستيجانوغرافي، تقنية التشفير، تقنية السنيغانوغرافي في الفيديو