 doi:10.20944/preprints202105.0176.v1

A graphical based video steganography

Payal Bose ,Prof. Samir K Bandyopadhyay and Prof. Vishal Goyal

GLA University, Mathura-Delhi Road Mathura, Chaumuhan, Uttar Pradesh 281406

Abstract: In today's digital media data communication over the internet increasing day by day. Therefore the data security becomes the most important issue over the internet. With the increase of data transmission, the number of intruders also increases. That's the reason it is needed to transmit the data over the internet very securely. Steganography is a popular method in this field. This method hides the secret data with a cover medium in a way so that the intruders cannot predict the existence of the data. Here a steganography method is proposed which uses a video file as a cover medium. This method has five main steps. First, convert the video file into video frames. Then a particular frame is selected for embedded the secret data. Second, the Least Significant Bit (LSB) Coding technique is used with the double key security technique. Third, an 8 characters password verification process. Fourth, reverse the encrypted video. Fifth, signature verification process to verify the encryption and decryption process. These five steps are followed by both the encrypting and decrypting processes.

Keywords: *Video Steganography, Least Significant Bit (LSB) Coding, Double key Encryption, Decryption, Password Verification, Signature Verification*

1. INTRODUCTION

In today's digital world transmission of secure data through the internet is the biggest challenge. Therefore for secure data transmission two types of security techniques are available 1) Steganography, and 2) Cryptography.

Steganography is the most commonly used data secure technique. It is used to conceal the secret data inside a cover medium. The cover medium embedded the secret data in a very efficient that it is too difficult to find the original data from it. In steganography several types of cover mediums available. Figure-1 shows the details of it.

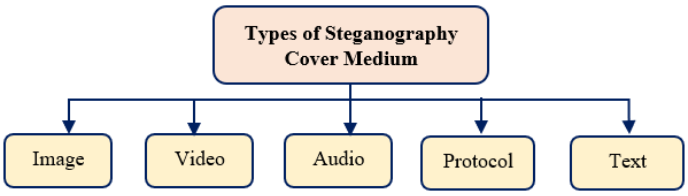


Figure 1: Types of Steganography Cover Medium

Cryptography is a technique where a secret key is used to convert the secret data into encrypted secure data. This paper proposed a steganography technique with a video cover medium. In this technique to secure data or information, the Least Signification Bit algorithm (LSB) with dual key encryption method is used to encrypt and decrypt the secret data.

2. LITERATURE REVIEW

Video Steganography technique is the extension of the image steganography process. The most common technique for steganography is the Least Significant Bit technique (LSB). In this technique, the least significant or the last bit of the frame holds the value of the secret message. For this reason, this technique is vulnerable and can be break very

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 May 2021 doi:10.20944/preprints202105.0176.v1

easily. There are several authors who proposed several steganography techniques. For hiding the secret data, the authors proposed an affine transformation technique. The data embedded into the video frame based on the coefficient of wavelet transformation. The affine transformation is used to distribute the pixel values [1]. In today's world for secure communication authors describe several steganography techniques. Finally, they proposed a method that is useful and more compatible with steganography [2]. The authors survey different techniques of the steganography method and gave a detailed analysis of each process [3-5]. The authors compare the two most popular steganography techniques LSB and Discrete Wavelet Transform (DWT) base on two factors efficiency and capacity of accepting multiple images into one cover image. They also evaluate the performance of the algorithm based on the cover image capacity, imperceptibility of data, and security [6]. To enhance security and avoid data hacking the authors implemented an edge-based steganography technique. They used an adaptive embedded process over Dual-Tree Complex Wavelet Transform (DT-CWT) method. They show that this method is significantly better than other steganography techniques [7].

3. PROPOSED METHODOLOGY

This experiment is the extended part of the image steganography. It has five major parts for both the Encryption and Decryption method. The parts are 1) Pre-Processing, 2) LSB Coding, 3) Double key Protection, 4) Reverse the video with password verification, and finally 5) Signature Verification. Figure 2 shows the basic structure of the process.

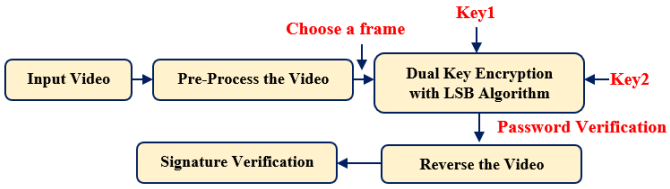


Figure 2: Basic Structure of video steganography process

3.1. Pre-Processing

To perform this, experiment the first step is to pre-process the input cover medium. Here a video cover medium is used. Therefore, for pre-process it needed to split the input cover video into its corresponding frames. The next step is to select a particular frame among all the frames and perform the next steps [8].

3.2. Least Significant Bit (LSB) Coding

LSB is a common coding technique in steganography used to embedded secret code into images [9-10]. According to this technique first, it converted all the image pixels and the secret data into their binary values. Then it embeds each bit of the binary value of secrete data at the least significant position of pixels value. This is an easy method to implement and easy to decode. For an RGB frame, this process can embed a 3-bit value into each pixel.

For example, let consider the pixels of a 24bit image-

$$Pixel_1 = (11110000 \quad 00110001 \quad 01011000)$$

$$Pixel_2 = (11100011 \quad 10110000 \quad 11011001)$$

$$Pixel_3 = (11100000 \quad 10110011 \quad 11010101)$$

Now a secret message '$A' = 11001010$ needs to embed into the above image. After applying the LSB algorithm the message 'A' embeds into the above pixels, it converted into unrecognizable pixels.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 May 2021 doi:10.20944/preprints202105.0176.v1

$$Pixel_1 = (11110001 \quad 00110001 \; 01011000)$$

$$Pixel_2 = (11100010 \quad 10110001 \; 11011000)$$

$$Pixel_3 = (11100001 \quad 10110010 \; 11010101)$$

3.3. Double Key Protection

To secure the embedding and decrypting process in this experiment two keys are used [10-11]. Key1 is a 64bit secret key and Key2 is a secret key with 128bit or greater. These two keys help to perform the LSB Algorithm to encrypt or decrypt the secret message.

3.4. Reverse the video with Password Verification

Reverse video is a display mechanism. It used to invert the video sequences from end to beginning. In this experiment, this technique is used to make a secure encrypting process. When the video sequence is inverted then the number of the encrypted frame in the video file also changed. This process helps to hide the exact encrypted frame very securely. Equation 1 shows the calculation for finding the $Reverse\ Encrypted_{frame}\ No.$

$$Reverse\ Encrypted_{frame}\ No = \left(Total\ Video_{frames} - Actual\ Encrypted_{frame} No\right) + 1 \quad (1)$$

Finally, a password with 8 characters used for the verification process to perform this mechanism more securely. The below algorithm shows the whole verification process for encryption and decryption.

```
Encryption Method
    - Select a particular frame from the input video file
    - Start LSB coding with Dual key encryption
    - Register a password (exact 8 characters long)
    - Reverse the encrypted video
Decryption Method
    - Calculate the Reverse Encrypted_Frame No and Verify
    - If Correct
      - Apply Password Verification
      - If Correct
        - Check Key1 & key2
        - If ok
            - Apply LSB Coding for decryption
        - else
            - Inavalid!
      - else
        - Invalid!
     - else
      - Invalid!
```

3.5. Signature Verification

In this section, a handwritten signature database is used for final verification. The database contains more than 1000 handwritten signature images. This database contains genuine and forged signature images. Both encryption and decryption methods needed two-step signature verification [13-14] to complete the process. For signature verification, Local Binary Pattern and multiclass support vector machine mechanism are used. In the encryption method for signature registration, the very last two frames of reverse encrypted video are used. The below algorithm shows the verification process.

```
Encryption Method
    - Register Sender Signature [Sender_Encryption] from sender
    - Register Receiver Signature [Receiver_Encryption] from sender
```

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 May 2021 doi:10.20944/preprints202105.0176.v1

Decryption Method

- Accept Receiver Signature [Receiver_Decryption] from receiver
- Accept Sender Signature [Sender_Decryption] from receiver
- If(Sender_Decryption==Sender_Encryption)and(Receiver_Decryption== Receiver_Encryption) then
  - Message Decrypt Successfully!
- Else
  - Invalid!

Figure 3 shows the entire encrypting and decrypting process of this experiment.

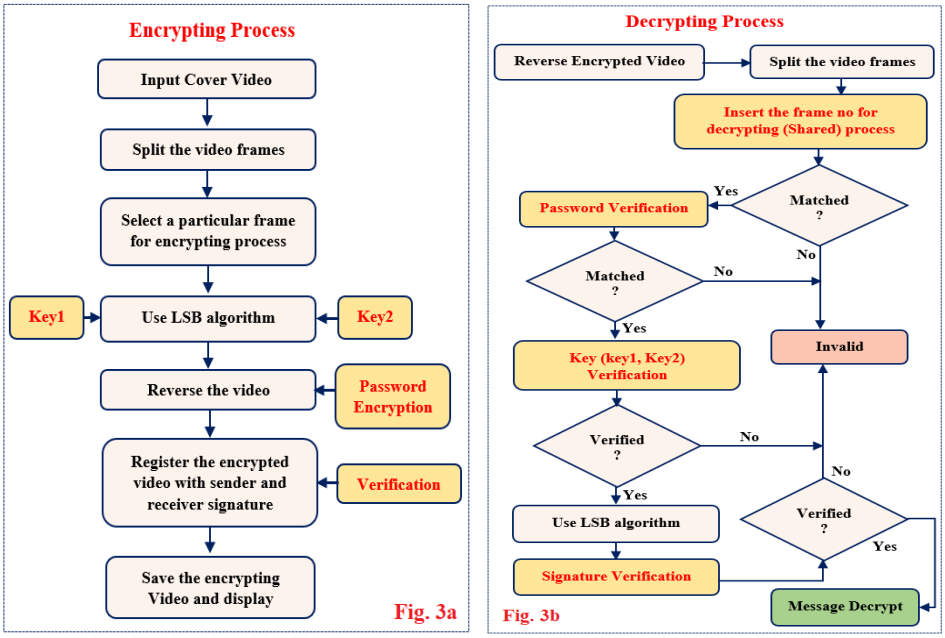


Figure 3: a) Encrypting and b) Decrypting Process

4. EXPERIMENTAL RESULT AND DISCUSSIONS

The proposed methodology was applied on a random audio-video interleaved (.avi) video file. For implementing this process MATLAB 2020a App designer was used. The initial interface is shown in figure 4.

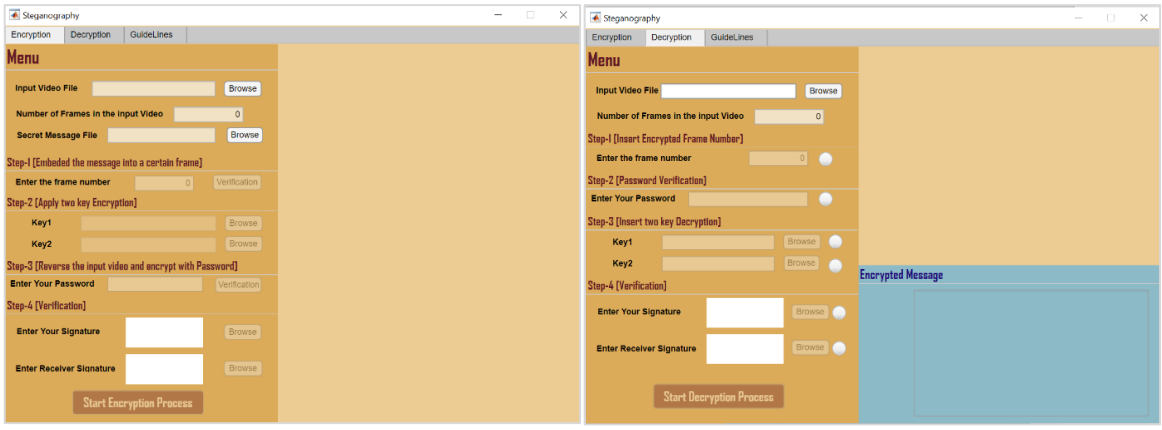


Figure 4: Initial Interface a) Encrypting process, b) Decrypting Process

The encrypting process is shown in Figure 5. The secret Key1 and 2 and secrete message shown in figure 6a, 6b, 6c.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 May 2021 doi:10.20944/preprints202105.0176.v1

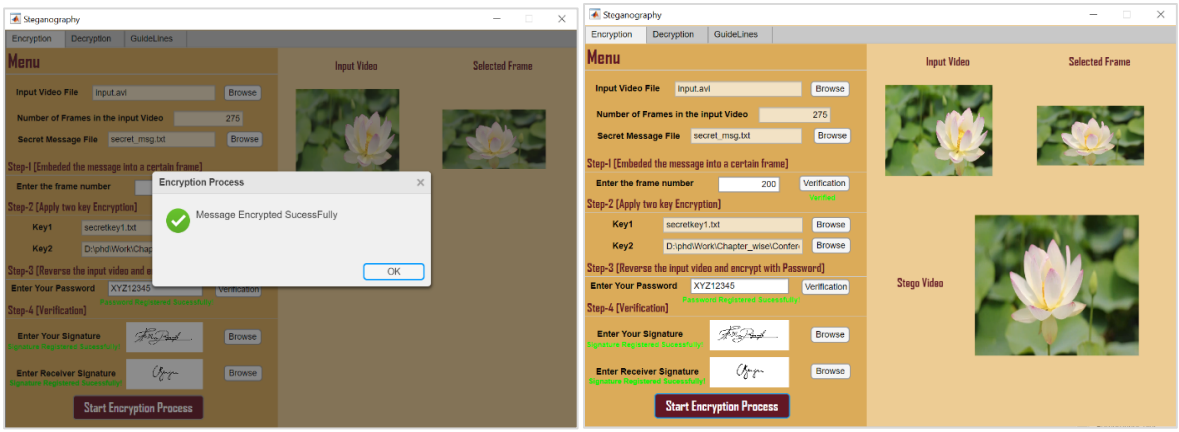
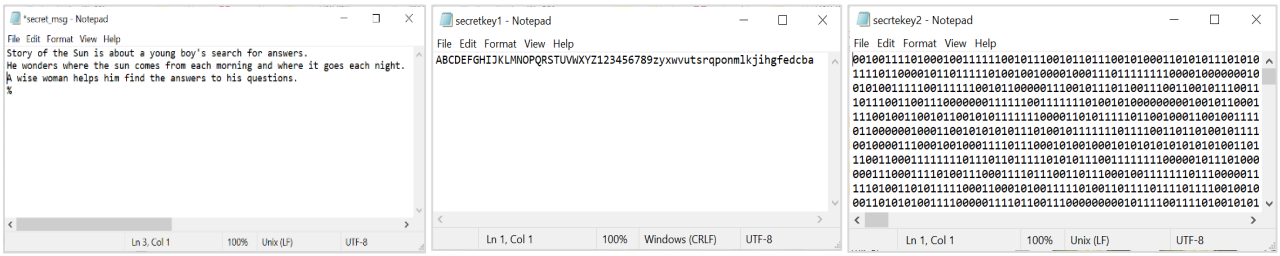


Figure 5: Encrypting Process



Figue:6) (a) Secret Message , (b) Secret Key1, (c) Secret Key2

The decrypting process is shown in Figure 7.

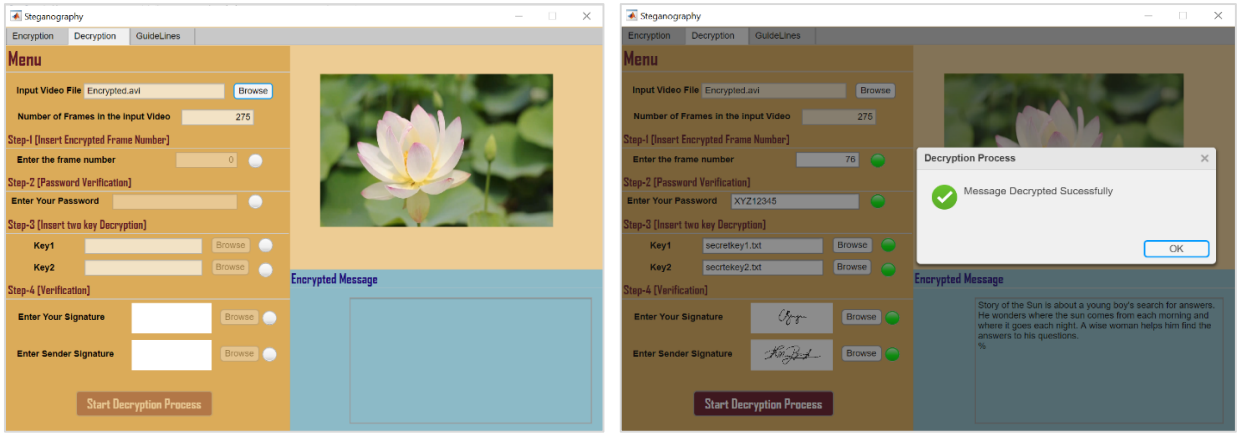


Figure 7: Decrypting Process

In the decryption process, if any verification process goes wrong the system returns the error message. Figure 8 shows the error output of the system.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 May 2021 doi:10.20944/preprints202105.0176.v1

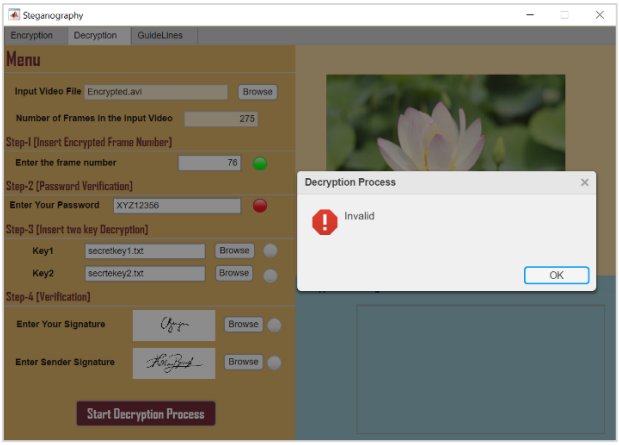


Figure 8: Decrypting Process (Error Output)

The experimental result in the signature verification process is shown in figure 9. The performance analysis of this process is shown in table 1.

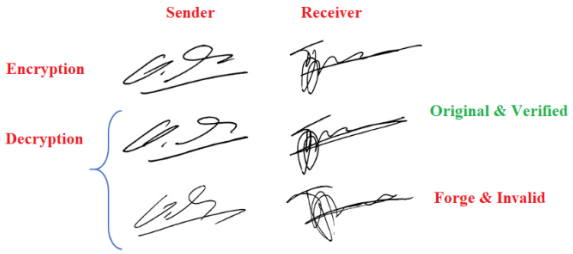


Figure 9: Signature Verification

Table 1: Performance Analysis for Signature Verification

Method		Accuracy (%)
Feature Extraction	**Classification**	
Linear Binary Pattern (LBP)	Support Vector Machine	96.2
	Decision Tree	91.2
	K-Nearest Neighbor	93.7

In this experiment in the secret message file, a special character is used. This indicates the end of the message. The limitations of this experiment are, 1) the input and output video file must be uncompressed audio-video interleaved (.avi) video file, 2) the secret message, secrete key 1and key2 file must be in text (.txt file) format.

5. CONCLUSION

The aim of the proposed methodology is to create a secure steganography process with a video cover medium. The dual key, secrete key1 and key2 and the Least Significant Bit Coding give the double protection. In this experiment reverse video encryption method is used. For a third-party intruder, this process is one of the disadvantages to identify the correct encrypted frame number. Finally, the password verification and the signature verification process give high security throughout the whole process. The entire process shows an efficient method to encrypt and decrypt the secret data using the steganography technique.

REFERENCES

1. Ramalingam, M., Mat Isa, N. A., & Puviarasi, R. (2020). A secured data hiding using affine transformation in video steganography. *Procedia Computer Science*, *171*(2019), 1147–1156. https://doi.org/10.1016/j.procs.2020.04.123.
2. Sindhu, R., & Singh, P. (2020). Information Hiding using Steganography. *International Journal of Engineering and Advanced Technology*, *9*(4), 1549–1554. https://doi.org/10.35940/ijeat.d8760.049420
3. Dhawan, S., & Gupta, R. (2021). Analysis of various data security techniques of steganography: A survey. *Information Security Journal*, *30*(2), 63–87. https://doi.org/10.1080/19393555.2020.1801911
4. Raja Ratna, S., Shajilin Loret, J. B., Merlin Gethsy, D., Ponnu Krishnan, P., & Anand Prabu, P. (2020). A Review on Various Approaches in Video Steganography. *Lecture Notes on Data Engineering and Communications Technologies*, *33*(7), 626–632. https://doi.org/10.1007/978-3-030-28364-3_64

5. Al-Omari, Z., & T. Al-Taani, A. (2015). *A Survey on Digital Image Steganography*. *August*, 109–115. https://doi.org/10.15849/icit.2015.0016
6. Gutub, A., & Al-Shaarani, F. (2020). Efficient Implementation of Multi-image Secret Hiding Based on LSB and DWT Steganography Comparisons. *Arabian Journal for Science and Engineering*, *45*(4), 2631–2644. https://doi.org/10.1007/s13369-020-04413-w
7. Kadhim, I. J., Premaratne, P., & Vial, P. J. (2020). High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform. *Cognitive Systems Research*, *60*, 20–32. https://doi.org/10.1016/j.cogsys.2019.11.002
8. Darbani, A., Alyannezhadi, M. M., & Forghani, M. (2019). A New Steganography Method for Embedding Message in JPEG Images. *2019 IEEE 5th Conference on Knowledge Based Engineering and Innovation, KBEI 2019*, 617–621. https://doi.org/10.1109/KBEI.2019.8735054
9. A. Saleh, M. (2018). Image Steganography Techniques - A Review Paper. *Ijarcce*, *7*(9), 52–58. https://doi.org/10.17148/ijarcce.2018.7910
10. C.P, S., T, S., & G, U. (2013). A Study of Various Steganographic Techniques Used for Information Hiding. *International Journal of Computer Science & Engineering Survey*, *4*(6), 9–25. https://doi.org/10.5121/ijcses.2013.4602
11. Duan, X., Guo, D., Liu, N., Li, B., Gou, M., & Qin, C. (2020). A New High Capacity Image Steganography Method Combined with Image Elliptic Curve Cryptography and Deep Neural Network. *IEEE Access*, *8*, 25777–25788. https://doi.org/10.1109/ACCESS.2020.2971528
12. Sahu, A. K. (2020). *Review Article DIGITAL STEGANOGRAPHY FOR PREVENTING CYBERCRIME USING ARTIFICIAL*. *7*(6), 749–753.
13. Poddar, J., Parikh, V., & Bharti, S. K. (2020). Offline Signature Recognition and Forgery Detection using Deep Learning. *Procedia Computer Science*, *170*(2019), 610–617. https://doi.org/10.1016/j.procs.2020.03.133
14. Hatkar, P. V, & Tamboli, Z. J. (2015). Image Processing for Signature Verification. *International Journal of Innovative Research in Computer Science & Technology (IJIRCST)*, *3*(3), 127–129.