Systematic Approach for Data Hiding using visual cryptography in videos for acquiring reliable data security: A Review

Zainab Pervaiz, Farhan Ali Arshad, Sundas Hanif, Jawwad Ibrahim

Abstract— In this digitalized world, people have developed strong communication using digital means of information sharing but Security in the field of information correspondence have remained a topic of dialog throughout the years. Steganography is the art and science of message hiding. This involves a risk by the hand of unauthorized people. There have been used different techniques to cope up with such issues. This paper has aim to provide improve data security, maintain the quality of cover-image and compress the stego-video. An algorithm based on 3 stages is used with LSB and DCT. However, it is a very difficult to find out the specific algorithm. Presently continuous researches on the new cryptographic algorithms are going on and it is expected to grow with more advancement in technology in future

Index Terms— Cryptography; Security; Secure data; attacks; LCP; Discrete Cosine Transform Palatino

1 Introduction

Cryptography is science of art of hiding message into other sources like text, audio, image, watermark, video etc. cryptography done for the purpose of hiding data and make communication more secure and invisible from others[1]. It is also known as invisible communication. The words Cryptography is derived from two words Krypto and Graphene. Krypto's mean hidden and Graphene's mean writing.

During communication, the sender node usually transforms a plain text message into cipher text and sent over the network[2]. When the encrypted message reached to destination it is again transform into plain text by receiver node. The mechanism of transforming plain text to cipher text (encryption) and then to its original form (decryption) is known as cryptography[3].

Cryptography not only used to provide confidentiality, but also to provide solutions for other problems like: data integrity, authentication, non-repudiation[4].

Primary Functions:

There are primary five functions of cryptography

1.1 Privacy: Ensuring that no one can have access sent message except the authorized user to whom data is sent

1.2 Authentication: It is process to check the identity to proof as an authenticate user

1.3 ***Integrity:*** It assures that the data receiver get original data. Assuring the data is not altered by someone during transmission

1.4 ***Non-repudiation:*** It is a process that is used to check whether the message really send by the sender

1.5 ***Key exchange:*** The mechanism in which sender share the crypto key to receiver. In this way the receiver will be able to decrypt the encrypted data

Cryptography has different modes of hiding data:

- *Text cryptography*: Text is being converted into cipher text that is unreadable by unauthorized person. According to some mechanisms extra bits adding to the original text to make it unreadable and the other approach is converted whole text into new pattern text using shift key
- ***Audio cryptography:*** The message is encrypted in recording or sound waves. After observing the pattern of the sound frequency one can be able to find and decrypt message [5]
- ***Watermark cryptography***: The mechanism of securing messages by hiding into watermark. The watermark cannot decrypt without breaking the functionality of program[6].
- ***Image cryptography:*** In recent years, many techniques are introduced for image cryptography one of them is hiding data in LSB. Least Significant Bit of RGB colors change and it is used to encrypt message[7].
- ***Video cryptography***Securing message by encrypting it into videos frames. Video is basically considered as the combination of multiple frames so, data encrypt in different frames using different algorithms.

The security risks are considered as a main concern of today's practical world. Advancement are made in each field of technology but security is core part of technology[8].

Literature Review

The study has been commenced as a systematic literature appraisal based on [1]. For secure transmission the technique to encrypt the image is used[9]. Furthermore with more advancement the cryptography in videos becomes popular.

According to research [5] a video of 30 frames per second is taken. Security measures of video cryptography include both security of cryptography as well as perceptual.

In [5] researcher proposed a high security technique to encrypt data into video using its cover image frame. The important data is hiding in boundaries using RGB color scheme Systematic encryption and Asymmetric techniques are being used[10].

In paper [12] a new technique to hide message into parity bits of close colors. The value of those parity bits is determined by adding RGB as (R+G+B) mod 2. The bit is embedded into image pixel by searching closest color palette entries that resembled to real image.

Using this technique it is guaranteed that the original colors are not modified too much in stego-image. The output concluded by Fridrich's method has incorrect contouring and noise [3].

In paper [1] color histogram based algorithm was introduced for video cryptography. Simply the data stream split into multiple frames and the results from histogram calculated and these values compare to threshold value.

Confidential data hidden to different frames by distributing pixels into two chunks, the bits are impacted in the right fragment and calculated in left fragment[11]. This procedure gives the capability to hide huge volume of data and written script can be extract without errors[12].

The method named as improved LSB is used to hide secret image into cover image [2]. The BITMAP images are lossless that is why these images mostly used for this process[13]. By applying bit plane slicing the cover image is distributed into different planes like Red, Green and Blue (RGB).

The confidential data bit is replaced by LSB Red, Green and Blue in sequence 4, 4 and 12 it represents 4 bits in Red, 4 bits in Green and 12 bits in Blue[14].

In the Least Significant Bit method the confidential data is impacted in front frame of video such as cover video [3].

Furthermore, the cover video sub divided to frame and the concealed data is extracted from the cover video. Security and complexity of hidden data is increased by embedded it into multiple frames of video[15]. The frames of video alienated and converted into .bmp images. The cover video pixels are changed into the binary digits. Then the pixels are replaced by binary value[16]. An algorithm derived from the principle if linear block code [4]. Sequence of nine uncompressed video sequence is used as cover data. Cover video and secret message's pixel position was recorded using private key[17].

The hidden message was encoded using Hamming code [7,4] to provide more secure message before embedding.

A secret video stream is embedded into the cover video [5]. The secret video is first distributed into individual component and further it converted into 8-bit binary value.

This value is then encrypted using XOR transmission with a secret key. While the cover frames stores the secret frames in a pattern BGRRGBCD. This secret frames proved to be enhance the security[18].

Visual file bit stream converted into a message file by changing the LSB. This is another way of video cryptography implementation. The message is embedded on carrier file but before this the message converted into byte code an encrypted[19]. A successful approach avifill32.dll used with wrapper files of C#, but the issue is the carrier file should be an uncompressed AVI file[20].

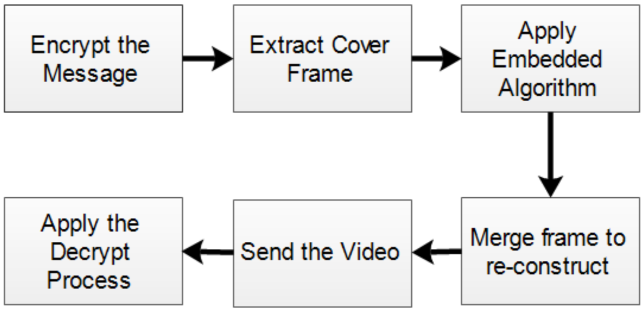

Fig 1: Process to embed data

Research Questions

R1. Does the quality of current video encryption is just enough to secure embedded data?

R2. How to resolve the noise issue in current video cryptographic technique?

R3. Are the uses of high quality color scheme can augment video quality?

The above questions are essential to get more reliable and secure data. It plays a vital role in this Research work.

Methodology

In this research paper the proposed work is to hide data inside the video. If the data is not encrypted in sequence than it will be more secure.

The previous research has not defined wide range of colors that is a reason of poor quality of a specific image in a video in which data is encrypted.

The color quality is the main factor that is targeted by the hacker.

Improvement of resolution and color of picture play a vital role to secure data from human eye.

- The data is divided into different chunks and these chunks encrypted into multiple images.
- The encrypted data will not place in proper sequence.
- The data will be encrypted in the middle of video that is difficult to tackle the hidden data.

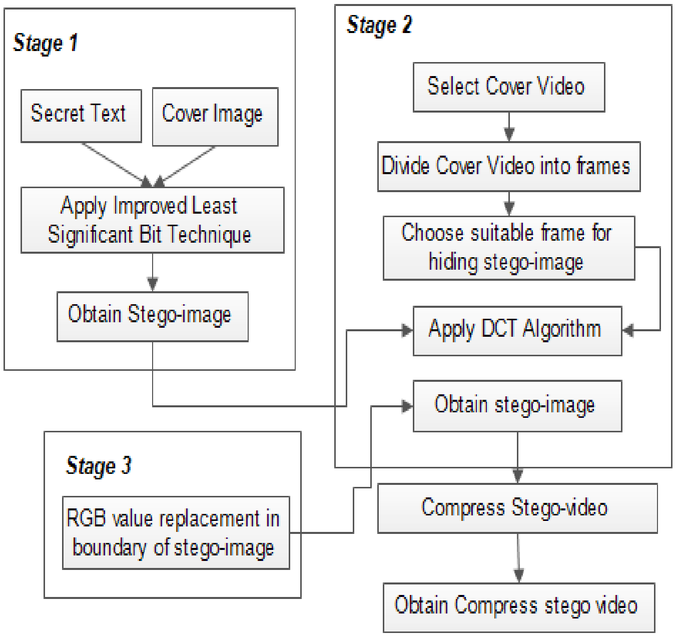
Stage 1
Secret Text
Cover Image
Apply Improved Least Significant Bit Technique
Obtain Stego-image
Stage 2
Select Cover Video
Divide Cover Video into frames
Choose suitable frame for hiding stego-image
Apply DCT Algorithm
Obtain stego-image
Stage 3
RGB value replacement in boundary of stego-image
Compress Stego-video
Obtain Compress stego video

Fig 2: Flow of proposed model

Improved LSB technique

The following steps are involves in LSB technique:

- Conversion of confidential message into binary digit.
- The cover slicing into three different planes Red, Green and Blue.
- The LSB of cover image replaced by bits of secret message in order more bits replaced in Red and Green as compare to Blue.

The more data bits replaced in blue is to increase the quality of hiding. According to [21][22] small changes in blue color can not be detected by human eye. Hence blue is les sensitive as compare to Red and Green. Therefore, more bits of Blue are replaced and fewer on Red and Green are replaced to get better output. In result of this stage we get stego-image which is then provided as an input to stage 2.

Stage 2: At this stage the cover video of AVI format is taken and divided into frames. Firstly, a suitable frame selected from all available frames. Frame selection criteria based on less distortion after hiding stego-image in it.

To conceal the stego-image into the selected frame DCT algorithm is used. DCT algorithm separates the frames into multiple parts according to their importance [11]. DCT changes the time domain signal into its frequency components[8].

This stage is mainly responsible for maintaining the quality of video. After embedding stego-image into different frames; stego video is founded as an output of this stage. These two stages are enhancing the security by applying steganography twice.

In stage 3 The RGB color boundary applied to cover frame of stego-video that contain a secret key.

Hence after stego video obtain the size of this video is huge that it take a lot of time for transmission therefore it is compressed. Compressed video can easily transferred over transmission medium. Compression is usually classified into two categories; lossy and lossless.

In our approach we use lossless compression. Therefore, the quality of sent video remain same after decryption.

Discussion

Quality of current video for secure embedded data

Current research proposed a strong mechanism to protect the data efficiently using cryptographic techniques but it creates many problems as well. By using cryptographic methods create distortion that compromises the quality of video encryption.

There methods and processes are very functional but provide poor quality that hackers are easily hack the original data.

According to [3] video quality measurement is an approach to find the quality of the video as it agrees more with human visual system.

So, the need of strong mechanism is required to be addressed RQ2 and RQ3 further described regards to the quality of video

Handle noise issue in current video encryption technique

According to [14] Least Significant Bit (LSB) modification is perhaps the most popular method to embed a message into cover data and the red, green and blue color components can be used, since they are each represented by a byte [3].

The LSB is an effective approach to encrypt data but it creates noise as well that become the reason of destroyed quality of video encryption that a human eye can be easily tackle the encrypted data.

Instead of this Optimal Pixel Adjustment Procedure (OPAP) is an effectual procedure and it reduces the distortion caused by the LSB.

In OPAP [3] method the pixel value is adjusted after the hiding of the secret data is done to improve the quality of the stego image without disturbing the data hidden.

Uses of high quality color scheme augment video quality

The data will have encrypted in the boundary of image using RGB colors. The research [2][3] have not defined wide range of colors that is a reason of poor quality of a specific image in a video in which data is encrypted. The color quality is the main factor that is targeted by the hacker. Improvement of resolution and color of picture play a vital role to secure data from human eye [7].

The data will be encrypted in the middle of video that is difficult to tackle the encrypted data. The data is divided into different chunks and these chunks encrypted into multiple images.

The encrypted data will not place in proper sequence. Hence by the proposed research the quality and other factors regards to video cryptography can be improved.

CONCLUSION

Cryptography plays an evolutionary role in security. Many techniques are used to hide data using images and videos but they have some flaws that are tried to overcome in this study. Data is encrypted in videos by reducing the distortion and noise and improve color scheme is used for better data security and in video data is placed in multiple frames not to next each other to secure data from illegal authorization. High security is achieved using the proposed method based on three stage process which doesn't let the attacker gain access to confidential and private message. In future even better techniques may be applied

ACKNOWLEDGMENT

I would like to express gratitude to Allah Almighty who makes me what I am today. I would like to thank my teacher: "Mr. Jawwad Ibrahim" to believe on my effort.

REFERENCES

1. Shinde, P. and T.B. Rehman, *A Novel Video Steganography Technique*. International Journal, 2015. **5**(12).
2. Pal, J.K., J. Mandal, and K. Dasgupta, *a (2, n) visual cryptographic technique for banking applications*. International Journal of Network Security & Its Applications (IJNSA), 2010. **2**(4): p. 118-127.
3. Limkar, S., et al., *Improved Data Hiding Technique Based on Audio and Video Steganography*, in *Smart Computing and Informatics*. 2018, Springer. p. 581-588.
4. Kocarev, L. and S. Lian, *Chaos-based cryptography: Theory, algorithms and applications*. Vol. 354. 2011: Springer Science & Business Media.
5. Saraireh, S., et al., *A HYBRID TEXT-IMAGE SECURITY TECHNIQUE*. Journal of Theoretical & Applied Information Technology, 2018. **96**(9).
6. Singh, T.R., K.M. Singh, and S. Roy, *Video watermarking scheme based on visual cryptography and scene change detection*. AEU-International Journal of Electronics and Communications, 2013. **67**(8): p. 645-651.
7. Roy, S., S. Mukherjee, and G. Sanyal. *Video Steganography Using Karhunen-Loève Transform*. in *Proceedings of the 2nd International Conference on Digital Signal Processing*. 2018. ACM.
8. Kaur, M. and A. Kaur, *Improved Security Mechanism of Text in Video using Steganographic Technique*. International Journal, 2014. **2**(10).
9. Bodhak, V. and L. Gunjal, *Improved protection in video Steganography using DCT & LSB" international journal of engineering and innovative technology (IJEIT) vol. 1, issue 4*. 2012, April.
10. Gosalia, S., S. Shetty, and A. Revathi. *Embedding audioinside a digital video using LSB steganography*. in *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*. 2016. IEEE.
11. Agarwal, P., S. Gupta, and A. Mehra, *Transmission and Authentication of Text Messages through Image Steganography*. International Journal of Computer Applications. **975**: p. 8887.
12. Arya, A. and S. Soni, *A Literature Review on Various Recent Steganography Techniques*. International Journal on Future Revolution in Computer Science & Communication Engineering, 2018. **4**: p. 143-149.
13. Kalyani, D.N. and D.K. Mahesh, *Safe Information Hiding Using Video Steganography*. International Journal of Computer Science and Mobile Computing, 2015. **4**(7).
14. Kadhim, I.J., et al., *Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research*. Neurocomputing, 2019. **335**: p. 299-326.
15. Al-Juaid, N.A., A.A. Gutub, and E.A. Khan, *Enhancing PC data security via combining RSA cryptography and video based steganography*. Journal of Information Security and Cybercrimes Research (JISCR), 2018. **1**(1).
16. Babatunde, A.N., R.G. Jimoh, and O.C. Abikoye, *Survey of Video Encryption Algorithms*. Covenant Journal of Informatics and Communication Technology, 2017. **5**(1).
17. Hooda, D. and P. Singh, *A comprehensive survey of video encryption algorithms*. International Journal of Computer Applications, 2012. **59**(1).
18. El-Bayoumy, M., et al., *A Proposed Technique for Hiding Encrypted Data in Video Files*. International Journal of Computer Applications, 2013. **79**(10).
19. Dominic, S.V.L.L., *Compress-Encrypt Video Steganography*.
20. Boudiaf, A., et al., *Image compression of surface defects of the hot-rolled steel strip using Principal Component Analysis*. Matériaux & Techniques, 2019. **107**(2): p. 203.