Academic City University College, Accra, Ghana
Society for Multidisciplinary & Advanced Research Techniques (SMART)
Trinity University, Lagos, Nigeria
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Harmarth Global Educational Services
ICT University Foundations USA
IEEE Computer Society Nigeria Chapter

33rd ECOWAS iSTEAMS ETech Multidisciplinary Conference (ECOWAS-ETech)

Safe Information Hiding Using Video Steganography

Peter Oppong Baafi
School of Technology
Ghana Institute of Management & Public Administration
GreenHill, Accra Ghana
E-mail: ; peeuncle3@gmail.com

ABSTRACT

The internet plays a significant role in transferring information from one person to another person. But some users can access or modify valuable information by using other techniques. Steganography is a data hiding algorithm that hides information in any medium. Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) methods were used for essential hiding data. The data gets hidden in a video file and can be extracted appropriately. The video file is chosen as a cover medium because a large volume of data can get resided inside it. The psnr value gained in this work is reasonable compared to an existing system.

Keywords: Steganography, Discrete Cosine Transform, Discrete Wavelet Transform, Least Significant Bit.

Proceedings Citation Format
Peter Oppong Baafi (2022): Safe Information Hiding Using Video Steganography. Proceedings of the 33rd ECOWAS iSTEAMS Emerging Technologies, Scientific, Business, Social Innovations & Cyber Space Ecosystem Multidisciplinary Conference. University of Ghana/Academic City University College, Ghana. 29th Sept – 1st Oct, 2022. Pp 39-44. www.isteams.net/ecowasetech2022. dx.doi.org/10.22624/AIMS-/ECOWASETECH2022P5

INTRODUCTION

A lot of information gets exchanged through the internet. The information can be sent from one person to another even in a second. Today technology gets improved in a fast manner. When the valuable data is sent through a communication channel, it can be accessed by unauthorized users. And they can modify the data. The illegal modification of unauthorized users is termed interception, so security measures must improve. Although many techniques are available for securing the data, the information hiding technique plays an efficient role. Information hiding means the secret information can be placed in the data source without making any changes to the quality of the medium. Information hiding technique involves imperceptibility, embedding capacity, and robustness.

The information hiding process includes cryptography, Steganography, and watermarking. In cryptography, the original text is converted into cipher text, which prevents the person from detecting the message. But the size of cipher text is larger than the plaintext, and it takes more time to encrypt the message. Steganography means that secret information can get hidden in some media. The media may be an image, audio, or video file. Cryptography and Steganography are used for security purposes. The difference between them is cryptography prevents valuable data, whereas Steganography protects the cover of the message. The cover medium is referred to as an object that holds useful information. The stego-object is the output that is sent to the destination. In text steganography, every nth letter of a word of the text message is replaced by private data. Then in image steganography, the message gets hidden inside an image by modifying the cover source in noisy areas. In audio Steganography, the private message is added to the audio signal, leading to changes to binary sequences of the audio file. The video steganography hides the message in many images, which makes the person unable to detect the message. Digital watermarking is nothing but hiding information in some digital objects. The digital thing includes audio, video, or an image file. It is impossible to eradicate the watermark without affecting the quality of the valuable data of a digital object. Imperceptibility and robustness get improved with watermarking.

2. RELATED LITERATURE

Majumder et al. (2012) have focused on the image steganography approach. It deals with the algorithm based on hiding a large amount of data- image, audio, and text file into a color bitmap image. In their work, it has been discussed that they use the Least Significant Bit (LSB) algorithm for embedding data into the Bitmap image. The LSB technique suggests that data can be hidden in the least significant bits of an image. BANOCI et al. (2011) proposed a novel steganography method for embedding secret data in the grayscale image. In their work, it has been discussed that the embedding process is performed in the transform domain of DWT to get good visual quality. Moon et al. (2013) used computer forensics to provide security to the data stored in the video file.

Text and images can be hidden in a video file. Suitable algorithms such as 1 LSB, 2LSB, and 4 LSB are used, and 4 LSB methods are found to be appropriate for hiding more personal information data. This paper deals with the idea of video steganography, cryptography, and computer forensics techniques in investigation and security. Kashyap et al. (2012) have focused on image watermarking. In their work, a multi-bit watermark is embedded into the low-frequency sub-band of a cover image by using the alpha blending technique. The watermarks generated with this algorithm are invisible, and the quality of the watermarked image and the recovered image are improved. Kelash et al. (2013) proposed a steganography algorithm based on color histograms for embedding data into video clips directly, where each pixel in each video frame is divided into two parts, and the number of bits that will be embedded in the right part is counted in the left part of the pixel. This proposed algorithm can hide a large amount of data, extracting the written text without errors.

Besides, it gives a massive level of authentication to guarantee the integrity of the extracted frames. Kaur et al. (2011) have focused on DCT based watermarking scheme, which provides higher resistance against attacks such as JPEG compression, noise, rotation, translation, etc. In their paper, it has been discussed that the watermark is inserted by adjusting the DCT coefficients of the image and by using the private key. The same secret key is used to extract the watermark.

3. FINDINGS

The paper reveals the processes of using video stenography to hide information safely. Any image is taken in this system for data hiding, and then encryption and decryption are used. In this application, the algorithm employed for encoding and decoding is several layers instead of using only an image of LSB. The beginning of data writing is from (the 8th or LSB layer) from the last layer because this layer has the most negligible significance compared to other layers. The encrypt module is used inside the image to hide files and information so that no one can see that information or file. Only one image file is given in output; this module can also have an image as input. For confidential information, the decrypting module is provided as output. It extracts the image file, and at the destination folder, two files are given: a hidden file (with the hidden message) and the original image file. The name and size of the file must be stored in a specified place of an image before encrypting them. File information can be saved after file information in the LSB layer and save file name size and file name of an image in most right-down pixels. The information must be written to extract files from encoded to decoded state.

Overview of LSB Technique and DES data encryption and Decryption with Video Steganography

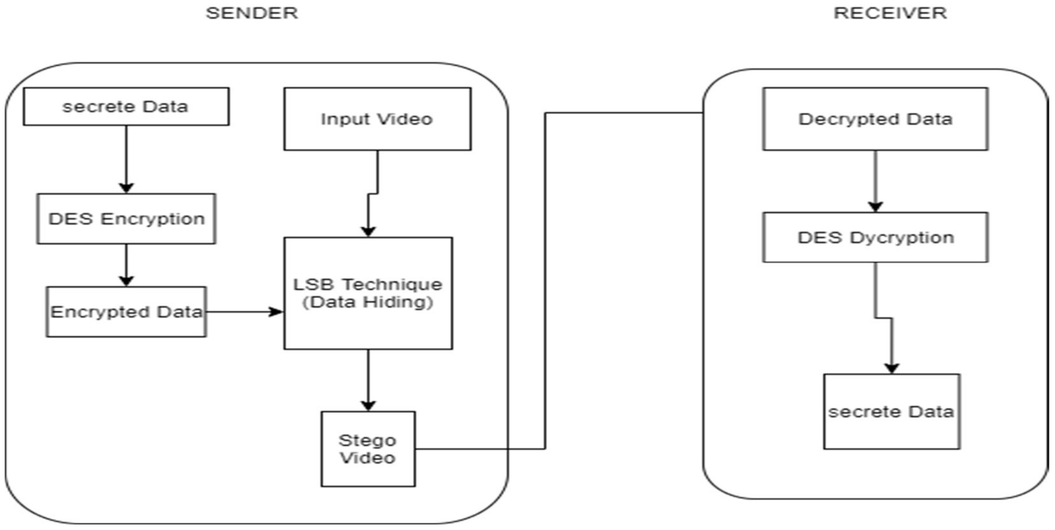

Figure 1: system architecture for Video Steganography
(LSB Technique and DES Encryption and Decryption)
Source: International Journal of Computer Network and Information Security (I. J. Computer Network and Information Security, 2017, 9, 38-45)

4. RESEARCH GAPS

The paper did not consider the application of the same processes to securely hide data (information) using other available approaches to securely hiding information. It investigated how secure it is to use only video steganography approaches in safe hiding information. It has also been studied that image stenography and other data encryption algorithms can also be used to secure data transmission safely. The paper did not extends to the comparison of the varied approaches when it comes to information hiding.

5. RECOMMENDATION FOR PRACTICES

The paper recommends practice by data security experts ensuring that data transmitted is always secure so that data interceptors along the proactive transmission routes are always cleared out of the information transmission process. Data have been hidden from hackers, and crackers are the best way to ensure that both the transmission channels and the transmitted data or information are always safe from the sending point to the receiving end.

6. POLICIES AND DESIGN

The paper seeks to standardize the framework and standards of steganography data under the following:

Loading Capacity

It shows the amount of confidential information the cover image can implant. The implantation rate, such as the secret message length, is given in the total amount.

Secured

A steganography system is said to be secure when there is an invisible difference between the cover and steganography images.

Cost-effective

The two parameters used to figure out cost-effectiveness are data hiding and any steganography approach to data retrieval.

Analytical Attacks

Analytical attacks are the attacks in which the embedded secret messages are extracted. The steganography algorithm used must show robustness to analytical attacks.

Quality: Increment in data amount decreases the rate. An appropriate amount of data and a correct approach should not degrade data quality. Indistinct: When the human eye does not distinguish the cover image from the steganography image, it is indistinguishable and perfect.

7. CONCLUSION

The proposed video Steganography system provides two levels of security, first with cryptography and second with Steganography. The proposed system results in hiding the encrypted information in the video clips. Each frame hides 3-bits of data. The proposed video Steganography is tested by taking the different sizes of videos and different sizes of confidential data. The proposed system shows no noticeable noise in the encrypted video. It is similar to that of the original video. The stego video is sent to the receiver, who knows the secret key. The existence of confidential information is impossible to detect. Hence the data is transferred safely and securely to the destination.

8. DIRECTION FOR FUTURE WORKS

In this paper, I have reliable use of video steganography approaches toward the secure or safe hiding of information.

The paper did not consider the other equally reliable approaches to safe information hiding and secure transmission. Future works can consider investigating different available information hiding algorithms and processes.

REFERENCES

1. Majumder J, Mangal S, 2012, "An Overview of image steganography using LSB Technique," IJCA.
2. Pal U, Chandra D, 2012, "Survey Of Digital Watermarking Using DCT," IJCSE Volume 4.
3. Hariri MNRKM, 2012, "Audio Steganography: A Survey on Recent Approaches," World Applied Programming, Vol (2), No (3).
4. Karim S.M.M, Rahman M.D.S, Hossain M.D.S, 2011, "A New Approach for LSB Based Image Steganography using Secret Key," IEEE.
5. Bhardwaj A, Ali R, 2009, "Image compression Using Modified Fast Haar Wavelet Transform," World Applied sciences Journal 7(5).
6. Paul R.T, 2011, "Review of Robust video watermarking Techniques," IJCA.
7. Chandra M, Pandel S, Chaudhary R, 2010, "Digital Watermarking Technique for Protecting Digital Images," IEEE.
8. Anju R, Vandana, 2013, "Modified algorithm for Digital Image Watermarking Using Combined DCT and DWT, "IJICT, Volume 3, No 7.
9. Kaur B, Kaur A, Singh J, 2011, "Steganographic approach for hiding image in dct domain," IJAET, Vol 1, Issue 3.
10. Moon S.K, Raut R.d, 2013, "Analysis of Secured Video Steganography Using Computer Forensics Technique for Enhance Data Security," IEEE.
11. Kelash H.M, Abdel Wahab O.F, Elshakankiry, Etsayed H.S, 2013, "Hiding Data in Video Sequences Using Steganography Algorithms" IEEE.
12. BANOCI V, BUGAR G, LEVICKY Dusan, 2011, "A Novel Method of Image Steganography in DWT Domain" IEEE.
13. Kashyap N, Sinha G.R, 2012, "Image Watermarking using 3-level Discrete Wavelet Transform (DWT)" IJMECS.
14. Kumar S, Latha M, 2014, “DCT Based Secret Image Hiding in video sequence” IJERA
15. Khosla S, Kaur P, 2014, “Secure Data Hiding Technique using Video Steganography and Watermarking” IJCA.
16. Poonam V, 2012, Improved protection in video steganography using DCT & LSB."