IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 3, March 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2023 ||

| DOI:10.15680/IJIRSET.2023.1203115 |

Video Steganography : Data Hiding Technique Using DCT, LSB, AES Algorithm

Rushikesh Shahane, Amar Tate, Omkar Pawar, Niraj Kumar

Department of Computer Engineering, K J College of Engineering and Management Research, Pune, India

ABSTRACT: Steganography is the practice of concealing information within other information in order to disguise the actual act of transmission. There are a variety of carrier file types. Frequently utilized, but due to their prevalence on the web, digital photos are the most well-liked. There are a wide variety of steganography techniques available for concealing sensitive information in video frames, some of which are more sophisticated than others and each of which has unique strength sand weaknesses. In recent decades, steganography has gained momentum due to its ability to communicate data covertly. Steganography embeds secret data into cover medium that are of many forms like text, image audio and video. Video steganography is drawing more impulse due to its scope of masking larger amount of secret information. This paper provides an overall view about the embedding and encryption techniques considering video as cover.

KEYWORDS: Encryption, Decryption, Data-hiding, Compression.

I. INTRODUCTION

Steganography may be a Greek word which suggests concealed writing. The word steganos means covered and graphical means writing. Thus, steganography isn't only the art of hiding data but also hiding the very fact of transmission of secret data. Steganography hides the key data in another enter such how that only the recipient knows the existence of message. In ancient time, the information was protected by hiding it on the rear of wax, writing tables and stomach of rabbits or on the scalp of the slaves. Steganography usually deals with the ways of hiding the existence of the communicated data in such how that it remains confidential.

It maintains secrecy between two. e. The propulsive intention of steganography is to communicate amid two parties in a covert manner. The secret data (important information) is concealed in the cover and this stego is communicated, so that the intruder will not identify the secret information. The stego object will be a single entity by the Human Visual system [11,80]. Further to make the secret data more secure, encryption is performed.
A steganographic method is tamper resistant if the receiver gets the secret data exactly in the same way sent by the sender.

II. LITERATURE SURVEY

1.Manohar N1,Peetla Vijay Kumar "Data Encryption Decryption Using Steganography"
Video steganography is a method that processes secu re communication. When we see the history of steganography, it was hidden in many ways such as tablets covered with wax, written on the stomachs of rabbits. Here in this paper, considering the video steganography methods to perfo rm secure steganography communication. Many methods have been proposed for video steganography but they're no more different types of formats, secu red, quality, of the results. So here propose secu re steganography methods i.e. Secure base LSB method, Neural Networks Fuzzy logic, and check their using PSNR and MSE data of the methods. That data-set has collected is from video streams. And the result was seen with the more formats, more security, quality of outputs, accuracy values of PSNR MSE which is better than other proposed methods.

2.Texture Based Video Steganography Technique Using Block-Wise Encryption (2017).
The video data hiding methods utilize uncompressed video data. Proposes a high-volume transform domain data hiding in MPEG-2 videos. They apply QIM (Quantization Index Modulation) to low frequency DCT (discrete cosine transformation) coefficients and adapt the quantization parameter based on MPEG-2 parameters. . The proposed algorithm can be applied in the following steps: - •Pre-processing Phase •Feature extracted -GLCM algorithm (for textual feature analysis) •Apply PCA algorithm (feature selection and block wise encryption) •Encryption of first image

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2023 ||

| DOI:10.15680/IJIRSET.2023.1203115 |

-Venkata Krishna et al. proposed in this paper a new image encryption mechanism that includes the AES and visual cryptography methods. -The main motive here is to protect the image for which an encoding mapping is proposed. -This method helps in converting the key into shared with respect to the Visual Secret Sharing mechanism. By making modifications in the key shares the confidentiality is tested here. [10.1109/SITIS.2017.28].

III. PROBLEM STATEMENT

In today's digital world, the security of information has become a major concern. Steganography is a technique of hiding information within other data such that the very existence of the message is concealed. This technique can be used to prevent unauthorized access to information and to ensure the security of the message being transmitted.
The aim of this project is to implement video steganography, which involves hiding information within a video file. The challenge in this project is to develop an algorithm that can embed the information within the video without degrading the quality of the video or making the hidden information easily detectable. The algorithm should also be able to retrieve the hidden information from the video file with high accuracy.
The project involves researching and implementing various steganographic techniques, as well as exploring different video formats and compression methods to find the optimal combination for video steganography. The success of the project will be measured by the effectiveness of the steganographic algorithm in hiding and retrieving the information without compromising the video quality.

IV. PROPOSED SYSTEM

Module 1: Video to Frames
Open Cv library can be used to perform multiple operations on videos Take a video as input and break the video into frame by frame and save those frame.
Steps:
Open video file using cv2.Videocapture()

Module 2: Secret Data Encryption
The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES) AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix

Module 3: Embedding Text and Video
In first step the cover video is converted to frames. Each frame is treated as an image. As this frame is a color image, each pixel comprises of 3 Channels, Red, Green and Blue. The secret data bits are stored in the last bit of each channel. Intuitively minimum of 3 pixels is needed to store 1 byte of secret data. This method involves embedding data in subsequent pixels.

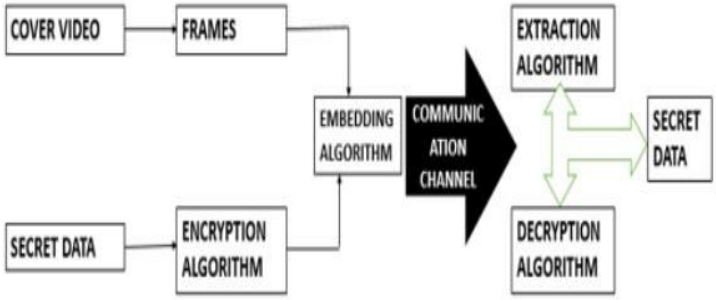
Module 4: Extraction and Decryption Algorithm
To Extract Cipher text from Video, LSB is used.
Each character is represented in 8 bits. So, the number of pixels in which the text is stored will be 13 * 8 = 104. We store the Least Significant Bit (LSB) of each pixel in an array extracted_bits. After extracting the LSBs of the required pixels, we need to take every 8 bits from extracted_bits and convert it to the corresponding character.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

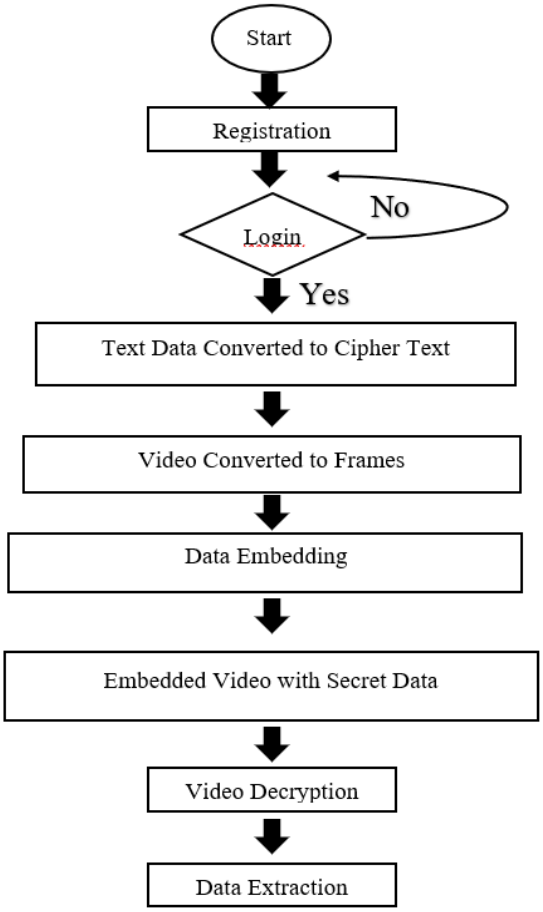
|| Volume 12, Issue 3, March 2023 ||

| DOI:10.15680/IJIRSET.2023.1203115 |

To Decrypt Text AES Algorithm is used.



V. METHODOLOGY



|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2023 ||

| DOI:10.15680/IJIRSET.2023.1203115 |

VI. FUTURE SCOPE

Designing a steganographic technique which maintains the balance among perceptual transparency, capacity, and tamper resistance. The algorithms reviewed so far consider the improvement in only one of these 3 metrics. Papers reviewed so far considers existing video as cover. As this video is already accessible, the intruder can calculate the distortion of the stego video with already existing original video. There is a high chance of data being revealed. To dodge this, a live video steganography can be proposed.

VII. CONCLUSION

The scope of the project is to limit unauthorized access and supply better security during message transmission. To meet the wants, I exploit the straightforward and basic approach of steganography. We have used different video steganographic techniques. The classification is broadly done as 1) early embedding where the secret data is first embedded and then further video processing is done. 2) Intermediate embedding where the data is embedded while the video processing is proceeding. 3) delayed embedding where the data is embedded into cover video at the later stages. We have used AES algorithm for Encryption and Decryption, along with LSB, DCT, WDCT algorithm.

REFERENCES

[1] Swathi, A., & Jilani, S. A. K. (2012). Video steganography by LSB substitution using different polynomial equations. International Journal of Computational Engineering Research, 2(5), 1620-1623.

[2] Dasgupta, K., Mandal, J. K., & Dutta, P. (2012). Hash based least significant bit technique for video steganography (HLSB). International Journal of Security, Privacy and Trust Management (IJSPTM), 1(2), 1-11.

[3] Bhattacharyya, S., & Sanyal, G. (2012, August). A novel approach of video steganography using pmm. In International Conference on Information Processing (pp. 644-653). Springer, Berlin, Heidelberg.

[4] Sampat, V., Dave, K., Madia, J., &Toprani, P. (2012). A Novel Video Steganography Technique using Dynamic Cover Generation. In National Conference on Advancement of Technologies–Information Systems & Computer Networks (ISCON–2012), Proceedings published in Int J of ComputAppl (IJCA).

[5] Atiea, M. A., Mahdy, Y. B., &Hedar, A. R. (2012). Hiding data in FLV video file. In Advances in Computer Science, Engineering & Applications (pp. 919-925). Springer, Berlin, Heidelberg.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details