Cryptography and Steganography Techniques in Video

Sharmila K. Wagh, Gaurav Upadhyay, Usha Bakan, Nikita Shinde, Shivani Nimbalkar

Abstract: ***Secure data transmission over the unsecured internet is an important aspect in communication. In recent times, data piracy, unauthorized access, loss of crucial information has been one of the important concern in secure communication of data. To provide security over data transmission, multiple techniques are provided each having its own benefits such as cryptography, steganography and watermarking. Cryptography is the technique for modification of data for secured transmission in an unreadable format. Steganography is the process of hiding the cover file with another file and transmitting the cover file without knowing the existence of hidden message. Watermarking is protection technique used to shield the information from intruders. Various combinations of cryptography and steganography is used to make data more secure. Such techniques differ in various aspects which are load capacity, security, efficiency, simplicity, and much more. Watermarking is the most used technique used for copyright protection in media files in recent times while cryptography and steganography are used to protect the data during communication so that the original data cannot be altered. In this paper, various techniques of cryptography and steganography are discussed which are used in the project.***

Keywords: Cryptography, Steganography, Watermarking, Data Piracy.

I. INTRODUCTION

In recent times, the digital world has become an unsafe medium due to the hackers and intruders present who are always looking to steal or access the data in an unauthorized way. To avoid loss of data during transmission, data should be kept safe and transferred in a protected way. This can be done using a variety of data hiding techniques where the original data is hidden or modified in an unreadable format which seems of negligible importance to the middle party. With secrecy of data being the main concern, such data hiding techniques are well used. Data hiding techniques are not new. Such techniques have been used since medieval times when important data needed to be hidden and sent during the times of wars and dispute. Ceaser cipher being one of the classical examples of data hiding technique where the original data was modified in a specific way to make it unintelligible. This data was then sent to other regions and deciphered in the same way to extract the original message. Information hiding implies embedding a secret message into a digital medium. The secret message can be of any form such as images, text, videos, files, etc. which can be represented in bits. In the techniques of steganography the cover file is used for embedding secret message onto it. This embedded cover file is called as stego-file.

II. LITERATURE REVIEW

A. "Review On Cryptography and Steganography Techniques in Video", Aiswarya.S, Gomathi.R [1].

In this paper, various techniques used in cryptography and steganography techniques used for hiding data in video is used. These techniques varies according to the availability of the resources and module used according to the users. These techniques include DWT (Discrete Wavelet Transform), DCT (Discrete Cosine Transform), Pixel Value Differencing Method. The authors concluded the paper by suggesting AES as the prominent video hiding technique as it is most widely used by looking at the accuracy of the proposed algorithm..

B. "Probing Image and Video Steganography based On Discrete Wavelet and Discrete Cosine Transform", Anitha Gnana Selvi. J, Maria kalavathy.G [2].

In this paper the authors have implemented Video Steganography using DCT and DWT algorithm. A Multiple Object Tracking(MOT) algorithm is also implemented in order to increase the embedding and extraction speed. The basic working of the system is to separate the video using MOT method, after which DWT is applied to categorize video in sub bands of high, low and approximate filters. Finally, DCT is applied on the low filter bands for transformation of high pass filter bands for hiding of data. Although the authors have proposed as the technique may lose some data after particular transformations of files.

C. "An Improved Video Steganography: Using Random Key-Dependent", Mohammad A. Alia, Khulood Abu Maria, Maher A. Alsarayreh, Eman, Abu Maria, Sally Almanasra [3].

The main aim of the paper is to extract the match between the RGB values of cover video and secret text. Using these values, a random stego-key is generated which is used at the receiver's side to extract the video and secret text by finding the values on the key.

Revised Manuscript Received on July 20, 2020.
***** Correspondence Author
Dr. Mrs. Sharmila K. Wagh, Modern Education Society's College of Engineering, Pune, India. Email: skwagh@mescoepune.org
Mr. Gaurav Upadhyay, Modern Education Society's College of Engineering, Pune, India. Email: gauravupadhyay1100@gmail.com
Ms. Usha Bakan, Modern Education Society's College of Engineering, Pune, India. Email: ushabakan@gmail.com
Ms. Nikita Shinde, Modern Education Society's College of Engineering, Pune, India. Email: nikitashinde504@gmail.com
Ms. Shivani Nimbalkar, Modern Education Society's College of Engineering, Pune, India. Email: rianimbalkar07@gmail.com

This exact matching algorithm along with random key-dependent data technique has a high embedding capacity and increased security as the cover video is not modified for hiding of data. This makes the proposed system highly effective and robust against various attacks.

D. "Optimized Data Hiding in Complemented or Non-Complemented Form in Video Steganography", Samar Kamil, Masri Ayob, Siti Norul Huda Sheikh Abdullah, Zulkifli Ahmad [5].

In this paper, the cover video frame is used which are embedded with secret data using a 2bit LSB technique in Non-Complemented form and a lookup table. The look-up table shows the number of times taken for the secret data bits to find complete matches with cover frame's pixel bits. The proposed technique has a drawback as the computational time increased with optimal match method. To overcome this drawback a non-complemented technique is proposed. This technique showed better accuracy than other existing techniques.

E. "MP4 Video Steganography in Wavelet Domain", Hemalatha S, U. Dinesh Acharya, Shamathmika [6].

An MP4 video steganography method that hides audio and image data in wavelet domain is proposed in this paper. A video file consists of collection of I-, P- and B- frames which are called as Group of Pictures (GOP). The I-frames are used for embedding process as they are not lost during transformation of any kind. The image frames and audio frames hides secret images and audio signals respectively. They are transformed using integer wavelet transform algorithm. The proposed technique is strong as compared to existing systems due to the fact that this technique incorporates both image and audio hiding together.

F. "Enhancing Audio and Video Steganography Technique Using Hybrid Algorithm", Shivam Teotia and Prakash Srivastava [7].

This paper presents review of various audio and video steganography techniques and their results using which a better, optimized algorithm is created for embedding secret data into cover file. Phase Coding and Parity Coding are some of the audio steganography techniques while LSB is the video steganography technique used. In the proposed system, AES algorithm is used for encryption and extraction process along with Huffman Coding for compression of data. The proposed system has better results and increased capacity.

G. "A Reversible Steganography Method With Statistical Features Maintained Based on the Difference Value", Tengfei Li , Huifeng Li , Liang Hu, Hongtu Li [8].

In the paper, Reversible Data Hiding (RDH) technique has been discussed which is used for hiding secret data within cover file and later the cover file can be extracted completely after extraction of secret data. The proposed technique for RDH is Difference Histogram Shifting (DHS) and Prediction Error-Histogram Shifting (PEHS) as these two techniques have high embedding capacity and increased robustness. The RDH techniques works same as sub bands technique discussed in [2] paper.

H. "Shortening the Cover for Fast JPEG Steganography", Weixiang Li, Wenbo Zhou, Weiming Zhang, Chuan Qin, Huanhuan Hu, Nenghai Yu [9].

The paper proposes the impact of cover selection under on average distortion under minimal distortion model by comparing various cover selection algorithms and their outputs. The best algorithm displays the speedup of embedding process with minimal impact on steganography model. This proposed system works with JPEG images as cover files which are used as a majority for DCT algorithm proposed in paper [1] and [2].

I. "An Video Steganography in Spatial, Discrete Wavelet Transform and Integer wavelet domain", Shailendra Kumar Yadav, Rosepreet Kaur Bhogal [10].

In this paper, DWT algorithm is applied and the cover video is divided into sub-blocks known as bands as proposed in paper [1] and [2] . These sub-bands of lowest filters are used for embedding and creating stego-video. Further, Inverse Integer Wavelet Transform (IIWT) algorithm is used for extracting the secret data and cover video at receiver's side. Various wavelet transform techniques are compared along with their results to analyze the better technique.

J. "Critical Analysis of Cryptography and Steganography", Alpa Agath, Chintan Sidpara, Darshan Upadhyay [12].

The paper proposes comparison of various symmetric encryption algorithms such as 3-DES, AES, Blowfish and RC5 algorithms among which AES provides the most facilities such as block sizes, rounds, flexibility and level of security. Also the traditional steganography techniques are compared with Hex-Symbol Steganography as the Hex-Symbol algorithm is proved to be more efficient than the existing symmetric algorithms.

III. DATA HIDING TECHNIQUES

Data hiding is the technique used for protection of alteration or modification of data in order to save it from the intruders. Such techniques improves security of the system and adds integrity and confidence to the users about the system. Authenticity and data integrity are the main goal of these techniques. When a message is sensitive, it should have added security in order to maintain its authenticity and avoid misuse of data or any unauthorized access over it. Such techniques have varied applications in fields of military and industrializations. It is mainly classified into three types such as

- Cryptography
- Steganography
- Digital Watermarking

Cryptography alters the data, Steganography hides the data and watermarking protects the ownership of data.

The different techniques listed are explained below in detail.

A. Cryptography Techniques

Cryptography is technique of securing information and communications through use of codes so that the data seems unintelligible to unauthorized user and only those person for whom the information is intended can understand it and process it. It uses mathematical procedures in encrypting and transmitting the secret data. Thus preventing unauthorized access to information. The prefix "crypt" means "hidden" and suffix graphy means "writing".

In Cryptography the techniques which are used to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for various applications such as cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.In general there are three techniques for cryptography. They are:

- Symmetric Key Cryptography
- Asymmetric Key Cryptography
- Hash Function

1) Symmetric Key Cryptography

In this technique, there is only a single communication key between sender and receiver during the entire duration of communication. This key can be a combination of letters, numbers, etc. Such techniques are faster and more reliable against third-party users but needs the key to be exchanged somehow between the users of the system. Examples of such cryptography techniques are Data Encryption System(DES), Triple DES or 3 DES, Advanced Encryption System(AES), etc. AES being the latest and most advanced of them all which allows encryption of 128 bits block of data with the communication key of sizes 128, 192 and 256 bits. AES provides encryption and decryption in rounds constituting byte substitution, shift rows, mix columns and transposition of bytes.

2) Asymmetric Key Cryptography

The difference between symmetric and asymmetric cryptography techniques is the use of keys. Asymmetric Cryptography techniques makes use of two different pair of keys instead of one. A public key is used for encryption and a private key is used for decryption. This technique provides additional security as even if public key is known to the attacker, the information cannot be decoded as private key is known only to the receiver. Example of such techniques are RSA, DSA and Elliptic Curve Cryptography(ECC). ECC being the safest of them as it uses a logarithmic function for encryption and decryption.

3) Hash Function

There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.

B. Steganography Techniques

Steganography is the technique of hiding sensitive data within an ordinary file also known as cover file in order to avoid detection, so that the messaged can be transmitted without the fear of getting leaked. The word steganography is derived from the Greek words "steganos" meaning hidden or unrevealed and "graph" meaning to write.

Steganography techniques can be used to conceal almost any type of data i.e. text, image, audio, video, etc. Its major advantage is that such data can be hidden using any kind of cover file which can totally hide the data with only minor changes on the surface. Such techniques find a majority of applications in the field of medical science, military and industry where data integrity is an important aspect. Fig. 1 represents the working module of a steganography system.

Various steganography techniques are:

1. Text Steganography

The text file is primarily used as the cover file to hide the sensitive data. This data is converted into binary format before hiding it behind the text file so as to maintain the quality of text file from degrading.

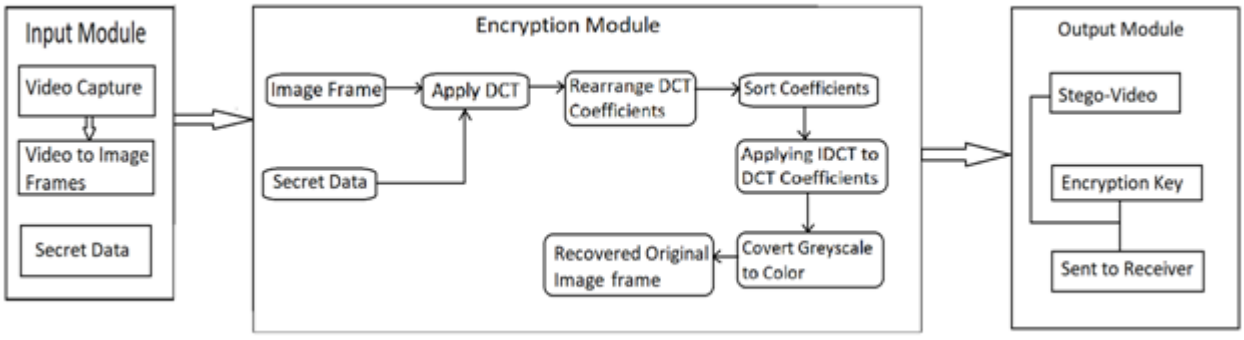

Fig 1. Steganography Working Module

2. Image Steganography

An image is used as a cover file to encrypt the sensitive data. Techniques such as spatial domain or LSB modification is used for which binary modification is done on to the data before encryption. Discrete Wavelet Transform (DWT) is one famous technique.

3. Audio Steganography

The sensitive data is hidden onto an audio file as cover. Bit positioning techniques are used for encryption of data onto the audio file.

4. Video Steganography

In this technique, a video file is used as a cover for hiding of data. A video file being a combination of audio and multiple images, variety of techniques can be used for encryption of any of the format. Video Steganography technique is much more complex methodology as it has larger capacity. The video is taken as collection of pixels which are then modified and selected for encryption. Some of the notable techniques used in video steganography are DCT, Integer Wavelet Transform(IWT), LSB, HSB modification, etc.

C. Digital Watermarking

Digital watermarking is a technology in which identification information is embedded into the data carrier in ways that cannot be easily noticed, and in which the data usage will not be affected. This technology often protects copyright of multimedia data, and protects databases and text files. Because of data's randomness and dynamics, methods of watermarking imbedded into databases and text files and multimedia carriers are quite different. And the basic precondition is that there is redundant information in the data, and tolerable precision error. For example, Agrawal embedded watermarking into the least important position of data, randomly based on the tolerance range of error in the numeric data in the database

IV. RESULT

The review of various symmetric key encryption algorithms have been stated in **Table- I**. These algorithms include DES, 3DES, AES and Blowfish along with various comparison factors such as Structure, Key length, Block size and more. Based on these factors, AES appears as the strongest symmetric key algorithm in working.

TABLE- I: COMPARISON OF SYMMETRIC KEY ALGORITHMS

Method	DES	3DES	AES	Blowfish
Developed By	IBM	IBM	NIST	Bruce Schneier
Structure	Feistel Network	Feistel Network	Substitution and Permutation Network	Feistel Network
Key Length	56 bits	Three 64 bit keys	128 bit, 192 bit, 256 bit	Variable key length with max size 448 bits
Block Size	64	64	128	64
No. of Rounds	16	48	9	16
Vulnerabilities	Brute Force Attack	Theoretical Attacks	Side Channel Attacks	Not Prone to Attacks
Efficiency	Slow	Slow	Highly Efficient	Highly Efficient

V. CONCLUSION

In this paper, various data hiding techniques are discussed. Many systems in current times use a combination of cryptography and steganography for providing premium security and reliability. ECC and AES being one of the widely used cryptography techniques which provide maximum security and less processing cost as compared to other systems. AES specifically being used for video steganography as it provides maximum security to the audio or image frames in the video format. Spatial domain and transform domain techniques are used for embedding secret data.

REFERENCES

1. Aiswarya.S, Gomathi.R, "Review On Cryptography and Steganography Techniques in Video" (2018).
2. Anitha Gnana selvi. J, Maria kalavathy.G, "Probing Image and Video Steganography based On Discrete Wavelet and Discrete Cosine Transform" (2019).
3. Mohammad A. Alia, Khulood Abu Maria, Maher A. Alsarayreh, Eman, Abu Maria, Sally Almanasra, "An Improved Video Steganography: Using Random Key-Dependent" (2019).
4. Arnold Gabriel Benedict, "Improved File Security System Using Multiple Image Steganography" (2019)
5. Samar Kamil, Masri Ayob, Siti Norul Huda Sheikh Abdullah, Zulkifli Ahmad, "Optimized Data Hiding in Complemented or Non-Complemented Form in Video Steganography" (2018)
6. Hemalatha S, U. Dinesh Acharya, Shamathmika, "MP4 Video Steganography in Wavelet Domain" (2017).
7. Shivam Teotia and Prakash Srivastava, "Enhancing Audio and Video Steganography Technique Using Hybrid Algorithm" (2018)
8. Tengfei Li , Huifeng Li , Liang Hu, Hongtu Li, "A Reversible Steganography Method With Statistical Features Maintained Based on the Difference Value" (2019).
9. Weixiang Li, Wenbo Zhou, Weiming Zhang, Chuan Qin, Huanhuan Hu, Nenghai Yu, "Shortening the Cover for Fast JPEG Steganography" (2018)
10. Shailendra Kumar Yadav, Rosepreet Kaur Bhogal, "An Video Steganography in Spatial, Discrete Wavelet Transform and Integer wavelet domain" (2018)
11. Tamer Rabie, Mohammed Baziyad, "The Pixogram: Addressing High Payload Demands for Video Steganography" (2018)
12. Alpa Agath, Chintan Sidpara, Darshan Upadhyay, "Critical Analysis of Cryptography and Steganography" (2018)

AUTHORS PROFILE

Dr. Mrs. Sharmila K. Wagh is an Associate professor at Modern Education Society's College of Engineering in Pune. With an educational qualifications of PhD in Computer Engineering, she as 20+ years of experience in teaching with specialized fields such as Cyber Security and Machine Learning. She was awarded the Best Paper Award: -Paper published and presented on, "Enterprise Based Backup Management System", at International Conference ICSCI 2008 Hyderabad. Andhra Pradesh. Paper awarded as best paper of the session. Period 1st to 5thJanuary 2008. She also has one patent published along with 18 papers in Journals and 5 of them presented in International Conferences.

Mr. Gaurav Upadhyay is currently a student pursuing Bachelors of Engineering in Computer Science at Modern Education Society's College of Engineering. He is the leader of the four student group and leading author towards the development of the following paper. A majority of research work has been done by him related to the paper. The paper developed by the authors is a part of the final year project done by him and the group. He is currently aiming to pursue higher studies in the near future. The paper done is a primary research paper of the domain cyber security for the author.

Ms. Usha Bakan is currently a student pursuing Bachelors of Engineering in Computer Science at Modern Education Society's College of Engineering. She has been a pivotal member of the group regarding the research work done related to the comparison of various techniques and their analysis. The paper developed by the author is a part of the final year project done by her and the group. She has been a consistent member of the paper development process providing valuable inputs at various stages. The paper done is a primary research paper of the domain cyber security for the author.

Ms. Nikita Shinde is currently a student pursuing Bachelors of Engineering in Computer Science at Modern Education Society's College of Engineering at Pune. The reference paper findings and information retrieval has been done by her along with Ms. Shivani Nimbalkar. This information was critical in development of paper at research phase cycle. Along with this information, the Journal research work and publication work has been done by her at the Journal along with Ms. Usha Bakan. The paper done is a primary research paper of the domain cyber security for the author.

Ms. Shivani Nimbalkar is currently a student pursuing Bachelors of Engineering in Computer Science at Modern Education Society's College of Engineering at Pune. The reference paper findings and information retrieval has been done by her along with Ms. Nikita Shinde. Along with this, she was also a part of paper table and diagram presentations which helped in extraction of pivotal information in the paper. The paper done is a primary research paper of the domain cyber security for the author.