Available online at: https://ijact.in

Date of Submission	03/08/2018
Date of Acceptance	23/08/2018
Date of Publication	30/08/2018
Page numbers	2803-2806 (4 Pages)

ISSN:2320-0790

COMPUSOFT
An International Journal of Advanced Computer Technology

A MODIFIED APPROACH OF VIDEO STEGANOGRAPHY FOR INFORMATION HIDING

[1]Bhavna Gupta

[1]Asst. Prof., GERIIT, Jaipur, India

Abstract: Steganography is a branch of information hiding. Steganography is a process of embedding the secret information inside the host medium (text, audio, image and video). Video Steganography is the technique of hiding some secret message inside a Video. For improving security we are also using Cryptography. Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is deliberate can read and process it. In this report Modified Advance Encryption Standard algorithm is used for converting the message in cipher text and then hides this cipher text in video using Discrete Wavelet Transformation technique. Proposed DWT technique is robust to the common attacks.

Keywords: Steganography, Cryptography, DWT, PSNR, MSE, MAES

I. INTRODUCTION

INTERNET have made people's lives much easier than before; they can use it to pay their bills, buy their goods, exchange important messages between parties at far distances, and many other things. Without protecting that valuable information, attackers can obtain them in different ways.Steganography is one of the methods that protects and hides valuable data from unauthorized people and even without them having any suspicion of the data's existence.[3] In ancient time, the data was protected by hiding it on the back of wax, writing tables, stomach of rabbits or on the scalp of the slaves. But today's most of the people transmit the data in the form of text, images, video, and audio over the medium. In order to safely transmission of confidential data, the multimedia object like audio, video, images are used as a cover sources to hide the data.[10] In new era of information technology, information security is a big issue. For information (data) to be sent from sender to user, it is more important that to give right information to right people at a right time. Cryptography converts the message into a non readable format and sends the message over an unsecure channel. The unauthorized person will try to read the unreadable message but it is not easier. "Encryption is a process of transferring plaintext information to a form called cipher text using an algorithm called cipher which is readable only by whom who has special knowledge called encryption key".[12]Discrete Fourier Transform, Discrete cosine Transform, Discrete wavelet Transform and spread transform are common frequency domain methods used for watermarking.

A. *Types of Steganography:*

1. Text Steganography: It consists of hiding information inside the text files. In this method, the secret data is hidden behind every nth letter of every words of text message.[10]
2. Image Steganography: This is used widely for hiding information in the cover image.[10]

3. Video Steganography: It is a technique of hiding any kind of files or data into digital video format. In this case video (combination of pictures) is used as carrier for hiding the data. Generally discrete cosine transform (DCT) alter the values (e.g., 8.667 to 9) which is used to hide the data in each of the images in the video.[10]
4. Audio Steganography: It involves hiding data in audio files. This method hides the data in WAV, AU and MP3 sound files.[10]

B. Steganography Techniques:

1. Spatial Domain: In this technique, the LSB of an envelope image is substituted without performing any modification. This maintains the quality of color image, and is very simple and effective for concealing image or data. However, there are weaknesses of this technique that can be easily attacked, such as compression, transformations, etc.[2]

2. Transform Domain: In this technique the secret message is embedded in the transform or frequency domain of the cover. This is a more complex way of hiding message in an image. Different algorithms and transformations are used on the image to hide message in it. Transform domain techniques are broadly classified such as i) Discrete Fourier transformation technique (DFT) ii) Discrete cosine transformation technique (DCT) iii) Discrete Wavelet transformation technique (DWT)[14]

3. Spread Spectrum Technique: In this method the secret data is spread over a wide frequency bandwidth. The ratio of signal to noise in every frequency band must be so small that it become difficult to detect the presence of data. Even if parts of data are removed from several bands, there would be still enough information is present in other bands to recover the data.[10]

4. Statistical Technique: In this technique message is embedded by changing several properties of the cover. It involves the splitting of cover into blocks and then embedding one message bit in each block. The cover block is modified only when the size of message bit is one otherwise no modification is required.[10]

5. Masking and Filtering: These techniques hide information by marking an image. This method is basically used for 24-bit and grey scale images.[10]

Distortion Techniques: In this technique the secret message is stored by distorting the signal. A sequence of modification is applied to the cover by the encoder. The decoder measures the differences between the original cover sequence of modifications and consequently recover the secret message.[10]

II. ORGANIZATION OF PAPER

The organization of the paper further is as follows. The Comparative study is presented in Section III, Proposed Method in Section IV, then Result Analysis in Section V and Conclusions and Future Scope discussed in Section VI.

III. COMPARATIVE STUDY

	Paper Title	Method	Advantage	Limitation
1	Highly Secure Image Steganography Algorithm using Curvelet Transform and DCT Encryption	Curvelet transform and DCT	DCT is robust against MPEG-2.	Hides in independent frames.
2	Image Steganography and visible watermarking using LSB Extraction Technique	LSB	Simple Implementation.	LSB insertion is a very little robust technique.
3	RGB Image Watermarking on video frames using DWT	DWT	DWT allows us to recover the exact RGB image without any distortion.	Hiding capacity drops if the used cover video doesn't have large motion component
4	A Highly secure video Steganography using Hamming code(7,4)	Hamming code(7,4)	Hamming code handles error correction as well as error detection.	Hamming code handles only single bit errors.
5	Modified AES Based Algorithm for MPEG Video Encryption	AES,MAES	MAES takes less time for encryption and decryption	AES takes more time for encryption and decryption

6	Separable Reversible Encrypted Data Hiding in Encrypted Image Using AES Algorithm	AES	Safe	Time and energy required against Brute-force

IV. THE PROPOSED METHOD

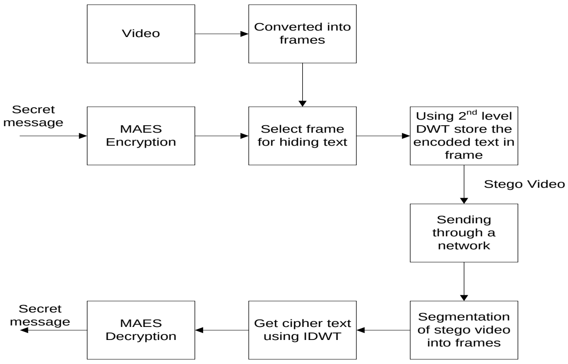

Video
Converted into frames
Secret message
MAES Encryption
Select frame for hiding text
Using 2nd level DWT store the encoded text in frame
Stego Video
Sending through a network
Secret message
MAES Decryption
Get cipher text using IDWT
Segmentation of stego video into frames

Fig. 1: Proposed system

Step 1: Video file is converted into a series of frames of equal size.
Step 2: Secret message is encrypting using MAES.
Step 3: Select frame for hiding text.
Step 4: Using 2^{nd} level DWT store the encoded text in frame.
Step 5: Stego video transmitted through a network.
Step 6: Stego video segmented into frames.
Step 7: Get cipher text using IDWT.
Step 8: Decode text using symmetric key.
Step 9: Get Secret message.

V. RESULTS

Table : PSNR Value of both approaches

Sequences	Frame no.	PSNR using AES	PSNR using MAES
Xylophone.mpg	1-100	85.89	85.93
	101-141	85.90	85.96
Clay 5.mpg	1-30	86.24	86.56

Above table shows the PSNR values Using AES and MAES of two different videos.
In Figure we show comparison of AES and MAES.

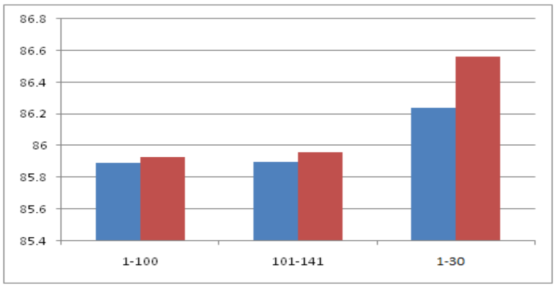
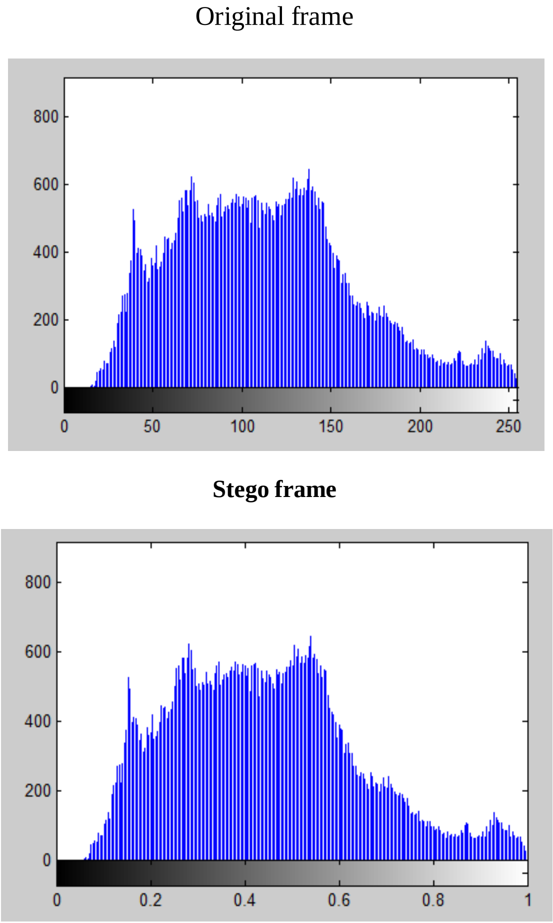


Figure : PSNR value comparison of AES and MAES


Original frame

Stego frame

Figure : Histogram of original frame and stego frame

VI. CONCLUSION & FUTURE SCOPE

During the review and analysis of various papers on Steganography techniques we have observed that Video Steganography is best technique for hiding large amount of data compare to the image Steganography. The proposed method use combination of 2^{nd} level DWT method and MAES algorithm. Here Video Steganography use MAES algorithm for encryption of the secret message and 2^{nd} level DWT method for hiding encrypted message to provide more security and robustness.The Future work may be extended by other transformation techniques.

VII. REFERENCES

[1] A.Elsayed, A.Elleithy, P.Thunga, Z.Wu, “Highly Secure Image Steganography Algorithm using Curvelet Transform and DCT Encryption ”,Systems, Applications and Technology Conference(LISAT) 2015 IEEE Long Island, Page(s): 1-6

[2] Santhoshi Bhatt, Arghya Ray, Avishake Ghosh, Ananya Ray, “Image Steganography and Visible Watermarking using LSB Extraction Technique” ,IEEE Sponsored 9th International Conference on Intelligent Systems and Control(ISCO) 2015 ,Page(s): 1-6

[3] Saket Kumar, Ashutosh Gupta, Ankur Chandwani, Gaurav Yadav, Rashmi Swarnkar, “RGB Image Watermarking on Video Frames using DWT”,IEEE Sponsored 5th International Conference 2014, Page(s):675-680

[4] Ramadhan J. Mstafa and Khaled M. Elleithy, “A Highly Secure Video Steganography using Hamming Code (7, 4)”,(LISAT) IEEE 2014 ,Page(s):1-6

[5] P.Deshmukh, V.Kolhe, “Modified AES Based Algorithm for MPEG Video Encryption” ,IEEE International Conference on Information Communication and Embedded Systems (ICICES)2014, Page(s):1-5

[6] Parag Kadam , Mangesh Nawale, Akash Kandhare, Mukesh Patil , “Separable Reversible Encrypted Data Hiding in Encrypted Image Using AES algorithm and Lossy Technique” Pattern Recognition, Informatics and Mobile Engineering (PRIME) IEEE 2013, Page(s):312-316

[7] Mennatallah M. Sadek, Amal S. Khalifa, Mostafa G. M. Mostafa, “Video steganography: a comprehensive review”, Multimedia Tools and Applications (2015) Volume 74,Springer ,Page(s):7063–7094

[8] Richa Khare, Rachana Mishra ,Indrabhan Arya, Oriental College of Tech Bhopal,” Video Steganography by LSB Technique using Neural Network” 2014 Sixth International Conference on Computational Intelligence and Communication Networks ,IEEE, Page(s):898-902

[9] Navneet Kaur, Sunny Behal “A Survey on various types of Steganography and Analysis of Hiding Techniques” International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 8 - May 2014,Page(s):388-392

[10] Jasleen Kour, Deepankar Verma “Steganography Techniques-A Review Paper”, International Journal of Emerging Research in Management & Technology, vol-3, May 2014,Page(s):132-135

[11] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt “Digital Image Steganography: Survey and Analysis of Current Methods”, signal processing, vol-90, march 2010, ELSEVIER ,Page(s):727-752

[12] Mohsin Khan, Sadaf Hussain, Malik Imran “Performance Evaluation of Symmetric Cryptography Algorithms: A Survey” International Journal of Information Technology and Electrical Engineering Volume 2, Issue 2 April 2013,Page(s):1-8

[13] Avinash kak , “AES: Advance Encryption Standard Lecture Notes on : Computer and Network Security” May 1, 2015 , Purdue University, pp 1-79 Date: 25/1/2016 Time: 10:09 AM

[14] Richa Khare,Dr.Kuldeep Raghuwanshi, “A Review of Video Steganography Methods”, International Journal of Research in Advent Technology, volume 2,January 2014,Page(s):447-451

[15] Madhuri Rajavat, D S Tomar, “ A Secure Watermarking and Tampering detection technique on RGB image using 2 level DWT”, Fifth International Conference on Communication System and Network Technologies 2015 IEEE, Page(s):638-642