I.J. Image, Graphics and Signal Processing, **2016, 9, 31-39**
Published Online September 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2016.09.05

XOR-EDGE based Video Steganography and Testing against Chi-Square Steganalysis

Ramandeep Kaur
Research Scholar, Department of Computer Engineering, CT Group of Institutions, Jalandhar, 144001, India
Email: raman177rk@gmail.com

Sharanjeet Kaur
Research Scholar, Department of Computer Engineering, CT Group of Institutions, Jalandhar, 144001, India
Email: sharanmarock6@gmail.com

Abstract—In this paper, our main aim is to compare different video formats and analyze what will be the effect on quality when we hide same secret message in different type of formats such as RGB color videos, .avi (colored and uncompressed video format), and mp4(colored and compressed video format) using edge detection and 7 pair identical match techniques. . In research work, edge areas are used to hide high capacity of secret data behind a video file. As edges are very sharp in nature and their frequency values are changed continuously, which can't be seen by the human visual system (HVS) due to the low probability of being perceived. The analysis is done on the basis of quality metrics such as PSNR, BER and Histogram Analysis for different format video clips. The Experimental results show that proposed algorithm provides resistance against Chi-square statistical attack and visual attacks.

Index Terms—Video Steganography, Edge Detector, LSB Substitution, Identical Match, Encryption, Histogram Analysis.

I. Introduction

Recently, video steganography has become very popular research area for concealing large amount data behind video without being noticed by the human eye and transfer it over the network with high security and without any degradation in the quality of the video. Steganography is an information hiding technique, which is used since the ancient times to protect the confidential information from the hacker's attacks using various type of digital media like text, image, audio, protocol based etc. & video steganography is one of the vital parts of steganography concept [1]. The main motive of video steganography is to hide the secret information inside the cover video. So it is a nontangible masking of confidential information. Steganography concept is different from the cryptography and digital watermarking. As cryptography is a process of encrypting or modify the hidden message in an unreadable format. It just scrambles the secret message bits and steganography is a process of hiding the existence of secret message by embedding it inside the video from intruders. It actually protects the confidential data. Digital watermarking is also information hiding technique but, it protects the media file from being pirated and provides copyright protection for authentication by embedding logos, captions etc [15].

Video steganography works in two phases; Embedding and extraction process. In embedding process, we actually hide the secret data inside video using various embedding algorithms and this process is carried out at the sender side. Whereas; Extraction process is carried out at the receiver side and only authorized users can extract secret message using Stego key, which is known to sender and receiver only to increase the protection of hidden data from intruders. It is the reverse process of embedding phase. The embedding algorithms are categorized into two basic domains i.e. spatial domain and transform domain. Spatial domain deals with a video file as it by replacing the secret bits with video frame's pixels directly. It is also named as time domain. The most basic spatial methodology is least significant bits (LSB). In transform domain, the manipulation of the coefficient is done using various transformations like Fourier (DFT), discrete cosine transformation (DCT), wavelet transformation (DWT), etc. The real life examples of steganography are QR codes, invisible inks, microdots and wax – candle etc. video steganography has various benefits to society as it is used in digital watermarking, feature tagging, in smart card to embed personal detail of person for verification, in biometrics to hide fingerprints detail and voice for recognition, for secret communication in military base, and by computer forensics to detect fake video files and cybercriminals [2].

A good video steganography must have three properties which are explained as follows:

A. Capacity

It means the total amount of data or number of bits that can be hidden inside carrier video. It defines the maximum size of the secret message or its length.

B. Perceptual Transparency (Perceptibility)

The data should be hidden in such a manner that it should not be visible to the human visual system. So it should be transparent. If we increase the capacity of data

then its transparency will be affected. Perceptual transparency is of two types: Quality and fidelity.

C. Security

Attackers can extract the important information by applying various attacks. So security of video steganography must be high using various encryption and security algorithms.

D. Cryptography vs. Steganography

Cryptography is the data security technique which is used to encrypt the secret or plain information into unreadable (Cipher) format. It just changes the message readability not imperceptibility like steganography. Cryptography is used only for text files and not used for digital files like audio, image and video files. There are various types of encryption algorithms are available which helps to increase the security of confidential information and protect data from any unauthorized access or cyber criminals such as hackers, attackers etc. Generally, cryptography is divided into two main classes i.e. symmetric key algorithm and Asymmetric key based algorithms:

- **Symmetric Key Based Cryptography**: In symmetric key based algorithm same key is used to encrypt or decrypt the secret message by sender and receiver respectively. The common method used for symmetric key encryption are substitution cipher (replacement of characters with another character or digit or special symbols like @, # , % etc), transposition cipher (no replacement, only locations of character changed to create cipher text from plain text), simple modern cipher (no character orientation, only bit orientation to make data more secure and used in digital video , audio, image & graphics e.g. XOR Cipher, Rotation Cipher, Substitution Cipher S-box and Permutation P- Box Cipher) and Modern round cipher (simple text is divide into blocks and then multiply encrypt the data for high security e.g. Data Encryption Standard (DES), it's advanced version Triple- Data Encryption Standard (3DES) and Advanced Encryption Standard (AES)) as shown in Fig 1.
- **Asymmetric Key Based Cryptography**: Asymmetric key-based encryption algorithms provides high security than symmetric key algorithm as there is no need of third party member to share a secret key between sender and receiver. Both sender and receiver have their own public and private key to encrypt and decrypt the plain text. The basic asymmetric encryption methods are RSA and Diffie-Hellman, Blowfish Algorithms. Both algorithms are highly secure methods and have high time and space complexity.

To increase the security and privacy of steganography, cryptographic algorithms can also be integrated with steganography process. It helps to provide one more layer protection to confidential information by converting original message into an unreadable format. Both Integrated data hiding and data security techniques such as steganography and cryptography are itself much secure that nobody can break it as easily as they can break alone by applying some hit & trial and SQL injections attacks.

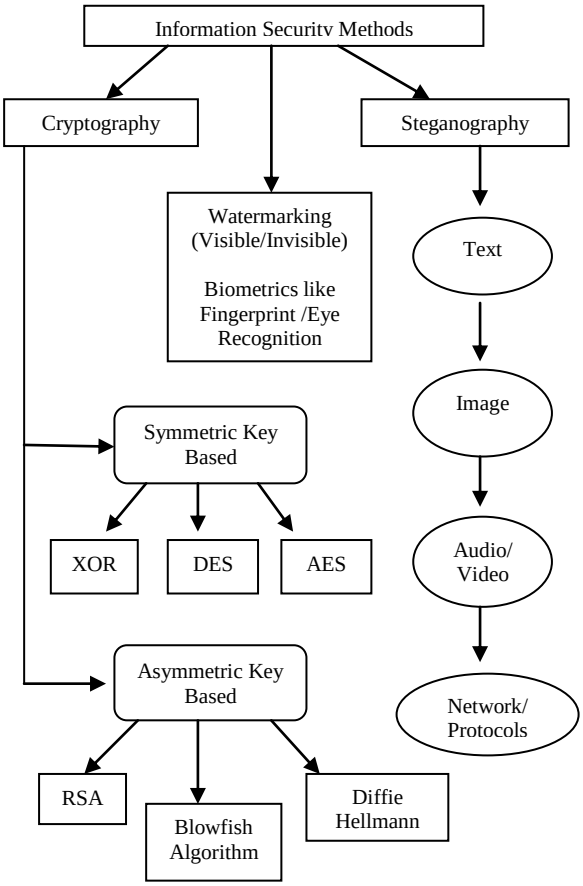

Fig.1. Information Security Methods

This paper explores the concept of steganography by using a hybrid approach for video steganography using edge detection and 7 pair based identical match techniques to enhance the hiding capacity, quality and security. Also, a comparative analysis has been carried out using different video formats to analyze the quality of Stego video and using histogram analysis. The results have been taken out practically by using MATLAB toolbox for simulation.

The whole research paper is arranged into various sections; Section II describes the related work, Section III presents the proposed methodology, Section IV explains the embedding and extraction algorithms, Section V consist of simulated results & discussion, and Section VI discuss the conclusion and future scope of the proposed work.

II. Related Work

The main issue of video steganography is to protect the confidential information from the intruders and provide it more security from the attacks. To avoid this problem,

many algorithm and steganography mechanisms have been proposed to reduce the effect of attacks on carrier video as well as to maintain its imperceptibility.

In the year 2013 Ref. [1], the author has proposed a new method to hiding secret message behind a video file using 4 LSB technique and used computer forensics as an authentication tool and achieves high capacity of data. It has one limitation of not providing resistance against statistical attacks. And in Ref. [4], the researcher has proposed another new methodology for video steganography. In this paper, video streams are used as a secret file and hide inside the host video file's streams using sequential encoding and symmetric encryption techniques and encrypted using XOR transformation. Then these encrypted frames are hidden inside the LSB bits of cover video streams using a sequential encoding. But it has the disadvantage that as attackers can easily identify the presence of secret message by sequentially analyzing the video frames.

In Ref. [7], hybrid edge detectors 3*3 matrix scanning and Sobel edge detectors are used to detect edges from the image and blue component of the image is used to embed secret messages on edges of the image. This scheme increases the capacity and quality of Stego image. But Sobel operator is not good enough to find edge pixels because it contains some noisy edges also. But Sobel operator is not good enough to find out more edge pixels and also contains false and noisy edges, which reduces the quality of the image. In Ref. [14], a novel hiding mechanism has been proposed in which an identical match technique is used. This method hides secret message bits by searching the identical bits between secret message and image pixels value. If there is no identical pair then it will hide in LSB bits of the image. It provides robustness against attacks with 83% accuracy ratio.

But in Ref. [8], an integrated steganography methodology has been proposed in which embed secret message embedded in an image. Hybrid feature detection (canny and Enhanced Hough transform) to detect edges and two component based LSB substitution technique for hiding encrypted message in edges and adaptive LSB substitution technique for hiding message bits in smooth areas and AES encryption technique to resist attacks. But AES encryption has been broken by attackers. In Ref. [9], the author has been proposed an Image Steganography based method using parameterized canny detector. This paper depends on three basic parameters named as the size of Gaussian filter, a low threshold and high threshold values and 3LSB substitution used for embedding process. But has the limitation of complex processing as it generates three different outputs corresponding to three parameters. In Ref. [10], the author proposed an algorithm based on RLSB technique & embed the secret message behind the video. Random LSB generates pseudo random numbers and selects random pixels to hide the secret message inside the video and achieve high PSNR and low MSE.

In the year 2014, a hybrid approach of video steganography with watermarking has been proposed to embed the secret message in career video. DCT & DWT techniques are used to hide a message inside the video and generate a Stego video. This Stego video is again used to embed a watermark using LSB technique to increase the security of Stego video Ref. [6].

III. Proposed Methodology

To maintain the security and to avoid the problems that are formulated in literature survey, we have been proposed a new methodology, in which we are detecting edge pixels of video randomly selected video frames to hide secret message bits using canny edge detector. The proposed methodology is a hybrid approach for video steganography using edge detection and identical match techniques based on different video formats. Our main objective is to analyze the impact of quality of Stego videos by using different video formats when we hide the same message by following the same algorithm of edge-based video steganography. The following are the main steps for proposed methodology.

- **Video Selection:** This is an initial step of methodology in which we select video format in which we want to embed secret data. There is different type videos of different video formats are available such as .avi and .mp4 etc. we can choose any one at a time.
- **Frame Extraction:** Extract 10 random frames from video using random frame selection algorithm on the basis of entered secret key.
- **Edge Detection:** Detect edges of selected random frames using canny edge detector.
- **Encryption:** Enter text secret message and encrypt it into an unreadable format using XOR algorithm.
- **Embedding Process:** Hide same secret message behind different videos such as .avi, .mp4 and another one by one using 4LSB and 7- pair identical match substitution techniques in edge and non-edge pixels respectively and generate Stego video for each selected video formats [17].
- **Extraction Process:** To extract secret message from Stego video, perform reverse process of embedding algorithm using secret key and display output as hidden text message.
- **Comparison:** Calculate PSNR, BER and Histogram Error for each video after hiding a secret message in different format videos to analyze the effect of quality and we analyzed that our methodology drops the risk of visual and statistical steganalysis.

IV. Algorithms

A. Embedding Algorithm

The embedding process is used to hide secret data behind media file as shown in Fig 2. It is carried out at

the sender side. In embedding process, the first step is to select one video of any format either .avi/.mp4 or any other format video. Suppose, we are selecting .mp4 format based video file and calculate total it's frame rate as shown in Fig 3. Then, in the second step select 10 random frames from video frames using secret key based generated random functions in which we hide a secret message [2] and detect edges of selected frames using canny edge detector [5]. After that, Enter text message and 10 digits secret key and encrypt a secret message using XOR encryption algorithm [4] and hide the secret key, selected frame addresses, and message length in the first frame of video.

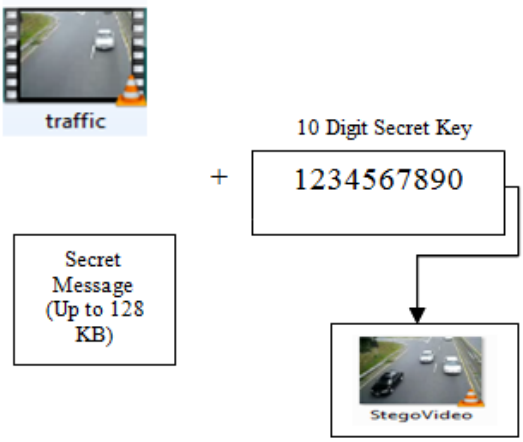

Fig.2. Embedding Process of Proposed Work

Now, hide encrypted secret message using 4 LSB and 7 pairs identical match method in edge pixels and non-edge pixels respectively and generate Stego video file [17]. Repeat the previous process for selecting next format based video i.e. Mp4, WMV or .AVI video and hide same secret message using same algorithm steps for embedding data behind video file. In the last step, analyze the effect of quality of different format based video files on the basis of PSNR, BER, and histogram Analysis and analyze effect of quality after hiding information in different format video files and apply Chi-Square Attack on Stego Video to analyze Chi Index value which should not exceed its critical value i.e. 0.05.

B. Extraction Algorithm

The extraction process is a reverse process of embedding algorithm used to extract hidden information from media file and it is carried out at the receiver side. The extraction process includes various steps. In the first step, Select Stego video and enter same 10 digits secret key at the receiver side to extract hidden data and extract the secret key, selected frame addresses and length of a message from the 1st frame of Stego video. Also, extract secret message by using the reverse process of embedding algorithm i.e. reverse of 4LSB substitution and using bit positions of 7 pair identical match techniques [3]. At the end, decrypt extracted message using the reverse of XOR encryption algorithm and display output as hidden secret text message.

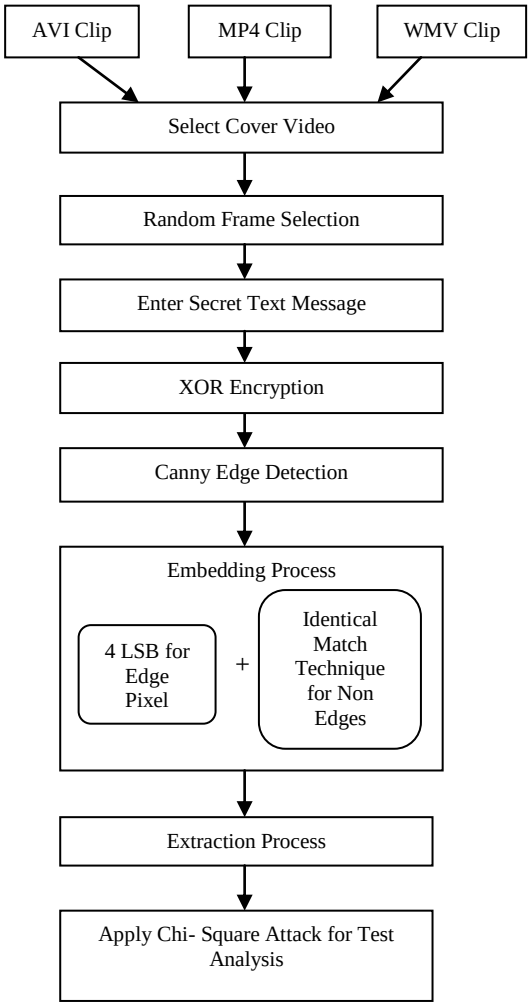

Fig.3. Flow Chart of Proposed Work

V. Experimental Results

The proposed algorithm simulation is done on MATLAB 7.0 version 2014a. The experimental results show that our algorithm is good enough to support different type of video formats such as AVI, MPEG, and MP4. It also shows that AVI video base steganography has high quality as compared to MPEG Video clip. But MP4 format video generates high-quality stego video during steganography process and it has high security and no loss of data after hiding information due to lossless compression mode.

A. Extraction Results

The experimental results are analyzed on the basis of PSNR (Peak signal to Noise Ratio), BER (Bit Error Rate), MSE (Mean Square Error) and Payload Capacity for a different type of video formats such as AVI, MP4, and WMV. The test analysis is conducted using different video formats such as AVI video named as 'Traffic.avi', MP4 named as 'MyKrishna.mp4' & WMV video named as 'Clip_1080_5sec_VC1_15mbps'.

The experimental results show that the Avi video formats have high PSNR value than Mp4 and WMV type

of videos as shown in Table 1, 2 & 3 respectively and Fig 4, 9, & 11 are showing the all the selected 10 random frames for different type of video frames such as AVI, MP4 and WMV respectively. The Fig 5, 10 & 12 are showing edged and corresponding stego frames for each one random frame for format AVI, MP4 and WMV respectively after hiding the secret text message of length 4 KB and 64KB and Fig 6 & 7 are showing performance parameters values for hiding the 64 KB data in 10 random frames of AVI video format and the average values of PSNR, BER and MSE after hiding data in all frames.

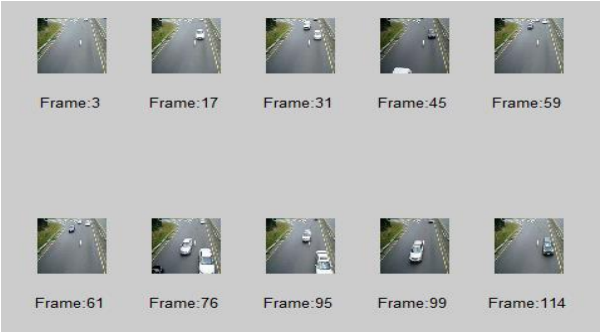

Fig.4. All Original Random Frames

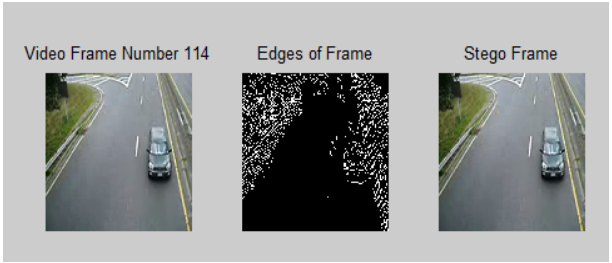

Fig.5. Edge and Stego Frames

Table 1. Test I for AVI Video Format

Video Clip Format	Data Capacity (KB)	PSNR (db)	MSE
Traffic.avi	4 KB	66.14	0.01511
	64 KB	54.40	0.01838

The average results of PSNR for AVI video is 54.66 dB, and for Mp4 & WMV video clips. It values are around 53.24dB. The AVI videos are uncompressed videos and contain full detail about video clip so there is no loss of data and quality of video due to which they have high PSNR values but Mp4 is compressed video format and there are chances of data loss so due to which PSNR values decreases. Also, as we hide a large amount of data the PSNR value goes on decreases as shown in each table after hiding the different amount of data. The maximum data hiding capacity of present algorithm is 128 KB than previous work i.e. 32 KB. The comparison graph between is shown in Fig. 8 and this algorithm has low time complexity & processing time and high capacity with high-quality stego video files which actually contains secret message behind all random frames.

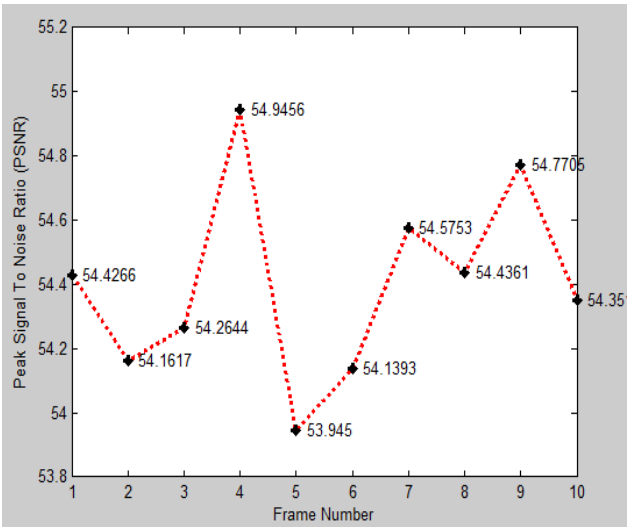

Fig.6. PSNR of all Random Frames (64 KB)

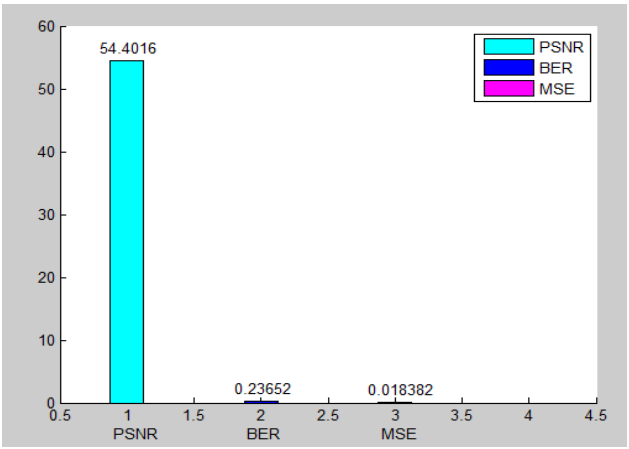

Fig.7. Average Psnr, Mse, & Ber Values (64 Kb Data)

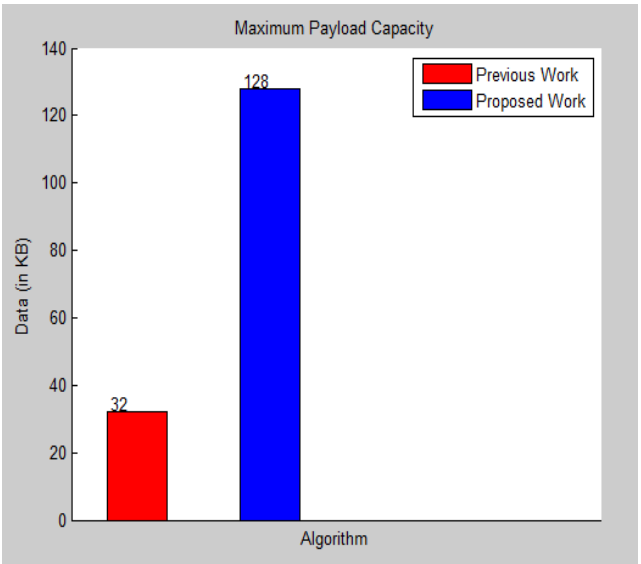

Fig.8. Maximum Data Hiding Capacity

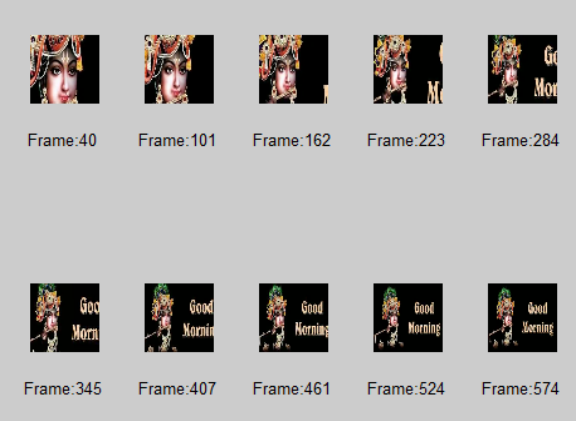

Fig.9. Showing MP4 Video's Original Random Frames

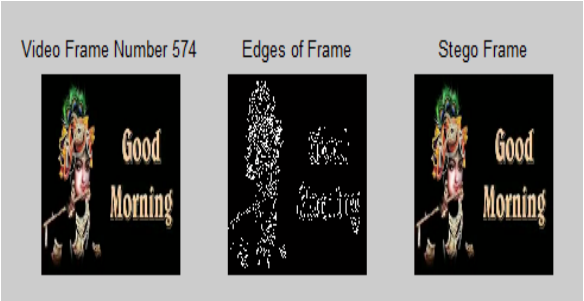

Fig.10. Showing Edge & Stego Frames for .mp4 Clip

Table 2. Testing Results for MP4 Video Format

Video Clip Format	Data Capacity (KB)	PSNR (db)	MSE
MyKrishna.mp4	4 KB	65.78	0.015202
	64 KB	53.5787	0.2871

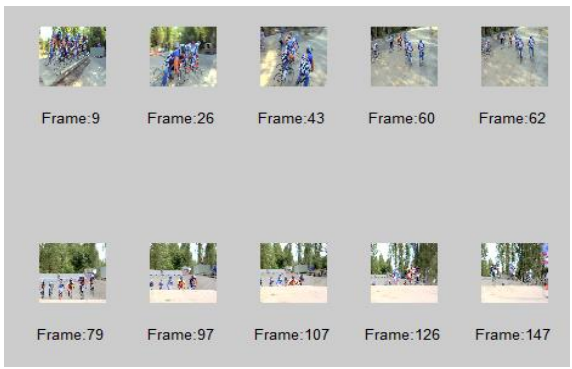

Fig.11. Showing WMV Video's Original Random Frames

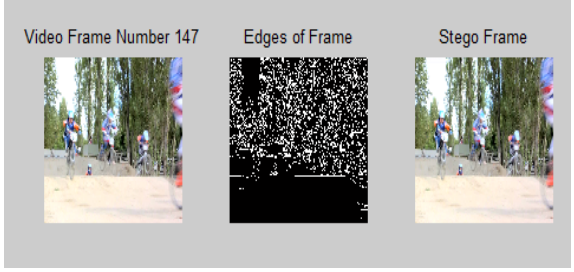

Fig.12. Showing Edge & Stego Frames for WMV Video Clip

Table 3. Testing Results for WMV Video Format

Video Clip Format	Data Capacity (KB)	PSNR (db)	MSE
'Clip_1080_5sec_VC1_15mbps.wmv	4 KB	65.4004	0.0189
	64 KB	53.2451	0.3107

The quality analysis is done on the basis of PSNR quality metrics for a different type of video formats. A video file can be of any type of video format such as AVI, Mp4, and Flv etc. But, in this work we are analyzing quality effect using Mp4, Avi, and WMV video formats and conclude that this algorithm supports different type of video formats. The present work is also an integrated approach of cryptography based steganography technique and provides 3-Tier security level using edge detection algorithms and Fig.13 is highlighting the main fundamentals and difference between data security techniques such as encryption techniques like cryptography, data hiding technique like digital steganography and copyright protection techniques like watermarking. It resists the risk of frame dropping and data manipulation problems as same data is hidden in all random frames and in case, due to some failure or attack some frames get damaged, then we can still recover secret message from another random frame.

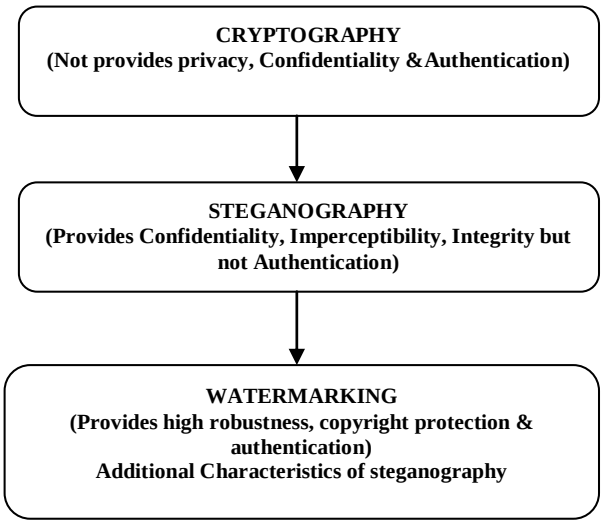

Fig.13. Three-Tier Security Approach

B. *Video Steganalysis Testing*

The steganalysis testing is done using visual and statistical attacks on the basis of histogram analysis and chi-square attack and find out that this algorithm is able to resist such type of attacks. Chi-square attack is a statistical attack which performs for detecting hidden data embedded by LSB based substitution techniques [20]. The test is conducted on a video file named as 'Traffic.avi' having 114 total number of frames used for hiding 4 KB data behind each 10 random frames of a video clip using 10 digits secret key i.e. '1234567890'. The experimental results of the test show that the data

hidden by proposed algorithm is undetectable when attackers will apply attack by chi-square steganalysis. The chi-square attack is analyzed by using chi-index value as shown in Fig.14, which is showing the Chi-index values for 10 random frames & Fig.15, which is showing the average results for Comparison of Chi-index values for different methodologies such as LSB, 4LSB and proposed work i.e. Edge-4LSB . The chi-square index's average value for basic LSB technique is analyzed larger than 0.5 and in 4LSB based substitution average index value is around 0.1443. But, in proposed algorithm its average value is near to 0.0107.

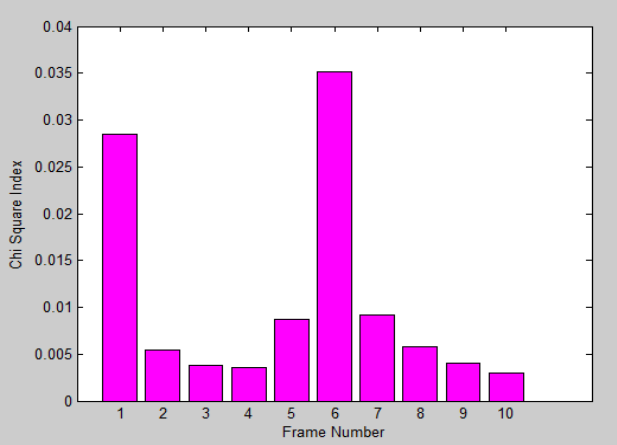

Fig.14. Chi Square Steganalysis (4 KB)

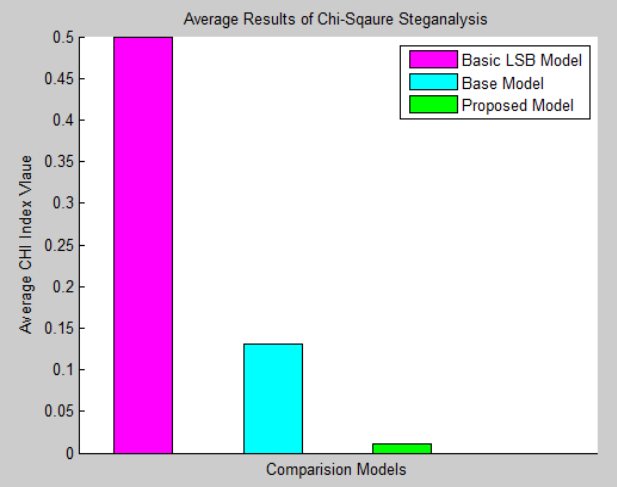

Fig.15. Comparison of Average Results for Chi-index

Other experimental results are analyzed using histogram analysis parameter. Histogram equalization process is used for doing test analysis against visual attacks. The histogram analysis is done between original and stego video to identify the difference between frequency distribution corresponding to each pixel's intensity value as shown in Fig.16 and experimental results show that there is a minor difference is seen by comparing both histograms visually and peak values of histogram are equal in original and stego video clip named as 'Traffic.avi'. So it resists visual attacks.

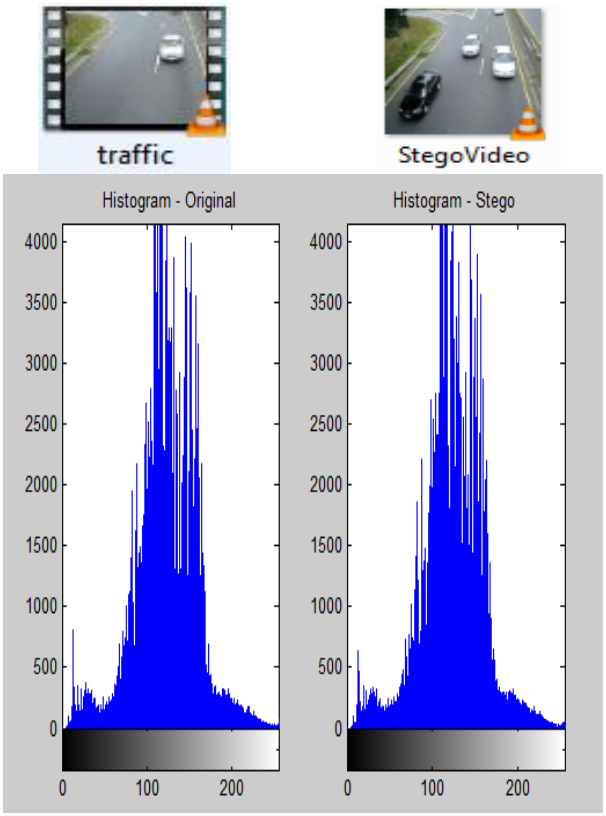

Fig.16. Histogram Analysis For Original and Stego Video

VI. Conclusion and Future Scope

The video steganography is a new & very vast research field and plays an important role in security branches such as cyber forensics to protect social media files from attackers attack. In this paper, the testing analysis concludes that the proposed algorithm drops the risk of detection of hidden message behind stego video frames if attacked by chi- square steganalysis. Therefore using the proposed algorithm is more secure than the traditional LSB substitution techniques and provides resistance against statistical and visual attacks of steganalysis and has less time complexity and provides one layer more protection to secret data using XOR encryption cryptographic algorithms. It also avoids unauthorized access to data using a secret key and avoid the frame dropping and data manipulations problems. In future, new research scholar can do their research work by following the same algorithm for audio steganography and by using different audio formats such as .mp3 and .wave etc and can integrate with watermarking also.

Acknowledgment

We wish to thank parents, teachers, supervisors and friends for their great support and help during the making of this research paper. We also thank all researchers whose previous work gives us a way to extend and complete research work.

APPENDIX A ABBREVIATIONS

AVI	Audio and Video Interleaved
MPEG	Motion Picture Expert Group
MP4	MPEG Type-4
WMV	Window Media Video Format
MP4	MPEG Layer 4 Type Format
FLV	Flash Video Format
XOR	Exclusive OR i.e. Boolean Expression
LSB	Least significant Bits
PSNR	Peak Signal to Noise Ratio
BER	Bit Error Rate

REFERENCES

[1] Ramandeep Kaur, Pooja, and Varsha, "The NonTangible Masking of Confidential Information using Video Steganography", International Journal of Computer Applications (IJCA), Vol.119, No.17, June 2015.

[2] Ramandeep Kaur, Pooja, "XOR Encryption Based Video Steganography", International Journal of Science and Research (IJSR), Vol.4, Issue 11, November 2015.

[3] Sunil. K. Moon, Rajeshree. D. Raut (2013), "Analysis of Secured Video Steganography Using Computer Forensics Technique for Enhance Data Security", IEEE Second International Conference on image information processing (ICIIP- 2013), pg 660-665.

[4] Pooja Yadav, Nishchol Mishra, and Sanjeev Sharma (2013)," A Secure Video Steganography with Encryption Based on LSB Technique", IEEE International Conference on Computational Intelligence and Computing Research.

[5] Geetha C.R., H. D. Giriprakash (2012), "Image Steganography by Variable Embedding and Multiple Edge Detection using Canny Operator", International Journal of Computer Applications (0975 – 888) ,Volume 48, No.16, June.

[6] Sarabjeet Kaur and Sonika Jindal (2013), "Image Steganography using Hybrid Edge Detection and First Component Alteration Technique", International Journal of Hybrid Information Technology Vol.6, No.5, pp.59-66.

[7] Amrinder Singh, Sukhjit Singh (2014), "A Robust Video Watermark Embedding and Extraction Technique Based on Random Frame Selection", IJRIT International Journal of Research in Information Technology, Volume 2, Issue 2, February, pp: 28-37.

[8] Soumyajit Sarkar, Arijit Basu (2014), "Comparison of various Edge Detection Techniques for maximum data hiding using LSB Algorithm", International Journal of Computer Science and Information Technologies, Vol. 5 (3).

[9] Shivani Khosla, Paramjeet Kaur (2014), "Secure Data Hiding Technique Using Video Steganography and Watermarking", International Journal of Computer Applications, Volume 95, No.20, June.

[10] Mamta Juneja and Parvinder Singh Sandhu (2014), "Improved LSB based Steganography Techniques for Color Images in Spatial Domain", International Journal of Network Security, Vol.16, No.6, pp.452-462, Nov.

[11] Mamta Juneja, Parvinder Singh Sandhu, "A New Approach for Information Hiding in Color Images using Adaptive Steganography and Hybrid Feature Detection with Improved PSNR and Capacity", International Journal of Engineering and Technology (IJET), Vol. 5, No. 2, Apr-May 2013.

[12] Youssef Bassil (2012), "Image Steganography based on a Parameterized Canny Edge Detection Algorithm", International Journal of Computer Applications, Volume 60– No.4, December.

[13] Arijit Basu, Gaurav Kumar, Soumyajit Sarkar (2014), "A Video Steganography Approach using Random Least Significant Bit Algorithm", International Journal of Science and Research (IJSR), Volume 3 Issue 6, June.

[14] A.Swathi, Dr.S.A.K Jilani (2012), "Video-Steganography by LSB Substitution Using Different Polynomial Equations", International Journal Of Computational Engineering Research, Vol. 2, Issue. 5, September.

[15] Vijay Kumar Sharma, Vishal Shrivastava (2012), "A steganography algorithm for hiding the image in image improved LSB substitution by minimizing Detection", Journal of Theoretical and Applied Information Technology, Vol. 36 No.1, February.

[16] Wen-Jan Chen, Chin-Chen Chang , T. Hoang Ngan Le (2010) , "High payload steganography mechanism using hybrid edge detector", Expert Systems with Applications, Elsevier (37).

[17] Atallah M. Al-Shatnawi (2012), "A New Method in Image Steganography with Improved Image Quality", Applied Mathematical Sciences, Vol. 6, no. 79, pp .3907 – 3915.

[18] Krishna Nand Chaturvedi, Amit Doeger (2014), "A Novel Approach for Data Hiding using LSB on Edges of a Gray Scale Cover Images", Volume 86 – No 7, January.

[19] K.V.Vinodkumar, V. Lokeswara Reddy (2013), "A Novel Data Embedding Technique for Hiding Text in Video File using Steganography", International Journal of Computer Applications, Vol. 77, No.17, September 2013.

[20] Yeuan-Kuen Lee, Graeme Bell, Shih-Yu Huang, Ran-Zan Wang, and Shyong-Jian Shyu, "An Advanced Least-Significant-Bit Embedding Scheme for Steganographic Encoding", Springer, 2009, pp-349-360.

[21] Poonam Dhankhar, Neha Sahu, "A Review and Research of Edge Detection Techniques for Image segmentation", International Journal of Computer Science and Mobile Computing, Vol. 2, Issue 7, July 2013, pp. 86-92.

[22] Dr.S.Vijayarani, Mrs. M. Vinupriya, "Performance Analysis of canny and Sobel Edge Detection Algorithm in Image Mining", International journal of Innovative Research in Computer and Communication Engineering, Vol.1, Issue 8, October 2013.

[23] http://Stegnao.net/tutorial/steh-history.html- accessed on 12 March 2016.

[24] K. Naveen BrahmaTeja, Dr.G. L. Madhumati, K. Rama Koteswara Rao, "Data Hiding using EDGE based steganography", International journal of Emerging Technology and advanced Engineering, Vol.2, Issue 11, November 2012.

[25] Parveen.P, Arun.R, "Audio-video Crypto Steganography using LSB substitution and advanced chaotic algorithm", International Journal of Engineering Inventions, Vol. 4, Issue 2, August 2014, pp. 01-07.

[26] Ramandeep Kaur, Pooja, Varsha, "A Hybrid Approach for Video Steganography using Edge Detection and Identical Match Techniques", IEEE WISPNET 2016 conference, March 2016.

Authors' Profiles

Ramandeep Kaur has completed her graduation under degree B-Tech (Computer Science and Engineering) from College of Engineering & Management, Kapurthala in 2013. Currently, she is pursuing Mtech (C.S.E) in CT Group of institutions, Shahpur (Jalandhar). Her fields of interest are digital image processing, networking, multimedia and ethical hacking. She has attended various seminars and national conferences regarding research work. She has published papers in international journals like IJCA, IEEE, & IJSR.

Sharanjeet Kaur has done has secured her BTech degree from College of Engineering & Management, Kapurthala (Computer Science and Engineering). Currently, she is pursuing Mtech (C.S.E) in CT Group of institutions, Shahpur (Jalandhar). Her fields of interest are digital image processing, networking, & Software Engineering. She has attended various seminars and national conferences regarding research work. She has published papers in international journals like IJCA, IEEE, & IJSR.

How to cite this paper: Ramandeep Kaur, Sharanjeet Kaur,"XOR-EDGE based Video Steganography and Testing against Chi-Square Steganalysis", International Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.8, No.9, pp.31-39, 2016.DOI: 10.5815/ijigsp.2016.09.05

