ISSN: 2321-7782 (Online)
Volume 2, Issue 10, October 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Improved Security Mechanism of Text in Video using Steganographic Technique

Manpreet Kaur[1]
Research Scholar, CSE Dept
Chandigarh University, Gharuan,
Mohali – Punjab

Amandeep Kaur[2]
Assistant Professor, CSE Dept.
Chandigarh University, Gharuan,
Mohali – Punjab

Abstract: ***Steganography is an art of hiding the secret message in a cover object without leaving a remarkable track on the original message. It is used to increase the security of message sent over the internet. In contrast to cryptography, it is not used to scramble the data but it is used to conceal the data in digital media. This research paper will deal with video steganography, cryptography, hash-LSB and a encryption algorithm. At the end, there will be a discussion about the goal of this paper and what types of techniques worked on video steganography. A proposed technique for video steganography say Hash-LSB with the RSA algorithm is implemented to provide more secure data and data hiding method. This technique uses a hashing function to generate a mask pattern for the data bits in the LSB of RGB pixel values of the cover video. This technique ensures that the message is encrypted before hiding in a cover video frame. If in any case the cipher text has revealed the cover video frames, the intermediate person other than the receiver cannot access the message as it is in encrypted form. So Hash- LSB technique is more secure and trustworthy to transfer the important data on any unsecure channel. As well as the encryption algorithm which is named as RSA (Rivest, Shamir & Adelman) algorithm, increase the security of valuable or precious data.***

Keywords: Steganography, Cryptography, Hash-LSB, Encryption algorithm, RSA.

I. INTRODUCTION

Digital Steganography is defined as method of hiding the data; system Steganography is a way to inset the secret data in a media of public coverage. There are two main features of steganographic techniques: the ability of Steganography and imperceptible. However, these two features are opposed to each other. In addition, his is very toughest task to expand the capacity of Steganography and manage the imperceptibility of system with steganography. In addition, there are many methods of Steganography for use with ways of communication; they are not conventional but describing media Steganography. Steganography in images uses a way to transmit a secret data through the images from one sender to other receiver side. In addition, this seeks without doubt of third party to such communication. Thus, this research focuses on and provides methods for improving these features of Steganography in video digitally. Therefore, the characteristic of video has been used to expand the capacity and improve steganographic quality of stego video.

Steganography and cryptography obtains different objectives. Cryptography technique covers the secret data by scrambling this message or by other way. On the other hand Steganography hides the secret data. In addition, Steganographic technique allows privacy and security of important information. Moreover, there is a weak point of encryption systems is that the existence of secret message is not removed. Although the Steganography and the cryptography techniques give private communication, these techniques can be defined in various ways.

In this approach, an implementation of a technique called Hash-LSB insertion, derived LSB for pictures and video frames. In this Hash-LSB, the hash function is used to check positions to hide the secret bits or to be combined. It is a difficult process that will lead other techniques to merge the two technologies, one of them is Hash-LSB steganography and other is RSA

cryptography. This research has concentrate on providing a solution for the transfer and sharing of important data without any kind of interference. All creditable organizations while sending any business documents on the internet or any channel always use encryption algorithm to protect important information from leakage. The proposed technique also provides security from frame dropping attack while sending the important data in cover video. This thesis used Hash-LSB and the RSA algorithm to create a secure steganography algorithm which is much safer than many systems in order to secretly send data.

II. PROPOSED TECHNIQUE

Hash-LSB (Least Significant Bit) technique

The least significant bit Hash Function (H-LSB) Steganography technique for LSB position in which to hide the secret data is determined using the hash function. Hash function finds the position of least significant bit of each RGB pixel, and then message bits are embedded in this RGB pixel independently. Then, the hash function returns hash values depends upon LSB in values of RGB of pixels. An image of the cover will be broken or fragmented in RGB format. Then Hash technical LSB will use the values from the hash function to integrate or hide data. In this technique, the secret message is converted into binary form as binary bits; each 8 bits at a time are included in the least significant values of RGB pixel image covering about 3, 2 and 3 bits respectively. Under this method three bits are embedded in red pixel LSB 3 bits are embedded in green pixel and 2 LSB bits are embedded in blue pixel.

Hash function

Hash technique the least significant bit as a function that produces the hash function. This hash function deals with the LSB position and the pixel position of each pixel masked image, and also with the number of LSB bits. Hash value takes a variable size input and returns a fixed-size digital output string. Hash function is also used to detect duplicate folder in large files.

Hash function generally given by

$$i = j \% k$$

Where, i is the position of LSB bit within the image or video frame pixels, j represents the position of each hidden video frame pixel and k is number of bits of LSB.

RSA algorithm

The RSA algorithm was defined by Rivest, Shamir and Adleman three MITs. This algorithm is used to encrypt the secret message into scrambled form. This algorithm works by taking two values of primes and then the product of these values. This product value is used to make a public and a private key and this is also used in the encryption and decryption methods. The RSA algorithm can be used in combination with Hash-LSB so that the original message is inserted into the cover video frame as cipher text. RSA algorithm increases the security level of video steganography.

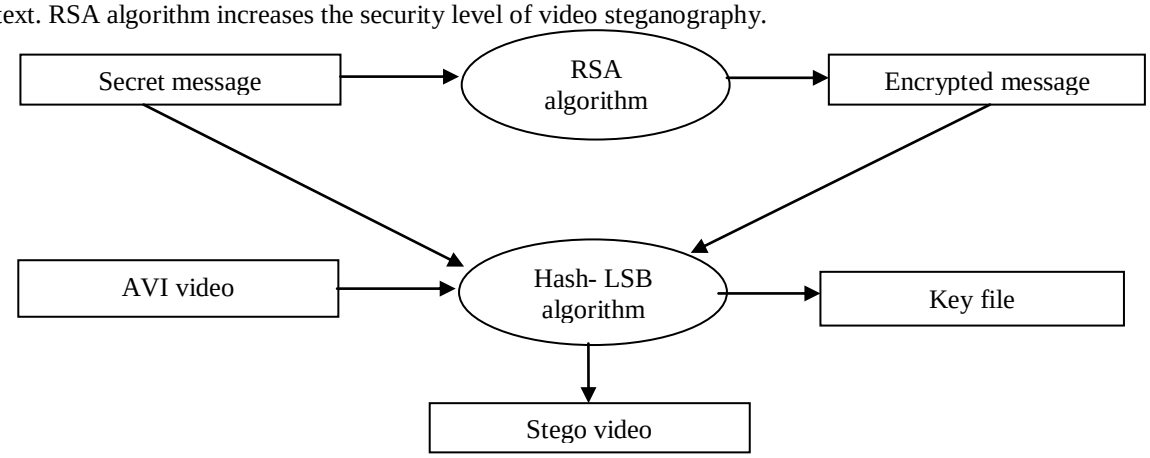

Fig.1 Proposed architecture of video steganography using Hash-LSB

III. ALGORITHM

A. For Embedding Process

1. Pre-processing:- Selection of the cover video to hide the data.
2. Frame Selection:- Frames are selected randomly from carrier video by applying the algorithm which detects the variation in scene of video.
3. Conversion:- Convert private data into cipher form using RSA algorithm**.**
4. Inserting Process:- Hide private information (.text) in cover frame using Hash-LSB to get stego frame. Hide the authentication key.
5. Replacement:- Replace the original frame with stego frame.
6. Recombination:- Recombine the frame to form into a stego video and transfer it using communication.

B. For Extracting Process

1. Select a stego video which have covert the secret data within it.
2. Pass the security key
3. Extract hidden message from stego frames
4. Make a cover video in the original form

IV. PARAMETERS IN VIDEO STEGANOGRAPHY

Some parameters like Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), and Bit Error Rate (BER) are defined to evaluate quality of stegano videos.

Peak Signal to Noise Ratio (PSNR)

The resolution of stego video is evaluated in form of PSNR (Peak Signal to Noise Ratio) & MSE (Mean Square Error). Sometimes, PSNR can have infinite values and the MSE can have zero values.

$$PSNR = 10 \, LOG10 \, (max*max) / MSE \qquad (3.1)$$

Mean Square Error (MSE)

MSE is defines as the parameter to find the quality of stego video. It is inversely proportional to PSNR.

$$MSE = \sum_{i=1}^{m} \sum_{j=1}^{n} [O(i, j) - S(i, j)] / m*n \qquad (3.2)$$

Where: m and n are the size of original video frame and max=255, O: original video frame

S: Stego video frame.

Bit Error Rate (BER)

The bit error rate is defined as ratio of number of bit errors to the total numbers of transferred bits. This parameter is used to measure the quality of stegano frames of video.

$$BER = \text{No of Bit Errors} / \text{Total Numbers of Transferred Bits} \qquad (3.3)$$

Frame Extract Time

The frame extract time is defined as the period of time in which selected frames are extracted from the total number of video frames.

Frame Re-Assemble Time

It is defined as the time in which extracted frames are assembled in specific sequence.

Message Hiding Time

The period of time, which is used to hide the secret message in the selected video frames.

V. RESULT AND DISCUSSION

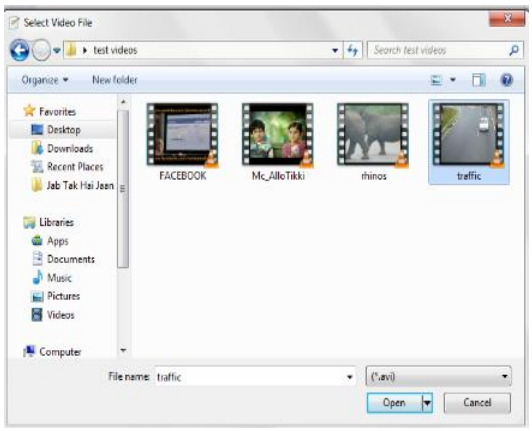

Fig. 2 Cover video is selected

Fig .3 Secret message which is hidden

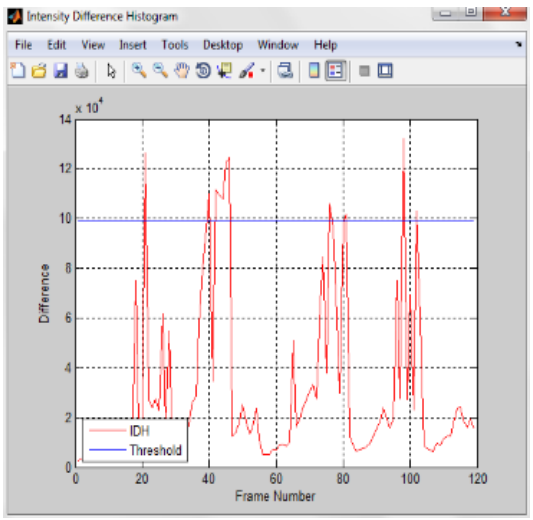

Fig. 4 Frame selection by IDH

Fig. 5 Stego video

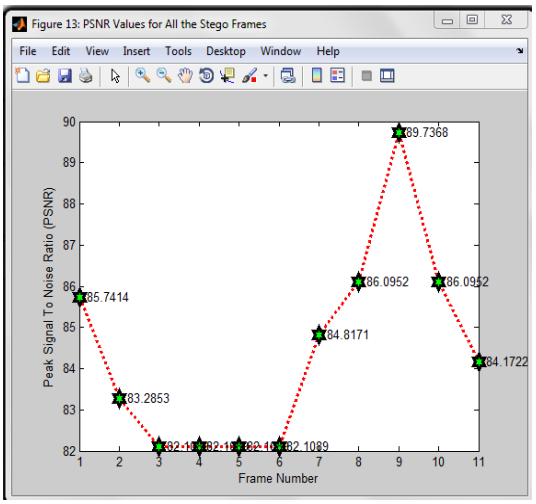

Fig. 6 PSNR Values of selected stego frames

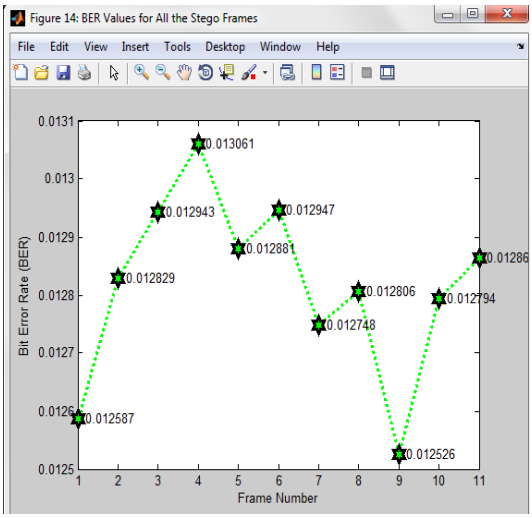

Fig. 7 BER of different stego frames

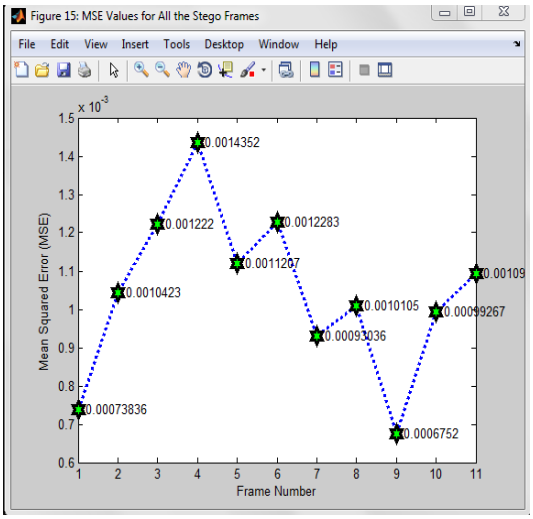

Fig. 8 MSE of selected Stego frames

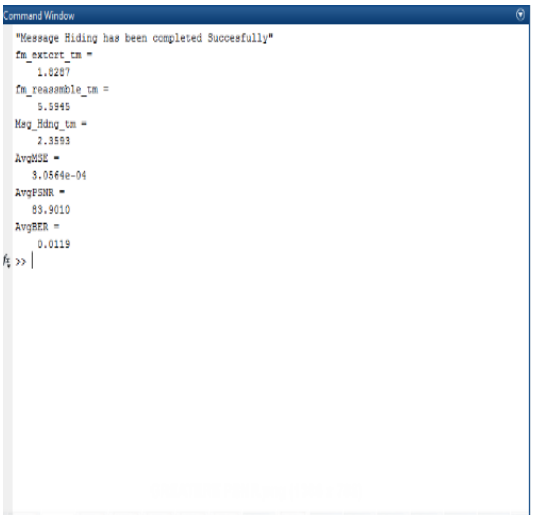

Fig. 9 Average MSE, PSNR & BER

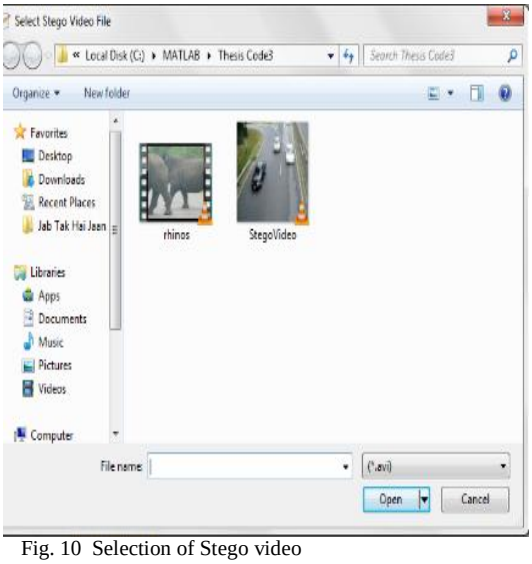

Fig. 10 Selection of Stego video

Fig. 11 Secret message which is retrieval

TABLE 1
Comparison between different LSB techniques

No of LSB	Embedding capacity(%)	Security	Recovered data(100%)
1LSB	12.5	LESS	100
2LSB	25	LESS	100
4LSB	50	MORE	100
Hash- LSB	100	MORE	100

TABLE 2
Comparison between 4LSB & Hash-LSB for traffic video

Techniques / Parameters	Average PSNR	Average MSE	Average BER	Frame Extract Time	Frame Reassemble Time	Message Hiding Time
4LSB	72.4692	0.0037	0.0138	4.7740	6.7911	4.0625
Hash-LSB	74.1869	0.0025	0.0135	1.7286	4.6630	2.3310

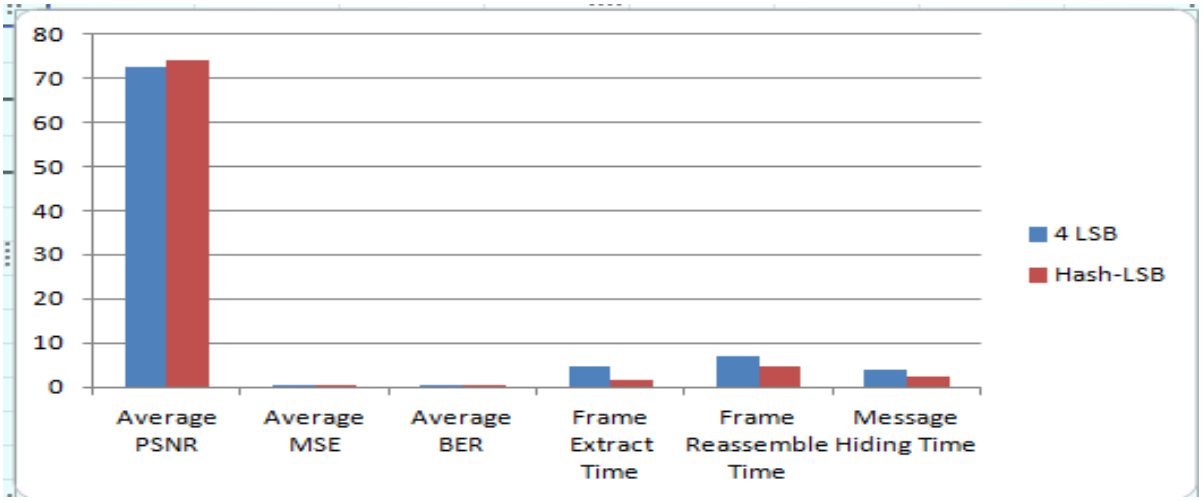

Fig. 12 Graphical Representation between different Parameters (in decibel and seconds)

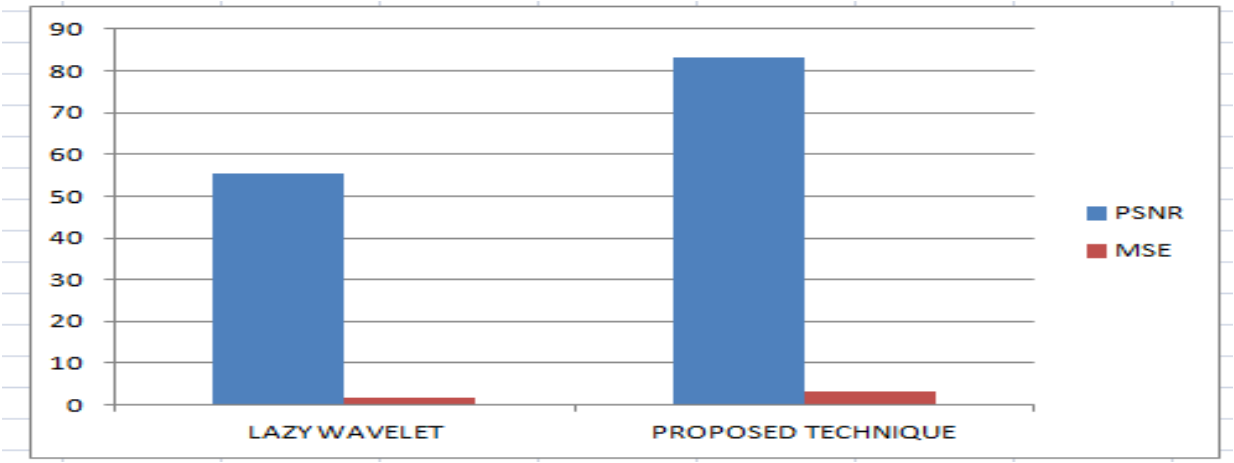

Fig. 13 Graphical Results between Lazy Wavelet & Proposed technique

VI. Conclusion and Future Work

In this video steganography, Hash-LSB technique is an efficient steganographic method for embedding secret message in the cover video without causing any resolution change in video quality. With the help of this method, it is a best way to hide information in a video with more safety. In this work, RSA algorithm is used to encrypt the secret data that is not easy to break. A specific technique uses the hash function and the RSA algorithm to protect the data over any insecure channel. A secure hash based LSB technique in video steganography has been implemented to locate the bit of secret data in the RGB pixel values. It is an efficient steganographic method for embedding secret messages without producing major changes in cover video. In this work, proposed techniques have created a efficient way of hiding information in video frames with less variation bits, making sure our technique is more perfect. This cryptographic algorithm RSA method is also applied to protect the secret message that is not easy to break the encryption without the key. RSA algorithm itself is very safe which is used to enhance the security of the secret message. A technique uses the specified hash function and also provides data encryption using the RSA algorithm; makes our technique a very useful and reliable for sending information through any internet unsecure channel. The Hash-LSB technique has been applied to video AVI. However, it can work with any format with small procedural change as compressed videos. Performance analysis of the developed technique has been evaluated by comparison with the 4LSB technique, which have resulted in a very good value of MSE, BER and PSNR for Stego video.

The future scope for the proposed method might be the development of an enhanced steganography that can have the authentication module along with encryption and decryption. Meanwhile the work can be enhanced for other data files like,

audio, text. Moreover, the steganographic technique can also be developed for 3D images. The further work may contain combination of this method to message digesting algorithms.

ACKNOWLEDGEMENT

I would like to express my deepest appreciation to Er. Amandeep Kaur for her guidance and expert contributions to this paper. Without her support it would be impossible to complete this paper. I would also have to appreciate the guidance given by other supervisor as well as the panels especially in my project presentation that has improved a lot. Thanks for their comments and advices.

References

1. Avudainayagam A., Dapeng Wu, "Hyper-Trellis Decoding of Pixel-Domain Wyner–Ziv Video Coding" *IEEE transactions on circuits and systems for video technology*, Volume 18, Issue 5, PP 557-568, May 2008
2. Bhowal K. and Jyoti Pal A., "Robust Audio Steganography using GA", *IEEE International Conference on Computational Intelligence and Communication Networks CICN 2010*, PP 449-453, Nov 2009.
3. Bodhak V. and Gunjal L., "Improved protection in video Steganography using DCT & LSB" *International journal of engineering and innovative technology (IJEIT)*, Volume 1, Issue 4, April 2012.
4. Budhia H., Kundur D. "Digital Video Steganalysis Exploiting Statistical Visibility in the Temporal Domain" *IEEE transactions on information forensics and security*, Volume 1, Issue 4, PP 502-516, December 2006.
5. Cao Y. et al, "Video Steganalysis Exploiting Motion Vector Reversion-Based Features" *IEEE signal processing letters*, Volume 19, Issue 1, PP 35-38, January 2012.
6. Christal Mary S. "Improved protection in video steganography used compressed video bit streams" *International Journal on Computer Science and Engineering*, Volume 02, Issue 03, Febuary2010.
7. Gudla S. et al "Key based least significant bit (LSB) insertion for audio and video steganography" *IEEE International Journal of Computer Science Engineering Research and Development (IJCSERD), ISSN 2248 – 9363(Print) ISSN 2248 – 9371(Online)*, Volume 3, Issue 1, Jan- March 2013.
8. Gupta S. and Gujral G., "Enhanced least bit significant algorithm for image Steganography" *IEEE international journal of computational engineering & management*, Volume 15, Issue4, July 2012.
9. Gupta S. et al "Enhanced Least Significant Bit algorithm For Image Steganography" *IEEE International journal of computational engineering & management*, Volume 15, Issue 4, July 2012.
10. Hussein A. Aly ", Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error" *IEEE transactions on information forensics and security*, Volume 6, Issue 1, PP14-18, March 2011.
11. Jiang H. and Joshi A., "Scene change detection techniques for video database systems" *Multimedia systems@* Springer-Verlag, Volume 6, Issue 3, PP 186-195, May 1998.
12. Kumari S., Singh K. "A robust and secure Steganography approach using hash algorithm" *IEEE International journal of latest research of science and technology*, Volume2, Issue 1, PP 573-576, January- February 2013.
13. Mozo AJ., and Obien M.E., C.J. Rigor, "Video Steganography using Flash Video (FLV)" *I2MTC 2009 -IEEE International Instrumentation and Measurement Technology Conference Singapore*, Volume 5, Issue 7, PP 822-827, May 2009.
14. Mr.Bobate V.R. & Prof. Khobragade A.S. "Optimal Implementation of Digital Steganography in an true color Image for the Secret Communication" *IEEE advanced in recent technologies in communicating and computing"* Volume 14, Issue 15, PP 91-95, November 2011.
15. Pan Z.,Shen H.,"A Low-Complexity Screen Compression Scheme for Interactive Screen Sharing" *IEEE Transactions on circuits and systems for video technology*, Volume 23, Issue 6, June 2013.
16. Patel K. and Kauwid Rora K., "Lazy Wavelet Transform Based Steganography in Video" *IEEE International Conference on Communication Systems and Network Technologies* Volume 6, Issue 8, PP 497-500, April 2013.
17. Paulpandi P., Dr.M.T "Hiding Messages Using Motion Vector Technique in Video Steganography" *IEEE International Journal of Engineering Trends and Technology*- Volume3, Issue3, June 2012.
18. Qin c., Ying-Hsuan Huang, "An In painting-Assisted Reversible Steganographic Scheme Using a Histogram Shifting Mechanism" *IEEE transactions on circuits and systems for video technology*, Volume 23, Issue 7, July 2013.
19. Sharp A. and Sharif H., "A Video Steganography Attack Using Multi-Dimensional Discrete Spring Transform" *IEEE International Conference on Signal and Image Processing Applications (ICSIPA)*, PP182-186, October 2013.
20. Shu-Ching Chen. et al " Video scene change detection method using unsupervised segmentation and object tracking" *IEEE Distributed Multimedia Information System Laboratory* 0-7695-1198-8/01/$10.00 (C), PP 56-59, August 2001.
21. Suneetha B. et al "Secured data transmission based video steganography" *IEEE International Journal of Mechanical and Production Engineering (IJMPE) ISSN No.: 2315-4489*, Volume2, Issue1, July 2013.
22. Sunil. K. Moon, "Analysis of secured video Steganography using computer forensics techniques for enhances data security" *IEEE second international conference on image information processing* (ICIIP), PP 660- 665, December 2013.

AUTHOR(S) PROFILE

Manpreet kaur, received B-tech degree in computer science engineering in 2009 from Punjab Technical University. During 2012-2014 session pursuing ME in information technology from Chandigarh University, Gharuan.