International Journal of Engineering Research and General Science Volume 3, Issue 3, May-June, 2015
ISSN 2091-2730

A Survey : Video Steganography techniques

Ms. Pooja Vilas Shinde [Mtech Student, SRIST] [1],

Dr.Tasneem Bano Rehman [Associate Professor, SRIST] [2]

poohnov@gmail.com[1], tasneem.bano@gmail.com[2] , +918956224336, +918889810626.

Abstract: Video Steganography is a method for hiding data in a video file and hence it reduces the chance of access by unauthorized user. In steganography various carrier file formats can be used, among which videos are popular due their frequent use on internet. Video steganography has a lot more scope of hiding secret data because of the nature of video which has many numbers of redundant bits. As per the requirement of user there are different video steganography technique proposed leading to own positive and negative points. The video steganography techniques are beneficial in application having high security requirements. The paper provides effective review of existing video steganography techniques and some guidelines for the design of video steganography system.

Keywords— Cover file, Stegofile, Least Significant Bit(LSB), Peak Signal Noise Ratio(PSNR), Mean Square Error(MSE), Encoding, Polynomial, Hybrid.

1. Introduction

Video Steganography is the art and science of writing hidden messages inside innocent looking videos, in such a way that no one apart from the sender and intended recipient realizes the existence of a hidden message. Steganography uses repeating portions of the Video files to embed the secret message. Although many distinct steganography techniques are discovered and implemented, an ideal solution has not been reached till now.[1]

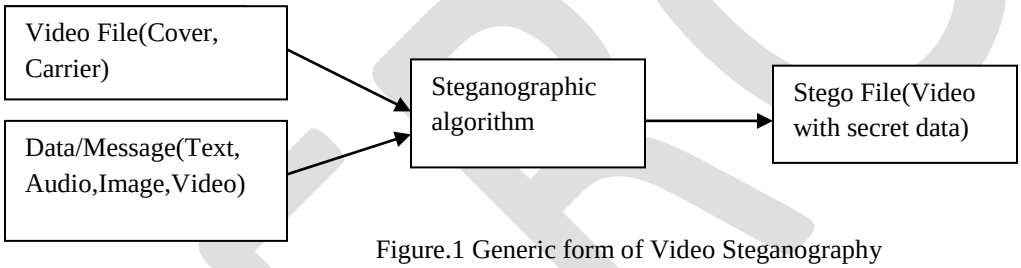

Figure.1 Generic form of Video Steganography

Several new techniques have been proposed for video steganography. In this paper, some of the most well-known techniques have been discussed. Most steganography techniques have been carried out on images, video, text, audio(figure1). Video based steganogrpahic techniques are broadly classified into temporal domain and spatial domain. In frequency domain, data are transformed to frequency components by using FFT, DCT or DWT and then data are embedded in some or all of the transformed coefficients. Embedding may be bit level or in block level. Moreover in spatial domain the bits of the data can be inserted in intensity pixels of the LSB positions of video. The advantage of the method is the amount of data (payload) that can be embedded is more in LSB techniques. A Steganographic technique should not be easily detectable by unauthorized person. If the secret message is been detected with random guessing, the existing steganographic technique is considered to be invalid. Similar to cryptography, steganography may suffer from the vulnerable attacks..

An effective Steganography technique should have the following characteristics[2] :

a. Secrecy: Extraction of hidden information from the video must not happen without prior permission of intended user having password .
b. Imperceptibility: The ability to be completely undetectable.
c. Capacity: The maximum length of the hidden message that can be embedded in a video.
d. Accuracy: The extraction of the hidden data from the medium should be accurate and reliable.

2. Existing Video Steganographic technique:

B.SUNEETHA et. al has proposed in his work Cryptography and Steganography based system for hiding data in video by encrypting it with ASCII code and provides a additional layer of security. Cryptography provides privacy whereas Steganography is intended to provide secrecy[2].Kousik Dasgupta, J.K. Mandal and Paramartha Dutta has proposed a secured hash based LSB technique for video steganography which uses cover video files in spatial domain to hide the presence of sensitive data regardless of its format. Performance analysis of the hash based LSB technique after comparison with LSB technique is better[3].A. Swathi , Dr. S.A.K Jilani

has proposed in his paper the LSB substitution using polynomial equation is developed to hide the information in specific frames of the video and in specific location of the frame by LSB substitution using polynomial equation. Here the information will be embedded based on the key. Key is in the form of polynomial equations with different coefficients. By using this the capacity of embedding bits into the cover image can be increased[4].

Mritha Ramalingam has proposed a More secured LSB method way in which video file is used as a host media to hide secret message without affecting the file structure and content of the video file. Because degradation in the video quality leads to visible change in the video which may lead to the failure of the objectives of Steganography[5]

.Ashawq T. Hashim et al has proposed a Hybrid Encryption and Steganography technique where there are two methods of hiding used, the first method is the Least Significant Bit (LSB) and the second is the Haar Wavelet Transform (HWT). This work is based on a combination of steganography and cryptography techniques to increase the level of security and to make the system more complex to be defeated by attackers.

R. Shanthakumari and Dr.S. Malliga in their proposed work has stated a LSB Matching Revisited algorithm (LSBMR) selects the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image. LSBMR scheme addresses two problems Lack of Security and Low Embedding rate[7].

2.1. SECURED DATA TRANSMISSION BASED VIDEO STEGANOGRAPHY (SLSB):

In Secured data transmission Steganography technique works on compression technique which is evaluated such that the data is been embedded in the vertical and horizontal component pixels. To evaluate the frames there are three types of images (or frames) used in video compression: I-frames, P-frames, and B-frames defined on amount of data compression. They have different characteristics: I (Intra-coded) frames don't require other video frames to decode but are least compressible. P- (Predicted)frames uses data from previous frames to decompress and are more compressible than I-frames. B- (Bi-predictive) frames use both previous and forward frames for data reference to get the higher amount of data compression.

Algorithm for Encoding based on secured transmission technique :

Step 1: Take Input cover video file or stream.

Step 2: Read the required information of the cover video file.

Step 3: Break the video into frames.

Step 4: Compress the frame where the data is to be inserted using any compression technique (DCT)

Step 5: Hide the data using LSB algorithm.

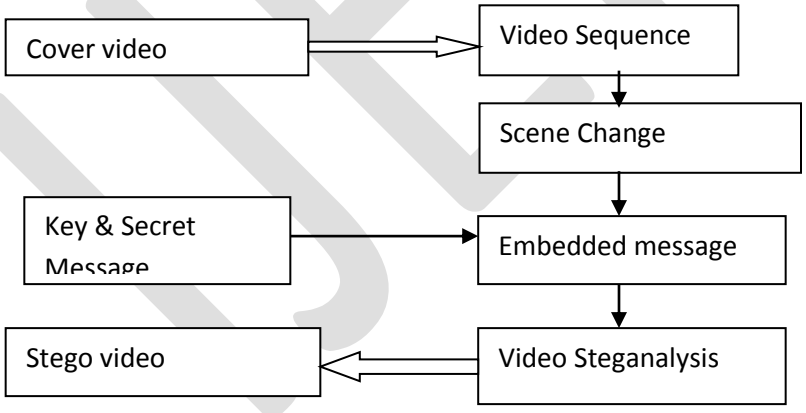

Figure 2. Block Diagram of Secured data transmission technique

Algorithm for Decoding based on secured transmission technique :

Step 1: Input stego video file or stream.

Step 2: Read required information from the stego video.

Step 3: Break the video into frames.

Step 4: Using the motion vector, the frame where the data is hide is chosen.

Step 5: The data is extracted from the LSBs of the identified frame.

The given Secured Data Transmission Technique provides high capacity and imperceptible, for human vision of the hidden secret information. By embedding the data in the moving pictures the quality of the video is increased. The compressed video is used for the data transmission as it can hold large amount of the data. Lacks data secrecy.

2.2. HASH BASED LEAST SIGNIFICANT BIT TECHNIQUE FOR VIDEO STEGANOGRAPHY(HLSB):

The Hash based Least Significant Bit (HLSB) technique for Video Steganography has been used, here the secret data is hided in the LSB of the cover frames. In this technique eight bits of the secret data is divided in 3, 3, 2 format and embedded into the RGB pixel values of the video frames. A hash function is used to select the position of insertion in LSB bits. For example the RGB pixel value of the cover frame is as given below:

R: 10110111 G: 10010100 B: 11001001

and a byte of message to be inserted in LSB as:**10001001**

LSB is lowest bit in a series of binary numbers, so in this case for R it will be 1, 0 for G and 1 for B. The proposed technique is applied in four lowest LSBs in each pixel value. So the LSBs for the above RGB values are:

R : 0111 G : 0100 B : 1001

The message is embedded in groups of 3, 3 and 2 in the respective RGB LSBs positions. The positions are obtained from the hash function given in equation k=p%n. The value of n number of bits of LSB for the present scenario is 4. Using the hash function let the position of insertion k returned for a particular iteration are,

k = 1,2,3 for R. k = 4,1,2 for G k = 3,4 for B

Considering the above positions of insertion, the bits from the message are inserted in four LSB positions and resulting RGB pixel value are as given below.

R: 10111001 G: 10011000 B: 11001001

Thus all the eight bits of the message are embedded in three bytes and number of bits actually changed is five out of twenty four bits. Further these five bits are randomly distributed among which increases the robustness of the scheme.

To decode the message, the valid user follows the reverse step. As the hash function is known to the intended the user, it calculates the k values to get the position of insertion. Taking the same embedded RGB value as above,

R: 10111001 G: 10011000 B: 11001001

The hash function will return the following k values for this particular iteration.

k = 1,2,3 for R. k = 4,1,2 for G k = 3,4 for B

using these k values which represent the four LSB positions, the data of the secret message is found as below,

10001001 Which is same as the data of secret message as considered above.

The flow of sequence of algorithm is shown in the figure 3.

The HLSB technique is applied to AVI files, however it can work with any other formats with some changes. For compressed video files format like MPEG the video needs to be decompress then the technique can be applied to the uncompressed video. Whereas for Flash Video FLV files the technique can be applied with no modification. It is less secure as data is directly hided in video.

2.3. Video Steganography by LSB Substitution Using Different Polynomial Equations (LSB Poly):

Least significant bit (LSB) insertion technique operates on LSB bit of the media file to hide the information bit. In this technique, a data hiding scheme will be developed to hide the information in specific frames of the video and in specific location of the frame by LSB substitution using polynomial equation. First read the original video signal and text, then embed the text into the video signal for

converting the text data into the binary format. Binary conversion is done by taking the ASCII value of the character and converting those ASCII values into binary format. The binary representation of samples of cover signal are inserted in the binary representation of text. The LSB bits of video signals are replaced by the binary bits of data and this encoded signal is called stego signal is ready for transmission through internet. The message which we want to hide is converted into ASCII and then converted into its binary representation with each word consist of 8bits.These bits are substituted in the Least Significant Bits of binary representation of each image sample. Here the polynomial equations are used to find the location of insertion of data bit in the video file.

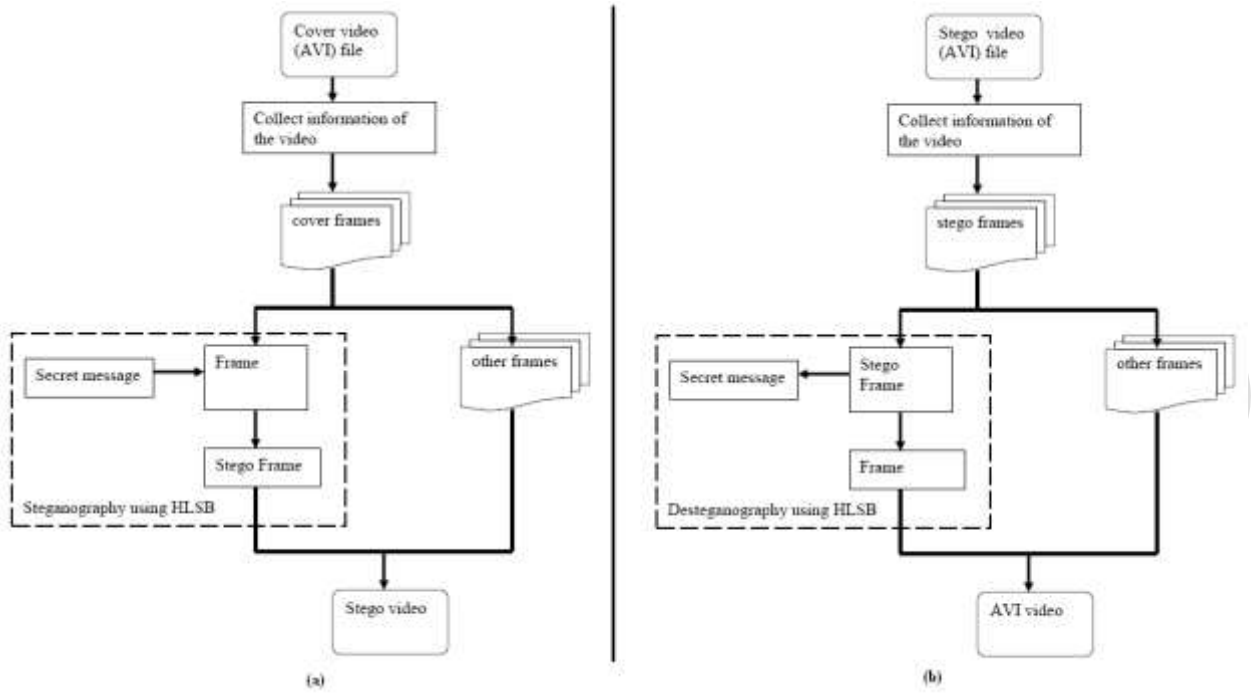

Figure 3: Block diagram of HLSB Video Steganography technique (a) Encoding and (b) Decoding

- Encoding for Substitution Using Different Polynomial Equations **:**

First take the original video in which we have to embed image, then convert the video file into number of frames, consider each frame as an image. Here set the counter value to frames. Then convert the text data into binary format. Binary conversion is done by taking the ASCII value of each character and converting those ASCII values into binary format .Set the counter value to the length of the binary message, so that the loop repeats that much times. The LSB bit of the image pixel is replaced by the binary data. This encoded image called as stego video is ready for transmission through the internet.

- Decoding for Substitution Using Different Polynomial Equations**:**

First take the LSB encoded image. Set the counter to the length of the binary data. Then extract the binary data from the LSB encoded image by extracting the LSB bits of the image pixels. In order to form the text file from the binary data group all the binary bits.

2.4. Stego Machine – Video Steganography using Modified LSB Algorithm (MLSB):

A stego machine is developed to hide data containing text in a video file and to retrieve the hidden information. This can be done by embedding text file in a video file in such a way that the video does not lose its functionality using Least Significant Bit (LSB) modification method. The message to be hidden inside the carrier file is encrypted along with a key to provides robustness to the Stego machine algorithm.

The least significant bit (LSB) algorithm is used to conceal the data in a video file. The main advantage of the LSB coding method is a very high watermark channel bit rate and a low computational complexity. The robustness of the watermark embedded LSB coding, increases with increase of the LSB depth. In this method, modifications are made to the least significant bits of the carrier file's individual pixels, thereby encoding hidden data. Here each pixel has room for 3 bits of secret information, one in each RGB values. Using a 24-bit image, it is possible to hide three bits of data in each pixel's color value using a 1024x768 pixel image; also it is possible to hide up to 2,359,296 bits. The human eye cannot easily distinguish 21-bit color from 24-bit color . As a simple example of LSB substitution, imagine "hiding" the character 'A' across the following eight bytes of a carrier file:

(00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

Letter 'A' is represented in ASCII format as the binary string 10000011. These eight bits can be "written" to the LSB of each of the eight carrier bytes as follows (the LSBs are italicized and bolded):

(0010011***1*** 1110100***0*** 1100100***0***)
(0010011***0*** 1100100***0*** 1110100***0***)
(1100100***1*** 0010011***1*** 1110100***1***).

With such a small variation in the colors of the video image it would be very difficult for the human eye to differentiate thus providing high robustness to the system .

2.5. Hybrid Encryption and Steganography (HES):

In HES, text data is hidden in Video.The Encryption algorithm used is Type-3 Fiestal and for embedding data HWT technique is used.The Type-3 Feistel Network of The 128-bits block size improved Blowfish encryption uses a variable-length key up to 129 bytes. Type-3 Feistel Network of the 128-bits block size improved Blowfish encryption algorithm: The algorithm takes four 32-bit plaintext data words A, B, C, D as input and produces four 32-bit cipher text data words A, B, C, and D. The cipher is word-oriented, here internal operations are performed on 32-bit words. It iterates simple function 16 times. This cipher has a variety of operations to provide a combination of high speed, high security, and implementation flexibility. It uses also four key dependent (S-box) tables of 255 32-bit words to provide good resistance against linear and differential attacks, as well as good avalanche of data and key bits .In additional, the source word is rotated by 13 positions to the left. The algorithm uses the same structure of F-function of previous Blowfish algorithm.

2-Haar Wavelet Transform Embedding Method: The frequency domain transform is applied in this technique. It is the Haar-Discrete Wavelet Transform . It consists of a series of averaging and difference steps. The operation can be divided into two steps: one is the horizontal operation and the other is the vertical one. Haar Discrete Wavelet Transform is described as below:

Step 1: At first, scan the pixel from left to right in horizontal direction. Then, do the addition and subtraction operation on neighboring pixels and then store the sum on the left and the difference on the right. Repeat the operation until all rows are processed. The pixel sums represent the low frequency part of the original image and denoted as symbol L. The pixel differences represent the high frequency part of the original image and denoted as symbol H.

Step 2: Secondly, scan the pixels from top to bottom in vertical direction. Then, do the addition and subtraction operation on neighboring pixels and store the sum on the top and the difference on the bottom. Repeat this operation until all the columns are processed. Finally 4 sub bands denoted as LL, HL, LH and HH respectively are created. The LL sub band is the low frequency part and looks very similar to the original image.

A variable-length key would make cryptoanalysis more difficult for potential attackers. All of the measures obtained as the test results indicate good results for PSNR (above 50db) and they increase when the number of frames used as a cover increases. The drawback of this method is complexity in design of actual system.

2.6. Video Steganography Using LSB Matching Revisited Algorithm (LSBMR):

LSB Matching Revisited(LSBMR) algorithm for Video Steganography selects the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image. [7] :

- Algorithm for Encoding in LSBMR video steganography :

Step 1 : Dividing Video into Frames ,the cover video file is decomposed into number of frames in which the secret message will be hidden. Shared key is used to select the frame for hiding the message.

Step 2 : Calculating the key using Diffie Hellman Algorithm. The Diffie-Hellman key exchange method allows two parties who have no prior knowledge of each other to jointly establish a shared secret key over a secure communication channel.

Step 3 : In Embedding the text, the scheme first initializes some parameters, which are used for subsequent data preprocessing and region selection, and then estimates the capacity of those selected regions. If the regions are large enough for hiding the given secret message, then data hiding is performed on the selected regions. Finally, it does some post processing to obtain the stego image.

Step 4: After data hiding, the resulting image is divided into non-overlapping BZ * BZ blocks. The blocks are then rotated by a random number of degrees based on key. The process is very similar to Step 1 except that the random degrees are opposite. Then we embed the two parameters into a preset region which has not been used for data hiding.

- Algorithm for Decoding in LSBMR video steganography :

Step 1: To extract data, first extract the side information, i.e., the block size BZ and the threshold t from the stego image. Then do exactly the same things as Step 1 in data embedding.

Step 2: The stego image is divided into Bz * Bz blocks and the blocks are then rotated by random degrees based on the secret key key1 .The resulting image is rearranged as a row vector V. Finally, the embedding unit is obtained by dividing V into non overlapping blocks with two consecutive pixels.

Step 3: Travel the embedding units whose absolute differences are greater than or equal to the threshold T according to pseudorandom order based on the secret key key2.

LSBMR algorithm due to low replacement rate, the MSE value is low which makes it secure when compared to LSB algorithm.It is expected that the idea can be extended by embedding the text in the different frames of same video.

3. Performance Metrics:

3.1. MEAN SQUARE ERROR (MSE) [10]:

MSE measures the average of the squares of the "errors". The average squared difference between an original image and resultant (stego) image is called Mean Squared Error

$$MSE = \frac{1}{H*W}\sum_{i=0}^{h}(P(i,j) - S(i,j))^2$$

Where,
H and W =Height and Width
P (i, j) =Original Frame
S (i, j) =Corresponding Stego frame.

3.2. PEAK SIGNAL TO NOISE RATIO [10]:

PSNR is the ratio between the maximum possible power of a signal and the power of corrupting noise. PSNR is usually expressed in terms of the logarithmic decibel scale. PSNR is most commonly used to measure of quality of reconstruction of lossy compression PSNR is an approximation to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases the reverse may be true. One has to be extremely careful with the range of validity of this metric. It is only conclusively valid when it is used to compare results from the same content.

PSNR is most easily defined via the mean squared error (MSE). It is expressed by,

$$PSNR = 10\ log\frac{L\text{^}2}{MSE}$$

Where,
L - Maximum intensity it is taken as 255
Typical values for the PSNR is 30 to 50 dB, where higher is better.

3.3. Payload [10]:

Maximum payload is bits per byte i.e. maximum amount of data that can be embedded into the cover file without losing the quality of the original file.

4. Comparison of Existing Video Steganography techniques:

In the Secured Data Transmission (SDT) the cover file is Bulb.avi with resolution 256*240 ,15 frames per second, total frames are 80 is taken as input. In HLSB the cover file is Drop.avi with resolution 256*240 , 30 frames per second, total frames are 182 is taken as reference video. In LSB Polynomial equation Algorithm, cover file is Drop.avi with resolution 256*240 , 30 frames per second, total frames are 182 is taken as reference. In MLSB Algorithm, cover file is Globe.avi with resolution 320*240 , 30 frames per second, total frames are 107 is taken as input video. In Hybrid Encryption and Steganography (HES), cover file is Globe.avi with resolution 320*240 , 30 frames per second, total frames are 107 is taken as input. In LSBMR, cover file is Rhinos.avi with resolution 320*240 , 15 frames per second, total frames are 105 is taken as reference. For these parameter the PSNR and MSE are calculated. The Comparison is given based on the results related in each steganography techniques [2][3][4][5][6][7].

Serial No.	Video Filename	Resolution	MSE	PSNR	Payload
1.SDT	Bulb.avi	256*240	9.51	38.71	199Kb
2.HLSB	Drop.avi	256*240	0.34	44.34	2.66Kb
3.LSB Poly	Drop.avi	256*240	0.42	48.56	1Kb

Table no. 1. Comparison of 3.1 to 3.3 algorithm based on MSE , PSNR , Payload.

Serial No.	Video Filename	Resolution	MSE	PSNR	Payload
4.MLSB	Globe.avi	320*240	0.295	53.43	13.3Kb
5.HES	Globe.avi	320*240	0.46	51.43	13.3Kb
6.LSBMR	Rhinos.avi	320*240	0.00065	80	136bits

Table no. 2. Comparison of 3.4 to 3.6 algorithm based on MSE , PSNR , Payload.

The larger the PSNR dB value, higher is the image quality i.e. there is a little difference in the original image and stego image. Therefore PSNR should be large. Small PSNR means there is distortion between original and stego image. MSE is the average of squares of the errors. If MSE = infinity then, two images are identical. It is required that the PSNR should be high and MSE must be less for an Video Steganography algorithm to be effective.

5. Conclusion and Future Work:

Although some of the Video steganography techniques were discussed in this paper, there exists a large selection of techniques for hiding information in Video. Various Steganography techniques have been studied where text and image are been embedded. When compared, it was found that embedding text in video is more secure than image. Hiding text in video makes the job of steganalyser more difficult as the secret message is not detected by unauthorized user. Among so many technique developed till now, none of these are ready to provide a effective mechanism for video Steganography with all formats(avi, mov , mpeg, etc) supported as cover file and versatile data format (image, text, audio, video). The future Video steganography techniques would be a effective when implemented using compression , decompression, encryption, decryption and randon data embedding.

REFERENCES:

1. Sharone Gorla --Report, ”Combination of Cryptography and steganography for Secure communication in Video file” , California State University, SACRAMENTO

2. B.SUNEETHA, CH.HIMA BINDU & S.SARATH CHANDRA “SECURED DATA TRANSMISSION BASED VIDEO STEGANOGRAPHY”International Journal of Mechanical and Production Engineering (IJMPE) ISSN No.: 2315-4489, Vol-2, Iss-1, 2013

3. Kousik Dasgupta, J.K. Mandal and Paramartha Dutta,” Hash based Least Significant Bit Technique”, International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012

4. A. Swathi 1, Dr. S.A.K Jilani,, “Video Steganography by LSB Substitution Using Different Polynomial national Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5

5. Mritha Ramalingam: Stego Machine – Video Steganography using Modified LSB Algorithm World Academy of Science, Engineering and Technology Vol:50 2011-02-26

6. Ashawq T. Hashim*, Dr.Yossra H. Ali** & Susan S. Ghazoul*” Developed Method of Information Hiding in Video AVI File Based on Hybrid Encryption and Steganography” Engg.and tech journal, vol 29,No.2,2011.

7. R. Shanthakumari1 and Dr.S. Malliga, “Video Steganography Using LSB Matching Revisited Algorithm”, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 6, Ver. IV(Nov – Dec. 2014), PP 01-06

8. J. Jayaseelan1 and B. Kruthika,” NOISE SECURES SECRET DATA! BY ACT AS A REFERENCE FOR EMBEDDING”, ICTACT JOURNAL ON COMMUNICATION TECHNOLOGY, MARCH 2014, VOLUME: 05, ISSUE: 01 ISSN: 2229-6948(ONLINE)

9. Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav" Steganography Using Least Signicant Bit Algorithm", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp. 338-341

10. S. Suma Christal Mary M.E (Ph.D)" IMPROVED PROTECTION IN VIDEO STEGANOGRAPHY USED COMPRESSED VIDEO BITSTREAMS", International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 764-766

11. Pritish Bhautmage, Prof. Amutha Jeyakumar, Ashish Dahatonde, " Advanced Video Steganography Algorithm", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 1, January -February 2013, pp.1641-1644

12. Steffy ,Jenifer.K1, Rajalakshmi.G2," Video Steganography for Embedded Images in Compressed Videos Using LSN Method", International Journal of Emerging Technology & Research Volume 1, Issue 1, Nov-Dec, 2013 ISSN (E): 2347-5900 ISSN (P): 2347-6079

13. ShengDun Hu, KinTak U," A Novel Video Steganography based on Non-uniform Rectangular Partition", EE International Conference on Computational Science and Engineering CSE/I-SPAN/IUCC 2011