Steganography over Video File by Hiding Video in another Video File, Random Byte Hiding and LSB Technique

Rachna Patel*
Asst. Prof., Computer Engineering/IT Department,
CGPIT, Uka Tarsadia University (UTU),
Maliba Campus, Bardoli, Gujarat, India
rachu.cuty@gmail.com

Mukesh Patel#
Asst. Prof., B.V. Patel Inst. of Business Management,
Computer & Information Technology,
BVPBMC&IT, Uka Tarsadia University (UTU),
Maliba Campus, Bardoli, Gujarat, India
mukesh.mt@gmail.com

***Abstract*— Steganography is an art of hiding the secret data or information inside the digitally covered information. The hidden message can be text, image, speech (audio) or even video and the cover can be chosen accordingly from either a text, an image, an audio or a video. The traditional method uses image as a cover which has the limitation of embedding dimension. So, cover should be a video to overcome the limitation of embedding dimension. Nowadays, the use of a video based steganography is common and numbers of steganalysis tools are available to check whether the video is stego-video or not. Most of the tools are checking for information hided by LSB, DCT, Frequency Domain Analysis etc and finds whether the video has hidden or secret data or not. In this paper, the video based steganography techniques are discussed specifically, video in another video technique this means that the cover is video and MATLAB based implementation is done to simulate the results.**

Keywords*— *LSB, Steganography, Stego-Video, Steganalysis, Video.

I. INTRODUCTION

Johannes Trithemius (1462-1516) was a German Abbot. His writing, "Steganographia: Hoe Est Ars Per Occultam Scripturam Animi Sui Voluntatem Absentibus Aperiendi Certa" is ostensibly a work describing methods to communicate with spirits. A rough translation of the Latin title is: "Steganography: the art through which writing is hidden requiring recovery by the minds of men." Although people have hidden secrets in plain sight—now called steganography—throughout the ages, the recent growth in computational power and technology has propelled it to the forefront of today's security techniques [1].

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message; this is somewhat contrast to cryptography, where the existence of the message itself is not disguised, but the content is obscured. Block diagram of a steganography system is shown in Fig. 1[2].

Steganography is often confused with cryptology because the both are similar in the way that they both are used to protect important and secrete information. The difference between the two is that Steganography involves hiding information so it appears that no information is hidden at all. If a person views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information [1][2].

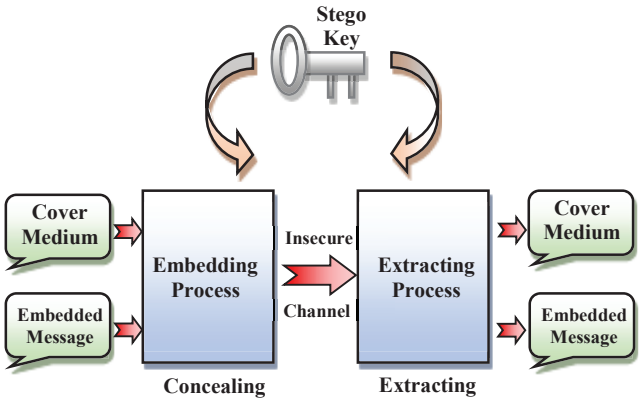

Fig 1. Block diagram of a Steganography System

II. VIDEO STEGANOGRAPHY

Video based steganography can be done in two ways: either frame to frame data storing or converting frame into frequency domain and then store the result. First way is something like spatial domain and the second way is like frequency domain. Whichever method is utilized for steganography, the video steganography can be also classified into two types: lossless and lossy steganography. In lossless steganography the hidden information and original video file both can be retrieved without any error or modification, while in lossy steganography the hidden information is retrieved correctly while the original video will have some errors [3].

The lossless steganography requires storing hidden information in specification location and will requires some time to run the algorithm in order to find the specific location where hidden information can be get stored. Thus, in real time application, the lossless algorithm is becoming tougher to implement, and that depends on the system specifications.

The lossy steganography requires storing data at some LSB location or at specific pixel locations. This is easy to implement

978-1-4799-3975-6/14/$31.00 ©2014 IEEE

and it can be apply in real time application with any normal system specifications.

The proposed lossy steganography technique will be explained here. The LSB (Least Significant Bit) is used here to hide the data. The first frame is selected as index frame and it contains the information regarding where the information is stored, in which form information is getting stored, what is file type of the information, etc information are stored in the Index Frame. If the first frame is received properly and if the receiver recognized the information then it is very easy to get hidden information from steganography video file [4].

III. VIDEO STEGANOGRAPHY OVER AVI FILE [2]

The high resolution AVI file is nothing but a sequence of high resolution image called frames. Initially, we stream the video and collect all the frames in bitmap format (Fig. 2). And also collect the following information: -

A) Starting frame: It indicates the frame from which the algorithm starts the message embedding.
B) Starting macro block: It indicates the macro block within the chosen frame from which the algorithm starts the message embedding.
C) Number of macro blocks: It indicates how many macro blocks within a frame are going to be used for data hiding. These macro blocks are may be consecutive frame according to a predefined pattern. Apparently, the more macro blocks we use, the higher the embedding capacity we get. Moreover, if the size of the message is fixed, this number will be fixed, too. Otherwise it can be dynamically changed.
D) Frame period: It indicates the number of the inter frames, which must pass, before the algorithm repeats the embedding. However, if the frame period is too small and the algorithm repeats the message very often, that might have an impact onto the coding efficiency of the encoder. Apparently, if the video sequence is large enough, the frame period can be accordingly large. The encoder reads these parameters from a file. The same file is read by the software that extracts the message, so as both of the two codes to be synchronized. After streaming the AVI video file into AVI frames we will use the conventional LSB replacement method [12].

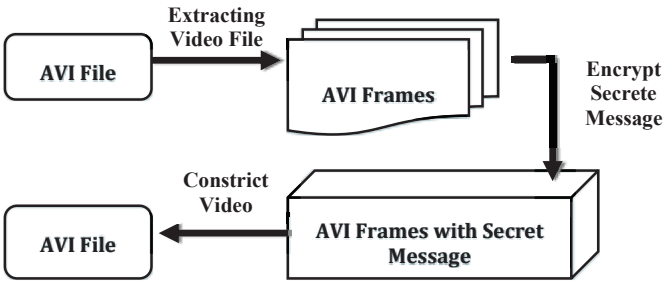

Fig 2. The AVI File

IV. VIDEO STEGANOGRAPHY TECHNIQUES

A. *Random Byte Hiding Technique [2]*

In this technique, the information is hiding in each line of the video frame at different place. For example, if the line begins with the pixel value of 'zz', the information is stored over the 'zz'+x location, where x is only known to the authorized receiver only. So, when unknown person view the video, he sees it as normal video, while the person knowing the steganography can detect the hidden message. The same kind of technique can be implemented by using 'y-zz' where y must be taken above the 256 (a bit higher than logical high level) so that 'y-zz' does not goes negative. The similar technique can be implemented over the column line also.

One of the popular frameworks is shown in Fig. 3 and Fig. 4 for the steganography and de-steganography. This algorithm is a LSB based lossy algorithm. The first frame, index frame is the one which has the agreement details.

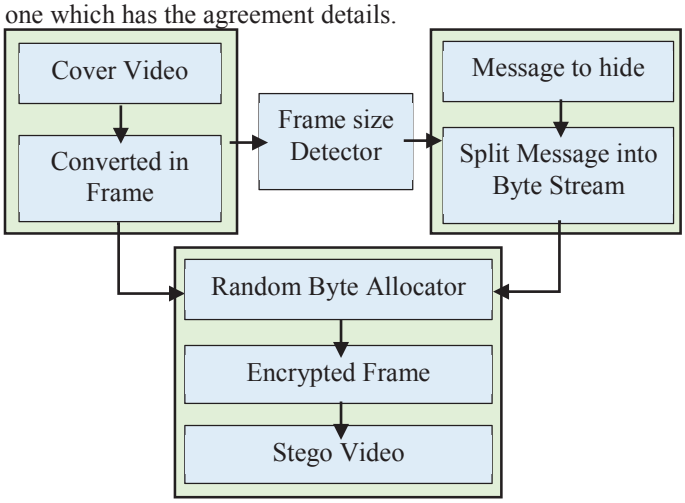

Fig. 3. Proposed Framework for Video Steganography Encoding for Random Byte Hiding Technique

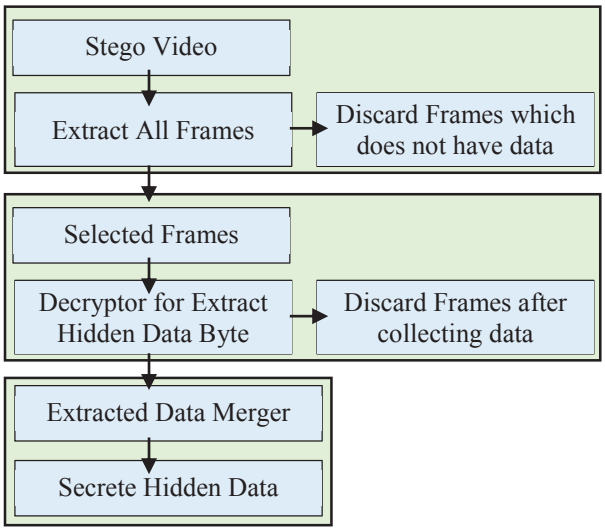

Fig. 4. Proposed Framework for Video Steganography (Decoding) for Random Byte Hiding Technique

B. *LSB Based Steganography Technique [2]*

In this technique, some predefined sequences are well known to sender and the receiver. Over this predefined location the secrete message is made hidden and this can be easily detected at the receiving end. This is something like private key technique. The most widely used technique to hide information, is the LSB (Fig. 5). To hide a secret message inside an image, a

proper cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm.

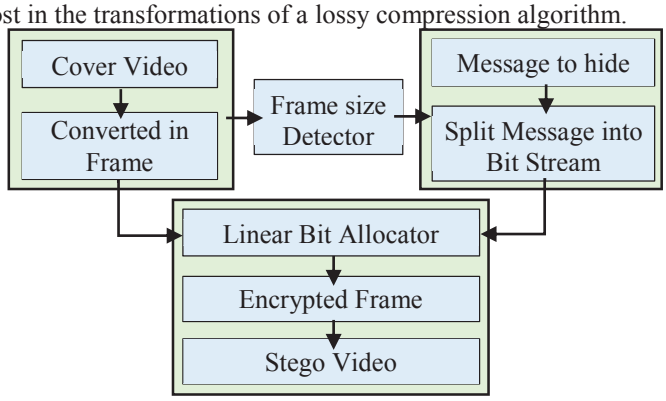

Fig. 5. Proposed Framework for Video Steganography (Encoding) for LSB Based Steganography Technique

(Fig. 6)Decoding method is just opposite to the Encoding method.

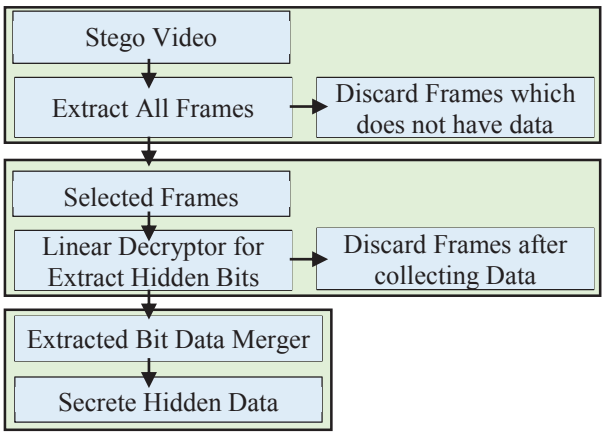

Fig. 6. Proposed Framework for Video Steganography (Decoding) for LSB Based Steganography Technique

C. Video in another Video Technique

In video steganography, we can hide the video in another video. Encoding method for video in another video is shown in Fig. 7. In this, first we will read cover file and segment that secret video streams into frames. After finding frames, find the size of cover video. Simultaneously segment video streams into frames then split the secret message bit stream into R × C group size then each group of messages are rearranged to specific pattern for hiding. Encrypt small message into a byte of data bit on LSB and check whether all small messages are completed or not. If completed then check in all frames hidden messages are included or not. If hidden messages are included then create the rule list for receiver and generate stego video.

Algorithm for proposed framework for Video Steganography Encoding for the video in another video is as follows:-

1. Read cover video and identify the frame size (R × C).
2. Read secrete video (secrete message) file.
3. Extract all frames of secrete video.
4. Rearrange each frame into bit stream.
5. If all frames are not arranged, go to step 3.
6. Rearrange the bit stream into the small groups of R × C size bit groups.
7. Rearrange each portion of the hidden message into hiding pattern.
8. Extract out frames from cover video.
9. Encrypt small message in to the frame over LSB of each pixel of the frame.
10. If all small messages are not completed, go to step 4.
11. Create the rule list for receiver and place it on first frame to determine parameters at recovery stage.
12. Generate the Stego video by integrating all frames which contains hidden information into a video.

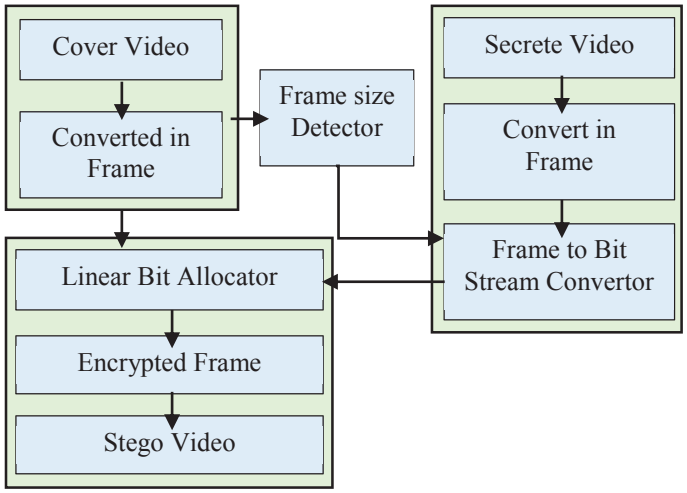

Fig. 7. Proposed Framework for Video in another Video (Encoding)

Decoding method for video in another video is shown in Fig. 8. First read the stego video then segment video streams into frames. As we know that video is made up with combining all frames of images. Read rule list from first frame and separate out frames which contain the hidden information. Decrypt small message from the frame for each column, row and extract LSB. Restore all extracted data bit as byte size vector. Check for rule list, is the last frame contains hidden data or not. If the last frame contains hidden data then merge all the data to single vector and split out vector into specific size of hidden message frame. Arrange splinted vector into hidden message frame size and generate the secret video message.

Algorithm for proposed framework for Video Steganography Decoding for the video in another video is as follows:-

1. Read stego video.
2. Extract the frame from the video.
3. Read rule list from first frame (for example, number of data per frames, how many frames contain information).
4. Separate out frames with hidden message and discard all other frames.
5. Decrypt message from the frame by extracting LSB of each pixel of the frame.
6. If all frames are not decrypted, go to step 5.
7. Rearrange bit stream to byte stream.
8. Rearrange byte streams in the small group array of frame size reference taken from the rule list.

9. If all byte streams are not arranged, go to step 8.
10. Integrate the frames in specific format
11. Generate the secrete video.

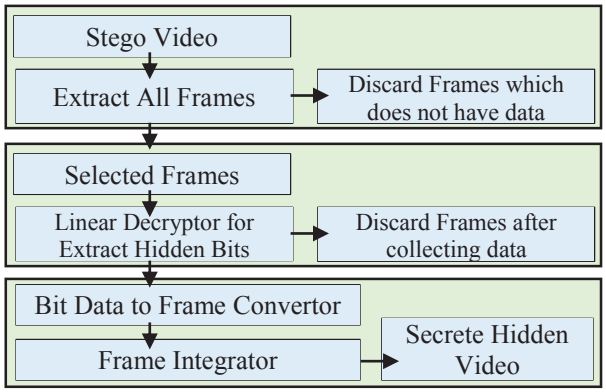

Fig. 8. Proposed Framework for Video in another Video (Decoding)

V. EXPERIMENTAL RESULTS

A. Result for Random Byte Hiding Technique [2]

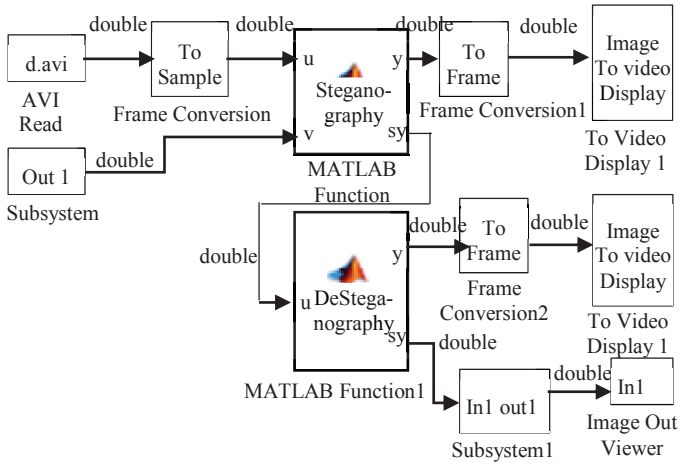

Fig. 9. Simulation for AVI Video

Fig. 9 shows that Simulation for AVI video. First, steganography process will be executed and after getting result that is .avi file then use De-Steganography. Fig. 10 shows the results obtained after simulation.

Fig. 10. Results of Random Byte Hiding Technique

B. Result for LSB Based Steganography Technique [2]

In this technique, some predefined sequences are well known to sender and the receiver. This is something like private key techniques. This technique is known as LSB based steganography. Result of LSB Based Steganography technique is shown in Fig. 11.

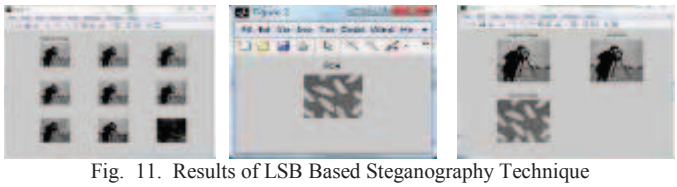

Fig. 11. Results of LSB Based Steganography Technique

C. Result for Video in another Video Technique

Steganography in video can be divided into two main classes. One is embedding data in uncompressed raw video, which is compressed later. The other, which is more difficult, tries to embed data directly in compressed video stream [1]. Here, we would like to embed data in the AVI file in such a way the steganography does not affect the quality of the video file, and although file is not going to compressed any further, even using steganalysis, it is not possible to find out whether the information is hidden or not in video.

Encoding method for video in another video, first we will read cover file and segment that secret video streams into frames. After finding frames, find the size of cover video. Simultaneously segment video streams into frames then split the secret message bit stream into R × C group size then each group of messages are rearranged to specific pattern for hiding. Encrypt small message into a byte of data bit on LSB and check whether all small messages are completed or not. If completed then check in all frames hidden messages are included or not. If hidden messages are included then create the rule list for receiver and generate stego video.

Fig. 12. Simulation for Video in another Video

D. Comparative Analysis of Video Steganography Techniques

TABLE I. COMPARATIVE ANALYSIS OF VIDEO STEGANOGRAPHY TECHNIQUES

Sr. No.	Parameter	Technique 1 Random Byte Hiding Technique	Technique 2 LSB based Steganography	Technique 3 LSB based Video in Video Steganography
1	Number of data hiding per frame	C Byte/Frame	RxC bits/Frame	RxC bits/ Frame
2	Techniques of Hiding	Random Allocation	Linear Allocation	Bit Wise Linear Allocation
3	Hiding Data Ratio (per frame)	1/R	1/8	1/8
4	Error rate for hidden message	0	0	0
5	Cover Video Type	Non Compressed .avi file format	Non Compressed .avi file format	Non Compressed .avi file format
6	Hidden Message Type	Text Image	Text Image	Video
7	Encryption time (In seconds)	32.97	76.514	363.15
8	Decryption time (In Seconds)	26.3537	81.04	443.78

*Cover Video Frame size is RxC (where R is length of Row Pixel and C is Length of Column Pixel) R × C = 480 * 680 = 326400, R = 480, C = 680

(1) Hiding Data Ratio (per frame):

Data hiding operations are executed in compressed domain. Here data are embedded in the macro blocks. Data hiding can be categorized into spatial and transform domain methods. In the spatial domain, secret data is directly embedded into the values of image pixels and in transform domain, for e.g., discrete cosine transform (DCT), Fourier transform, or wavelets, transformed coefficients of cover signals can be manipulated to hide messages [2]. Fig. 13 shows the results.

TABLE II. HIDING DATA RATIO (PER FRAME)

	Random Byte Hiding Technique	LSB based Steganography	LSB based Video in Video Steganography
Hiding Ratio (Hidden Bytes/frame size)	0.00208333	0.125	0.125
	1/R	1/8	1/8

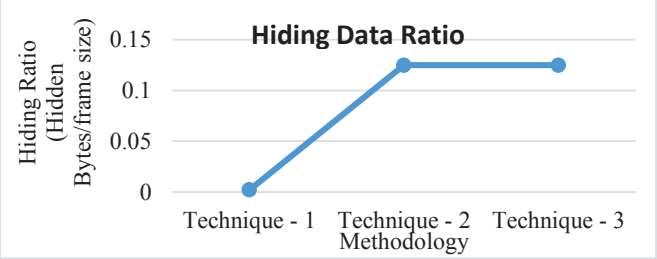

Fig. 13. Graph for Hiding Data Ratio (Per Frame)

(2) Encryption Time and Decryption Time:

Encryption is difficult to perform in real-time applications without harming the quality of video. To embed the message, LSB method is used. Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover file [2]. Fig. 14 shows the results.

TABLE III. ENCRYPTION TIME AND DECRYPTION TIME

	Random Byte Hiding Technique	LSB based Steganography	LSB based Video in Video Steganography
Encryption time (In Seconds)	32.97	76.514	363.15
Decryption time (In Seconds)	26.3537	81.04	443.78

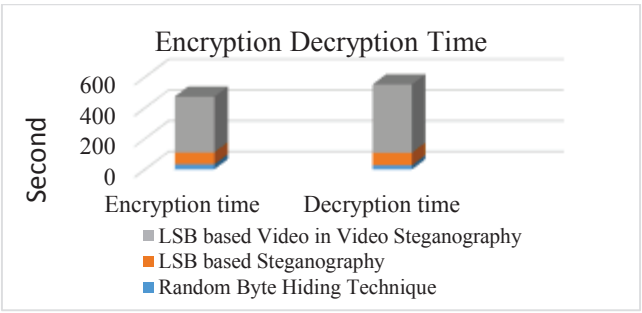

Fig. 14. Graph for Encryption and Decryption Time

VI. CONCLUSION

Steganography is an excellent means of conversing covertly if there are guarantees on the integrity of the channel of communication. It is not necessary for the two parties to agree to a specific hiding format. If the video is seen by normal person, it is found that there is nothing but the normal video, but only the known persons can find out the decrypted message from the video. The Different encryption format can be agreed by the two persons in such a way that no one can find the information from the video.

Each technique can be implemented easily, but if someone tries to find out the tricks after knowing that someone using the stego-video file, then there are good chances of finding out the hidden information. In order to avoid this, the some hybrid system is used, in such a way that even though someone finds out the one technique, it is used only on few frames and other frames contains different kind of steganography and hence total secrete message is not delivered.

REFERENCES

[1] Ashish T. Bhole, Rachna Patel, "Design and Implementation of Steganography Over Video File", The Indian Journal of Technical Education, Special Issue for NCEVT' 12, pp. 69-72, April 2012.

[2] Ashish T. Bhole and Rachna Patel, "Steganography over Video File using Random Byte Hiding and LSB Technique", International Conference on Computational Intelligence and Computing Research, pp. 189-194, 2012 IEEE.

[3] Amr A. Hanafy, Gouda I. Salama and Yahya Z. Mohasseb, "A Secure Covert Communication Model Based On Video Steganography", *Military Communications Conference (MILCOM),* pp. 1-6, 16-19 November IEEE 2008.

[4] Balaji R, Naveen G, "Secure data transmission using video Steganography", *2011 IEEE International Conference on Electro/Information Technology (EIT),* vol., no., pp. 1-5, 15-17 May 2011.

[5] Kousik Dasgupta, J.K. Mandal and Paramartha Dutta, "Hash Based Least Significant Bit Technique For Video Steganography(HLSB)", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, pp. 1-10, April 2012.

[6] Mritha Ramalingam,"Stego Machine – Video Steganography using Modified LSB Algorithm", *World Academy of Science, Engineering and Technology*, pp. 502-505, 2011.

[7] Natarajan Meghanathan, Lopamudra Nayak, "Steganalysis Algorithms for Detecting the Hidden Information in Image, Audio And Video Cover Media", *International Journal of Network Security and its Applications (IJNSA),* Vol.2, No.1, pp. 43-55, January 2010.

[8] P.Paulpandi1, Dr.T.Meyyappan, "Hiding Messages Using Motion Vector Technique in Video Steganography", *International Journal of Engineering Trends and Technology,* ISSN: 2231-538, Vol. 3, Issue 3, pp. 361-365, 2012.

[9] R.Kavitha, A. Murugan, "Lossless Steganography on AVI File using Swapping Algorithm", *International conference on Computational Intelligence and Multimedia Applications,* pp. 83-88, 2007 IEEE.

[10] Sheng Dun Hu, KinTak U, "A Novel Video Steganography Based on Non-uniform Rectangular Partition", *14th International Conference on Computational Science and Engineering (CSE),* pp. 57-61, 24-26 August IEEE 2011.

[11] S. Suma Christal Marry, "Improved Protection in Video Steganography Used Compressed Video Bitstreams", International Journal on Computer Science and Engineering (IJCSE), Vol. 02, No. 03, 2010, 764-766, pp. 764-766, 2010.

[12] Saurabh Singh and Gaurav Agarwal, "Hiding image to video: A new approach of LSB Replacement", *International Journal of Engineering Science and Technology*, Vol. 2(12), pp. 6999-7003, 2010.

[13] Sherly A P and Amritha P P, "A Compressed Video Steganography using TPVD", *International Journal of Database Management Systems (IJDMS),* Vol.2, No.3, pp. 67-80, August 2010.