International Journal of Emerging Technology and Innovative Engineering
Volume 1, Issue 12, December 2015 (ISSN: 2394 – 6598)

A SECURE ALGORITHM OF VIDEO STEGONOGRAPHY FOR DATA HIDING

Kedar Nath Choudry[1], Prof. Aakash Wanjari[2]

[1]*M.Tech. Scholar, CSE Department, DIMAT, Raipur*
[2]*Professor, CSE Department, DIMAT, Raipur*

[1]kedarnath2013@gmail.com

[2]aakash.mit1000@gmail.com

ABSTRACT

A sudden surge in the use of internet has made it easy to send the information from one place to another place while sitting in a bed room. Some of the information which is transferred through the internet are very crucial need to protected well before sending in to the internet because internet is full of hackers activity which are being carried out to steal some crucial information from the internet. One of the solution to protect the data is steganography which is the method of hiding the crucial data inside other unimportant data. In this paper, a combination of Video steganography and cryptography is adopted for securing the crucial data. Random selection of frames, swapping the pixel and encrypting the message before being embedded into the video has been performed for enhancing the security.

Keywords— *Least significant Bit(LSB), steganography , MSE, PSNR, Cryptography*

I. INTRODUCTION

In 90's, the emergence and growth of internet in all over the world has created a dramatic change in the people's life style. With the introductiont of internet and information revolution, shopping, rail reservation and even money transfer has become possible in online i.e. people is not required go anywhere to get all these job done, instead they are able to make all these job done even in sitting at their respective home. Apart from these, the introduction of social site like twitter, whatsapp and facebook has made is possible for the people to be in touch with each other 24/7 hours. Peoples are now able to exchange their information with each other very rapidly and promptly. Exchanging the information on the internet on one hand is very good as it require less amount of time and person can exchange the information all over the globe but on the other hand, it has some drawbacks. There are so many loop holes in the internet technology from where anybody can extract these crucial information and use it for its own interest. There are so many groups on the internet who does the same job and known as the hackers. So internet is good for information interchange but is very insecure place to exchange the information. So it is a need of the hour to design and develop some kind of algorithm which can be secure enough to be used in internet.

Two most widely used techniques can solve this problems i.e. Cryptography and Steganography.

Steganography is one of the technique which is designed and develop to fight with such type of problems. Steganography is basically an applicationprogram which is developed and designed for hiding the crucial,valuable or confidential data in a cover or host file in such a way that no one other than a authorised person knows the existence of such

hidden information in cover file or host file. Audio, Video Text or even image can be used as a cover file or host file[1].

Cryptography is basically a method of jumbling the secret information (otherwise known as Encryption) in such a way that nobody can decipher it. So it can also be used to fight with the above mentioned problems.

Though both the techniques are developed and designed for fulfilling the same purpose i.e. keeping the information secure from unauthorized person, both techniques are different in the way they present the secret information to the real world. Cryptography arrange the secret information in to the jumbled word which is very difficult to interpret. But for the hackers, jumbled word clearly indicates some kind of secret or confidential information. So they knows that there are some kind of secret information but they are not able to decipher it. On the other hand in steganography algorithm, the secret or confidential information is hidden purposely inside a innocent cover file in such a tactful way that nobody can even imagine or think that such kind of information is hidden inside the cover or host file which may be any image, audio or video.

Embedding payload and embedding efficiency are the two very important parameters of any steganography system [4]. Amount of data which can be hidden in the cover file is known as the embedding payload. The capacity of steganography system to hide as much data as it can without inducing significant distortion on the cover file is known as the embedding efficiency[2].

High embedding efficiency is the prime necessity of any steganography system. High embedding efficiency means least distortion in the cover file and hence it is very difficult to imagine or think an existence of any secret information in the cover file. This makes it difficult to apply any stego analysis tool for extracting out the information from the cover file [3].

Embedding efficiency and embedding payload are generally having inverse proportional relationship. Increasing the embedding efficiency will eventually decrease the embedding payload and vice versa [2].

II. STEGANOGRAPHY SYSTEM

Steganography is the algorithm or method of hiding the information in some other host object. It has been used since ancient time by the people for hiding the secret information. In ancient time, secret information is generally hidden in the back of wax, scalp of the slaves, in rabbits etc.

With the passage of time, the application and area of steganography has become widened. With the introduction of digitization era, digital steganography has emerged as the new and efficient tool for hiding the information secretly. Text, digital image, digital audio and digital video has become the host object for hiding the data.

Some of the common term which is necessary to understand any steganography system is given below-

Cover Media- It is the digital medium in which secret information is hidden or embedded in such a way that it is difficult to detect the presence of data.

Stego- Media- It is medium or entity obtained after embedding the secret information.

Secret data- This is the data or information which is to be hidden in cover media.

Steganalysis- The process of detecting the presence of secret data in cover media using some statistical operation.

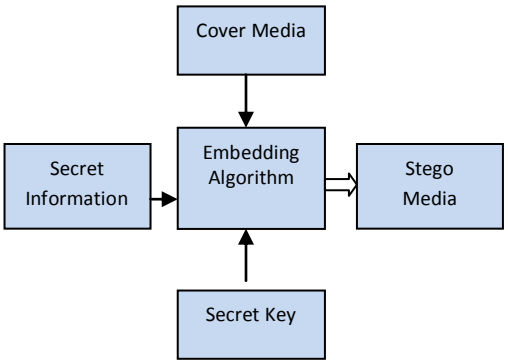

Figure 1 Typical Steganography System

III. RELATED WORK

Most of the research work in video steganography is the extension of image steganography. One of the most common method of image steganography is least significant bit method (LSB) which can also be applied to the video steganography. In this method least significant bit of the frames of host video is used to carry the secret information [5],[6],[7]. This method is simple and requires least computational power but in this method the secret information can be destroyed easily by some file transformation. Moreover the security of this method is very poor and can be broken easily.

Spread spectrum techniques is another well known method in video steganography which is still explored by the researcher for better performance [7][8].

The advantages of this method is its robustness.The loss of data after applying geometric transformation is very less in this method. The security of this method is also very strong and difficult to break[8].

Some more methods of data hiding have been introduced in the past which were based on the multi-dimensional lattice structure. Data embedding rate of these method is very high and is able to embed high amount of data by changing the number of quantization level[9].

In 2002 Wang presented a steganographic algorithm for High capacity data hiding[10]. In his approach discrete Cosine transform is used. Main aim of this method is to increase the payload capacity while keeping the robustness and simplicity intact. In this method , DCT coefficients of I-frames are computed and then secret information is embedded by performing modulation between quantized DCT coefficients and secret information.

In 2004[11], Hideki Noda and his fellow researcher presented a steganography method for wavelet compressed video. In this paper an steganography method for lossy compressed video is presented. This is a easy method to send large amount of secret data. This method first compressed the video data using wavelet and then bit plane complexity segmentation steganography is used for embedding the secret data. In this method DWT transformed video is quantized to a bit plane structure and then BPSC algorithm is applied to the video in wavelet domain.

This method is tested for 3-D SPIHT-BPSC steganography and JPEG 2000-BPSC. Former method is the combination of 3-D SPIHT coding and BPSC algorithm of steganography while the latter is the combination of JPEG 2000 standard and BPSC algorithm of steganography. Experimental results reveals that 3-D SPIHT-BPSC is better performer than the JPEG2000-BPSC as far as embedding performance is concerned.

In 2007, Lane presented a vector embedding method for data hiding[12]. This method uses the MPEG-I and MPEG-II video codec standard. In this method,

audio information is embedded in to the pixel of host video frames.

R. Kavitha, A. Murugan in 2007[13] proposed a steganography algorithm for AVI video file standard using swapping method. In this paper a comparative analysis of JPEG image steganography and Audio-video interleaved (AVI) steganography has been accomplished with respect to quality and size. Author suggested that by using UTF-32 encoding in the swapping algorithm will increase the strength of the key and also the security of this steganography system. The drawback of this steganography system is its low payload capacity.

In 2007, Yueyun Shang in his paper [14] presented a invertible data hiding techniques foe compressed video. This scheme is suitable for Motion Picture Expart Group (MPEG) standard. In this method , Hidden embedded data of the video can be extracted without the need of copy of original MPEG video and covert video. This scheme work only in frequency domain. Low complexity and low visual distortion is the high points of this method while low payload capacity is the disadvantage of this method.

In 2008, Amr A. Hanafy and his associates presented a steganography model[15] for hiding the presence of secret information in a cover video of any format.

In this model colored video file is pixel-wise manipulated to insert a secret data . this method first segment the secret information in to a blocks before embedding it in to the cover video. In the next level, this method embed these block in psudo random location in video file.

Loaction for embedding is derived by re ordering the secret key which is shared by both sender and receiver. Re-ordering operation is dynamic and changed with each video frames. This increase the security of the algorithm and nullify and chance of getting the order using statistical analysis for identifying the secret message block location. Interceptor is not able to find the locations of secret message block even if cover video is available to him.

In this paper, a quantitative evaluation of this model has also been presented for four different types of secret information. Peak signal to Noise ratio(PSNR) and Mean Squared error(MSE) is computed between original cover video file and stigo video file.

Simulation result shows least degradation in stigo video file as compared to the original video file for different kind and size of secret data. The authors also estimated the capacity of video files for different video format and size.

IV. METHODOLOGY

Procedure of the proposed method of video steganography is shown in the block diagram provided in figure 2. From this block diagram it is clear that this video steganography method consist of two phase. First is designed for embedding the message in to a video frames i.e. creating stego video.

Second phase of the proposed methodology is shown in the figure 3 which is designed for extracting the message from the stego video obtained at first phase.

Next section gives the algorithm steps adopted for creating the stego video or for embedding the message to the host video.

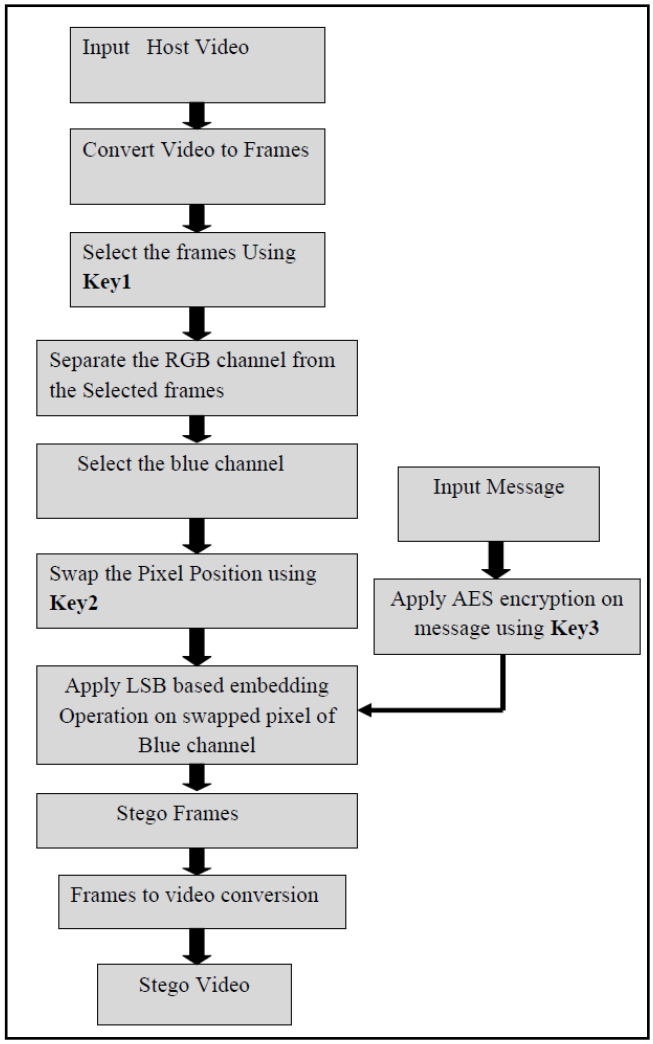

Figure 2 Block Diagram of Proposed Video Stegnography Algorithm

Step 1 Input the Host video.

Step 2 Apply Video resizing operation if necessary..

Step 3 Apply video to frame conversion operation to get all the frames of the host video and store them in a folder for further processing.

Step 4 By using Key1 Randomly select the frames for message embedding.

Step 5 Apply RGB channel separation operation on Selected frames to separate all the three channel.

Step 6 Select the Blue channel of each frames.

Step 7 Using Key 2 Apply swapping operation on pixels of selected blue channel for rearranging the pixel position.

Step 8 Input the Secret Message.

Step9 Apply the AES encryption algorithm for Encrypting the message by using Key3.

Step 10 Apply LSB based embedding algorithm for embedding each message bit to the pixel.

Step 11 Carry on these steps till all the message bit exhausted and get the stego frames.

Step 12 Apply frames to video conversion operation to obtain the stego video from stego frames.

In the proposed method, message is encrypted before the embedding operation for extra security. Algorithm steps for AES encryption of message are as follows-

Step 1: Input The Secret Message (Image or Text)

Step 2: Covert this message pixel to a one dimensional vector for further processing.

Step 3: By using Key3 encrypt the message by AES algorithm.

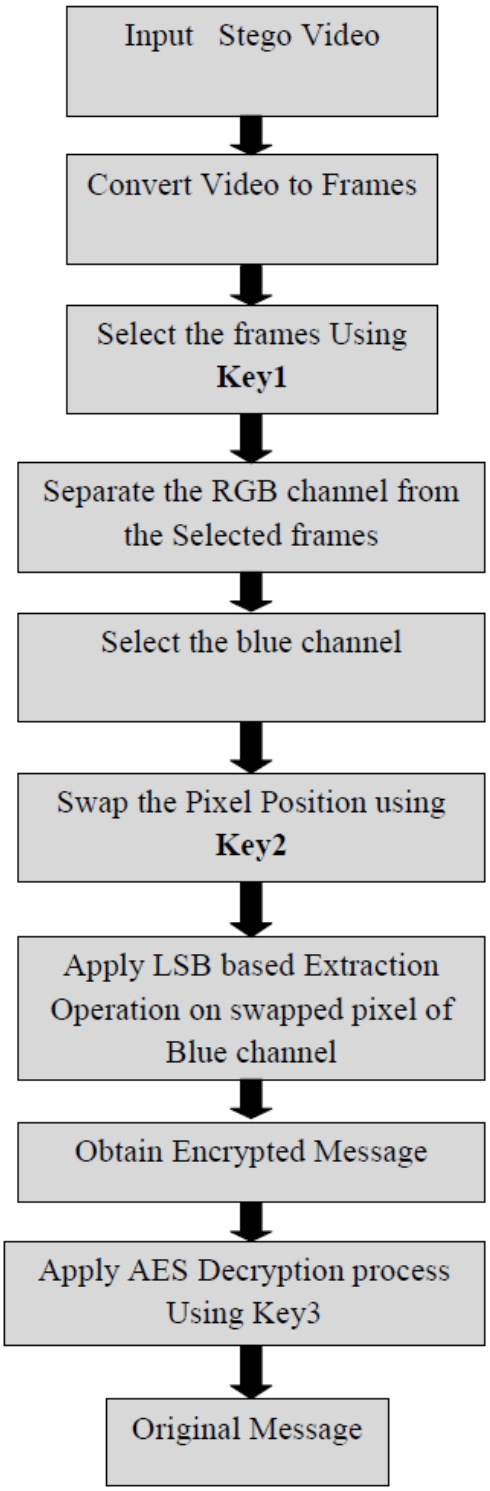

Figure 3 Message Extraction process

Once the message is embedded in the host video, we get the stego video. In order to extract the the message bit from the stego video, reverse operation is applied. Message extraction process from the stego video is shown in the figure 3.

Various algorithm steps adopted for extracting the message from the stego video is described in the next section.

Step1 Input the stego video obtained in the first phase.

Step2 Apply video to frame conversion operation on stego video and store all the frames in a folder.

Step3 By using Key1 select the frames randomly which contain the secret message.

Step4 Apply RGB channel separation operation on Selected frames to separate all the three channel.

Step5 Select the Blue channel of each frames.

Step6 Using Key 2 Apply swapping operation on pixels of selected blue channel for rearranging the pixel position.

Step7 Apply LSB based Extraction algorithm for extracting each message bit from the pixel. and obtain the secret message in encrypted form.

Step8 Apply the AES based decryption method to get Back the original message from the encrypted Message.

In this method, frame selection and pixel swapping operation is performed using random sequence generator which is used to generate the random number of predefined values. For selecting the frames randomly and swapping the position of the pixel randomly two keys i.e. key1 and key2 are used. These keys are very important because random number generator, generates the number by using these keys. Different key generate different random numbers. So this operation makes this method very secure. Apart from this secret message itself encrypted before embedding operation which enhance the security level

of this method further. It is necessary to know all the three keys for extracting the secret message from the stego video.

V. EXPERIMENTAL RESULT

In order to check the security, capacity and efficiency of the proposed video steganography method, Simulation program is designed using algorithm steps provided in the previous section. This simulation program is designed in MATLAB environment. This algorithm is tested for 10 different videos out of which some of the standard videos while some others are the videos are self made videos. For the similarity purpose all the videos are first converted in to a dimension of 256x256. These videos are of different length and hence gives different number of frames after converting the video in to a frames.

First of all a secret message of size 1 KB is taken for embedding purpose and embedded in to the host video by using proposed method.

For observing the effect of the data embedding on the quality of the stego video some statistical parameters like PSNR(Peak signal to noise ratio) and MSE(Mean squared Error) are calculated. For MSE calculation, following formula is used-

$$MSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left[I(i,j) - I'(i,j)\right]^2}{M \times N}$$

In this formula,

I= Original host Frame

I'= Stego Frame

M= Number of rows in original frame.

N= Number of Column in Original frame.

It is clear from this formula is that the value of this parameter must be as less as possible. If the value of MSE is zero that means the distortion in the stego video is zero i.e. the quality of the stego video is same as the quality of the host video. A good video stegography algorithm must produce least distortion in the stego video.

Second statistical parameters which was used in this method is PSNR i.e. Peak signal to noise ratio.

For Estimatimng the PSNR measure, following formula is used-

$$PSNR = 10log_{10}\frac{P \times P}{MSE}$$

Figure 4 Video for testing the steganography algorithm, newsreader.avi(Upper),Rhino.avi(Middle) and coastguard.avi(Lower)

Here

P= Maximum pixel value in the frame.

From this formula it is clear that PSNR and MSE are inversely proportional i.e. zero MSE means zero distortion and Infinite PSNR. So for good quality stego image the value of PSNR must be as high as possible.

Table 1 PSNR and MSE Comparison(text size=1kb)

Video	**PSNR between Original and Stego Video**	**MSE between Original and Stego Video**
Rhino.avi	66.2903	0.5220
Newsreader.avi	64.1126	0.6572
Coastguard.avi	64.5191	0.5717

For observing the effect of different pay load capacity(size of message)on the quality of the stego video, a text data of different size is taken and then MSE and PSNR is computed for different data size. These values of PSNR and MSE is tabulated in table2, table3 and table 4 for different video.

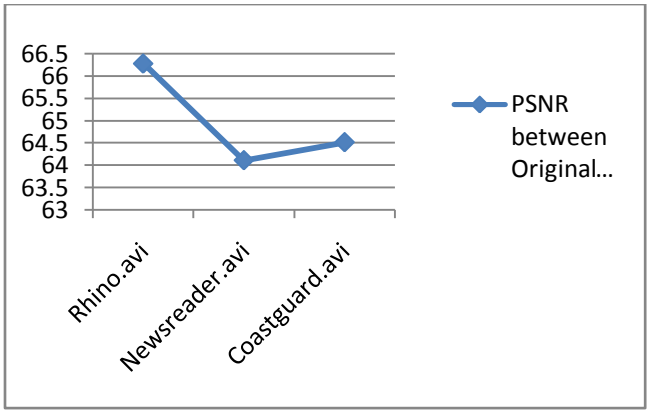

Figure 5 PSNR Comparison Graph Between Original and Stego Video

Practically it has been observed that some distortion is always produced in stego frame if we are using the LSB based algorithm for data hiding hence the actual values of PSNR never comes to be infinite but it must be as high as possible.

PSNR and MSE for the secret message of size 1KB is tabulated in table1 for three different standard videos. Higher value of PSNR and Lower value of MSE for all the three cases clearly indicates that this algorithm produced least distortion.

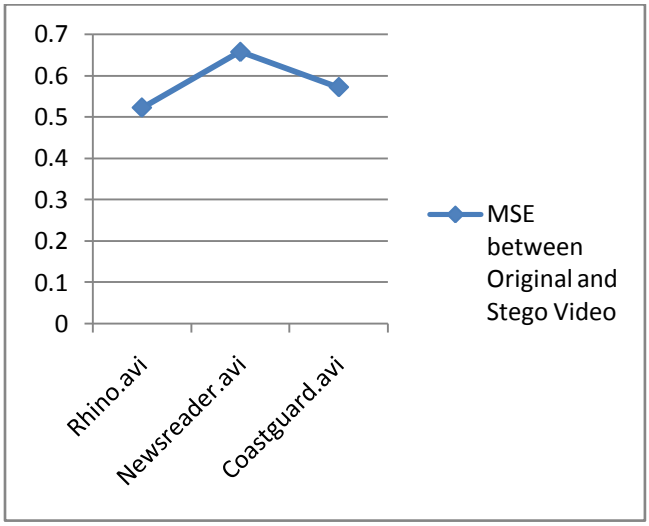

Figure 6 MSE comparision Graph Between Original and Stego Video

VI. CONCLUSION

Steganography is one of the tool to send the secret information from one place to another place. This paper present an algorithm of video steganography for sending the secret information or embedding the secret information in to the video. The secret information here can be of Image, text ,audio and even video. In this algorithm, LSB(Least significant bit) method is used for embedding purpose. Though this method is known to least secure and least resource hungry method of steganography, an attempt has been made to enhance the security of this method by incorporating random frame selection and pixel swapping operation along with the AES based message encryption operation. It can be concluded from the analysing the result that this method is able to hide the secret data without creating the significant distortion in the host video. The security of this method is also enhanced with new modifications.

Table 2 PSNR and MSE Comparison for different payload

Video	**PSNR between Original and Stego Video**	**MSE between Original and Stego Video**	**Capacity of Text Data i.e. Payload**
Rhino.avi	66.2903	0.5220	1kb
	66.9126	0.5290	2kb
	65.4914	0.5428	3kb
	64.1273	0.5861	4kb

Table 3 PSNR and MSE Comparison for different payload

Video	**PSNR**	**MSE**	**Capacity**
	between Original and Stego Video	**between Original and Stego Video**	**of Text Data i.e. Payload**
Newsreader.avi	64.1126	0.6572	1kb
	64.7750	0.6689	2kb
	63.1972	0.6991	3kb
	63.8849	0.7110	4kb

Table 4 PSNR and MSE Comparison for different payload

Video	**PSNR between Original and Stego Video**	**MSE between Original and Stego Video**	**Capacity of Text Data i.e. Payload**
coastguard.avi	64.5191	0.5717	1kb
	64.8190	0.5998	2kb
	63.2714	0.6371	3kb
	63.8735	0.6761	4kb

REFERENCES

[1] H. Yuh-Ming and J. Pei-Wun, "Two improved data hiding schemes," in *Image and Signal Processing (CISP), 2011 4th International Congress on*, 2011, pp. 1784-1787.

[2] C. Chin-Chen, T. D. Kieu, and C. Yung-Chen, "A High Payload Steganographic Scheme Based on (7, 4) Hamming Code for Digital Images," in *Electronic Commerce and Security, 2008 International Symposium on*, 2008, pp. 16-21.

[3] L. Guangjie, L. Weiwei, D. Yuewei, and L. Shiguo, "An Adaptive Matrix Embedding for Image Steganography," in *Multimedia Information Networking and Security (MINES), 2011 Third International Conference on*, 2011, pp. 642-646.

[4] W. Jyun-Jie, C. Houshou, L. Chi-Yuan, and Y. Ting-Ya, "An embedding strategy for large payload using convolutional embedding codes," in *ITS Telecommunications (ITST), 2012 12th International Conference on*, 2012, pp. 365-369.

[5] C.S. Lu: Multimedia security: steganography and digital watermarking techniques for protection of intellectual property. Artech House, Inc (2003).

[6] J.J. Chae and B.S. Manjunath: Data hiding in Video. Proceedings of the 6th IEEE International Conference on Image Processing, Kobe, Japan (1999).

[7] Provos, N., Honeyman, P.: Hide and Seek: An Introduction to Steganography. IEEE Security & Privacy Magazine 1 (2003).

[8] I.J.Cox, J. Kilian, T. Leighton, T.Shamoon: Secure spread spectrum watermarking for multimedia. Proceedings of IEEE Image processing (1997).

[9] J.J. Chae, D. Mukherjee and B.S. Manjunath: A Robust Data Hiding Technique using Multidimensional Lattices. Proceedings of the IEEE Forum on Research and Technology Advances in Digital Libraries, Santa Barbara, USA (1998).

[10] Y. Wang, E. Izquierdo, "High-Capacity Data Hiding in MPEG-2 Compressed Video", 9th International Workshop on Systems, Signals and Image Processing, UK, 2002.

[11] Hideki Noda, Tomonori Furuta, Michiharu Niimi, Eiji Kawaguchi. Application of BPCS steganography to wavelet compressed video. In Proceedings of ICIP'2004. pp.2147-2150

[12] D.E. Lane "Video-in-Video Data Hiding", 2007.

[13] R. Kavitha, A. Murugan, "Lossless Steganography on AVI File Using Swapping Algorithm," Computational Intelligence and Multimedia Applications, International Conference on, vol. 4, pp. 83-88, 2007

[14] Yueyun Shang, "A New Invertible Data Hiding In Compressed Videos or Images," icnc, vol. 5, pp.576-580, Third International Conference on Natural Computation (ICNC 2007), 2007

[15] Amr A. Hanafy, Gouda I. Salama and Yahya Z. Mohasseb "A Secure Covert Communication Model Based on Video Steganography," in Military Communications Conference, 2008. MILCOM. IEEE on 16-19 Nov. 2008.