ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

A Secure Data Hiding Technique Using Video Steganography

Gopal Krishn Pandey[1], Mrs. Sameena Zafar[2]

M.Tech Student, Department of E&TC, Patel College of Science and Technology, Ratibad, Bhopal, India[1]

Associate Professor, Department of E&TC, Patel College of Science and Technology, Ratibad, Bhopal, India[2]

ABSTRACT: Emergence of internet has made it possible to transfer the data from one place to another place rapidly and accurately. This data when goes through the internet may become a victim of the hackers who can steal, modify and misuse the information. Therefore it is necessary to transfer the data with utmost security. Steganography is one such solution to this problem. In this paper, combination of cryptography and steganography is used for data hiding in video clips. Random frame selection, pixel swapping and encryption of message has been done to enhance the security of the secret information which goes under the cover of video clips. The method is also able to accommodate large amount of data in video.

KEYWORDS: Steganography, Least significant Bit (LSB), PSNR, Cryptography, Discrete Cosine Transform (DCT).

I. INTRODUCTION

In 90's, the emergence of internet in all over the world has generated a drastic change in the people's life style. With the advancement of internet and information revolution, shopping, rail reservation and even money transfer has become online i.e. people need not go anywhere to get all these above job done instead they are able to make all these job done even in sitting in their respective home. Apart from these, the emergence of social site like twitter, wat's up and facebook has made all the people to be in touch with each other 24/7 hours. People are now able to exchange the information with each other very rapidly and promptly.Interchanging the information online has started creating problems of intercepting these information by some unauthorised, unsocial group of people famously known as hackers. So this is a need of the hour to design or develop some kind of application which can be able make sage and secure transfer of utmost important or valuable information without being recognized by the unauthorized person.

The solution of these problems lies in two most widely used techniques i.e. Cryptography and Steganography. Steganography is one of the technique which is designed to fight with such type of problems. Steganography is basically application which is developed for hiding the valuable or confidential data in a cover file in such a way that no one other than a authorised person knows the presence of such hidden information in cover file. Audio, Video Text or even image can be used as a cover file [1].

Cryptography is basically an art of jumbling the secret information (otherwise known as Encryption) in such a way that nobody can understand it. So it can also be used to counter the above mentioned problems.

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

Embedding payload and embedding efficiency are the two crucial 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

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

system to hide as much data as it can with inducing as least distortion as it can on the cover file is known as the embedding efficiency[2].

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

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

II. RELATED WORK

Research work done in the field of image steganography can be extended to the to the video steganography. One of the most commonly used algorithm of image steganography is least significant bit (LSB) method. Least significant bit based steganography method can also be applied to text, audio and even for video.

In this algorithm, Least significant bit of every pixel of frames is used to hide the secret information bit[5],[6],[7]. This method of steganography is simple and require less computational power.

But least security is one of the problem of this method. Since least significant bit is used in this method to hide the secret information, it is easy to extract the least significant bit from each pixel which reveals the actual information. Some of the variants are therefore introduced to enhance the security of the LSB based method. Another disadvantage of this method is even a simple file transfer can destroy the LSB bit and hence the secret information.

Spread spectrum technique is another one of the well known technique of video steganography. Lots of research work is still going on spread spectrum technique for better performance [7][8].

Robustness is one of the high point of this method. Experimental results shows that the loss of data in this method after geometrical transformation is very less. Security of this technique is very strong and it is very difficult to break its security.

The advantages of this method are 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].

Data hiding method based on the multi-dimensional lattice structure were also introduced in the past. One of the key point of this method is its high data rate. High amount of data can be stored in this method by just changing the number of quantization level[9].

In 2002 Wang, suggested a steganographic method for hiding high capacity data[10]. Discrete Cosine Transform is used in this approach. Increasing the pay load while keeping the robustness and simplicity intact is the main objective of this work, In this technique.

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 result 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.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

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 works 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 block before embedding it in to the cover video. In the next level, this method embed these blocks in pseudo random location in video file.

Location 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.

III. STEGANOGRAPHY SYSTEM

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

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

Below are some of the common term which is necessary to understand any steganography system.

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

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

Secret data- The data or information to be hidden in cover media.

Steganalysis- The process of detecting, presence of secret data in cover media.

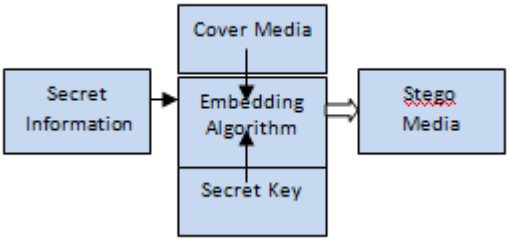

Figure 1 Steganography System.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

IV. METHODOLOGY

Block diagram of the proposed video steganography technique is shown in the figure 2. The overall process is divided into a two parts. First part deal with the message embedding process in the video sequence i.e. making stego video while the second part deal with the extraction of message from the stego video.
Algorithm steps which are used in this algorithm to hide the message in the video sequence are as follows-
Step 1: Input the video.
Step 2: Resize the video.

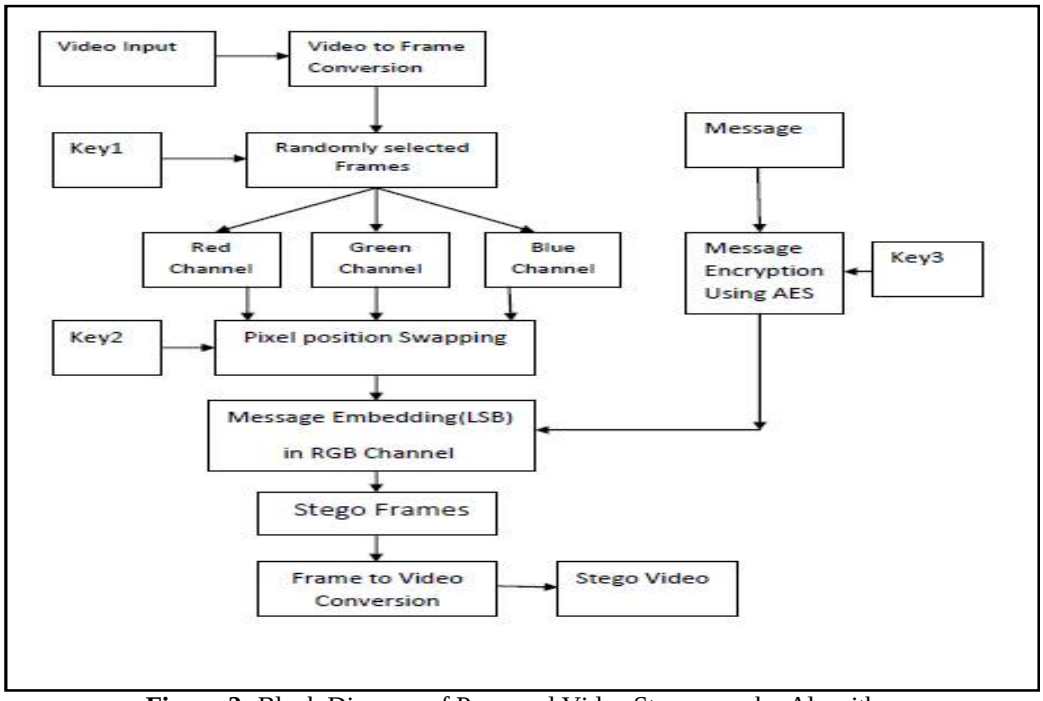

Figure 2: Block Diagram of Proposed Video Stegnography Algorithm

Step 3: Convert the video into a frames and store all the frames in to a folder.
Step 4 With the help of Key1 select the random frames for data hiding.
Step 5 Separate the Red , Green and Blue channel from the selected frames.
Step 6 Select the Blue channel of each frames for data hiding.
Step 7 With the help of Key 2 swap the position of pixel of the blue channel of the selected frames.
Step 8 Enter the message which is to be hidden.
Step 9 Encrypt the message by applying AES algorithm with the help of Key 3.
Step 10 Embed each message bit to the pixel obtain in the step 7 using LSB method to get the stego frames.
Step 11 Continue this process till all the message bit is embedded.
Step 12 Convert all the stego frames in to a video to get a stego video.

Algorithm steps for encrypting the message are as follows-
Step 1: Input The Message(Text or Image)
Step 2: Covert this message pixel in to a one dimensional vector.
Step 3: Apply AES (Advanced Encryption) operation in this one dimensional vector with the help of key3 to get the encrypted message pixel.

Block diagram of Message extraction process is shown in the figure 3.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

The steps of algorithm for extracting the message from the stego video are as follows-
Step1: Input the stego video.
Step2: Convert the video in to frames and store all the frames in to a folder.
Step3: With the help of Key1 select the random frames for data hiding.
Step4: Separate the Red, Green and Blue channel from the selected frames.

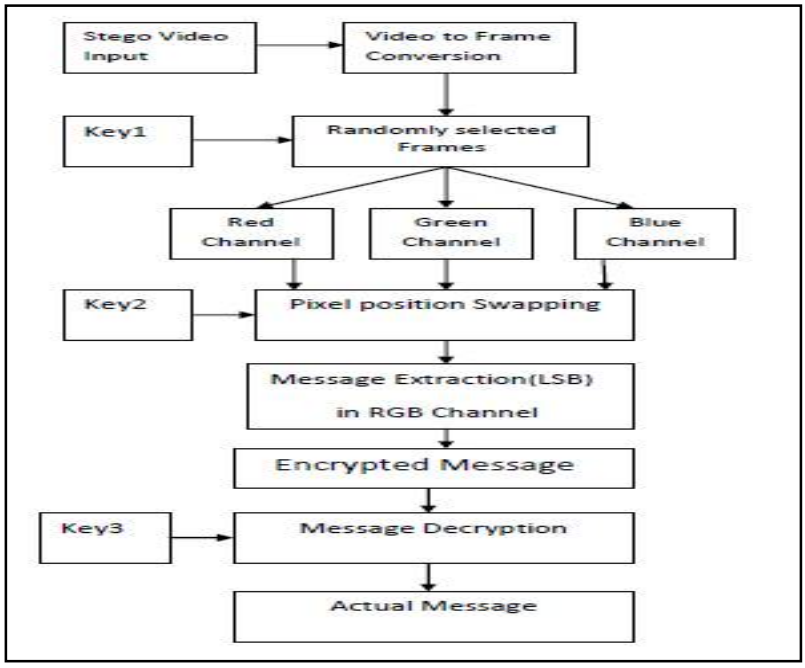

Figure 3: Message Extraction process

Step5: Select the Blue channel of each frames for data hiding.
Step6: With the help of Key 2 swap the position of pixel of the blue channel of the selected frames.
Step7: Apply LSB based extraction Procedure to get the message in encrypted form.
Step8: Apply the AES decryption method to get the original message from the encrypted form.
In this algorithm, random sequence generator is used for random frame selection and pixel swapping operation randomly.
It is important to note that in the proposed method, random frame selection with the help of key1 and pixel swapping operation with the help of key2 makes this algorithm very secure even after using simple LSB embedding method for message bit insertion. Only the person who knows both the key is able to extract the hidden message from the video sequence. Moreover message is also encrypted for even more security.

V. EXPERIMENTAL RESULT

In order to verify the efficiency and capacity of the proposed video steganography algorithm. A program is designed as per the algorithm described in the previous section. MATLAB is used as a programming environment. Since the steganography algorithm is meant for video sequence. Therefore as many as 3 different video has been taken. Fames dimension in all the video is 256x256.number of frames in all the videos are different.
In the first phase of testing, a text data of 1 KB size is taken and hidden by applying the proposed algorithm. In order to check the effect of the data hiding in the quality of the stego frames performance measure like PSNR (Peak signal to noise ratio) and MSE (Mean squared Error) are computed. For MSE computation, following formula is used-

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

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

In this formula,

I= Original host Frame

I'= Stego Frame

M= Number of rows in original frame.

N= Number of Column in Original frame.

From the above formula it is clear that the value of this measure must be as less as possible. 0 value of MSE represent zero distortion in the stego frames as compared to the original frame. A good steganography must be able to produce less distortion in the stego video.

For computing the PSNR measure, following formula is used-

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

Here

P= Maximum pixel value in the frame.

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

The value of MSE for zero distortion stego frames or video is zero and hence the PSNR is infinite for the zero distortion frames or video.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

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

Here above table describes comparison of PSNR and MSE. Lower the value of MSE gives us high PSNR. higer In order to test how the quality of the stego video is affected with different capacity of payload i.e. text data. Similar test is performed by taking different capacity of pay load.
Practically there are always some distortion in the stego frames as compared to the original frames and hence the value of PSNR must be as high as possible.

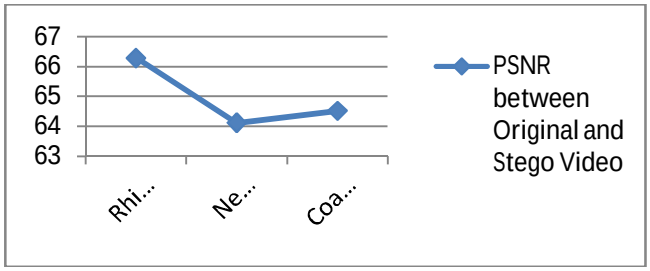

Figure 5: PSNR Comparison Graph Between Original and Stego Video

Figure **5** Above graph shows the comparison of PSNR at different inputs.

Computed PSNR and MSE values for all the three different videos for the text size of 1 Kb is tabulated in the table 1.

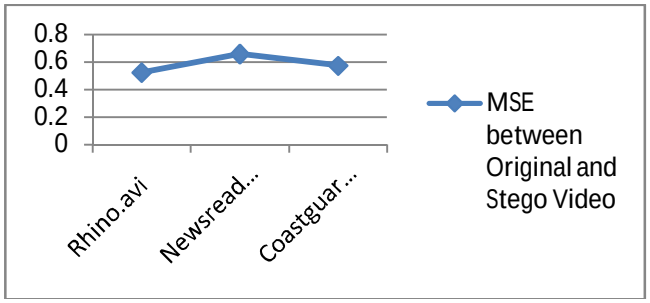

Figure 6: MSE comparision Graph Between Original and Stego Video

Higher values of PSNR and Lower values of MSE clearly shows that the proposed algorithm is very good at producing least distortion.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

VI. CONCLUSION

In general, steganography is used to transfer secret information in communication system. In this paper, a video steganograpgy method has been developed to transfer the secret data. Text, image, audio and video can be taken as the secret data which can be hidden in the video clips. In this scheme, though, least significant bit method is used for data hiding. LSB method of data hiding is not secure method for data hiding therefore in this method random frames selection algorithm and pixel swapping algorithm is incorporated to enhance the security of this method. Moreover the data itself is encrypted before embedding operation to make this system more secure. Both the modification in the existing method enhanced the security.

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

Here, Video (Rhino.avi) is taken to send data and by comparison we get the result of PSNR according to text size taken.

Table 3: 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**
Newsreader.avi	64.1126	0.6572	1kb
	64.7750	0.6689	2kb
	63.1972	0.6991	3kb
	63.8849	0.7110	4kb

Here, Video (Rhino.avi) is taken to send data and by comparison we get the result of PSNR according to text size taken.

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

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 4, April 2016

Here, Video (Rhino.avi) is taken to send data and by comparison we get the result of PSNR according to text size taken. Computed PSNR and MSE is tabulated in table2, table3 and table 4 for different video.

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.