A Novel Video Steganography Algorithm for Secure Data Hiding

Iti Naidu, Prof. Deepak Kumar Xaxa

[1]M.Tech. Scholar, CSE Department, MATS University, Raipur
[2]Professor, CSE Department, MATS University, Raipur

---***---

Abstract - *Unprecedented increase in the use of internet has made it possible for the person to send the information from one corner of the world to the another corner of the world. Not all the information is for all the people in the internet. Some of the information are very crucial and confidential and is intended for a particular person. These information need to be protected before sending it to the internet. Anybody can steal such kind of information or data and use it to serve their own purpose. Steganography is one of the efficient method to protect the data inside the innocent file. This paper present very efficient and secure data hiding techniques for sending the crucial information online.*
Scrambling operation on the pixel and on the frames are applied to make the system more secure. Experimental results shows the efficiency and security of the proposed data hiding techniques.

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

INTRODUCTION

From the last two decades, the life style of the people in all over the world has changed dramatically due to the widespread of the internet and emergence of on line services. It is now possible for the people to avail all most all the public services by using their finger tips. Shopping, railway reservation, banking and money transfer etc services are now online. Apart from this, the emergence of the social networking site like face book, twitter , Watsup etc has made it possible for the people to be in touch with each other 24 hours.

With the widespread application of the internet all over the world, it is now possible for the whole world to exchange the information very rapidly from one corner of the world to the other corner. Though this advantageous on one hand but it has disadvantages also. Since the internet is open to all, anybody can access the data transmitting through the internet. Last decades, fraud cases in internet has increased significantly which shows that there are so many loop holes in the internet and the data security is of prime concern for the use of internet. There are so many groups and so many people are 24 hors eying on the internet to steal the confidential data and in so many cases they are reported to be successful in breaching the security and getting the confidential data[1].

So internet is good place for the information interchange and very insecure place for exchanging the information. So it is very essential to design and develop some kind of system or algorithm which can be used in insecure internet for exchanging the information.
Two most feasible solutions to this problem is cryptography and steganography[2].

In steganography, confidential data is embedded inside the host object in such a way that nobody can detect the presense of the data inside the host object. In steganography, ant video, audio and text file can be used s the host file[1].
Cryptography, on the other hand uses the different approach to secure the data. In cryptography, data is jumbled in such a way that it become difficult to decipher the data. Jumbling the data is known as the encryption and the reverse of this is called the decryption[3]. Though both the techniques are basically designed to fight the insecurity of the data but both the techniques are different in their execution. Cryptography jumbled the simple data and make it difficult to decipher while on the other hand steganography, hide the information inside the host object making it difficult for the unauthorized person to even know the existence of the secret data[4].
Video steganography is a kind of steganography in which the host file is any video file i.e. secret data is embedded in side the video file.
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].

related work

Video file is basically composed of the still images otherwise known as the frames. So Video steganography can be considered as the extension of the image steganography.
Most wide spread used algorithm for steganography is Least significant bit(LSB) method. In this method, first of all the host file (Text/audio/video/image) in converted in to a 8 bit value. Then the least significant bit(LSB) of this 8bit value is used for embedding the information or secret bit. Least significant bit (LSB) method can also be used with the video as well i.e. in video steganography. In such cases, video is converted in to a frames and 8 bit pixel value of each frames can be used to embed the secret information bit[5],[6],[7].
It is most simple method of steganography and need very low computational power but secret data in this method can easily be destroyed by some file transformation operation. Apart from this least security is also one of its disadvantages.
Another most widely used techniques of steganography is spread spectrum technique on which more research work is going on for improving the performance[7][8].
Robustness is one of the advantage of this method.Moreover this method is almot geometric transformation proof. Strong security is alos one of its advantage[8].
Multi-dimensional lattice structure based steganography method is also one of the noteworthy contribution. This method s known for high data embedding rate and high payload capacity. This is possible in this method by changing the quantization level [9].
Wang, in the year 2002 suggested a Steganography method[10] based on the discrete cosine transform (DCT). It is high eapacity data hiding technique. DCt coefficients of the I-frames are used for embedding the secret information.
Hideki noda in the year 2004 proposed steganography method which was designed for the wavelet lossy compressed video. The payload capacity of this method is also high. In this method BPSC algorithm is also applied for embedding the secret information. Experimental results reveals its high efficiency.
Another noteworthy contribution came in the year 2007 when Lane suggested vector embedding method for data hiding[12]. This algorithm is designed for MPEG-I and MPEG-II standard.
Steganography method for AVI video format was proposed in the year 2007 by R. Kavita[13] in which swapping method is used for embedding operation. This paper also compared the performance of the JPEG steganography with the AVI steganography method. Low payload capacity of this method is one of its drawback.
In the same year 2007 Yueyun Shang presented a invertible data hiding algorithm[14] for compressed video.
This method is useful for MPEG (motion Picture expert Group) standard. This is frequency domain scheme. Less complexity and lower visual distortion are the advantages of this method. The only disadvantage of this scheme is its low payload capacity.
In the year 2008, Amr A. Hanafy suggested another steganography model [15]. In this method, video stream is first converted to the frames and then each frame is pixel wise manipulated. In this method , secret information is segmented in to a block before embedding into a cover video. These blocks are then embedded in random location of the frames .
In this algorihm, embedding location is obtained by reordering the secret key which is shared by the sender and receiver. Re-ordering opearion is dynamic in nature and hence different for different video frames.

Methodology

Figure 2 shows the block diagram of the proposed methodology for this steganography model. It is clear from this block diagram that the overall methodology has two phase. The first phase of this methodology is designed to create the stego video i.e. for embedding the secret data in to a host file. Figure 3 shows the second phase of the methodology i.e. extracting the secret data from the host video.

Following are the algorithm steps for creating the stego video or in other words it is designed for embedding the secret data in to host file.

Step1 Input Host video to the steganography model.
Step2 Resize the video to the dimension 262x262 if required.
Step3 Convert the video in to a frames by applying the video to frames conversion module.
Step4 Input the key1
Step5 Input the key 2
Step6 Carry out the Random frame selection operation for embedding the secret information

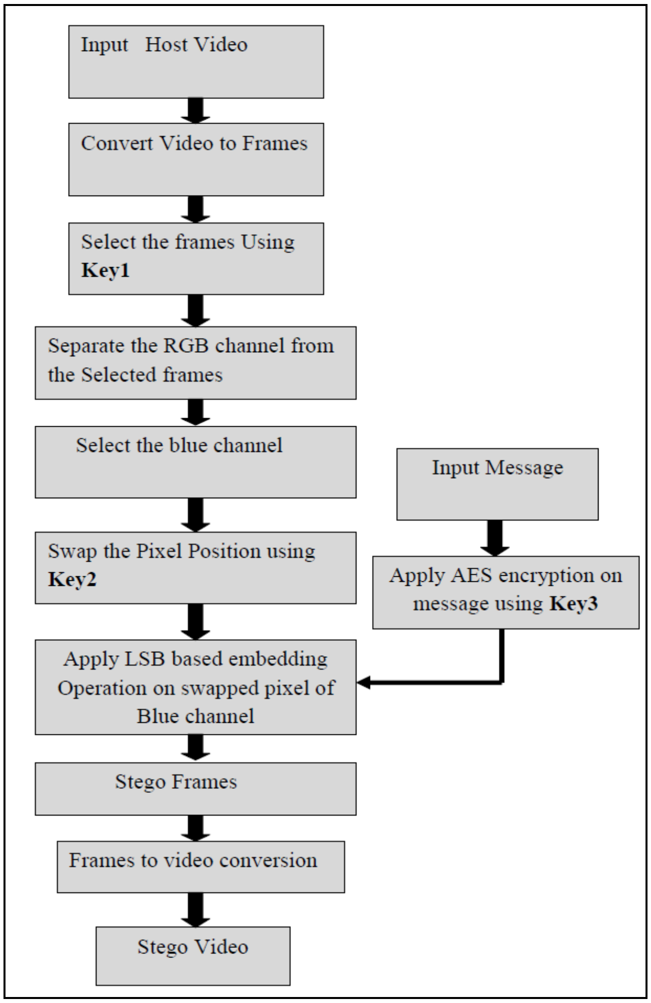
Input Host Video
Convert Video to Frames
Select the frames Using **Key1**
Separate the RGB channel from the Selected frames
Select the blue channel
Input Message
Swap the Pixel Position using **Key2**
Apply AES encryption on message using **Key3**
Apply LSB based embedding Operation on swapped pixel of Blue channel
Stego Frames
Frames to video conversion
Stego Video

Figure 2 Block Diagram of Proposed Video Stegnography Algorithm

Step7 By using Key1 Randomly select the frames for message embedding.
Step8 Separate the Red Green and Blue channel from the selected frames.
Step9 Select blue channel from each frames.
Step10 With the help of key 2 scramble the pixel position in the blue channel of each frames.
Step11 Enter the secret message.
Step12 Input the key3.
Step13 Apply AES encryption module to the system to encrypt the secret message.
Step14 Now with the help of LSB algorithm insert the secret information bit to the scrambled pixel of the selected frame and make it stego frame.
Step 15 Repeat these steps till the last bit of the secret message.
Step 16 Convert all the frames to the video again with the help of frame to video conversion module.

In this method, secret message in encrypted before embedding operation. Encryption is done with the help of AES encryption module. This step add extra security to the present steganography system.
For AES encryption module following steps are followed-
|Step1 Enter the secret message.
Step2 Arrange the message pixel in one dimensional vector form.
Step3 Activate the AES operation with the help of key3.
Once the above mentioned steps are carried out, stego video is generated. For getting back the secret message from the stego video, just reverse process is applied.

Flow diagram of extracting the message from the stego video is shown in the figure 3.
Following are the steps of the algorithm applied for extracting the secret message from the video.

Step1 Enter the stego video obtained in the Embedding phase to the system as input.
Step2 Apply video to frame conversion module for Getting the frames of the stego video.

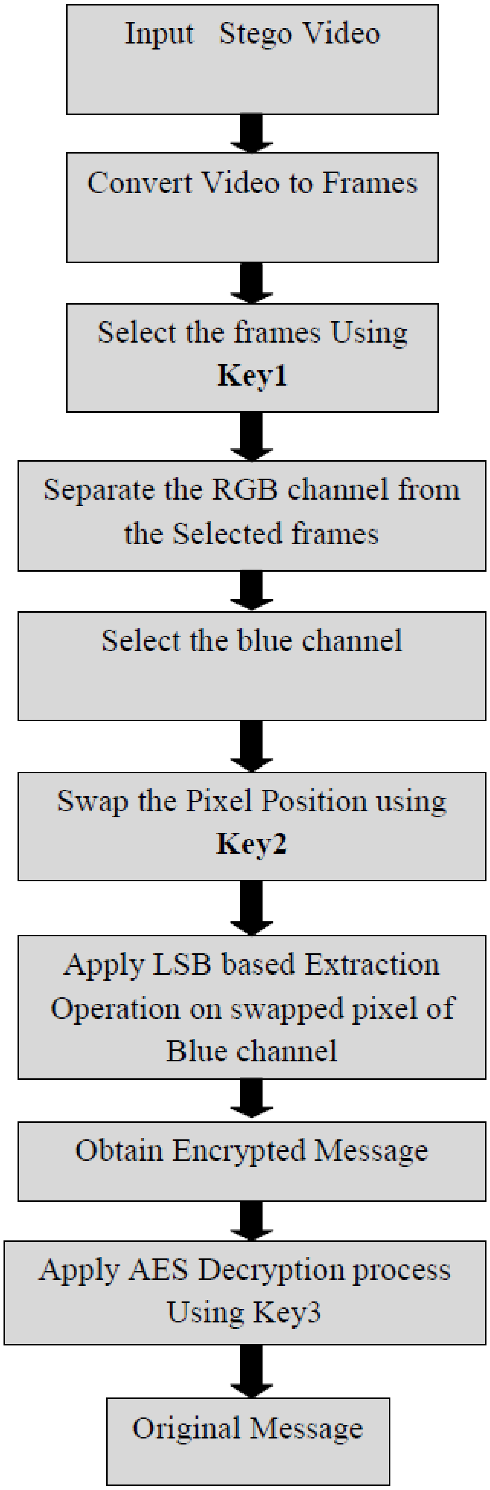
Input Stego Video
Convert Video to Frames
Select the frames Using Key1
Separate the RGB channel from the Selected frames
Select the blue channel
Swap the Pixel Position using Key2
Apply LSB based Extraction Operation on swapped pixel of Blue channel
Obtain Encrypted Message
Apply AES Decryption process Using Key3
Original Message

Figure 3 Message Extraction process

Step3 Input the Key1 to the system for selecting the frames randomly.
Step4 Separate all the three channel i.e. R,G,B from the stego video.
Step5 Select the blue channel from each frames.
Step6 Input the Key2 for pixel scrambling of chosen blue channel of each frames.
Step7 Apply LSB module to extract the message bit from each selected pixel.
Step8 Arrange these pixel to form a secret message in encrypted form.
Step9 Apply AES Decryption module to decrypt the secret message.

This algorithm uses random sequence generator to produce random number of predefined value which is used as the index for pixel scrambling operation and frame scrambling operation.

For frames scrambling operation and pixel scrambling operation two keys i.e. key1 and key2 are used. Random number generator number generate the random number of predefined values with the help of these keys. By changing these keys random number generator , generate the different random number. So by performing this operation, this method can be made more secure. Moreover, the secret information is also encrypted before embedding which also enhance the security of the system even more. In order to extract the secret information, it is necessary for the person to know all the keys. If any one of the keys in unknown then it is impossible to get back the original secret information.

Experimental Result

For validating and checking the efficiency, payload capacity and the security of the proposed video steganography model, a simulation program is developed as described in the previous section. MATLAB is used as the platform for designing this system. This model is tested for 15 and more different videos. Some of the videos are standard video while some other videos are either self made or downloaded from the internet. All videos are resized to the dimension 256x256. The length of the videos are different and hence give different number of frames after converting video in to frames.

Secret data of size 1 KB is used for hiding in the stego video by using proposed method.

In order to test the effect of the embedded data on the quality of the stego video, some statistical parameters like PSNR (Peak signal to noise ration) and MSE (Mean Square Error) are also computed with the help of following formula-

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

In this formula,

I= Original host Frame

I'= Stego Frame

M= Number of rows in original frame.

N= Number of Column in Original frame.

For PSNR

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

Here

P= Highest pixel value in the frame.

From the formula of MSE it is clear that the value of the MSE must be as low as possible.

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

Zero value of the MSE represents the zero distortion in the stego video. It means the quality of the video is same as that of the original video. A video steganography algorithm which produce least distortion in the stego video is considered as the good video algorithm.

It is evident from the above discussion that PSNR and MSE values are inversely proportional. Zero MSE and highest PSNR (Theoretically infinite) represent zero distortion in the stego video. So for zero distortion stego video, value of MSE must be equal to zero or PSNR must be equal to infinite or as musch 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

Table 2, table3 and table4 represent the effect of different payload (i.e size of secret data) on the quality of the stego video stream. For this secret data of different payload capacity are embedded into the stego video and then PSNR and |MSE is computed between original video and the stego video. From the tables it is clear that by increasing the size of payload , PSNR, decreases while MSE increases because of increase in distortion in the stego video by increasing the payload capacity.

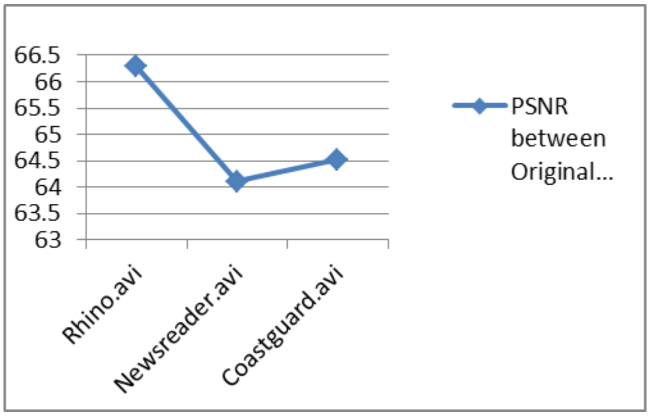

Figure 5 PSNR Comparison Graph Between Original and Stego Video

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.

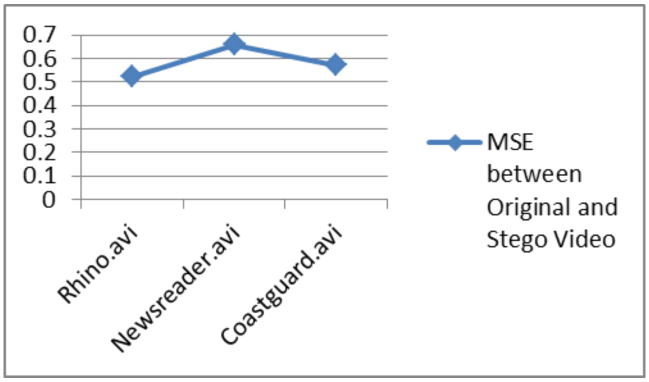

Figure 6 MSE comparision Graph Between Original and Stego Video

conclusion

Among all the techniques of sending the secret information from one place to other, steganography find important place. This paper suggest an efficient and highly secure video steganography algorithm for sending the secret data in the internet. Secret information that can be sent through this method can be any text material, audio, video and even in image form. This algorithm aplly LSB(Least significant based) method for embedding the secret data in to the host video file. Scranmbling operation in frames and among the pixel along with the use of AES encryption algorithm makes this method highly secure which is evident from the experimental values obtained. This method also produce least distortion in the stego video which is also of prime importance.

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
	65.9126	0.5290	2kb
	65.4914	0.5428	3kb
	64.1273	0.5861	4kb

Table 3 PSNR and MSE Comparison for different payload

Video	PSNR 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

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.