Enhancement of Data Security using Video Steganography

Mandeep Kaur
Research Scholar
GPCG Patiala, PB

Kanwalvir Singh Dhindsa, PhD
Professor (CSE)
BBSBEC, Fatehgarh Sahib, PB

ABSTRACT
Steganography is an approach used to transfer secret information by updating data carrying medium i.e video, audio, text file in an imperceptible manner and is a manner of masking secret data in ways that prevents revealing of hidden messages. By using steganography secure data transmission over internet could be achieved. Video files are generally a batch of still images. So, most of the techniques used for images and audio can also be applied in video steganography. The main advantage of video stream is amount of data they carry that cannot be easily detectable. Above all, it is a moving sequence of still pictures. The internet provides a method of communication to distribute information to the masses. With the growth of data communication over computer network, the security of information has become a major issue. Steganography and cryptography are two different data hiding techniques. Cryptography, on the other hand obscures the content of the message. In this research work a high capacity data embedding approach is developed by the combining two approaches LSB and DWT.

Keywords
Steganography, Data hiding, File Security, Frame Extraction, LSB, DWT.

1. INTRODUCTION

1.1 Steganography
Steganography is a technique to protect the hidden message from unidentified users. Steganography includes hiding important information (secret message) inside another medium i.e cover data. The Visual capabillty of humans is not strong enough to see the minor changes made in the cover medium. The carrier medium and data to be embedded can be of any form i.e audio, video, image and text. The rapid advancement in steganography techniques are dominating existing insecure steganography methods and making them obsolete. So, there is a need of more efficient steganography systems to be developed by cyber security experts that could work as shield against malicious users. The three important parameters that are observed for any successful steganography system: imperceptibility (small changes in cover medium that are hard to be detected by human eye in context of steganography), ingrained capacity, and stability against attacks [2].

To start with, ingrained capacity is aggregate of data to be sent masked by cover data. The stability, visual aspect and safety of stego are inversely proportional to embedding efficiency. Second, compromise with quality of cover and data as well as low modification rate leads to high embedding efficiency. The security of the steganographic scheme directly affected the embedding efficiency [3]. In previously used steganographic schemes, embedding efficiency and embedding payload are contradictory. Increased size of hidden data will decrease video quality ultimately reduces embedding efficiency. Embedding capacity and cover video quality are major issues to be discussed and resolved for secure communication. The deciding factors bridge gap between steganography algorithm and the legitimate user. To develop stable steganographic systems, various mechanisms are used such as hamming code, block coding, matrix encryption, BCH, Reed-Solomon codes, spatial domain techniques, Transform domain techniques and Bit Insertion [2,5,11]. Third, stability is a supplementary factor which measures the toughness of steganography method against attacks and threats [2,5].

2. STEGANOGRAPHY, CRYPTOGRAPHY AND WATERMARKING
Steganography and cryptography does not work alike. In cryptography the secret message to be sent is known as plain text. That is modified to a new form called cipher text using encryption algorithm and secret key. So that, only the intended user could read the message using same secret key by decryption. Whereas in steganography, secret message is wrapped inside the cover medium to form stego object to make it unnoticeable to intruders or attackers even though they are watching the same. Steganography is art of hiding data inside data.[1,7]

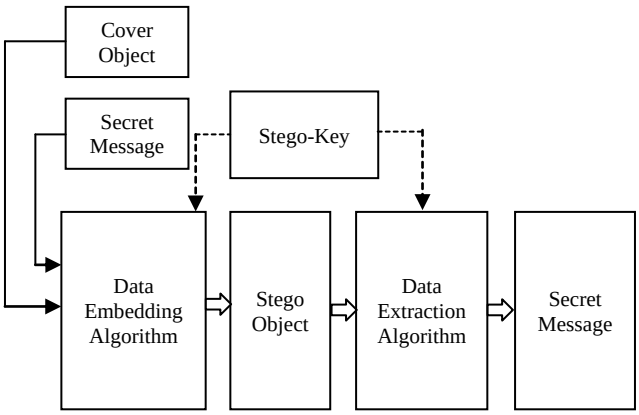

Fig.1: General model of the steganography method [16]

The one more technique which is basically analogous to steganography is the concept of digital watermarking. This technique utilizes a digital signal to be implanted inside the secret data. This digital signal becomes essential part of the data that cannot be removed and ensures evidence of authenticity. Watermarking is divided into two forms: visible watermarking and invisible watermarking. In visible watermarking, the inserted signal or watermark is visible on host data such logo, image or text written in different forms . In invisible watermarking, the inserted watermark cannot be seen. This is like steganography where embedded message is invisible. The significant differences between both techniques are: watermarking ensures ownership of host data and one to

many communication, whereas in steganography secret message can be understood by only receiver and this is one to one communication [7,16].

2.1 Video Steganography Techniques

Although different multimedia files are used as carrier to secure data over internet. But among all techniques, Video steganography has overcome many issues like imperceptibility, capacity, robustness. A video is a sequential arrangement of fast moving images and audio clips. Thus, it is very difficult for attackers to reveal secret data without analyzing every single frame of video. Using this technique, a natural property of human beings can be exploited Due to dynamic nature of the video, it reduces the chances of secret message detection in contrast with image steganography [6,18]. Video steganography is extension of image steganography, But there is significant difference between threats on both for example, lossy compression, formats update, increased or decreased frame rate, addition or deletion of frames during video processing. Above all, embedding capacity in video is very high [6]. There are various kind of techniques used for video steganography.

On basis of payload capacity, these are classified into following types [12,16].

1. Spatial Domain Techniques

2. Transform Domain Techniques

3. LITERATURE REVIEW

A literature survey is a study and scrutiny of the existing work in chosen area. It provides insight about the similarity of research idea with existing research work.

Reddy et al. [8] focused on providing undamaged data over web. By applying discrete wavelet transform, wavelet coefficients of both cover and payload are calculated. By considering only coacting band of payload, capacity of this method has been inceased. Performance parameters MSE, Entropy, Capacity are increased in contrast with PSNR.

Nag et al. [9] presented a technique for image steganography using 2-DWT. Discrete wavelet transform converts cover image from spatial domain into frequency domain. Auhtors focused on both capacity and security of secret data i.e hidden image. Quality of secret data is also maintained by preserving image wavelet coeffiecients in low frequency bands. Before embedding into cover image, by performing Huffman encoding sufficient secrecy is achieved.

Sherly et al. [10] discussed about a approach where all the process are executed in compressed domain using tri-way pixel-value differencing (TPVD) algorithm. I frames are used to store maximum scene change, whereas P and V frames are used store motion vectors having maximum magnitude. TPVD algorithm works on P and V frames by embedding data thus increases capacity. Imperceptibility is obtained by exploiting natural property of human eye that is sensitive to changes in smooth areas, whereas data is embedded into high magnitude motion vectors.

Rani and Senthoorpandi [11] figured out two major transform domain techniques. Authors concluded that DCT provides better security but reduced data capacity than spatial domain techniques. Whereas DWT decompose cover video into four frequency bands and maximum secret data is embedded into high frequency bands. Secret image quality is maintained by preserving smooth details of image into low frequency bands.

Baby et al. [12] proposed a new technique using discrete wavelet transform. Here, cover image is decomposed into three planes R,G,B. N-level decomposition is performed to split cover image and secret image upto N-level. Then some frequency components of both are combined to form stego image. Thus a multiple color image is embedded into single colour image to hide data. Thus High capacity and imperceptibility is is implemented due to randomly embedding data.

Prabakaran et al. [13] proposed a new method to hide high capacity secret image into low capcity cover image. Arnold transformation is used to scramble secret image bits before performing Discrete Wavelet Transform. After performing DWT on cover image, bits of cover and secret image are mixed using alpha blend operation. At receving end, IDWT is performed to get stego image. This method provides good quality and invisibilty

Suryawanshi and Belsare [14] developed a hardware approach to provide secure data transmission using LSB substitution and Lifting DWT. First of all, cover video is decomposed into frames then LSB substitution is done to embed secret image. Thus increases payload capacity. For compression, Lifting DWT is used to increase security. Finally, the whole process is implemented on FPGA hence reduces computational time..

Jenifer et al. [15] proposed LSB approach for video steganography to Embed secret images. This method improves the visual quality of secret images.This new video steganography method has many advantages such as user friendliness and simple method of processing images. Security is also increased.

4. ENCODING AND DECODING PROCESS

The major objective of this work is to establish a protected system that could provide enough security during data transfer from source to destination. Proposed method consists of encoding and decoding process.

4.1 Encoding Process:

First of all read video. Extract frames from video. Select random frames and compress them using DWT domain. Convert secret image into binary form that is to be embedded into video frames. Secret image is embedded into compressed frames using bit-ex-oring.

Step 1: Read cover video and secret image (S) of N*N size .

Step 2: Decompose video into frames and select random frames to embed secret image.

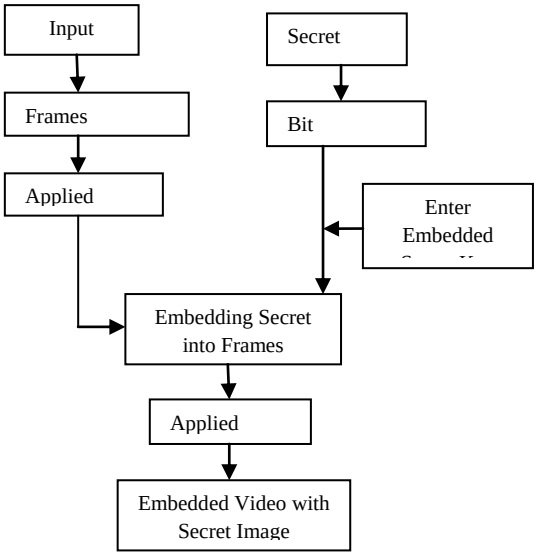

Fig.2: Encoding Process

Step 3: Compression of Video Frames File

Compression technique DWT is used for the compression of video file. This method easily compresses video without distorting original video. After that, encryption is done to enhance the security and to ensure safety from attackers.

Step 4: Read Secret Image. By providing full path in MATLAB command window, secret Image is selected. Convert secret image pixels to binary numbers. Binary numbers are easily embedded into any file.

Step 5: Generate Secret Key and Embed Secret Image

Generate secret key for embedding secret image into video file. The binary numbers of image will be embeded into compressed video frames using bit-exoring.

Step 6: Reconstruction of Video File

After embedding secret image into video, reconstruct the video by IDWT (inverse discrete wavelet frames) to form stego video. This reconstructed stego video contains secret data.

4.2 Decoding Process:

Decoding is actually reverse process from encoding. During decoding video with secret image is received. Steps for decoding process are:

Step 1: Receive video with secret image, Secret key is retrieved which is same as used for encoding process. Decompose video into frames.

Step 2: Embedded Data Retrieved

Apply IDWT to reconstruct compressed video frames. Using extraction key, retrieve the secret image from random frames of video.

Step 3: Restore the Original image after conversion.

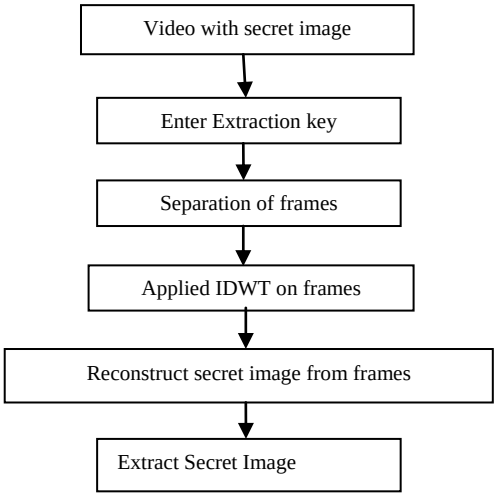

Fig 3: Decoding Process

Afterward compiling, the embedded image as well as the secret data is retrieved at the end of the process. Original image and embedded image together are duplicated but decoded secret image and original image will remain same and variations cannot be easily detected by human eye.

5. RESULTS

The results of this improved approach led to important conclusions. This method mainly relies upon DWT_LXOR, an effort is made to develop a better method then existing methods. Two performance parameters PSNR and MSE in order to evaluate the performance of this new method.

Fig. 4 : Basic GUI Design

Fig. 4 shows the basic GUI design. Two axes, two edit boxes and four buttons are used for implementation. It shows the method for inputting video on axis '1' with Select video button. After clicking on SELECT VIDEO button, folder with different videos will open; select a video for hiding secret image.

Fig. 5 given shows the extracted image on 2nd axes box, extraction and embedding keys must be same otherwise program will show error. Secret key is actually a password to open hidden data that means data is password protected. It also shows PSNR and MSE Value in Edit Boxes as calculated.

Fig. 5: Extracted image showing PSNR & MSE

Fig. 6 given below shows the PSNR graph. PSNR is peak signal to noise ratio. PSNR should be more for better performance. In this graph y-axis represents no. of images and x-axis shows calculated PSNR for respective image. Average PSNR calculated in new method is 67.76.

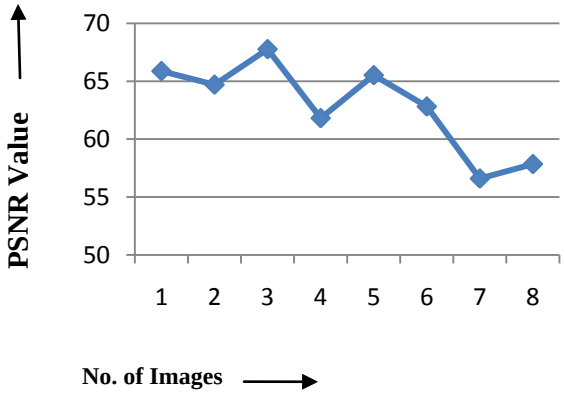

Fig. 6 : PSNR Graph

Fig.7 given below shows MSE graph. MSE is mean square error.MSE must be minimized to get better performance. Here, X-axis represents MSE and Y-axis represents different images. In new method error rate is reduced to 0.010966.

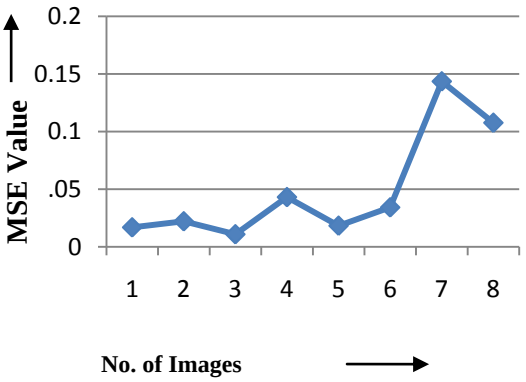

Fig. 7 : MSE Graph

Here, PSNR and MSE are varying for some images due to noise in images. Calculated PSNR ad MSE for different images is given in table 1.

Table 1:Calculation of PSNR & MSE values

No. of Images	PSNR value	MSE value
Image 1	65.8712	0.016957
Image 2	64.6984	0.022215
Image3	67.7642	0.010966
Image 4	61.81	0.043199
Image 5	65.5181	0.018394
Image 6	62.8136	0.034286
Image 7	56.5943	0.14357
Image 8	57.8434	0.10768

As shown above in Table 1 PSNR & MSE are varying i.e. getting low and high for different images. This variation is due to noise in images. Noise can be removed by applying filters to improve performance. The average PSNR of this method is 67.7 that is much better as compared to other techniques given in [19].

6. CONCLUSION

Implementation of DWT_LXOR for hiding secret image into video is a new technique and it is found that results i.e. secret images (original image) and extracted image are same. It is concluded that DWT using filters (high pass and low pass) which increase capacity, security, Imperceptibility and decrease noise. In this method secret key is generated for embedding which provides larger secrecy. It shows that the results achieved by combining both DWT_LXOR techniques are better than using Bit-exoring technique alone. Also the new technique which is now implemented is more secure and robust than previous implemented technique. In Future, This method can be extended to embed secret video inside video and text as well. Different video formats can also be used to embed secret information. Some other performance parameters can also be taken to check effectiveness of system

7. REFERENCES

[1] R. Kumar, J.Singh "Understanding Steganography over Cryptography and Various Steganography Techniques" International Journal of Computer Science and Mobile Computing, Vol. 4, Issue. 3, pp.253 – 258, 2015.

[2] R. J. Mstafa, K. M. Elleithy, E.Abdelfatteh "Video Steganography techniques:Taxonomy, Challnges and Future Directions" IEEE Conference on System Applications and Technology (LISAT). Long,pp-1-6, Farmingdale, NY, USA.

[3] W. Jyun-Jie, C. Houshou, L. Chi-Yuan, and Y. Ting-Ya, "An embedding strategy for large payload using convolutional embedding codes," 12th international conference on ITS Telecommunications, pp. 365-369,Taipai, Taiwan, 2012.

[4] R. Zhang, V. Sachnev and H. Kim, "Fast BCH Syndrome Coding for Steganography," In Information Hiding.vol. 5806, S. Katzenbeisser and A. R. Sadeghi, Eds., ed: Springer Berlin Heidelberg, pp. 48-58, 2009.

[5] R. J. Mstafa and K. M. Elleithy, "A high payload video steganography algorithm in DWT domain based on BCH codes (15, 11)" International IEEE Conference on wireless telecommunications symposium, pp.1-8, Newyork, America, 2015.

[6] R. J. Mstafa and K. M. Elleithy, "A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes" International journal of Multimedia Tools and Applications, Vol. 75, pp. 1-23, 2015.

[7] S. K. Dubey and V. Chandra "Steganography Cryptography and Watermarking: A Review" International Journal of Innovative Research in Science, Engineering and Technology, Vol. 6, Issue 2, pp.2595-2599, February 2017.

[8] H. S. M Reddy and K. B. Raja. "High capacity and security steganography using discrete wavelet transform." International Journal of Computer Science and Security (IJCSS), Vol. 3, Issue.6, pp.462-472, 2009.

[9] A. Nag, S. Biswas, D. Sarkar and P. P. Sarkar. "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding" International Journal of Computer Science and Security, Vol. 4, Issue.6, pp.561-570, 2011.

[10] Sherly A. P. and P. P. Amritha. "A compressed video steganography using TPVD." International Journal of Database Management Systems, Vol. 2, No.3, pp.67-79, August 2010.

[11] M. S. Rani and L. Senthoorpandi "A Study on Video Steganography using Transform Domain Techniques" 5th National conference on Computational Methods, Communication Techniques and Informatics, Vol.1, pp.257-260, Gandhigram, Dindigul, India, 2017.

[12] D.Baby, J.Thomsa, G.Augustinea, E. Georgea, N.R.Michael "A Novel DWT based Image Securing Method using Steganography" International Conference on Information and Communication Technologies,pp.216-218,Kochi, India, 2015

[13] G. Prabakaran, and R. Bhavani. "A modified secure digital image steganography based on Discrete Wavelet Transform." International Conference on Computing, Electronics, Electrical Technologies pp. 1096-1100, Kumaracoil, India, 2012.

[14] D. B. Suryawanshi and S. S. Belsare "An Efficient Implementation of Video Steganography on FPGA using DWT and LSB Algorithm" International Journal of Scientific & Engineering Research, Vol.7, Issue.5, pp.450-453, 2016.

[15] K. S. Jenifer, G. Yogaraj, K. Rajalakshmi "LSB Approach for Video Steganography to Embed Images" International Journal of Computer Science and Information Technologies, Vol. 5 , pp.319-322, 2014.

[16] Disha and K.Saini. "A review on video steganography techniques in spatial domain" IEEE Conference on Recent Developments in Control, Automation & Power Engineering , Noida, India, 2017.

[17] S. Kamesh, K. Durga Devi, S. N. V. P. Raviteja " DWT based data hiding using video steganography" international journal of engineering sciences & research technology, pp.361-367, 2017.

[18] M. Ramalingam & N. A. Mat "A steganography approach for sequential data encoding and decoding in video images" International Conference on Computer, Control, Informatics and Its Application, pp.120-125, Indonesia, 2014.

[19] H. Almara'beh "Steganography Techniques - Data Security Using Audio and Video" International Journal of Advanced Research in Computer Science and Software Engineering Volume 6, Issue 2, pp.45-50, February 2016.SW

[20] R. Singh and K. S. Dhindsa "Critical Path Based Ant Colony Optimization for cloud Computing using meta heuristic approach", International journal Research in Electronics and Computer Engineering, Vol.5, No.4, pp.225-230, 2017.

[21] K. K. Jassar and K. S. Dhindsa "Comparative Study and Performance Analysis of Clustering Algorithms" International Journal of Computer Applications (0975 – 8887), pp.1-6, 2015.