An Advanced Approach for Motion Video Steganography Using LSB Technique

Megha Patel[1], Kalpesh Patel[2]
[1]Student LCIT, Bhandu, India, [2]Assistant Prof. LCIT, Bhandu
[1]Computer Engineering Department
[1] LCIT, Bhandu, India,

Abstract: *Need of hiding information from intruders has been around since ancient times. Nowadays digital media is getting advanced like text, image, audio, video etc. To maintain the secrecy of information different methods of hiding have been evolved. One of them is Steganography which means hiding information under some other information without noticeable change in cover information. Video Steganography is the technique of hiding some covert message inside a video. In these paper work on improve data hiding capacity using video Steganography and use motion vector here for hiding data using LSB approach for hide text data. Using proposed system to improve images accuracy, embedding capacity. To enhance more security each bit of secret frames will be stored in covered frames. That are achieves good images quality when compared with existing method.*

Keywords: *Steganography, Motion vector, LSB*

1. INTRODUCTION

"Steganography is hiding a secret message within a larger one in such a way that others cannot discern the presence or contents of the hidden message". The Steganography term is deducted from the Greek words "stegos" implying "cover" and "grafia" implying "writing" and literally means "Cover writing".

Security is the major concern now a day since number of internet users is increasing and secret information is getting shared every second. This has also hiked the cyber crime and threat of malicious access. The two main techniques that are used for information security are Steganography and cryptography. Cryptography is basically secret writing; on the other hand Steganography is data hiding. Any Steganography technique must satisfy a no of requirements- the integrity of the secret message which is embedded in stego-object must be accurate; the alteration in the stego-object should not be detected by the naked eye; choice of stego-object must be dependent on the size of secret message to be hidden and last but not the least we must always presume that malicious person knows that Steganography is being used (that the stego-object is carrying some secret message).

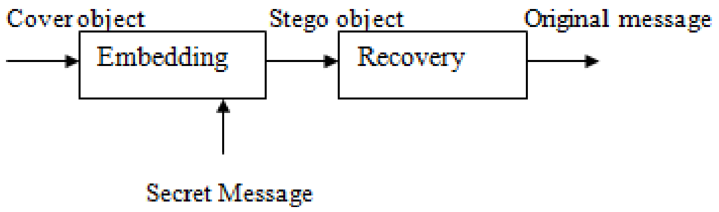

Fig.1 Block diagram of Steganography

- **Video Steganography: -** In video Steganography, video is used as cover object. Since videos are basically aggregation of images and sounds, that is why many of the techniques can be implemented on video files also. The advantage of concealing secret information in video is the fact that it is a moving flow of images and sounds and a large amount of information can be concealed inside a video. Any noticeable change might remain unobserved by humans because it is an uninterrupted flow of information. AVI (Audio Video Interleave), MPEG, and MP4 etc. are the file formats for video which are used.[8]

The Steganography systems consist of following elements:

- **Cover Object:-** In Steganography, the cover objects are those in which we hide secret message. The cover object can be images, audio, videos, text. The most used cover object for hide information is image.
- **Secret Message:-** In Steganography, the secret message is the message to be hidden in cover object. The secret message can be images, text messages etc.
- **Stego Object:-** The stego object is generated after hiding the secret message in cover image. After that stego object is transmitted and then at receiver side processing is done on stego object to retrieve message from it. Secret message is

embedded into cover object using some embedding algorithms and it is extracted at the receiver side by reversing that procedure as shown in Fig.1.

Video Steganography use for information hides and transfer third party. The video data share so video compression is most important. The compression is most important because video data consume more memory, without compression video must be compressed before it is encrypted, transmitted, stored or put up on the web. There are two types of compression (1) Lossy compression and (2) Lossless compression. Compression use for large file to small size compressed. Compress the video and then apply preprocessing. Preprocessing is unnecessary noise remove to data. Preprocessing is most important because noise remove to data and good quality of video and better result of video. The median filter apply so data unnecessary remove noise and good quality of data. The data encode and decode data properly so good output. The data is encrypted properly but decode is not properly so not output of data display. [8]

In video steganography embedding frame is most important. The embedding process in one content to another content data hides in one frame. Embedding capacity increase because maximum data embedd. In video Steganography embedding frame and deembedding frame is important .The embedding of data 3 bit LSB. embedding and de-embedding not properly so data loss. The least significant bit embedding are general Steganography technique that may be employed to embed data into a variety of digital media replacing least significant bits of digital data with message bits. For example, in the binary number: 1011100**1**, the **least significant bit** is the far right **1**

1.1 Motion Vector

Motion vector is the key element in the motion estimation process. It is used to represent a macro block in a picture based on the position of this macro block (or a similar one) in another picture, called the reference picture. Motion vector is technique of live video moment behind data fed using LSB approach. Motion vector is live movement or behind the frame save data .Third party is not the identify data so data is safe. Motion vector is basically work on macro model and patches. Patches is smallest element of the pixel. Motion vector basically in video frames current fame I as reference and second frame is i+1 upcoming frame using macro model pixel by pixel variation in term motion using magnitude value. Magnitude means weighted value and pixel value variation to data store and steady frame data is not change. The value is change so next i+1 change.i+1 frame is compare to i+2 fame and continuously moving or steady frame analysis and then movement on frame so data hide. The data is hide so not third party identify data.

1.2 Motion Estimation

The temporal prediction technique used in MPEG video is based on motion estimation. The basic premise of motion estimation is that in most cases, consecutive video frames will be similar except for changes induced by objects moving within the frames. In the trivial case of zero motion between frames (and no other differences caused by noise, etc.), it is easy for the encoder to efficiently predict the current frame as a duplicate of the prediction frame. When this is done, the only information necessary to transmit to the decoder becomes the syntactic overhead necessary to reconstruct the picture from the original reference frame. When there is motion in the images, the situation is not as simple.

Example of a frame with 2 stick figures and a tree. The second half of this figure is an example of a possible next frame, where panning has resulted in the tree moving down and to the right, and the figures have moved farther to the right because of their own movement outside of the panning. The problem for motion estimation to solve is how to adequately represent the changes, or differences, between these two video frames. [16]

2. Introduction LSB METHOD

The least significant bit (LSB) method is based on the fact that since most of the information in any message MSB rather than LSB, if one has to hide any information in video he has to done it by replacing the LSB with secret message bit. The LSB method is suitable to embedding process.

MSB	Sample	LSB table
000	i+1	3rd LSB
001	i+2	3rd LSB
010	i+3	2rd LSB
011	i+4	2rd LSB
100	i+5	1rd LSB
101	i+6	1rd LSB
110	i+7	1rd LSB
111	i+8	1rd LSB

Table 1: LSB Method

3. RELATED WORK

In [1] this paper encryption of compressed video bit streams and hiding privacy information to protect videos during transmission using H.264/AVC .To maintain security and privacy video needs to be stored and processed in an encrypted format. Here, data hiding is done directly in the encrypted version of H.264/AVC which includes the following three parts i.e,H.264/AVC video encryption, data embedding and data extraction. choas encryption is used to encrypt/decrypt the secret data before/after data embedding/extraction.

In [2] this paper the embedded data motion vectors which are gotten from the bouncing box might not have this element since object tracker utilizes a settled transfer speed. Inserting limit is expanded by a low threshold however the video quality is decreased.

In [3] this paper large amount of digital information such as video, audio or image is spread over the internet. So it should be a great challenge for all researchers to provide security to such a type of digital data. Also the piracy and copyright is emerging issue when digital information in the form of video, audio & image is transmitted over the transmission media. So to prevent the problem of piracy and security of digital data such as video, video watermarking techniques has been introduced. There are various watermarking schemes to give the security to videos but they were unable to provide the quality in terms of robustness and security

In [4] this paper simple and robust method of audio data embedding into videos. Robustness in this method comes because of the use of double coding mechanism. Here double coding means using two kinds of codes on the same data one after another. This provides more security and reliability to the hidden data into video. As security is the most important matter of concern in present data communication scenario, thus our proposed method provides satisfactory results. The method performed in wavelet domain by using pseudo random codes and morse codes. The performance of this method is evaluated by MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio).

In [5] this paper steganalytic approach against motion vector-based video steganography that does not depend on the detailed knowledge of embedding algorithms. In most state-of-the-art video coding standards, the motion vector is the result of block-based motion estimation using rate-distortion optimization. That is to say, each motion vector is locally optimal in a rate-distortion sense, and any modification will inevitably shift the motion vector from locally optimal to non-optimal. As a consequence, it is a very strong evidence of steganography if some motion vectors are found to be locally non-optimal. Based on this fact, the core of our method is an estimator to check the local optimality of motion vectors in a rate-distortion sense.

In [6] this paper detecting data hiding in motion vectors of compressed video and propose a new steganalytic algorithm based on the mutual constraints of motion vectors. The constraints of motion vectors from multiple frames are analyzed and formulized by three functions, then statistical features are extracted based on these functions. Moreover, we also incorporate calibration method to improve the detection accuracy

In [7] this paper, the same video sequences and SNR. The algorithm decreases the file size, but also decreases the embedding capacity.

4. PROPOSED WORK

According to analysis video security also play important role for area of data computing system so still round some issues related to PSNR, Embeddeding capacity, Quality of video etc so using proposed model to improve quality of video with high embedding capacity

4.1 Proposed System

The video steganography is hide message. The message is embedding and deembedding.

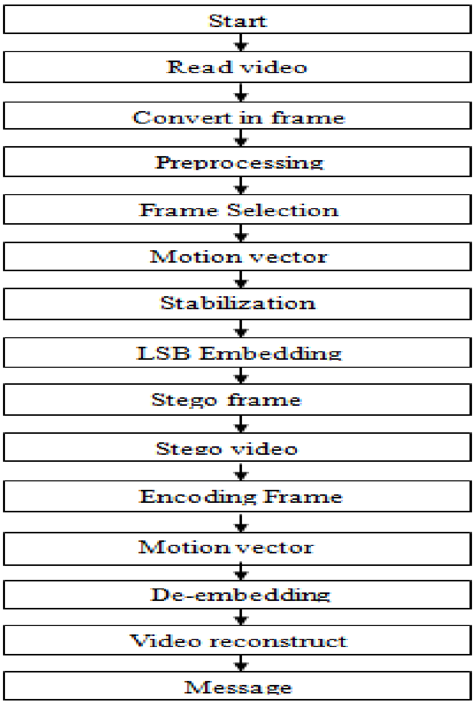

Fig.2 Data Embedding

Read the video from MATLAB and after it converts in frames. Preprocessing is use for unnecessary noise remove. Preprocessing after number of frame select which fames are use in embedding. Number of frame selection then motion vector apply to fame and identify motion analysis for calculate live movement. Apply stabilization use for live movement data not blur or destroy and proper way to retrieve after apply stabilization use embedding approach with last 3 LSB bit. Create stego frame and stego video. The stego video create then encoding frame. Motion vector apply previous motion movement find and apply deembedding approach for remove or extract message. Create video of reconstruct video and create message.

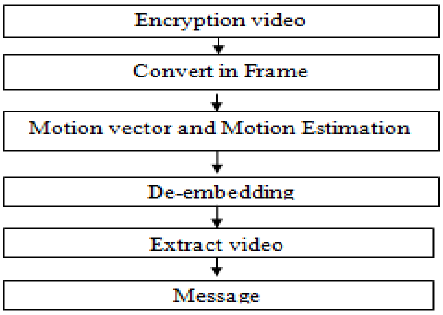

Fig.3 Data Extract video phase

The encryption video in convert in frame .The convert frame then motion vector and motion estimation process apply for reconstruct video. Motion vector is inverse process follow because retrieve the information motion estimation is apply for stady frame. Deembedding apply for fetch the content. Extract video and extract message

5. EXPERIMENTAL EVALUATION

Experiment of proposed method is executed on computer having Intel (R) Core (TM) i3-5200U CPU@2.20GHz with 4GB RAM having Windows 10 (64 bit) operating system and MATLAB 2017R . The LSB method is tested on video. The tested done is xylophone video. The message is embedding and deembedding. Our method is improved the PSNR value and embedding capacity.

Text	Motion Threshold	PSNR	MSE	SSIM	FSIM
Buzzword	1	40.1137	0.3100	0.9946	0.9955
Buzzword	2	40.6308	0.5947	0.9946	0.9951
Buzzword	3	38.2592	0.9691	0.9903	0.9919
Buzzword	4	37.7536	1.0585	0.9913	0.9927
Buzzword	5	38.4553	0.7219	0.9931	0.9942
Buzzword	6	44.5954	0.3935	0.9971	0.9977

Table 2: Threshold base parameter comparison

The buzzword text hides in to video and threshold value change so parameter value change. Threshold value is 6 so PSNR is 44.5954. Threshold value is important because good video quality and capacity.

Video	No of frames	Proposed Method	[1]	[2]`	[7]
Foreman	1-60	N/A	N/A	38.9	37.5
Container	1-60	N/A	N/A	42.40	37.12
Xylophone	1-123	44.20	N/A	N/A	N/A

Table 3: PSNR comparison

Video	No of frames	Proposed Method	[1]	[2]`	[7]
Foreman	1-60	N/A	N/A	112,586	43,801
Container	1-60	N/A	N/A	13,190	9,641
Xylophone	1-123	327,680	N/A	N/A	N/A

Table 4: Comparison of embedding capacity

In [1], [2] and [7] papers less embedding capacity and PSNR. The Xylophone video proposed method achieved PSNR 44.20 and embedding capacity achieved is 327,680. Our method is increases embedding capacity and parameters. The video quality good and parameter performance increase and also embedding capacity achieved.

- **PSNR chart comparison**

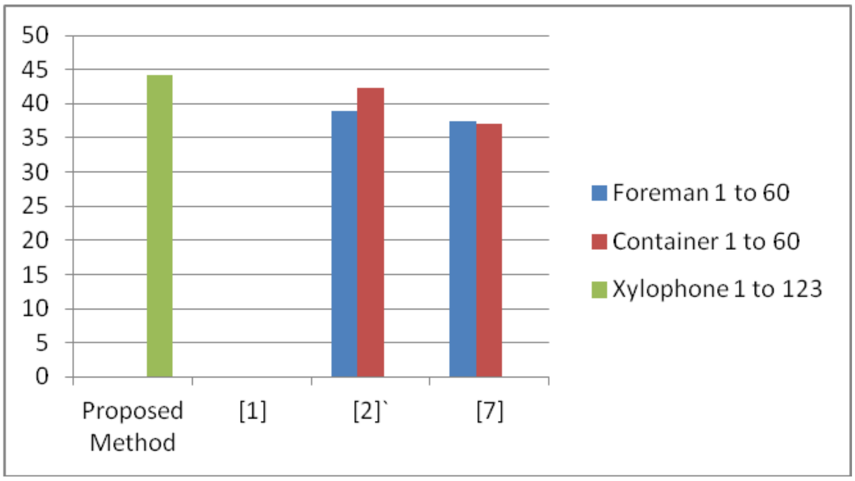

Fig 4: PSNR chart comparison

Show above the result achieves the good PSNR value. The 1-123 frames achieve the PSNR value is 44.20

- **Chart comparison of embedding capacity**

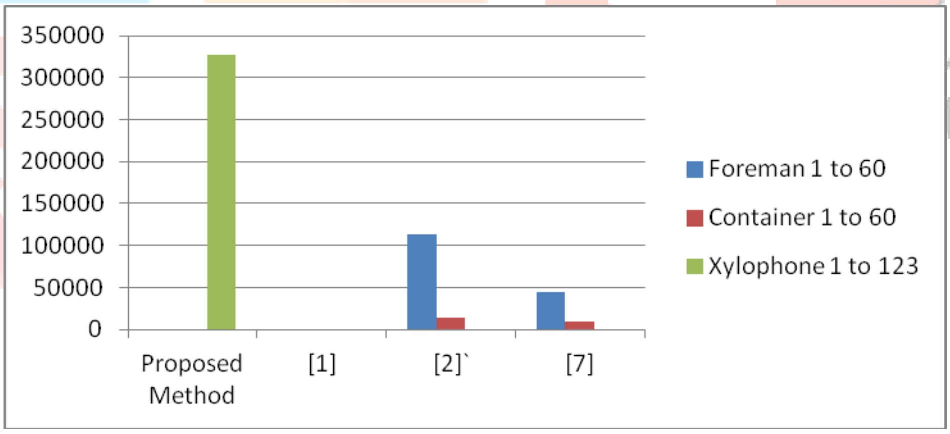

Fig 5: Chart comparison of embedding capacity

Show above the result achieves the embedding capacity. In [1], [2] and [7] papers less embedding capacity and PSNR. The Xylophone video proposed method achieved PSNR 44.20 and embedding capacity achieved is 327,680. Our method is increases embedding capacity and parameters. The video quality good and parameter performance increase and also embedding capacity achieved

6. CONCLUSION

According to literature analysis we found different algorithm for video steganography. The work on video steganography and also work on embedding capacity. Achieve high PSNR with embedding capacity as compare to exiting system. Motion vector is technique of live video moment behind data fed using LSB approach. Motion vector is live movement to save data. Third party is not the identify data so data is safe. Motion vector is basically work on macro model and patches.

7. REFERENCES

1) S. Lokesh, M. A. Bennet, N. Priya, D. Chitra, S. Karthika and K. Divyakanni, "An efficient security for privacy information through hiding data in encrypted compressed videobit streams," *2016 International Conference on Communication and Electronics Systems (ICCES)*, Coimbatore, 2016, pp. 1-8.
2) K. Rezagholipour and M. Eshghi, "Video steganography algorithm based on motion vector of moving object," *2016 Eighth International Conference on Information and Knowledge Technology (IKT)*, Hamedan, 2016, pp. 183-187.
3) N. A. Shelke and P. N. Chatur, "Optimized and hybrid based watermarking system for digital video security," *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, 2016, pp. 1068-1074.
4) S. Shakeela, P. Arulmozhivarman, R. Chudiwal and S. Pal, "Double coding mechanism for robust audio data hiding in videos," *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, 2016, pp. 997-1001.
5) H. Zhang, Y. Cao and X. Zhao, "A Steganalytic Approach to Detect Motion Vector Modification Using Near-Perfect Estimation for Local Optimality," in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 2, pp. 465-478, Feb. 2017.
6) X. Xu, J. Dong, W. Wang and T. Tan, "Video steganalysis based on the constraints of motion vectors," *2013 IEEE International Conference on Image Processing*, Melbourne, VIC, 2013, pp. 4422-4426.
7) M. Zhang and Y. Guo, "Video steganography algorithm with motion search cost minimized," *2014 9th IEEE Conference on Industrial Electronics and Applications*, Hangzhou, 2014, pp. 940-943.
8) S. Chauhan, Jyotsna, J. Kumar and A. Doegar, "Multiple layer text security using variable block size cryptography and image steganography," *2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT)*, Ghaziabad, 2017, pp. 1-7.
9) D. Xu, R. Wang and Y. Q. Shi, "Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution," in *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 4, pp. 596-606, April 2014.
10) M. N. Asghar and M. Ghanbari, "An Efficient Security System for CABAC Bin-Strings of H.264/SVC," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 23, no. 3, pp. 425-437, March 2013.
11) Huiyun Jing, Xin He, Qi Han, and Xiamu Niu, “Motion vector based information hiding algorithm for h.264/avc against motion vector steganalysis,” in Proc. Asian conference on Intelligent Information and Database Systems. 2012, vol. 8, pp. 91–98, Springer-Verlag.
12) Yuting Su, Chengqian Zhang, and Chuntian Zhang, “A video steganalytic algorithm against motion-vector-based steganography,” Signal Process, vol. 91, pp. 1901–1909, Aug. 2011.
13) Y. Yao, W. Zhang, N. Yu, and X. Zhao, “Defining embedding distortion for motion vector-based video steganography,” Multimedia Tools and Applications, vol. 74, no. 24, pp. 11 163–11 186, Dec. 2015.
14) Ramadhan J. and Khaled M. “A High Payload Video Steganography Algorithm DWT Domain based on BCH Codes (15,11)”. IEEE Wireless Telecommunications Symposium (WTS),pp. 1-8, 15-17 April 2015.
15) Yun Cao, Hong Zhang, Xianfeng Zhao and Haibo Yu, “Covert Communication by Compressed Videos Exploiting the Uncertainty of Motion Estimation”, IEEE Communications Letters, vol. 19, no. 2, February 2015
16) https://users.cs.cf.ac.uk/Dave.Marshall/Multimedia/node259.html