A Survey on An Advanced Approach For Motion Video Steganography Using LSB Technique

Megha K.Patel[1], Ujas S.Patel[2]

[1]*Student(Master of Engineering), Computer Engineering Department, Laljibhai Chaturbhai Institute of Technology (LCIT), Bhandu, Gujarat, India*
[2] *Assistant Professor, Computer Engineering Department, Laljibhai Chaturbhai Institute of Technology (LCIT), Bhandu, Gujarat, 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).

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.

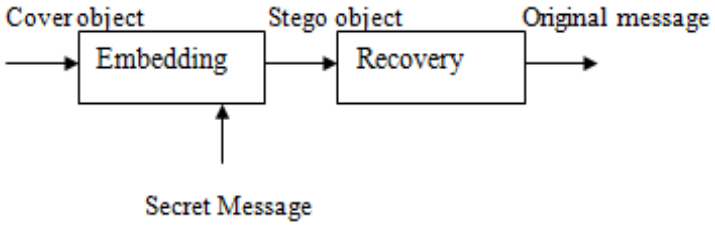


Fig.1 Block diagram of Steganography

- **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]

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.

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: 10111001, the **least significant bit** is the far right **1**

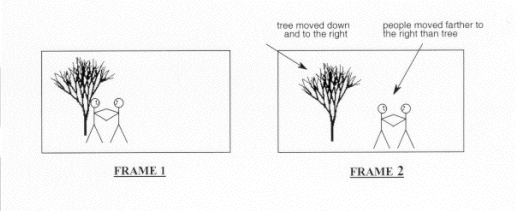
1.1 Motion Vector

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.[10]

Fig 2 shows an 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.



2. LITERATURE REVIEW:

2.1 An Efficient Security For Privacy Information Through Hiding Data In Encrypted Compressed Video bit Streams

- 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.

2.2 Video Security Protection Technology based on Shot Segmentation and Bit Commitment

- In [2] this paper video publishing in the public network is transmitted safely and recognized with liability, this study aims to provide a video feature extraction method based on shot segmentation, moreover video coding and tamper feature have been fully taking into consideration. Besides, the extraction data will be researched with bit commitment, and the tampered part of the video will be figured out through verifying the data of bit commitment. The sender can adjudge the liability of illegal video transmission through verify the bit commitment.

2.3 Optimized and Hybrid based Watermarking System for Digital Video Security

- 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

2.4 Double Coding Mechanism for Robust Audio Data Hiding in Videos

- 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).

2.5 A Steganalytic Approach to Detect Motion Vector Modification Using Near-Perfect Estimation for Local Optimality

- 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.

2.6 Video steganalysis based on the constraints of motion vectors

- 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

2.7 Efficient and adaptive switching error concealment method using neighboring motion vector statistics

- In [7] this paper combine two state-of-theart error concealment algorithms and Copy method, to adaptively deal with different lost MBs based on the surrounding motion vector statistics

3. COMPARATIVE TABLE:

Table -1: Comparative Table

Sr .No.	Paper Title	Method	Advantage	Disadvantage
1	An Efficient Security For Privacy Information Through Hiding Data In Encrypted Compressed Video bit Streams	H.264/AVC,Chaos encryption, Discrete cosine transform	H.264 is an industry standard for video compression, the process of converting digital video into a format that takes up less capacity when it is stored or transmitted..Chaos encryption is high level security provide.	The requirement of large cipher storage and slow in speed are considered the major disadvantages. Increase embedded payload while maintaining the robustness and low distortions.

2	Video Security Protection Technology based on Shot Segmentation and Bit Commitment[2]	Bit commitment, Shot segmentation, Discrete cosine transform,Tamper feature	Goodsecurity, Roubustness, Flexibility, very low frequency coefficients is recover original image.	The feature extraction method is Low. Grouping bit commitment is used to the features sending and receiving two side public key encryption for secret communication.
3	Optimized and Hybrid based Watermarking System for Digital Video Security[3]	Genetic algorithm, Discrete stationary wavelet transform, Principal component analysis, Singular value decomposition	highly secure, The provide the security & copyright protection to the video of small size.	The currently scheme is proposed for small Size AVI formatted. Improve PSNR value.
4	Double Coding Mechanism for Robust Audio Data Hiding in Videos[4]	Double coding, MSE, pseudo random code, Stegnography, DWT,Morse codes	The double coding method provides more security and reliability to the hidden data in to video	The concerned secret media is audio when this is extracted from the video, it will not be exactly same as the original embedded audio.
5	A Steganalytic Approach to Detect Motion Vector Modification Using Near-Perfect Estimation for Local Optimality[5]	Motion estimation, Motion vector, Steganalytic , Steganography	Better rate distortion. The steganalytic method performance and robustness is demonstrated. Detection accurancy	The Lossy compression is lost information. The problem of CSM can be largely alleviated, which indicates that our method is suitable to be used for blind steganalysis in situations where a very limited priori knowledge is available.
6	Video steganalysis based on the constraints of motion vectors[6]	Incorporate calibration, MV- based Steganography, Motion vector, Mutual constraints	The advantage of much less distortion to the visual quality of the reconstructed frames. MV is maintaining low distortions and robustness. High performance. Detecting data. We can find the constraints of these motion vectors easily	It is expected that the constraints of MVs may play a greater role in the future if we can find a better way to describe and measure the statistical changes of such constraints

7	Efficient and adaptive switching error concealment method using neighboring motion vector statistics[7]	Error Concealment Adaptive switch algorithm,Motion vector	Error concealment use information in the spatial/temporal neighborhood of the lost MB (Macro block) to recover the pixel information of the lost MB. Better performance. Time complexity	optimum choice of the modeling error threshold , Incorporate different encoding factors (e.g. DCT coefficients) into the decision process.

4. CONCLUSION:

The security is most important to data because third party not access data. So use video steganography is the technique of hiding some covert message inside a video. According to literature review analysis problem likes PSNR, Embeddeding capacity so in future quality of video etc so using proposed model to improve quality of video with high embedding capacity. Improve data hiding capacity using video Steganography and use motion vector here for hiding data using LSB approach for hide text data.

5. 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) P. Yu, Y. Wang, F. Duan and J. An, "Video security protection technology based on shot segmentation and bit commitment," *2016 9th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*, Datong, 2016, pp. 104-108.

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. 4422-4426.8)Bhavani Thuraisingham,"A primer for understanding and applying data mining". 1520 9202/00/$10.00©2000IEEE

7) W. C. Chen, T. L. Lin and H. C. Lee, "Efficient and adaptive switching error concealment method using neighboring motion vector statistics," *2013 IEEE International Symposium on Consumer Electronics (ISCE)*, Hsinchu, 2013, pp. 47-48.

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) J. Vimal and A. M. Alex, "Audio steganography using dual randomness LSB method," *2014 International*

Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kanyakumari, 2014, pp. 941-944.

10) https://users.cs.cf.ac.uk/Dave.Marshall/Multimedia/node259.html