A Review on Secured Video Steganography Techniques

Shekar R[1], Dr. Siddappaji[2]
[1] *M Tech Student, B.M.S College of Engineering, Bengaluru, India*
[2] *Associate Professor, B.M.S College of Engineering, Bengaluru, India*
(E-mail: shekarpvgd1234@gmail.com, siddu.ece@bmsce.ac.in)

***Abstract*—**Information Technology has growing day by day, so providing security to the secret information is also very important for secure communication between two trusted parties. In the field of computer networks, steganography is the well-known features of providing security. The secret information is hided into the carrier files: audio, image, text and video files. Video steganography is one of the growing technologies to transfer high data. The data hiding capacity of video is more compared to the other file formats. In video steganography data can be embedded in two different ways: Spatial domain and Frequency domain methods. This paper shows an investigation of various best in class of video steganography methods in spatial and frequency area created in previous decade which are extremely helpful for video steganography investigators to obtain good results, high data hiding capacity and security.

Keywords*—Video Steganography, Spatial Domain, Frequency Domain, Imperceptibility, Robustness, Hiding Capacity, Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE).*

I. INTRODUCTION

Information technology is growing rapidly, so usage of internet to transfer the user data is also increasing day by day. Providing security to the user data is also very important in the field of communication. When the data is exchanging between two users, there is a chance of attacks to misuse the embedded data. Steganography technology used to prevent this for secure communication. The hiding of secret information within a cover-file, so that other cannot identify the existence of hidden secret information is called Steganography [1], [11]. Fig 1 presents the General block model of steganography. Steganography originated from Greek word Steganos and Graphein. Steganos means secured and Graphein means writing. Depending upon the type of carrier file utilized to hide secret information, steganographic techniques are divided into Text, Audio, Image and Video steganography [9].

A. Text Steganography

In this steganography approach, the text document is used as a cover file to convey secret data inside it without decreasing the nature of content text document. The secret data such as text can be hidden and no other information's i.e. image, audio and video cannot be possible to hide in this method. This approach can be implemented by Format-based, Statistical-Generation, Random and Linguistic type.

B. Audio Steganography

In this steganography approach, by utilizing the concept of audio masking that is a secret audio signal can be masked with the unwanted noise signal. In the concept of audio masking presence of loud signal (unwanted noise signal) another weaker signal (low volume audio signal) is inaudible. Audio steganography can be implemented by: Low-bit Encoding and Spread-spectrum coding creating stego audio file, Phase-Encoding and Echo-hiding. Secret information such as text and image hiding is not possible in this technique.

C. Image Steganography

In this steganography approach, the image can be used as a cover image to hide digital information (text and image) inside it which generates stego-image. This technique can be accomplished by spatial-domain and frequency-domain algorithms. Very less data can be hidden into the image. More hiding of secret information causes the distortion of image which results in less imperceptible.

D. Video Steganography

This type of steganography approach is considered as the most authenticated type of steganography, since in video the more data can be embedded into the video frames. A video consisting of group of image frames and audio file. Therefore, the secret data (text and image) can be incorporated in to video (image frames) and an audio file of the video is masked with loud noise signal. Image and audio steganography techniques can also be connected to video steganography [8].

Currently video steganography is the most emerging technology because of the data embedding capacity is more in video steganography compared to other types. The hiding capacity, imperceptibility and robustness are three important parameters which are used to analyze the performance of video steganography.

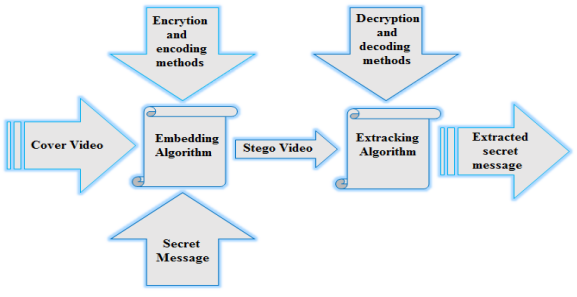

Figure 1: General block model of steganography [1]

TABLE I: Difference between Steganography, Cryptography and Watermarking [10]

Criteria	Steganography	Cryptography	Water marking
Carrier Object	Any media file	Text file or image	Digital Image or Audio
Secret Data	Text, Image, Audio and Video	Text	Watermark
Private Key	Optional	Required	Optional
Imperceptibility	Never	Yes	May be or may not be
Main Objective	Secure Communication	Protection	Digital Copyright
Security	Very high	High	High
Hiding Capacity	More	More	Less
Attacks	Steganalysis	Cryptanalysis	Signal processing operation

Section II presents the difference between Steganography, Cryptography and Water-marking. Introduction to Video Steganography techniques are explained in Section III. Section IV provides comparative study of Video steganography techniques. Finally, Section V draws the conclusion.

I. STEGANOGRAPHY VS CRYPTOGRAPHY AND WATERMARKING

The word steganography refers to the art of secured transfer of data communication. Steganography means data hidden within the other data file. The resulting output is known as stegogramme. Steganography is an encryption approach that can be utilized along with cryptography to provide extra-security to the system.

Cryptography or cryptology has originated from Greek word, Crypto implies hidden. Graphein intends to write or study. In cryptography the sender changes plain-text to cipher-text by using Encryption key and decrypts the cipher-text to plain-text at receiver by using the decryption key.

Watermarking is the approach of embedding binary data in to carrier-signal. This approach can be used in the copyright protection, video authentication. Digital watermarks are utilized to check the authenticity/reliability of the carrier-signal and also to indicate uniqueness of authorized owners.

TABLE. I presents the general comparisons and differences between steganography, cryptography, and watermarking methods.

II. VIDEO STEGANOGRAPHY TECHNIQUES

Steganography means implementation of covering secret information such as text, image and audio inside the carrier files such as text, image, Audio and Video. Video steganography is the extension of image steganography. Video is nothing but the group of image frames, so that information hiding in video is similar to hiding information in image. However, there are several aspects which distinct video steganography from image steganography. Video steganography method is dynamic that is video frames are changing from time to time, chances of attack is less and it is difficult to identify the secret information hidden inside the video file by the attackers. The data hiding capacity in the video can be more compared to other carrier files. There are two types of techniques utilized in video steganography to hide information, such as

A. Spatial Domain Steganography Techniques
B. Transform Domain Steganography Techniques

A. Spatial Domain Steganography Techniques

In spatial domain approach, embedding of secret messages will be done directly at pixel levels of carrier. The following are few important techniques such as Least Significant Bit (LSB), Most Significant Bit (MSB), Pixel Value Differencing and RGB (Red, Green, Blue) used to embed data in video steganography.

1). Least Significant Bit Steganography

The simplest and most standard spatial domain steganography method is Least Significant Bit (LSB) insertion technique. In this method secret information's are hided into carrier image by directly altering the Least-Significant-Bits. The carrier image is separated into number of pixels and each pixel is represented by 8 bits value which defines the color in each image. By changing the LSB bits in each of these color pixels, the secret data can be hided bit by bit without altering the color values of the image pixels too much. The altering of image color pixels too much leads to the image distortion. The advantage of LSB method is easy to understand and implement, high capacity, and can't be noticed by the naked eye. But it lacks robustness (Easy manipulation by attackers) and susceptible to noise [15].

2). Most Significant Bit Steganography

Most Significant Bit (MSB) Steganography is a minor change of the LSB steganography. In this scheme instead of altering the least significant bits, the most significant bits are altered. In this instance the embedded values are stored in the MSB bits of the image [13]. Easy to implement and also hiding capacity is more but lack of Robustness results in distortion or degradation of image.

3). Pixel Value Differencing Steganography

The Pixel Value Differencing (PVD) method utilizes modification between the successive pixels of an image to find out how many secret bits can be hided into carrier file. The secret data can be hided based on the difference between the pixel values, such that if the pixel's difference between two consecutive pixels is 5 bits then 5 bits of data can be hidden. So in PVD if there are more edges imply more information can have embedded into the file. This approach accomplishes more imperceptible outcomes compared with LSB and MSB based methodologies with the same data embedding capacity. The

PVD approach is more complex compared to LSB and MSB techniques [12].

4). Gray Level Modification

Gray Level Modification (GLM) steganography approach used to outline secret information by changing carrier image pixels gray values. In this approach the image used is a gray scale image. The information that is hidden in to the image should be in binary (0 and 1) data format. GLM steganography utilizes the possibility such as odd and even numbers for outlining the secret information inside an image [14]. This approach is very easy to implement and understand. It has more chances of attacks.

B. *Transform Domain Steganography Techniques*

In this domain of transformation, embedding of secret message requires transforming the video frames from spatial to frequency-domain by utilizing appropriate transform methods such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD).

1). Discrete Cosine Transformation

The Discrete Cosine Transformation (DCT), primarily utilized in image and video compression. DCT generally converts a video frame into its equivalent frequency domain partitioning video frame pixel matrix into blocks of size NxN, N depends upon the type of video frame. This approach helps to isolate the video frames into parts of differing importance. The Discrete Cosine Transform resembles the discrete fourier transform: it converts video frame from spatial to the frequency-domain. Generally, in order to achieve high robustness, the amount of secret message embedding can be reduced. The DCT is more robust technique to lossy compression and image visibility is protected. The drawbacks of this method are Block effect Picture cropping effect [2] [3]. Consider a frame of video 'A' which is of MxN is the size, two-dimensional DCT (2D-DCT) and the inverse 2D - DCT can be evaluated as [1]:

$$Bpq = \propto p \propto q \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} Amn * \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N} \quad (1)$$

$$Amn = \sum_{p=0}^{M-1}\sum_{q=0}^{N-1} \propto p \propto q\, Bpq * \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N} \quad (2)$$

$$\propto p = \begin{cases} \frac{1}{sqrt(M)}; & (p=0) \\ sqrt\left(\frac{2}{M}\right); & (1 \le p \le M-1) \end{cases}$$

$$\text{And} \propto q = \begin{cases} \frac{1}{sqrt(N)}; & (q=0) \\ sqrt\left(\frac{2}{N}\right); & (1 \le (q) \le N-1) \end{cases}$$

Here p, q are m and n transformations, M × N is the corresponding resolution. This method is highly robust but bit error rate is more.

2). Discrete Wavelet Transformation

First we know that the wavelet transformation is broadly utilized in image compression. Discrete Wavelet Transform (DWT) is usually a multi-resolution study of images such as video frames [4]. It converts the input video frames into the bands of low pass and high pass wavelet coefficients. In this approach the embedding of secret data is conceded in LL, LH, HL, and HH bands. It's been verified that the embedding of data in the only high frequency bands such as in HH bands provides the good PSNR values [3]. At first, the 2 Dimensional DWT decomposition such as low pass filter and high pass filter decomposition which is carried out for carrier video frames. This decomposes video frames into four sub bands: LL, LH, HL and HH bands. High- High is a high frequency sub band and Low-Low is a low frequency sub band. Low-High and High-Low are the middle frequency sub bands. Low-Low sub band is the quarter size of the compressed original image. Data hiding in only High frequency coefficients results in better PSNR values [1]. The 2-dimentional decomposition is shown in Fig. 2.

$$LowD(z)\, HighD(z) + LowR(z) = 2 \quad (3)$$

$$LowD(z) = z^{-k}\, HighD(-z) \quad (4)$$

$$HighR(z) = z^{k}\, LowD(-z) \quad (5)$$

Here *LowD(z)* and *HighD(z)* indicates the decomposition of the wavelet filters. *LowR(z)*, *HighD(z)* indicates re-establishment of the filtered wavelets. The advantage of DWT is it is more robust and imperceptible. The drawback of this method is that long compression time, noise/blur close to edge of image. Compared to DCT, DWT gives high PSNR values [3]. DWT has good robustness with moderate complexity.

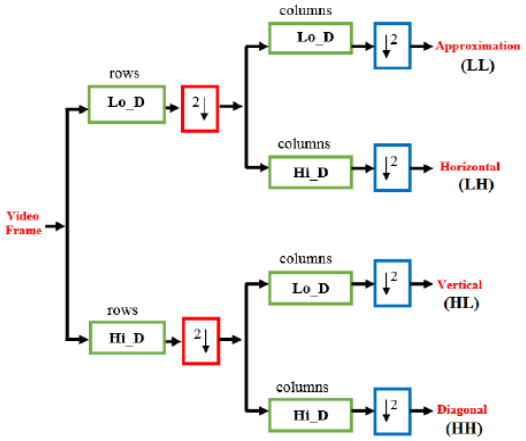

Figure 2: 2-Dimensional DWT decomposition [1]

3). Singular Value Decomposition

This approach is a mathematical method based upon the linear algebra and is a factorization of real or complex matrix.

It declares a Rectangular matrix (B) of size M x N which is analyzed it in to three matrices, U, S, and V individually, i.e. [5]:

[P S R] = svd (B) (6)

Here P-size is M x N, R-size is N x N in which both are unitary-orthogonal matrices. The size of S is M x M which is an orthogonal matrix.

$P = [p_1, p_2, \ldots\ldots\ldots\ldots p_r, p_{r+1}, \ldots\ldots, p_m]$ generating an orthogonal set, which are column vectors.

$p_i^j p_j = \{1, \text{if } i=j; 0, \text{else.} \quad \text{for } i= 1,2,3\ldots\ldots,m$ (7)

Similarly, R = orthogonal matrix so,

$R = [r_1, r_2, \ldots\ldots\ldots..r_r, r_{r+1}, \ldots\ldots..., r_n]$ forming an orthogonal set, which are the column vectors.

$r_i^t r_j = \{1, \text{if } I=j; 0, \text{else} \quad \text{for } i=1,2,3,\ldots\ldots\ldots n$ (8)

This technique provides high security to the system but hiding capacity is low and complex process to implement.

II. COMPARATIVE STUDY

From the above discussion, we come to know that spatial-domain and transform-domain are the two techniques utilized for video steganography. In spatial domain, the Least Significant Bit insertion technique is easiest and best methods to embed the secret information compared to all other methods. In this LSB technique data hiding capacity can be increased by increasing the number of LSB bits up to 3 bits used to embed the data with increase in complexity [1]. In Transform domain steganography technique, the Discrete Wavelet Transform is best for extracting data hiding coefficients in the video images compared to all other existing methods since it has high robustness, moderate complexity and low Bit Error Rate (BER). Using LSB and DWT techniques together in video steganography to achieve Robustness, Data hiding capacity and Imperceptibility of the system [1]. Therefore, in video steganography for secure communication LSB technique is best to hide data in spatial domain and DWT technique in transform domain is best to hide data.

TABLE. II presents comparison between data hiding methods with respect to domain, robustness, capacity and complexity of each steganography method.

TABLE II: Comparison between Spatial and Transform domain

Domain	Techniques	Robustness	Capacity	Complexity
Spatial	LSB	Low	High	Low
Spatial	MSB	Low	High	Low
Spatial	PVD	Low	High	High
Spatial	GLD	Moderate	High	Low
Transform	DCT	High	Low	Low
Transform	DWT	High	Low	Moderate
Transform	SVD	High	Low	High

Performance parameters:

The following parameters such as visual quality, embedding capacity and robustness of the system are used to analyze performance of video steganography.

A. *Visual quality*

The imperceptibility can be measure by using the Peak Signal to Noise Ratio (PSNR) values which is evaluated by Mean Square Error value (MSE) as follows [1]:

$$PSNR = 10 \log_{10} (square(MAXa)/(MSE)) \quad \text{(dB)} \qquad (9)$$

$$MSE = \frac{\sum_{i=1}^{x} \sum_{j=1}^{y} \sum_{k=1}^{z} square[a(i,j,k) - b(i,j,k)]}{aXbXc} \qquad (10)$$

Here ‘a’ & ‘b’ represents original embedded frames, ‘x’ & ‘y’ indicates the dimensions of the video and ‘c’ indicates the constituents of RGB color. MAXa indicates the maximum value of the pixel in the frame ‘a’.

B. *Embedding capacity*

The embedding capacity or Hiding Ratio (HR) in the cover video file can be estimated as [1]:

$$HR = \frac{Size\ of\ embedded\ information}{Size\ of\ the\ carrier\ Video}\ X\ 100\% \qquad (11)$$

C. *Robustness*

The Robustness of the system is calculated by using the Bit Error Rate (BER) values as follows [1].

$$BER = \sum_{i=1}^{a} \sum_{j=1}^{b} [I(i,j)\ mod\ \breve{I}\ (i,j)] / (aXb) \qquad (12)$$

Here I and $\breve{I}$ refers to the original information & obtained information, a X b indicates hided information size.

III. CONCLUSION

This paper presents various techniques/methods used in video steganography for secure communication. Steganography is the technique which presents authenticated communication between two users. In video steganography, video can be used as a cover media and the data hiding capacity will be more compared to all other techniques. Spatial-Domain and Transform-Domain are two methods utilized in video steganography to hide secret information. Least Significant Bit insertion technique is easiest and best methods to embed the secret information compared to all other methods in spatial domain and DWT is the best techniques in transform domain and is more robust compared to other methods. The combination of LSB and Discrete wavelet transform techniques provides the better performance in video steganography.

REFERENCES

[1] R. J. Mstafa and K. M. Elleithy, "A Robust and Secure Video Steganography Method in DCT-DWT Domains Based on Motion Object Trackingand ECC," *IEEE journal*, vol. 5, no. July, pp. 2–3, 2017.

[2] R. J. Mstafa and K. M. Elleithy, "A novel video steganography algorithm in DCT domain based on hamming and BCH codes," *37th IEEE Sarnoff Symp*, pp. 208–213, 2016.

[3] V. V Korgaonkar, "A DWT-DCT Combined Approach for Video Steganography," pp. 17–20, 2017.

[4] N. M. Surse and P. Vinayakray-jani, "A Comparative Study on Recent Image Steganography Techniques Based on DWT," pp. 1308–1314, 2017.

[5] R. Gupta, P. Mundra, "DWT-SVD based watermarking scheme of JPEG images using elliptic curve cryptography," *2016 5th Int. Conf*, pp. 359–365, 2016.

[6] D. Job and V. Paul, "An efficient video Steganography technique for secured data transmission," *Int. Conf. Data Min. Adv. Comput. SAPIENCE 2016*, pp. 298–305, 2016.

[7] R. J. Mstafa and K. M. Elleithy, "A novel video steganography algorithm in the wavelet domain based on the KLT tracking algorithm and BCH codes," *IEEE LISAT*, pp. 1-7, 2015.

[8] Y. Kakde, "Audio-video steganography" *International Conference on ICIIECS*, pp. 1-6, 2015.

[9] V. Sathya, K. Balasubramaniya., "Data Hiding in Audio Signal , Video Signal Text and Jpeg Images*" IEEE Int. Conf. on ICAESM*, pp. 741–746, 2012.

[10] Bharti Chandel, Dr. Shaily Jain, "Vidoe steganography: A survey" *IOSR Journal of Computer Engineering*, 2278-0661, p-ISSN, Volume 18, 2016.

[11] P. Yadav, N. Mishra, Sharma, Sanjeev, "A secure video steganography with encryption based on LSB technique" *IEEE Int. Conf. on CICR*, pp. 1-5, *2013*.

[12] M. Hussain, A. Wahab, "Pixel value differencing steganography techniques: Analysis and open challenge" *IEEE Int. Conf. on CE*, pp. 21-22, 2015.

[13] A. Islam, F. Khalid, "An improved image steganography technique based on MSB using bit differencing" *IEEE 6th Int. Conf. on INTECH*, pp. 265-269, August 2016.

[14] V. Potdar, E. Chnag, "Grey level modification steganography for secret communication" *2nd IEEE Int. Conf*,. pp, 223-228, june 2004.

[15] S. Sugathan, "An improved LSB embedding technique for image steganography" *2nd IEEE Int. Conf. on iCATccT*, pp, 609-612, issue, 4, 2017.