Video Steganography: A Survey

Bharti Chandel¹, Dr. Shaily Jain²
¹(Computer Science, Chitkara University, India) ²(Computer Science, Chitkara University, India)

Abstract: Recent advances in information technology have made quick delivery and sharing of multimedia information possible. But these advances in technology are leading breaches to information security and personal information. Digital Steganography provides capability to protect private communication that has become necessity in today’s Internet era. Steganography is a technique to protect and conceal multimedia information in disguised manner or we can say it is the study of invisible communication. Steganography is a mixture of compression, encryption, watermarking and cryptography. Generally sharing of information takes place in the form of text, image, audio and video. Steganography uses image, text, video and audio to disguise secret information. In this paper we have analyzed only video steganography. In video steganography secret information is enveloped inside a video to make it safe from intruders. In this paper we have critically analyzed fundamental concepts, performance metrics and security aspects of video steganography. Different methods used for protecting secret information by using a video as cover media are explored. Comparisons between different video steganography techniques are also provided. Steganalysis is also discussed in brief.

Keywords: Frequency Domain, Steganography, Steganalysis, Spatial Domain

I. Introduction

Steganography is a method of sharing secret information by making it inconspicuous to non-authenticated users. [1] Steganography has been originated from Greek word Steganos and graphics. Steganos means covered or hidden and graphics means writing. Greek People used steganography to convey secret message through different methods [2]. Other method to maintain security of information is Cryptography and Watermarking. Of which former is mainly used for authentication and later is used for hiding message using encryption. A comparison of cryptography, watermarking and steganography has been provided through Table 1. Steganography is mainly used in security applications like covert communication, legal fields and copyright Control.

Security systems are mainly focusing on protection of secret information by using encryption or cryptography. Cryptography [3] provides security of information by altering meaning of information through scrambling or encoding by using encryption key. No matter how shatter proofed is our encrypted message, it will always be vulnerable to attack as intruder already knows the existence of secret information. Steganography is better than cryptography as it hides the existence of secret message from intruder. Adding information to a media file by altering its contents in an imperceptible way is known as Watermarking [4]. Watermarking is used for protection of copyright material as it must be robust against any type of attack. Watermarking makes our data protected through hiding data in the form of copyright protection but steganography hides data inside a cover object. In summary we can say that steganography provides us the mixture of cryptography and watermarking by adding imperceptibility.

On the basis of type of cover object steganographic has been classified in five forms as shown in Fig 1[13]. Text Steganography mainly deals with concealing Text in Text Files and in Binary Files.[14] Text can be scrambled or concealed in any way inside a video. Text steganographic has very high capacity to hide text data in Cover Text File. Digital image steganography mainly deals with concealing data inside a cover image [15]. Being very popular in current internet era Digital images are considered to be highly used cover media in steganography [16]. Digital Image can be defined as a collection of pixels. Pixels based on their intensities are selected to hide data. Video can be considered as combination of audio and collection of still images which moves in constant time sequence. Videos are getting popular as a cover object in steganography due to high embedding payload than a digital image [5] [13] and temporal features of video also provide perpetual redundancy which is not available in digital images. Due to availability of large number of frames secret data can be easily disguised inside a video. Disguising secret information in some network protocols is known as protocol steganography. Noreka et al. [17] described steganography in application layer TCP/IP protocol. Bartosz et.al [18] had described protocol steganography using relation between two or more protocols.DNA
Table 1.1 Comparisons between Cryptography, Steganography and Watermarking

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Cryptography</th>
<th>Steganography</th>
<th>Watermarking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carrier Object</td>
<td>Text files or image</td>
<td>Any media file</td>
<td>Digital image/Audio</td>
</tr>
<tr>
<td>Secret information</td>
<td>Text</td>
<td>Any type of file</td>
<td>watermark</td>
</tr>
<tr>
<td>Secret key</td>
<td>Necessary</td>
<td>Optional</td>
<td>optional</td>
</tr>
<tr>
<td>Visibility</td>
<td>YES</td>
<td>Never</td>
<td>May or may not be</td>
</tr>
<tr>
<td>Objective</td>
<td>Protection</td>
<td>Secret communication</td>
<td>Copyright protection</td>
</tr>
<tr>
<td>Security</td>
<td>High</td>
<td>Very High</td>
<td>High</td>
</tr>
<tr>
<td>Capacity</td>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
</tbody>
</table>

steganography is getting popular due to high security, high embedding capacity and high embedding efficiency. Andre et.al [19] had described steganography using DNA binary strands.

In this article Section II and Section III describes the General model of video steganography and describes the Video Steganography technique evaluation parameters, In Section III we have provided brief introduction of various video steganography techniques and Section IV provides the Literature review and Critical analysis of various techniques followed by conclusion in Section V.

II. General Model Of Video Steganography

The Video Steganography refers to using video as a cover object (carrier file) to hide some secret message inside the video file by using some embedding procedure. Video Steganography procedure can be mathematically represented as follows (Fig 1 is showing the graphical representation of video steganography procedure).

Let $S_M$ denote the secret message to conceal inside cover video. Before applying anything on video (V) it must be divided into video frames. $C_f$ denotes video the individual video frame. $S_M$ will be embedded in $C_f$ after applying Encryption algorithm ($E_C$). $S_M$ can be anything like text file, video, audio or any other type of message. Three main procedures are included in this approach, namely Video file to frame conversion ($VTF_f$), Embedding Procedure ($Em$) and Extraction Procedure ($Ex$) [12].

$$
VTF_f: V -> C_f
$$

$$
Em: C_f + E_M(E_C(S_M, E_K)) -> S_f
$$

$$
Ex: E_X(D_C, D_K, S_f) -> S_M
$$

Where $E_C(S_M, E_K)$ is $S_M$ encryption procedure which combines with video frame to produce Stego Frame ($S_f$). Further $S_M$ is extracted from $S_f$ using Extraction Procedure as shown in Fig 1.2.

III. Video Steganography Measures

A. Imperceptibility

Imperceptibility refers to the visibility of modification inside the cover media. High Imperceptibility means increasing the invisibility of slight modifications in cover object. Modern day steganalysis approaches are highly intelligent to detect slight modifications. High Imperceptibility has motivated researches to design steganalysis resistant video steganography methods [6] [7].

B. Payload

Payload or capacity refers to the amount of secret message that can be concealed inside cover media [8]. Video are gaining popularity as highly used cover media object due to their high embedding capacity and embedding efficiency.
C. Statistical Attacks
The attacks or methods applied on stego object to extract hidden or secret information are known as statistical attack [9]. Steganography algorithm must be robust against statistical attacks.

D. Security
The most important feature of any steganographic algorithm is security. The embedding process should have high security with minimum vulnerability to attacks. Several approaches have been proposed to secure message in steganography [10].

E. Computational Cost
Data hiding and Data retrieval are the two parameters used to calculate computational cost of any steganography approach [11]. Data hiding time refers to the time required to embed data inside a cover video frame and data retrieval refers to extraction time of secret message from the stego frame.

IV. Video Steganography Techniques

A. Spatial Domain Based Method
Spatial Domain Methods basically deals with hiding information in pixels of video frames. The most popular method of steganography is Least Significant Bit method (LSB) [12] due to its high embedding capacity, less embedding complexity and ease in implementation. Least Significant method performs embedding of secret message in least significant or most significant bit by randomly selecting pixel from a digital image or a digital video frame. Let $P[i]$ is representing pixel of an image. Binary form of this pixel can be $P[i] = \{a_7, a_6, a_5, a_4, a_3, a_2, a_1, a_0\}$.

Where $a_7$ is most significant bit (MSB) and $a_0$ is least significant bit (LSB). Pixel Value Differencing (PVD) [29] is another approach of achieving spatial domain based steganography. Secret message bits are concealed in pixels by dividing them on the basis of their difference which provides better results in terms of imperceptibility and high embedding capacity.
Spatial Domain based methods are popular due to high embedding capacity but these are highly vulnerable to statistical attacks like image filters, rotation, cropping and scaling. To achieve high robustness and high security against steganalysis attacks Transform domain methods are preferred as described below.

**B. Transform Domain Based Technique**

Table Transform Domain Based Techniques are considered to be less prone to attacks due to high security. Digital image is collection of pixels which are present in high and low frequency components of image. The edge pixels are high frequency pixels and non edge pixels are low frequency pixels. Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are the two most popular transform based techniques in video steganography. DCT coefficients are considered as main destination of hiding in DCT transform method. Yanquing et al. [30] had achieved high security and high visual quality by using DCT coefficients based on Genetic algorithm. Difference of non-zero DCT coefficients had been chosen to achieve PSNR of 38.26 at high embedding rate with high security [31].

DWT method decompose the digital image or frame into four sub band with lower sub band having relevant information and high sub band having finer details [12]. Ghasemi et al.[32] had proposed embedding in 4 X 4 block of DWT coefficients using Genetic algorithm based functions and then OPAP is applied to achieve PSNR of 35.17 db.

**C. Format Based Method**

Various techniques have been designed for a particular video format. H.264/AVC is latest video compression standard with high efficiency in compression and well adaptation for network transmission [12]. Due to simple structure and small size Flash Video (.FLV) format video files are considered to be very popular on internet. Mozo et al [33] has described a technique based on its simple structure to embed secret message in video tags to achieve good visual quality without any distortion.

**V. Literature Survey**

In 2007 Daniel Socek et.al [20] has proposed an extended version of encryption algorithm of video which is applicable on both lossy and lossless low motion video codec and extension to this encryption algorithm as a new steganography algorithm to disguise a video inside a video with high security and low computational cost. There are two main types of video encoding standards i.e. compressed and uncompressed. Bin Liu et.al [26] has proposed compressed video secure steganography algorithm to achieve high security with robustness against statistical attacks without decompression process. Run level pairs which are formed by quantization of 8X8 discrete cosine transformed (DCT) are selected as positions to embed secret bits. Video steganography is famous due to high spatial and temporal redundancy. This feature can be easily applied to
design a steganography algorithm with high security and high embedding efficiency. For example M.Jafar et.al [34] has proposed a compressed video steganography using temporal and spatial features of video signal. The proposed algorithm has constant bit rate, high imperceptibility and embedded data has been extracted without full decomposition. There are many video steganography schemes proposed on motion vectors as they are used to remove temporal redundancies in video frames. Feng Pan et. al [35] has proposed an enhanced version of motion vector based video steganography algorithm by concealing data in motion vectors of cover media. This algorithm has maintained embedding capacity of 4 bits of secret message per 6 motion vectors i.e. approximately 2/3 of total number of motion vectors and PSNR value of more than 30dB. Due to low computational complexity and high bit rate of watermark channel Least Significant bit (LSB) is high used to embed secret data in steganography algorithm. R.Mritha [23] has proposed a modified least significant algorithm for video steganography with high security.

Significant growth of video data over internet had made it a popular choice for steganography. Embedding capacity and embedding efficiency are contrary to each other. Maintaining security along with high embedding capacity in steganography is a difficult task. Ramadhan et.al [25] had proposed high payload and high secure video steganography algorithm with hiding ration of 28.12% and PSNR ranged between 35.58-45.68dBs. To achieve high security BCH(15,11) encoding and segmentation has been applied on secret message before embedding using 2D-DWT domain, two security keys have been used to provide additional security. Ramadhan et.al [43] had also proposed another technique using Wavelet Domain based on the KLT Tracking Algorithm and High security using BCH codes. KLT algorithm has been applied for the detection of facial region of interest in video frames and message has been embedded in RGB pixel values of these pixels using 2D-DWT domain method by generating four sub bands. This proposed algorithm needs some further modification for robustness against some video processing attacks and artificial attacks. RGB pixel’s intensity values can be easily used to embed information in LSB of cover video file because modifications made to these pixels are almost invisible to HVS (Human Visual System) [25]. LSB substitution being the most simple and less complex method can be easily utilized to embed secret information. A.Swathi et.al [37] has proposed a method of video steganography using selection of embedding location by applying polynomial equations. Speed of data extraction and data embedding depends on the steganography algorithm. M.Ramalingam et.al [45] has proposed an enhanced version of Hidden Markov model to increase the speed of data embedding and extraction process. Hidden Markov models (HMM) are based on markov chains which are considered to be most suitable for increasing the speed of retrieval and extraction process due to no use of memory for states and independence of conditional probabilities of all states on the time in sequence. The HMM performs embedding of secret data by locating colored objects and applying some mathematical tools to model these objects in spatial domain.

Any successful steganography technique must consider some factors like imperceptibility, antisteganalysis and payload capacity but some factors contradict to each other, for example increasing payload capacity leads to distortion of imperceptibility and distortion of imperceptibility leads to vulnerability to attacks. Hence any steganography scheme can be considered as optimization problem where steganography technique hides secret message inside the cover video frame. Koushik et.al [38] had proposed an optimized technique for basic video steganography technique using genetic algorithm. Optimizer has been used to optimize a 3-3-2 LSB technique to achieve PSNR between 20 to 40dB and improved image fidelity (IF) as compared to previous existing method.

VI. Conclusion

In this paper summarization of common approaches and tools used for digital video steganography techniques has been done. A comparison between common video steganographic methods in digital video is also provided with a highlight on strength and weakness of each method in conclusion. The research of video steganography techniques can be explored in effective selection of cover media, to identify methods for embedding secret message with high imperceptibility, high embedding capacity, high embedding efficiency with optimum data hiding locations, low computational cost of data retrieval and data embedding rate, high security, different video files extension, different types of secret message like video inside video, image inside video, audio inside video and so on. Research can be also be explored in the area of embedding secret text message in different language other than English language. Further video encryption techniques can also be improvised.
References


[42] Ramadhan J. Mstafa, Khaled M. Elleithy, A Novel Video Steganography Algorithm in the Wavelet Domain Based on the KLT Tracking Algorithm and BCH Codes.