Empirical Study of Algorithms and Techniques of Video Steganography

Dr. Namarata Agrawal
Professor
NIFM, An Institute of Ministry of Finance, GoI, India
Chitkara University, Punjab

Ms. Parveen Mor
Assistant Professor
Lingayas GVKS Institute of Management & Technology,
Faridabad, India

Abstract

Steganography is the art and science of hiding the actual important information under graphics, text, cover file etc. These techniques may be applied without fear of image destruction because they are more integrated into the image. Information can be in the form of text, audio, video. The purpose of steganography is to covert communication and to hide a message from a third party or intruder. Steganography is often confused with cryptography because the two are similar in the way that both are used to protect confidential information. Though there are many types of steganography, video Steganography is more reliable due to high capacity image, more data embedment, perceptual redundancy etc. This research paper deals with various Video Steganography techniques and algorithms including Spatial Domain, Pseudorandom permutations, TPVD (Tri-way pixel value differencing), Motion Vector Technique, Video Compression, and Motion Vector Technique. The Video compression which uses modern coding techniques to reduce redundancy in video data has been also studied and analyzed. In fact, Video compression operates on square-shaped groups or blocks of neighboring pixels, often called macro blocks. These pixel groups or blocks of pixels are compared from one frame to the next and the video compression code sends only the differences within those blocks. Generally, the motion field in video compression is assumed to be translational with horizontal component and vertical component and denoted in vector form for the spatial variables in the underlying image, such as three steps search, etc. The study also discusses and focusses on the evolution of the Video Steganography techniques and algorithms over the years based on its application and subsequent merits and demerits. Further, Advanced Video Steganography Algorithm/Bit Exchange Method based on the bit shifting and XOR operation in the secret message file has been studied and implemented. The encrypted secret message is embed in the cover file in alternate byte. The bits are substituted in LSB & LSB+3 bits in the cover file. Finally, the simulation and evaluation of the above mentioned approach is performed using MATLAB tools.

Keywords: Video, Ex-OR, LSB, TPVD, Steganography

I. INTRODUCTION

A. Information Security

Information security means securing the information and information systems from unauthorized access, usage, disclosure, alteration and inspection.

These fields are interrelated and share the common goals of protecting the privacy, integrity and availability of information; however, there are some subtle differences between them [12].

There are two different ways for securing the data are:

- Cryptography
- Steganography

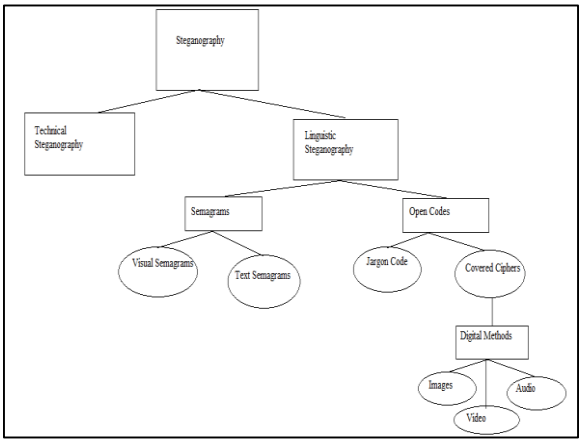

Fig. 1: Steganography taxonomy

B. Cryptography

In cryptography, the plain text is changed in cipher text and the cipher text is sent over the network. It is the alteration of data into a sequence of bits that shown as random and meaning-less to an attacker.

C. Steganography

This word comes from the Greek word steganos (covered or secret) and graph (writing or drawing). It may be defined as the hiding of information by embedding messages within other, apparently harmless messages, graphics or sounds [4].

Steganography and cryptography can be differentiated in such a way that in Steganography, the attacker or the evader would not be able to access the content of data whereas in cryptography, the attacker would not be able to detect the secret message present in the Steganographic medium.

1) *Types of Steganography*

a) Text Steganography:

An encoded message just screams you're using encryption, which may attract unwanted attention to your activities even if snoopers cannot read the text of your messages. Its attempt to conceal the presence of an encrypted message; over history a wide variety of techniques have been used: secret compartments in objects, invisible ink, microdots, and grilles used to hide letters of a message among innocent text, and in the digital age, embedding messages as imperceptible noise in images and audio files [5].

b) Image Steganography:

The main purpose of steganography is to hide a secret message in a carrier and the carrier used to hide the data is any image file that is said to be image steganography [6].

c) Audio Steganography:

Totally, it focused on hiding secret information in an innocent cover audio file, signal securely and robustly [7].

d) Video Steganography:

It is an electronic medium for the recording, copying, playback, broadcasting, and display of moving visual media.

It is a method to hide any kind of files in any extension. The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images and sounds.

It can be divided into two main classes. First one is embedding data in uncompressed raw video, which is compressed later. Other one is try to embed data directly in compressed video stream. [3].

e) ADVANTAGES OF VIDEO STEGANOGRAPHY:

- A video has higher capability then other image.
- More data can be embed in the video.
- Perceptual Redundancy formed in videos is due to their temporal features.
- Steganography video provides confidential communication and secret data storing.
- Protection of data alteration.
- Access control system for digital content distribution Media Database systems.

f) VIDEO STEGANOGRAPHY TECHNIQUES:

(1) Spatial Domain:

In this technology, embedding is done by using Integer Wavelet Coefficients. Generally wavelet domain allows hiding data in regions that the Human Visual System (HVS) is less sensitive to the hiding resolution detail band (HL, LH, HH). Hiding data in these regions allows us to increase the robustness while maintaining good visual quality [11].

(2) Pseudorandom permutations:

If all cover bits can be accessed in the embedding process, the secret message bits can be distributed randomly over the whole cover. This technique further produces the complexity for an attacker, since it is not guaranteed that subsequent message bits are embedded in the same order [13].

(3) TPVD (Tri-way pixel value differencing)

Actually, it is the same technique as the original PVD method for data embedding. However, the embedding capacity of images is increased 1.7 times by using the diagonal and vertical edges in image for data embedding in addition to horizontal edges. As it was declared earlier, original PVD method only embeds data in horizontal pixel blocks only [15].

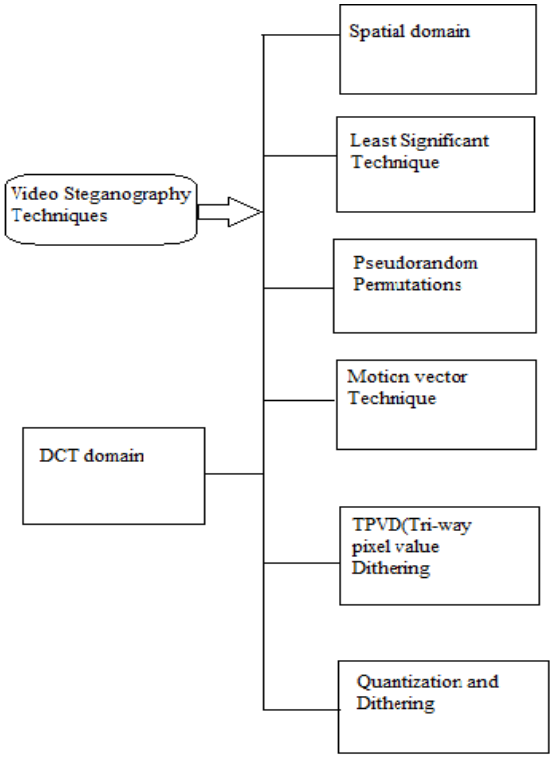

Fig. 2: Video Steganography techniques

This method is a modified form of PVD (pixel value differencing), which tends to increase embedding capacity and security of its successor by hiding secret bits in both vertical and diagonal edges of a cover image[8].Generally, the edges in an image are roughly classified into vertical, horizontal, and two kinds of diagonal directions. PVD method use only two-pixel pairs on one directional edge which can work efficiently for information hiding.

However, since the changing of pixel values for the fourth pixel pair affects the first and the second pair, the fourth pair is useless and has to be discarded. Therefore, we propose that three pairs are used to embed the secret data. Before introducing the proposed algorithm, the Pre-procedure is to partition the cover image into non overlapping 2×2 blocks with 4 pixels. In this scheme, each 2×2 block includes four pixels of p(a, b), p(a+1, b), p(a, b+ 1), and p(a+1, b+1) where x and y are the pixel location in the image. Let p(a, b) be the starting point, then three pixel pairs can be found by grouping p(a, b) with the right, the lower, and the lower right neighboring pixels. Those three pairs are named by P_0, P_1 and P_2 where P_0= (p(a, b), p(a+1, b)), P_1= (p(a, b),p(a, b+1)) and P_2 = (p(a, b), p(a+1, b+1)) respectively. When using the tri-way PVD method to embed the secret data, each pair has its modified P'_i and a new difference value d'_i for i = 0, 1, 2. Now, the new pixel values in each pair are different from their original ones. That is, we have three different values for the starting point p(a, b) named $p'_0(a, b)$, $p'_1(a, b)$ and $p'_2(a, b)$ from P_0, P_1, and P_2 respectively. However, only one value for $p'_1(a, b)$ can exist after finishing the embedding procedures. Therefore, one of $p'_1(a, b)$ is selected as the reference point to offset the other two pixel values. That is, two pixel values of one pair are used to adjust the other two pairs and construct a new 2×2 block. Selecting different reference points results in varied distortion to the stego-image. Here, we propose an optimal selection approach to achieve minimum Mean-Square-Error (MSE). Suppose that $m_i=d'_i-d_i$, d_i and d'_i are the difference values of pixel pair i before and after embedding procedures. The rules that can exactly determine one optimal reference pair without really estimating MSE are introduced as follows.

1) If all values of m_i are great than 1 or smaller than −1, the optimal pixel pair $i_{optimal}$ is the pair with the greatest | m|.
2) If all m_i have the same sign and only one m_i C {0,1,-1}, then the optimal pixel pair $i_{optimal}$ is selected from the other two pairs with the smallest | m| .
3) If only one m_i has a different sign from the other two pairs, the optimal pixel pair $i_{optimal}$ is selected from the other two pairs with the smallest | m|.
4) If only one m_i Є {0, 1, -1} and the other two m_i has different signs, the optimal pixel pair $i_{optimal}$ is the pair with m_i Є {0, 1, -1}.
5) If there exists more than one pair with mi Є {0, 1, 1}, the optimal pixel pair $i_{optimal}$ can be selected as any one pair with mi Є {0, 1, 1}.

By following those selection rules described above, we can skip the calculation steps of MSE estimation to obtain the optimal reference pairs. Thus, the total computational complexity can be greatly reduced [3]

(4) Motion Vector Technique:

Unlike the data-hiding methods in the motion vectors, we choose a different approach that selects those motion vectors whose associated macro blocks prediction error is high than the candidates for hiding a bit in each of their horizontal and vertical components [14].

g) Video Compression

It uses modern coding techniques to reduce redundancy in video data. It operates on square-shaped groups or blocks of neighboring pixels, often called macro blocks. Generally, the motion field in video compression is assumed to be translational with horizontal component and vertical component and denoted in vector form for the spatial variables in the underlying image, such as the three step search(TSS), The conjugate directional search(CDS), one at a time search(OTS),the 2D-Algorithm search(2-DLOGS),1-D full search(1-DFS),the parallel Hierarchical one-dimensional search(PHODS),efficient-simple search(ESS) and their modified algorithms etc [9].

(1) Motion Vector

In video compression, a motion vector is a key element in the motion estimation process. It is used to represent a macro block in a picture based macro block (or a similar one) in another picture, called the reference picture. Authenticated person, only after taking the second privacy key has the authority to check the video which was sent by Admin. The member can see the video and can detect the motion vector. After seeing this, the member obtains both the key [9].

D. Encryption

Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people. Original message is being hidden within a carrier such that the changes so occurred in the carrier are not observable. The information is the user defined information, the private key used to encrypt the text and the average time of the frame format is given. The encryption of the text is done by using the AES standard algorithm since the key size is larger for the AES [9].

1) *Extracting the original data*

Decryption is the process of convert encrypted data back into its original form. When the user inputs the correct key that is used at the decryption process, this will extract the original message that is encrypted and embedded [9].

2) *Peak Signal-to-Noise Ratio*

Larger SNR and PSNR indicate a smaller difference between the original and reconstructed image. The main advantage of this measure is ease of computation but it does not reflect perceptual quality. [9].

3) *Least Significant Technique:*

The least significant bit (LSB) plane of the pixel values of an image is substituted with the message bits for low-bit modulation. The receiver extracts the hidden message bits if he knows which pixels are modified [1].

Video steganography of late has also gained quite significance for researchers. Various techniques of LSB exists, proposes the data is first encrypted using a key and then embedded in the carrier AVI video file in LSB keeping the key of encryption in a separate file called key file. The cover video is then broken down into frames. [10].

E. Algorithm of Encoding

1) Step 1: Input the cover video file.
2) Step 2: Read required information of the cover video.
3) Step 3: Break the video into frames.
4) Step 4: Find 4 LSB bits of each RGB pixels of the cover frame.
5) Step 5: Obtain the position for embedding the secret data using hash function given in equation 1.
6) Step 6: Embed the eight bits of the secret image into 4 bits of LSB of RGB pixels of the cover frame in the order of 3, 3 & 2 respectively using the position obtained from step 5.
7) Step 7: Regenerate video frames.

II. ALGORITHMS

A. Tiny Encryption Algorithm:

In this algorithm, the sender encrypts the data in some form by using "Tiny encryption Algorithm". It is basically a cryptographic algorithm. It minimizes the memory & maximizes speed. It seems to be highly resistant to differential cryptanalysis. It achieves complete diffusion (where a one bit difference in the plaintext will cause approximately 32 bit differences in the cipher text) after only six rounds.[21]

The following notation is necessary:

1) Hexadecimal numbers will be subscribed with "h, e.g. 12=18.h
2) Bitwise Shifts: The logical left shift of x by y bits is denoted by x<<y. The logical right shift of x by y bits denoted by x>>y.
3) Bitwise Rotations: A Left rotation of x by y bits is denoted by x<<<y. A right rotation of x by y bits is denoted by x>>>y.
4) Exclusive-OR: It is logical operation of addition of n-tuples & is denoted by x+y.

B. Advanced Video Steganography Algorithm:

In this we encrypt the secret message file using simple bit shifting and XOR operation in the secret message file. We substitute bits in LSB & LSB+4 bits in the cover file.

1) *Bit Exchange Method:*

The following steps for encryption method are:

- Read one by one byte from the secret message file & convert each byte to 8-bits then we apply 1 bit right shift operation on the entire file so that each byte will be modified accordingly.
- We read 8-bits at a time and divide into two blocks 4 bits each and divide into two blocks 4 bits each & then perform the XOR operations & substitute the new bits in right four bit positions. The same thing repeated for all bytes in the file.
- Repeat step one by performing 2 bits right shift for all bytes in the secret message file, then repeat step two again.[22]

2) *Comparative list of Video Steganography Techniques and Algorithms*

Annexure

III. CONCLUSION & RECOMMENDATIONS

It has been concluded that in case of stego image, the strength of the Steganography technique depends on various parameter viz. robustness, embedding capability, imperceptibility level etc.

ANNEXURE

Table – 1
Video Steganography Techniques & Algorithms

Sr no.	*Author*	*Year*	*Technique*	*Algorithm*	*Application*	*Advantages*	*Disadvantages*	*Ref*
1.	*Kousik Dasgupta J.K. Mandal and Paramartha Dutta, Mritha Ramalingam*	*April 2012, may 2011*	*Least Significant Bit*	*HLSB algorithm for encoding and decoding*	*Steganography and watermarking*	*perceptual imperceptibility, security, high portability and high consistency*	*Less secure then others*	*[10], [16], [17]*
2.	*Nazanin Zaker & Ali Hamzeh*	*2011*	*Tri-way pixel value differencing*	*Embedding Algorithm ,TPVD algorithm*	*Tri-way Pixel, horizontal, vertical and diagonal*	*Imperceptibility , Robustness, Capacity*	*Pixel pair can hazards the security of tpvd*	*[8], [15], [12]*
3.	*P.Paulpandi , Dr. T.Meyyappan*	*2012*	*Motion vector technique*	*AES algorithm*	*For moving objects*	*improve the quality, no visual distortion*	*Hide the data only in two directions*	*[9]*
4.	*Neil F. Johnson and Stefan C. Katzenbeisser*	*2010*	*Pseudorandom permutations*	*Pseudorandom permutation*	*Distribution of secret message bits in a random selection*	*Increase the complexity*	*Some bits can be corrupted*	*[13]*
5.	*Neil F. Johnson and Stefan C. Katzenbeisser*	*2010*	*DCT Domain*	*Encoding and decoding algorithm*	*Steganography in DCT domain*	*Robust against JPEG compression*	*Image data can be destructed in some blocks*	*[13]*
6.	*Than Naing Soe*	*2000*	*Simple LSB Method after encryption*	*LSB Method*	*Can be done in all media forms*	*Simple*	*Limited data carrying capacity*	*[18]*

7.	***Neil F. Johnson and Stefan C. Katzenbeisser***	***2010***	***Quantization and dithering***	***Zhao and Koch algorithm***	***Steganography through quantized diff. b/w pixel values***	***Efficient***	***Error Prone***	***[13]***
8.	***Arun Sharma***	***2014***	***Image Steganography Technique***	***Image Encoding algorithms***	***Secret communication, improved communication, data storage***	***Simple, Efficient & secure***	***Lot of overhead to hide few bits***	***[20]***
9.	***Manisha Yadav, Mauli Joshi, Akshita***	***2013***	***Video Steganography Technique***	***Tiny Encryption Algorithm***	***Provide security to data, designed for simplicity & better performance***	***Requires Less memory & maximize speed***	***Storing of data in unprotected mode, password leakage may occur, intruders will affect stegos***	***[21]***
10.	***Pritish Bhautmage, Prof. Amutha Jeyakumar, Ashish Dahatonde***	***2013***	***LSB Technique***	***Bit Exchange Method, Steganographic Algorithm***	***To Embed the secret message with full security***	***Highly Secure, Capacity, Imperceptibility, Video error correction, less computational time***	***password leakage may occur***	***[22]***
11.	***R.Rejani,D.Murugan and Deepu V.Krishnan***	***2013***	***JSON using LSB based steganography***	***STEGANODB package***	***Insert, upsert, delete, remove, find***	***Integrity, security***	***Image quality degrades***	***[23]***

REFERENCES

[1] A P Sherly and P P Amritha, "A compressed Video Steganography using TPVD" published in august 2010.
[2] Al-Othmani Z. Abdulaleem 1, Manaf Abdul Azizah 2 and Zeki M. Akram 3 "A Survey on Steganography Techniques in Real Time Audio Signals and Evaluation" published in January 2012.
[3] Ali Hamzeh and Nazanin Zaker "A novel steganalysis for TPVD steganographic method based on differences of pixel difference histogram"
[4] Aly A. Hussein, Member, IEEE, "Data hiding in motion Vectors of compressed Video Based on Their Associated Prediction Error" published in march 2011.
[5] Andem, Reddy Vikram."A Cryptanalysis of the Tiny Encryption Algorithm",2003
[6] Ayhan, Yılmaz,"ROBUST VIDEO TRANSMISSION USING DATA HIDING" published in 2003.
[7] Chanu bern Jina Yam, Department of Computer Science & Engineering, NERIST, Nirjuli, Arunachal Pradesh, "A Short Survey on Image Steganography and Steganalysis Techniques".
[8] Dasgupta Kousik, Mandal J.K. and Dutta Paramartha, "Hash Based Least Significant Bit Technique for Video Steganography(HLSB)"
[9] Eloff J.H.P. , Morkel T. , Olivier M.S., "An overview of image steganography" published in 2002
[10] https://docs.google.com/viewer
[11] http://www.fourmilab.ch/javascrypt/stego.html
[12] Joseph Raphael Sundaram Dr. V. , Head & Director Research Scholar Department of Computer Applications Karpagam University Karpagam College of Engineering Coimbatore, India. Coimbatore, India. "Cryptography and Steganography – A Survey"
[13] Johnson F. Neil and Katzenbeisser C. Stefan, "A Survey of Steganographic techniques"
[14] Lecture Notes on" Information security", http://en.wikipedia.org/wiki/Information_security
[15] Paulpandi P. 1, Meyyappan Dr.T., M.sc., M.Phil., M.BA., Ph.D, "Hiding Messages Using Motion Vector Technique In Video Steganography " published in 2012
[16] Prof Bhautmage Pritish, , Jeyakumar Amutha, Dahatonde Ashish, "Advance Video Steganography Algorithm" ISSN:2248-9622
[17] Ramalingam Mritha "Video Steganography using Modified LSB Algorithm" published in 2011.
[18] Rejani R., Murugan D. and Krishnan V. Deepu,"Steganodb-A Secure Database" Volume 04,ISSUE 03,2013.
[19] Subhashini D., Nalini P., G. Chandrasekhar,"Comparison analysis of spatial Domain and compressed Domain steganographic techniques" published in june 2012.
[20] Sharma Arun,"An overview and survey on image Steganography Technique" ISSN 2277 128X,2014
[21] Zaker Nazanin & Hamzeh Ali, "A novel steganalysis for TPVD steganographic method based on differences of pixel difference histogram" published in Springer Science Business Media, LLC 2011
[22] Zaker Nazanin, Hamzeh Ali*,"* Security Enhancement For TPVD Steganographic method" published in 2010.
[23] Zin Wai Wai, Than Naing Soe, "Implementation and Analysis of Three Steganographic Approaches"

