Volume 5, Issue 4, April 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

# A Review on Various approaches for Video Digital Steganography

**Navdeep Ghotra***
Computer Science & Engineering
HEC, Jagadhri, India

**Aashdeep Singh**
Computer Science & Engineering
HEC, Jagadhri, India

**Kamal Gupta**
Computer Science & Engineering
GNI, Mullana, India

***Abstract— In Video Steganography data encrypted behind the least significant bits of video frame. Main problem arises because due to embedding behind least significant bits of video frames stagnalysis can be one easily on these frames to retrieved data. This does not provide security to secret data. Second issue is that on embedding the data size of data gets increases which are not easy to transmit over the network. To overcome these problem occurred in video Steganography various types of approaches has been studied and MLSB is taken as most appropriate approach for embedding of data. Size of embedded data can be reduced by performing compression to stego video file. We will implement this by using MATLAB.***

***Keywords— Stegnography, Video Stegnography, MATLAB,LSB,DCT.***

## I. INTRODUCTION

Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated. The strength of steganography can thus be amplified by combining it with cryptography. The idea and practice of hiding information has a long history. In *Histories* the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave's scalp. When the slave's hair grew back the slave was dispatched with the hidden message. In the Second World War the Microdot technique was developed by the Germans. Information, especially photographs, was reduced in size until it was the size of a typed period. Extremely difficult to detect, a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels.

### 1.1 Different kind of Stenography:

#### *1.1.1 Text stenography:*

Hiding information in text is the most important method of steganography. The method was to hide a secret message in every nth letter of every word of a text message. After booming of Internet and different type of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of redundant data.

#### *1.1.2 Image stenography:*

Images are used as the popular cover objects for steganography. A message is embedded in a digital image through an embedding algorithm, using the secret key. The resulting stego image is Send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of steno image unauthenticated persons can only notice the transmission of an image but can't guess the existence of the hidden message.

#### *1.1.3 Audio stenography:*

Audio stenography is masking, which exploits the properties of the human ear to hide information unnoticeably. An audible, sound can be inaudible in the presence of another louder audible sound .This property allows to select the channel in which to hide information.

#### *1.1.4 Protocol steganography:*

The term protocol steganography is to embedding information within network protocols such as TCP/IP. We hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used

### 1.2 Steganography Techniques

#### *1.2.1 Substitution Technique*

In the substitution technique; the redundant parts are covered with a secret message. This technique includes the Least Significant Bit Substitution method, where we choose a subset of cover elements and substitute the least significant bits of each element by the message bits .Message may be encrypted or compressed before hiding. A pseudorandom number generator may be used to spread the secret message over the cover in a random manner. This is an easy method but is vulnerable to corruption due to small changes in carrier

### *1.2.2 Transform Domain Technique*

In the transfer domain technique; the secret message is embedded in the transform space (e.g. frequency domain) of the cover.

An example of this method includes the Discrete Cosine Transform (DCT) domain. The cover image is split into 8*8 blocks and each block is used to encode one message bit. The blocks are chosen in a pseudorandom manner. The relative size of two predefined DCT coefficients is modulated using the message bit. The two coefficients are chosen from middle frequencies.

### *1.2.3 Spread Spectrum Technique*

This technique uses the concept of spread spectrum. The message is spread over a wide frequency bandwidth. The signal to noise ratio in every frequency band is so small that it is difficult to detect. Even if parts of message are removed from several bands, enough information is present in other bands to recover the information. Thus it is difficult to remove the message completely without entirely destroying the cover .It is a very robust technique that finds application in military communication.

### *1.2.4 Statistical Techniques*

In the statistical techniques, the information is encoded by changing several properties of the cover. The cover is split into blocks and each block is used to hide one message bit .If the message bit is one, then the cover block is modified otherwise the cover block is not modified. This technique is difficult to apply because a good test must be found that allows for proper distinction between modified and unmodified cover blocks.

### *1.2.5 Distortion Techniques*

The information is stored by distorting the signal. The encoder applies a sequence of modifications to the cover. This sequence corresponds to the secret message. The decoder measures the differences between the original cover and the distorted cover to detect the sequence of modifications and consequently recover the secret message. This method is not used in many applications because the decoder must have access to the original cover.

### *1.2.6 Protection of Data Alteration*

We take advantage of the fragility of the embedded data in this application area If it is implemented, people can send their "digital certificate data" to any place in the world through Internet. No one can forge, alter, nor tamper such certificate data. If forged, altered, or tampered, it is easily detected by the extraction program.

### 1.3 Applications of Steganography

- Steganography can be a solution which makes it possible to send news and information without being censored and without the fear of the messages being intercepted and traced back to us.
- It is also possible to simply use steganography to store information on a location. For example, several information sources like our private banking information, some military secrets, can be stored in a cover source. When we are required to unhide the secret information in our cover source, we can easily reveal our banking data and it will be impossible to prove the existence of the military secrets inside [3].
- Steganography can also be used to implement watermarking. Although the concept of watermarking is not necessarily steganography, there are several steganography techniques that are being used to store watermarks in data. The main difference is on intent, while the purpose of steganography is hiding information, watermarking is merely extending the cover source with extra information. Since people will not accept noticeable changes in images, audio or video files because of a watermark, Steganography methods can be used to hide this.
- E-commerce allows for an interesting use of steganography. In current e-commerce transactions, most users are protected by a username and password, with no real method of verifying that the user is the actual card holder. Biometric finger print scanning, combined with unique session IDs embedded into the fingerprint images via steganography, allow for a very secure option to open ecommerce transaction verification.
- Paired with existing communication methods, steganography can be used to carry out hidden exchanges. Governments are interested in two types of hidden communications: those that support national security and those that do not. Digital steganography provides vast potential for both types. Businesses may have similar concerns Regarding trade secrets or new product information.
- The transportation of sensitive data is another key use of steganography. A potential problem with cryptography is that eavesdroppers know they have an encrypted message when they see one. Steganography allows to transport of sensitive data past eavesdroppers without them knowing any sensitive data has passed them. The idea of using steganography in data transportation can be applied to just about any data transportation method, from E-Mail to images on Internet websites.

## II. RELATED WORK

**Mstafa, R.J. et al [1]** “A highly secure video steganography using Hamming code” In this paper, author propose a protected feature steganography calculation in light of the guideline of straight square code. Nine uncompressed feature successions are utilized as spread information and a double picture logo as a mystery message. The pixels' positions of both spread features and a mystery message are haphazardly reordered by utilizing a private key to enhance the framework's security. At that point the mystery message is encoded by applying Hamming code (7, 4) preceding the installing methodology to make the message considerably more secure. The consequence of the encoded message will be added to irregular created values by utilizing XOR capacity. After these steps that make the message sufficiently secure, it will be prepared to be inserted into the cover video outlines.

**ShengDun Hu et al [2]** "A Novel Video Steganography Based on Non-uniform Rectangular Partition" This paper proposes a novel Video Steganography which can hide an uncompressed secret video stream in a host video stream with almost the same size. Each frame of the secret video will be Non-uniform rectangular partitioned and the partitioned codes obtained can be an encrypted version of the original frame. These codes will be hidden in the Least 4 Significant Bits of each frames of the host video. Experimental results showed that this algorithm can hide a same-size video in the host video without obvious distortion in the host video.

**Bin Liu et al [3]** "Secure Steganography in Compressed Video Bit st**reams" A new compressed** secure steganography (CVSS) calculation is proposed. In the calculation, implanting and discovery operations are both executed completely in the compacted area, with no requirement for the decompression process. The new criteria utilizing factual imperceptibility of adjoining edges is utilized to modify the installing technique and limit, which builds the security of proposed calculation. Along these lines, the plot safe properties are acquired. Feature steganalysis with shut circle input way is outline as a checker to discover evident bugs. Trial results demonstrated this plan can be connected on packed feature steganography with high security properties.

**Balaji, R. et al [4]** "Secure data transmission using video Steganography" It is extremely fundamental to transmit imperative information like saving money and military data in a safe manner. Video Steganography is the methodology of concealing some mystery data inside a feature. The expansion of this data to the feature is not conspicuous by the human eye as the change of pixel shading is unimportant. This paper means to give a productive and a safe strategy for feature Steganography. The proposed system makes a list for the mystery data and the record is put in a casing of the video itself. With the assistance of this record, the casings containing the mystery data are placed. Consequently, amid the extraction process, as opposed to examining the whole feature, the casings containing the mystery information are investigated with the assistance of list at the less than desirable end. At the point when stegano graphed by this strategy, the likelihood of discovering the shrouded data by an aggressor is lesser when contrasted with the typical technique for concealing data outline by-edge in a successive way. It additionally diminishes the computational time taken for the extraction process.

**Keren Wang et al [5]** "Video Steganalysis Against Motion Vector-Based Steganography by Adding or Subtracting One Motion Vector Value" This paper exhibits a strategy for location of movement vector-based feature steganography. To begin with, the alteration on the minimum noteworthy bit of the movement vector is displayed. The impact of the installing operation on the entirety of outright contrast (SAD) is represented, which permits us to concentrate on the distinction between the real SAD and the by regional standards ideal SAD after the including or-subtracting-one operation on the movement esteem. At long last, taking into account the way that most movement vectors are by regional standards ideal for most feature codec, two capabilities are extricated and utilized for arrangement. Examinations are completed on features debased by different steganography strategies and encoded by different movement estimation systems, in different bit rates, and in different feature codec. Execution results exhibit that our plan beats past works all in all, and is better for certifiable applications.

**Amirtharajan et al. [6**] "An evaluation of image based steganography methods" Author use one component case: here we have 3 ways to determine the bits * 3 ways to decide the component R, G or B. this results in 9 cases. Using two component case: here we have 3 ways to determine the bits * 3 ways to decide the component RG, RG or GB. This results in 9 cases. Using three component case: here we have 3 ways to determine the bits * one way to decide the component which is RGB. This results in 3 cases. The average capacity ratio is around 1/7 or 14% of the original cover media size. The secret data is scattered throughout the whole image. Also, extracting the secret data without the knowledge of seeds is almost impossible. The capacity of the triple technique is higher than the previous techniques. By using this algorithm, the ratio between the number of bits used inside a pixel to hide part of the secret message; and the number of bits in the pixels itself, which is defined as the capacity factor can be in the range from 1/24 to 9/24 if we use a maximum of 3 bits.

## III. TECHNIQUES USED

### LSB

Least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The lsb is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digit further to the right. It is analogous to the least significant digit of a decimal integer, which is the digit in the ones (right-most) positioned and Technology.

### DES/IES

Data/Information Encryption Standard was at one time a prevalent symmetric-key calculation for the encryption of electronic information. It was exceedingly powerful in the progression of present day cryptography in the scholastic world. Grown in the early 1970s at IBM and in light of a prior outline by Horst Feistel, the calculation was submitted to the National Bureau of Standards (NBS) taking after the office's welcome to propose a possibility for the assurance of touchy, unclassified electronic government information. In 1976, after conference with the National Security Agency (NSA), the NBS in the end chose a somewhat altered variant (fortified against differential cryptanalysis, yet debilitated against animal power assaults), which was distributed as an authority Federal Information Processing Standard (FIPS) for the United States in 1977. The distribution of a NSA-affirmed encryption standard all the while brought about its speedy universal selection and far reaching scholarly investigation. Discussions emerged out of grouped configuration components, a generally short key length of the symmetric-key piece figure outline, and the contribution of the NSA, sustaining suspicions around a secondary passage. The exceptional scholastic examination the calculation got over the long haul prompted the advanced comprehension of piece figures and their cryptanalysis.

## VI. CONCLUSIONS

If the video is seen by normal person, it is found that there is nothing but the normal video, but only the known persons can find out the decrypted message from the video. The Different encryption format can be agreed by the two persons in such a way that no one can find the information from the video. Each technique can be implemented easily, but if someone tries to find out the tricks after knowing that someone using the stego-video file, then there are good chances of finding out the hidden information. In order to avoid this, the some hybrid system is used, in such a way that even though someone finds out the one technique, it is used only on few frames and other frames contains different kind of steganography and hence total secrete message is not delivered. Due to these embedding the video Steganography get dispersed using different types. In our work we will apply Direct Cosine Transform for retrieval of frames of video file, implement MLSB on each frames of video file for extraction of least significant bits of each region, and implement compression for reducing size of video data.

## REFERENCES

[1] Mstafa, R.J., Elleithy, K.M. "A highly secure video steganography using Hamming code" *IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2014*, pp. 1 – 6.

[2] ShengDun Hu , KinTak, U. "A Novel Video Steganography Based on Non-uniform Rectangular Partition" *14th International Conference on Computational Science and Engineering (CSE), 2011*, pp. 57 – 61.

[3] Bin Liu, "Secure Steganography in Compressed Video Bit streams" *Third International Conference on Availability, Reliability and Security, 2008*, pp. 1382 – 1387.

[4] Balaji, R. "Secure data transmission using video Steganography" *IEEE International Conference on Electro/Information Technology (EIT), 2011*, pp. 1 – 5.

[5] Keren Wang "Video Steganalysis against Motion Vector-Based Steganography by Adding or Subtracting One Motion Vector Value" *IEEE Transactions on Information Forensics and Security, 2014,* pp. 741 – 751.

[6] Bailey, K. "An evaluation of image based steganography methods", Journal of Multimedia Tools and Applications, Vol. 30, No. 1, pp. 55-88,IEEE,2006.

[7] Chapman, M. Davida G, and Rennhard M. "A Practical and Effective Approach to Large Scale Automated Linguistic Steganography" found online at http://www.nicetext.com/doc/isc01.pdf.