International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

A Review on Various Approaches of Video Steganography

Sapanpreet Kaur[1], Mandeep Kaur[2]

[1]Research Scholar, Sri Guru Granth Sahib World University

[2]Assistant Professor, Sri Guru Granth Sahib World University

Abstract: ***Steganography is the art and science of invisible communication. In recent years, the rapid growth of information technology and digital communication has become very important to secure information transmission between the sender and receiver. Therefore, steganography introduces strongly to hide information and to communicate a secret data in an appropriate multimedia carrier, e.g., image, audio and video files. In this paper, a new algorithm for image steganography has been proposed to hide a large amount of secret data presented by secret color image. This algorithm is based on different size image segmentations (DSIS) and modified least significant bits (MLSB), where the DSIS algorithm has been applied to embed a secret image randomly instead of sequentially; this approach has been applied before embedding process. The number of bit to be replaced at each byte is non uniform, it bases on byte characteristics by constructing an effective hypothesis. The simulation results justify that the proposed approach is employed efficiently and satisfied high imperceptible with high payload capacity reached to four bits per byte.***

Keywords: Steganography, image segmentation, LSB, MLSB, DSIS

1. Introduction

1.1 Digital Image Processing

An image is digitized to convert it to a form which can be stored in a computer's memory or on some form of storage media such as a hard disk or CD-ROM. This digitization procedure can be done by a scanner, or by a video camera connected to a frame grabber board in a computer. Once the image has been digitized, it can be operated upon by various image processing operations. Image processing operations can be roughly divided into three major categories, Image Compression, Image Enhancement and Restoration, and Measurement Extraction. Image compression is familiar to most people. It involves reducing the amount of memory needed to store a digital image. Image defects which could be caused by the digitization process or by faults in the imaging set-up can be corrected using Image Enhancement techniques. Once the image is in good condition, the Measurement Extraction operations can be used to obtain useful information from the image. Some examples of Image Enhancement and Measurement Extraction are given below. The examples shown all operate on 256 grey-scale images. This means that each pixel in the image is stored as a number between 0 to 255, where 0 represents a black pixel, 255 represents a white pixel and values in-between represent shades of grey. These operations can be extended to operate on colour images. The examples below represent only a few of the many techniques available for operating on images. Details about the inner workings of the operations have not been given, but some references to books containing this information are given at the end for the interested reader.

1.2 Steganography

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words "*stegos*" meaning "cover" and "*grafia*" meaning "writing defining it as "covered writing". In image steganography the information is hidden exclusively in images. 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.

Figure: Steganography

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.

1.3 Fundamental Steps in Digital Image Processing

1.3.1 Image acquisition: It is the first process shown in Figure. Note that acquisition could be as simple as being given an image that is already in digital form. Generally, the image acquisition stage involves preprocessing, such as scaling.

1.3.2 Image enhancement: It is among the simplest and most appealing areas of digital image processing. Basically, the idea behind enhancement techniques is to bring out detail that is obscured, or simply to highlight certain features of interest in an image.

1.3.3 Image restoration: It is an area that also deals with improving the appearance of an image. However, unlike enhancement, which is subjective, image restoration is objective, in the sense that restoration techniques tend to be based on mathematical or probabilistic models of image degradation.

1.3.4 Color image processing: It is an area that has been gaining in importance because of the significant increase in the use of digital images over the Internet.

1.3.5 Wavelets: These are the foundation for representing images in various degrees of resolution.

1.3.6 Compression: As the name implies, deals with techniques for reducing the storage required saving an image, or the bandwidth required transmitting it. Although storage technology has improved significantly over the past decade, the same cannot be said for transmission capacity.

1.3.7 Morphological processing: This deals with tools for extracting image components that are useful in the representation and description of shape.

1.3.8 Segmentation: These procedures partition an image into its constituent parts or objects. In general, autonomous segmentation is one of the most difficult tasks in digital image processing. A rugged segmentation procedure brings the process a long way toward successful solution of Imaging problems that require objects to be identified individually.

1.3.9 Representation and description: Almost always follow the output of a segmentation stage, which usually is raw pixel data, constituting either the boundary of a region (i.e., the set of pixels separating one image region from another) or all the points in the region itself. In either case, converting the data to a form suitable for computer processing is necessary.

1.3.10 Recognition: It is the process that assigns a label (e.g., "vehicle") to an object based on its descriptors. We conclude our coverage of digital image processing with the development of methods for recognition of individual objects.

1.4 Different kind of Steganography

1.4.1 Text steganography: 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 steganography using digital files is not used very often because the text files have a very small amount of redundant data [6].

1.4.2 Image steganography: 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.

1.4.3 Audio steganography: Audio steganography 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.

1.4.4. Video Steganography: Video Steganography is a method to conceal any sort of records into a convoy Video document. The utilization of the feature based Steganography can be more qualified than other interactive media documents, on account of its size and memory prerequisites. Video Steganography is a system to hide any sort of records in any extension into a carrying Video file. This venture is the application created to insert any sort of data (File) in an alternate document, which is called transporter record. The bearer document must be a feature record. It is concerned with inserting data in a harmless spread media in a protected and powerful way. This framework makes the Files more secure by utilizing the ideas Steganography and Cryptography.

1.4.5 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.

1.5 Steganography Techniques

1.5.1 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.

1.5.2 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.

1.5.3 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.

1.5.4 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.

1.5.5 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.

1.6 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.
- Steganography can also be used to implement watermarking. Although the concept of watermarking is not necessarily steganography, there are several steganographic techniques that are being used to store watermarks in data.
- 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.

2. Review of Literature

V. Saravanan et al [1] "Security Issues in Computer Networks and Steganography" This paper reduces the detectable distortion in a joint photographic experts group (JPEG) file during data hiding process, by introducing new region selection rule. The new region selection rule considers three factors, i.e., the horizontal difference (HD), vertical difference (VD) and region size (RS). The JPEG image will be split into number of blocks and each pixel in it will be examined to calculate the variations. Depends upon the variation, the amount of secret information will be hide in an image. This proposed method of information hiding will help to solve the security issues in computer networks.

Bin Liu et al [2] "Secure Steganography in Compressed Video Bitstreams" A new compressed feature 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 are 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 [3] "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 a 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.

Keren Wang et al [4] "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 codecs, two capabilities are extricated and utilized for arrangement.

Mstafa, R.J. et al [5] "A highly secure video steganography using Hamming code" Because of the rapid of web and advances in innovation, individuals are getting to be more agonized over data being hacked by aggressors. As of late, numerous calculations of steganography and information stowing away have been proposed. Steganography is a procedure of installing the mystery data inside the host medium (content, sound, picture and feature). Simultaneously, a large portion of the intense steganographic examination programming projects have been given to unapproved clients to recover the significant mystery data that was inserted in the bearer documents. Some steganography calculations can be effectively

recognized by steganalytical locators in view of the absence of security and installing productivity. In this paper, we 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.

3. Approaches Used

DCT: A discrete cosine transform (DCT) expresses a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies. DCTs are important to numerous applications in science and engineering, from lossy compression of audio (e.g. MP3) and images (e.g. JPEG) (where small high-frequency components can be discarded), to spectral methods for the numerical solution of partial differential equations. The use of cosine rather than sine functions is critical for compression, since it turns out (as described below) that fewer cosine functions are needed to approximate a typical signal, whereas for differential equations the cosines express a particular choice ofboundary conditions. In particular, a DCT is a Fourier-related transform similar to the discrete Fourier transform (DFT), but using only real numbers. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since the Fourier transform of a real and even function is real and even), where in some variants the input and/or output data are shifted by half a sample. There are eight standard DCT variants, of which four are common.

MLSB: Image segmentation is the process that uses to partition cover image into a set of sub images depending on a new hypothesis. Different methods proposed by many researchers had been implemented to achieve image segmentation based on the value of intensity, similarity, and variance between neighboring bytes. In the proposed algorithm, the hypothesis that is created is based on cipher key with three operations to make hard to detect the segments edges from the attacker.

Blowfish Algorithm: Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. However, the Advanced Encryption Standard (AES) now receives more attention. Schneier designed Blowfish as a general-purpose algorithm, intended as an alternative to the aging DES and free of the problems and constraints associated with other algorithms. At the time Blowfish was released, many other designs were proprietary, encumbered by patents or were commercial or government secrets. Schneier has stated that, "Blowfish is unpatented, and will remain so in all countries. The algorithm is hereby placed in the public domain, and can be freely used by anyone."

4. Conclusion

The meaning of steganography is hiding text or secret messages into another media file such as image, text, sound or video. The word “steganography” is often considered similar to “cryptography” and “watermarking”. The biggest problem steganography faces is that of size. There is a limit to the size of a file which you can embed information into. The technique used LSB i.e. least significant bit works on a particular region of an image. . 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 and Text steganography using digital files is not used very often because the text files have a very small amount of redundant data. Other problem also faced in the proposed work no extraction of images is done. So, due to these problems we have applied the techniques which solved many of them.

References

[1] V. Saravanan “Security Issues in Computer Networks and Steganography”, IEEE Conf. on Computer network & steganography, 2012, pp 56-67.
[2] Bin Liu, “Secure Steganography in Compressed Video Bitstreams” *Third International Conference on Availability, Reliability and Security, 2008*, pp. 1382 – 1387.
[3] Balaji, R. “Secure data transmission using video Steganography” *IEEE International Conference on Electro/Information Technology (EIT), 2011*, pp. 1 – 5.
[4] 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
[5] Mstafa, R.J. “A highly secure video steganography using Hamming code” *IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2014*, pp. 1 – 6.
[6] Marwaha, P. “Visual cryptographic steganography in Video”, *Second International conference on Computing,* Communication and Networking Technologies, pp. 34-39, IEEE, 2010.
[7] Martinez-Enriquez “An adaptive algorithm for fast inters mode decision in the H.264/AVC video coding standard” *IEEE Conf. on Consumer Electronics*, 2010, pp 826 – 834.
[8] Mazen Abu Zaher “Modified Least Significant Bit (MLSB)” IEEE Conf. on MLSB, 2011, pp 60-67.
[9] Robertson, M.A. “Reducing the computational complexity of a MAP post-processing algorithm for video sequences”, *IEEE Conf. on Image Processing*, 2008, pp 372 - 376 vol.1.
[10] 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.
[11] Suhad A.H.Al-A “Steganography Image in Image using Modified method in Least Significant Bit (LSB) substitution”, IEEE conf. on MLSB, 2007, PP 65-70.