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

Various Approaches of Video and Image Stenography: A Review

Mandeep Singh[1], Garima Mahajan[2]

[1]M-Tech, Baba Farid College of Engineering & Technology, Deon (Bathinda)

[2]Assistant Professor, Baba Farid College of Engineering & Technology, Deon (Bathinda)

Abstract: ***Steganography is process of hiding secret information behind any image and video file for the secure transmission of data. Video steganography comprises various frames in a single video file from which prediction of secret data availability is not come so easy process. In video steganography various frames has been extracted from a video file and secret information has to be embedded in these frames for transmission of video file. Video steganography comprises various types of data that can be embedded i.e. video data, text data or image data. In this type of steganography various approaches have been proposed yet, but the main issue of security is remaining always because of increase in attack on transmission line. Audio data available in the video file also can be utilized for the purposes of text data steganography. Text data can be easily embedded into audio data which does not distort the quality of audio available in video data. In video steganography the purpose of security is done by using audio and video steganography both in a single video file. Due to two types of data can be send through video steganography.***

Keywords: Digital Image Processing Techniques of steganography, Video Steganography, LSB, MLSB, RGB

1. Introduction

1.1 DIP (Digital Image Processing)

Image with two dimensional function f(x ,y), where x and y are spatial co-ordinates. Digital image field refer to processing. The field of digital image processing refers to processing digital images by means of a digital computer. Note that a digital image is composed of a finite number of elements, each of which has a particular location and value. These elements are referred to as picture elements, image elements and pixels [1].

1.2 Steganography

Steganography differs from cryptography in the sense that where cryptography focuses on custody 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 [2].

1.3 Different Kind of Stenography

1.3.1 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 [6].

1.3.2 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 [3].

1.3.3 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.

1.3.4 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 [4].

1.4 Steganography Techniques

1.4.1 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 [7].

1.4.2 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 [8].

1.4.3 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 [9].

1.4.4 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 [10].

1.4.5 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.

2. Review Of Literature

Bin Liu et al [1] "Secure Steganography in Compressed Video Bit-streams" In this paper a new secure steganography is proposed. The calculation, implanting and discovery operations both are executed completely in the compacted area. 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. They draw safe properties are acquired among these lines. 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 [2] "Secure data transmission using video Steganography" This is extremely fundamentally to transmit imperative information like saving money & military data in a safe manner. Video Steganography is the method of conceal some ambiguity data inside a feature. The expansion of this data to the trait is not obvious by the human eye as the modify of pixel shading is unimportant. This paper means to give a productive and a protected 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 contain the mystery data are to be found. Consequently, amid the extraction process, as opposed to examining the whole feature, the casing containing the mystery information are investigated with the assistance of list at the less than desirable end.

Keren Wang et al [3] "Video Steganalysis Against Motion Vector-Based Steganography by Adding or Subtracting One Motion Vector Value" This paper exhibits a strategy for location of group vector-based feature steganography. To begin with, the alteration on the least amount noteworthy bit of the movement vector is displayed. The collision of the installing operation on the total of outright gap (SAD) is represented, which permits us to concentrate on the difference between the real SAD and the by local standards ideal SAD after the including or-subtracting-one operation on the movement esteem. Examinations are completed on features debased by dissimilar steganography strategies and encoded by different movement opinion systems, in different bit rates, and in different feature codecs. Execution fallout exhibit that our plan beats past works all in all, and is better for certifiable applications.

Mstafa, R.J. et al [4] "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 aggressor. As of late, many calculations of steganography and information stowing away have been proposed. Steganography is a procedure of install the anonymity data inside the host medium. Simultaneously, a large portion of the intense steganographic examination programming projects have been given to unapproved clients to get well the significant mystery data that was inserted in the carrier documents. Some steganography calculations can be effectively familiar by steganalytical locators in view of the lack of security and installing productivity.

Bailey et al [5]"Visual cryptographic steganography in Video" Author describe an image based multi-bit steganography method to increase capacity hiding secret in number of bits, i.e. Stego-1bit, Stego-2bits, Stego-3bits and Stego-4bits. Stego-1bit is the simplest of this, where it insert the secret message data into one MLSB (lower order bit) of the image pixels, which is untraceable. Hide and Seek is an example of this technique. Note that if this bit placing is performed into the higher order bit (most significant bit), the value of the pixel will show a great detectable change spoiling its security. It is known that insertion of hidden bits into lowest order MLSB in all color RGB channels of the image pixels is unnoticeable. In the Stego-2bits method two bits of minor order MLSB in RGB image steganography is used; Stego-2bits doubled the capacity of message hitting with negligible security reduction. The capacity can be enhanced more since in Stego-3bits and even more in stego-4bits, which are jeopardizing security accordingly.

3. Approaches Used

Least significant bit: LSB can also stand for least significant byte. The meaning is parallel to the above: it is the byte in that place of a multi-byte number which has the least potential value. If the abbreviation's meaning smallest amount significant byte isn't obvious from context, it should be affirmed explicitly to avoid confusion with least significant bit. To avoid this ambiguity, the less abbreviated terms "lsbit" or "ls byte" are often used. In computing, the least significant bit (LSB) is the bit position in a dual 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) position.

$$\sum_{n=1}^{\infty} lsb(n)\,\frac{x^n}{1-x^n}=\frac{\ln\left(1-x^2\right)+\Psi_{x^2}\left(\frac{1}{2}\right)}{\ln(x^2)}$$

Most significant bit: In computing, the most significant bit (MLSB, also called the high-order bit) is the bit position in a binary numeral having the greatest value. The MSB is sometimes referred to as the left-most bit due to the gathering in positional notation of writing more significant digits further to the left. The MLSB can also correspond to the sign bit of a signed binary number in one's or two's complement notation, "1" meaning negative and "0" meaning positive. It is ordinary to assign each bit a position number, ranging from zero to N-1, where N is the number of bits in the binary representation used. Normally, this is simply the exponent for the corresponding bit weight in base-2.

$$\sum_{i=0}^{N-1} bi\,.\,2^{N-1-i}$$

RGB pixel indication

The RGB pixel indication is an additive color model in which red, green, and blue light are added jointly in various ways to reproduce a broad array of colors. The name of the model comes from the initials of the three additive primary colors, red, green, and azure. The main purpose of the RGB pixel indication is for the sensing, representation, and display of images in electronic systems, such as televisions and computers, though it has also been used in conventional photography. Before the electronic age, the RGB pixel indication ready had a solid theory behind it, based in human perception of colors. RGB is a *device-dependent* color model: different devices detect or reproduce a given RGB value in a different way, since the color elements and their response to the individual R, G, and B levels vary from manufacturer to manufacturer, or even in the same device over time. Thus an RGB value does not define the same *color* across devices without some kind of shade management.

4. Conclusion

Video steganography is used for secure transmission of secret data over a communication network. In video steganography various frames has been extracted from a video file and secret information has to be embedded in these frames for transmission of video file. Video steganography comprises various types of data that can be embedded Audio data available in the video file also can be utilized for the purposes of text data steganography. Text data can be easily embedded into audio data which does not distort the quality of audio available in video data. To overcome these issue various approaches has been proposed for the purpose of steganography. In video steganography the purpose of security is done by using audio and video steganography both in a single video file. Due to two types of data can be send through video steganography. By using LSB and MLSB we will improve the issue of security. To overcome the issue of security in proposed work encryption has been introduced.

References

[1] Bin Liu, "Secure Steganography in Compressed Video Bitstreams" *Third International Conference on Availability, Reliability and Security, 2008*, pp. 1382 – 1387.
[2] Balaji, R. "Secure data transmission using video Steganography" *IEEE International Conference on Electro/Information Technology (EIT), 2011*, pp. 1 – 5.
[3] 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
[4] Mstafa, R.J. "A highly secure video steganography using Hamming code", *IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2014*, pp. 1–6
[5] Marwaha, "Visual cryptographic steganography in Video", *Second International conference on Computing*, Communication and Networking Technologies, pp. 34-39, IEEE, 2010.
[6] 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.
[7] Mazen Abu Zaher "Modified Least Significant Bit (MLSB)" IEEE Conf. on MLSB, 2011, pp 60-67.
[8] Chengdu Hub "A Novel Video Steganography Based on Non-uniform Rectangular Partition" *14th International Conference on Computational Science and Engineering (CSE), 2011*, pp. 57 – 61.
[9] Tasdemir, K "Video steganalysis of LSB based motion vector steganography", IEEE Conf on Visual Information Processing (EUVIP), 2013, pp 260 – 264.
[10] Dehkordi, A.B. "Robust LSB watermarking optimized for local structural similarity", IEEE Conf. on Electrical Engineering (ICEE), 2011, pp 1
[11] Islam, M.R. "An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography", IEEE Conf. on Informatics, Electronics & Vision (ICIEV), 2014, pp 1 – 6.
[12] Yi-Chun Liao "Data hiding in video using adaptive LSB", IEEE Conf. on Pervasive Computing (JCPC), 2009, pp 185 – 190.