IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

A Review on Secure Video Steganography Technique using LSB & MSB

Er. Ginni[1], Er. Pushpinder Singh[2]

Research Scholar, M.Tech, Rayat Bahra University, Mohali, India [1]

Assistant Professor, Rayat Bahra University, Mohali, India [2]

Abstract: Steganography is used for secure transmission of secret information by hiding information behind a cover object. Various types of steganography have been used for security of data. Text, audio, image and video steganography were utilized for different purposes. Video steganography can be used for more data to be transmitted under different frames of video. In these paper different types of steganography and different approaches for steganography has been reviewed. On the basis of study of different approaches approach for steganography can be easily adopted.

Keywords: Steganography, Audio Steganography, Video steganography, Security, LSB, MLSB.

1. INTRODUCTION

Steganography is the craftsmanship or practice of covering a record, message, picture, or feature inside an alternate document, message, picture, or feature [1]. The statement steganography joins the Ancient Greek words steganos (στεγανός), signifying "secured, hid, or ensured", and graphein (γράφειν) signifying "written work". The shrouded messages will have all the earmarks of being (or be a piece of) something else: pictures, articles, shopping records, or some other spread content. Case in point, the shrouded message may be in undetectable ink between the unmistakable lines of a private letter [2].

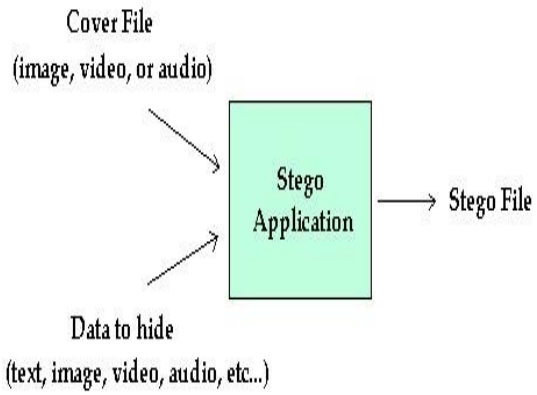

Fig 1: Video Steganography [11]

A few usage of steganography which fail to offer an imparted mystery are manifestations of security through in distinct quality, while key-subordinate steganography plans hold fast to Kirchhoff's' principle. The playing point of steganography over cryptography alone is that the proposed mystery message does not pull in regard for itself as an object of investigation. Doubtlessly unmistakable scrambled messages—regardless of how Unbreakable will move investment, and may in them be implicating in nations where encryption is illegal [3]. Thus, while cryptography is the act of ensuring the substance of a message alone, steganography is concerned with disguising the way that a mystery message is being sent [4]. Video Conversion process is used to reduce the spatial and temporal redundancy of Group of Pictures. Temporal redundancy can be reduced by registering differences between frames. Spatial redundancy is reduced by registering differences between parts of a single frame Video to frame conversion is the process of converting a video to cinematic motion picture. The number of still pictures per unit of time can be separated from the video using this Stego model. 120 or more frames per second of images can be retrieved from new professional cameras as efficiently with clarity motion pictures [5].

In the substitution method; the repetitive parts are secured with a mystery message. This procedure incorporates the Least Significant Bit Substitution strategy, where we pick a subset of spread components and substitute the minimum critical bits of every component by the message bits .Message may be encoded or compacted before covering up. A pseudorandom number generator may be utilized to spread the mystery message over the spread in an irregular way. This is a simple system however is defenceless against defilement because of little changes in transporter.

The main stenographic techniques are as follows [6]:

- **Transform Domain Technique:** In the exchange space strategy; the mystery message is implanted in the change space (e.g. recurrence area) of the spread. A sample of this technique incorporates the Discrete Cosine Transform (DCT) area. The spread picture is part into 8*8 pieces and each one piece is utilized to encode one message bit [7].

- **Spread Spectrum Techniques:** This system uses the thought of spread reach. The message is spread over a wide repeat transmission limit. The sign to tumult extent in every repeat band is little to the point that it is tricky to find. Despite the likelihood that parts of message are ousted from a couple of gatherings, enough information is acquainting in diverse gatherings with recover the information. Thus it is tricky to clear the message absolutely without totally destroying the spread. It is an

outstandingly vivacious method that finds application in military correspondence [8].

• **Statistical Techniques:** In the factual methods, the data is encoded by changing a few properties of the spread. The spread is part into pieces and each one piece is utilized to conceal one message bit. If the message bit is one, then the spread square is adjusted generally the spread piece is not changed. This strategy is hard to apply on the grounds that a decent test must be discovered that takes into consideration fitting refinement in the middle of adjusted and unmodified spread pieces [9].

• **Distortion Techniques:** The data is put away by misshaping the sign. The encoder applies an arrangement of alterations to the spread. This grouping compares to the mystery message. The decoder measures the contrasts between the first cover and the mutilated spread to locate the arrangement of changes and subsequently recuperate the mystery message. This system is not utilized as a part of numerous applications on the grounds that the decoder must have entry to the first cover [10].

• **Protection of Data Alteration:** We exploit the delicacy of the inserted information in this application zone. On the off chance that it is actualized, individuals can send their "computerized endorsement information" to wherever on the planet through Internet. Nobody can fashion, change, nor alter such authentication information. In the event that manufactured, modified, or altered, it is effectively located by the extraction program1.3.6 Protection of Data Alteration.

2. RELATED WORK

S. D. Hu et al [3] "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.

P. Yadav et al [5] "A secure video steganography with encryption based on LSB technique" Need of hiding information from intruders has been around since ancient times. Nowadays Digital media is getting advanced like text, image, audio, video etc. To maintain the secrecy of information, different methods of hiding have been evolved. One of them is Steganography, which means hiding information under some other information without noticeable change in cover information. Recently Video Steganography has become a boon for providing large amount of data to be transferred secretly. Video is simply a sequence of images; hence much space is available in between for hiding information. In proposed scheme video steganography is used to hide a secret video stream in cover video stream. Each frame of secret video will be broken into individual components then converted into 8-bit binary values, and encrypted using XOR with secret key and encrypted frames will be hidden in the least significant bit of each frames using sequential encoding of Cover video. To enhance more security each bit of secret frames will be stored in cover frames following a pattern BGRRGBGR.

K. Patel et al [6] "Lazy Wavelet Transform Based Steganography in Video" Visual steganography is the most widely practiced form of steganography. It started with concealing messages within the lowest bits of noisy images or sound files. We shall perform steganography on video files and hide the message in an encrypted format, thus achieving a multiple cryptographic system. The most commonly used technique is Least Significant Bit steganography (LSB steganography). But instead of traditional LSB encoding, we will use a modified encoding technique which will first transform the video using a Lazy Lifting Wavelet transform and then apply LSB in the sub-bands of the video that has been obtained. The proposed approach to video steganography utilizes the visual as well as the audio component. The lazy wavelet transform is applied to the visual frames, and the data is stored in the coefficients of the visual component. The length up to which it is stored is hidden using LSB in the audio component. Experimental results show that the proposed technique does not affect the higher and lower ends of the frequency distribution of the signal. Moreover, it has a high payload capacity and low computational requirements.

S. K. Moon et al [8] "Application of data hiding in audio-video using anti forensics technique for authentication and data security" Steganography is the method of hiding any secret information like password, text, and image, audio behind original cover file. In this paper we proposed the audio-video crypto steganography which is the combination of image steganography and audio steganography using computer forensics technique as a tool for authentication. Our aim is to hide secret information behind image and audio of video file. As video is the application of many still frames of images and audio, we can select any frame of video and audio for hiding our secret data. Suitable algorithm such as 4LSB is used for image steganography and phase coding algorithm for audio steganography. Suitable parameter of security and authentication like PSNR, histogram is obtained at receiver and transmitter side which are exactly identical, hence data security can be increased. This paper focus the idea of computer forensics technique and its use of video steganography in both investigative and security manner.

Y. Kakde et al [9] "Audio-video steganography" Steganography is the art and science of writing messages which is to be hide behind original cover file which may be audio, video or image. In this paper we are working on audio-video steganography which is the combination of Audio steganography and Image steganography, in this we are using computer forensics technique for authentication purpose. In this paper our aim is to hide secret information behind audio and image of video file. As we know that

DOI 10.17148/IJARCCE.2016.53156

video is the combination of many still frames of images and audio. We can select any frame of video and audio for hiding our secret data. This paper proposed an algorithm for hiding image in selected video sequence is an image-hiding technique based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) and random LSB (Least Significant Bit) audio steganography method for hiding secret text information inside audio of the audio-video file, it reduce embedding distortion of the host audio. This paper focuses the idea of computer forensics technique which is use as a tool for authentication and data security purpose and its use in video steganography in security manner.

R. J. Mstafa et al [10] "A New Video Steganography Algorithm Based on the Multiple Object Tracking and Hamming Codes" In the modern world, video steganography has become a popular option for secret data communication. The performance of any steganography algorithm is based on the embedding efficiency, embedding payload, and robustness against attackers. In this paper, we propose a new video steganography algorithm based on the multiple object tracking algorithm and Hamming codes. The proposed algorithm includes four different stages. First, the secret message is pre-processed, and Hamming codes (n, k) are applied in order to produce an encoded message. Second, a motion-based multiple object tracking algorithm is applied on cover videos in order to identify the regions of interest of the moving objects. Third, the process of embedding 3 and 6 bits of the encoded message into the 1 LSB and 2 LSBs of RGB pixel components is performed for all motion regions in the video using the foreground mask. Fourth, the process of extracting the secret message from the 1 LSB and 2 LSBs for each RGB component of all moving regions is accomplished. Experimental results of the proposed video steganography algorithm have demonstrated a high embedding efficiency and a high embedding payload.

3. APPROACHES USED

3.1 LSB (Least Significant Bit): 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. Although LSB hides the message in such way that the humans do not perceive it, it is still possible for the opponent to retrieve the message due to the simplicity of the technique. Therefore, malicious people can easily try to extract the message from the beginning of the image if they are suspicious that there exists secret information that was embedded in the image. Therefore, a system named Video Steganography System to embed secret image is proposed to improve the LSB scheme. It overcomes the sequence-mapping problem by embedding the massage into a set of random pixels, which are scattered on the cover-image. It is a common, simple approach to embedding information in a cover image [1]. The least significant bit (in other words, the 8th bit) of some or all the bits inside an image is changed to a bit of the secret message the technique for increased capacity of information hiding in LSB,,s method gives better performance in all the parameters and is a safe technique for embedding secret messages.[3]For example a grid for 3 pixels of a 24- bit image can be follows:-

(00101101 00011100 01011110)
(10100110 11100100 00001100)
(11011010 10101101 01101011)

When the number 200, whose binary representation is 11001000, is embedded into the Least Significant Bit of this part of the image, the resulting grid is as follows:

(00101101 00011100 01011110)
(10100110 11100100 00001100)
(11011010 10101101 01101011)

Although the number was embedded into the first 8 bits of the grid, only the 3 underlines bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size [2]. Since there are 256 possible intensities of each primary colour, changing the LSB of a pixel results in small changes in the intensity of the colour. In its simplest form LSB makes use of BMP images, since they use lossless compression.

3.2 PSNR (Peak-Signal-to-Noise-Ratio)
Peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. PSNR is most commonly used to measure the quality of reconstruction of loss compression codec's. The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codec's, PSNR is an *approximation* to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not. One has to be extremely careful with the range of validity of this metric; it is only conclusively valid when it is used to compare results from the same codec (or codec type) and same content.

The PSNR (in dB) is defined as:

$$\text{PSNR}=10.log_{10}(\frac{MAX_I^2}{MSE})=20.log_{10}(\frac{MAX_I}{\sqrt{MSE}})$$

$$=20.log_{10}(MAX_I)-10.log_{10}(MSE)$$

3.3 MSB (Most significant bit)
Most significant bit (MSB, also called the high-order bit) is the bit position in a binary number having the greatest value. The MSB is sometimes referred to as the left-most bit due to the convention in positional notation of writing more significant digits further to the left. The MSB can also correspond to the sign bit of a signed binary number

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

in one's or two's complement notation, "1" meaning negative and "0" meaning positive. It is common 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 (such as in 2^{31}...20). Although a few CPU manufacturers assign bit numbers the opposite way the *MSB* unambiguously remains the *most* significant bit. This may be one of the reasons why the term *MSB* is often used instead of a bit number, although the primary reason is probably that different number representations use different numbers of bits.

3.4 RGB pixel indication

The RGB pixel indication is an additive color model in which red, green, and blue light are added together 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 blue. 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 differently, 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 color management.

3.5 DWT Steganography

In DWT Steganography In this method secret data is embedded in the skin region of the image. For that skin colour tone detection is needed to be performed. It is by using HSV colour space. Then cropping is needed to be performed. DWT is needed to be applied on that cropped region of the image. Then one of the high frequency sub band is selected to embed the secret data. Before embedding the secret data it is needed to be encrypted using spread spectrum technique i.e. generating pseudo random noise sequence by using a session based key. Then that encrypted data is embedded on the number of skin pixels in that high frequency sub-band. Then data is extracted at the decoder side by using the session key and size of the secret data.

4. PROPOSED WORK

Steganography is process of hiding secret information behind any image and video file for the secure transmission of data. Image steganography is used for hiding information in the form of text and images. But due to lack of security reason and early detection of hiding information video steganography has been come into utilization. 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. 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.

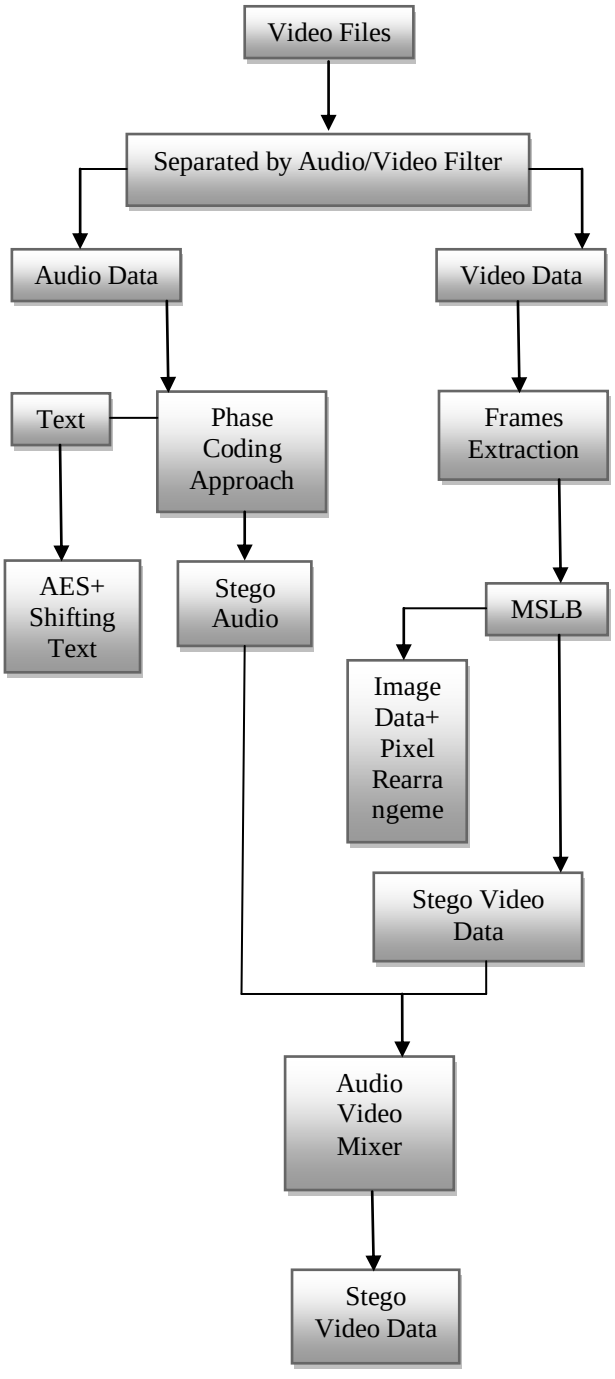

Figure 4.1: Sender Side

DOI 10.17148/IJARCCE.2016.53156

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

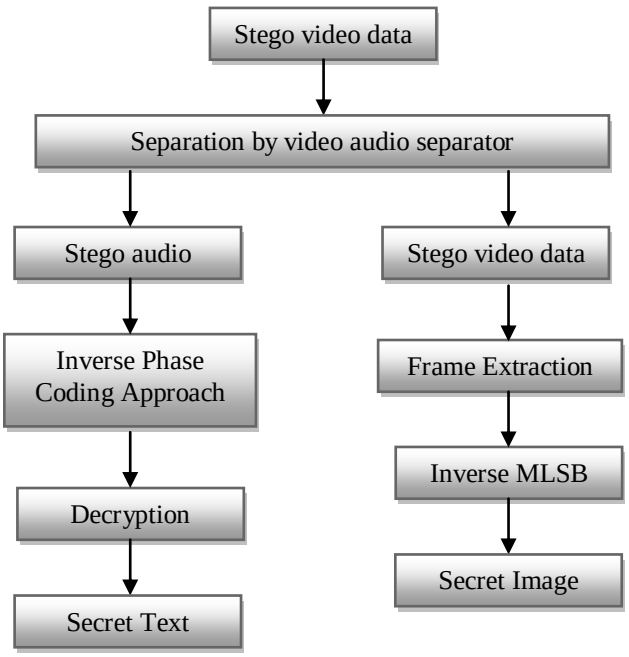

Figure 4.2: Receiver Side

Due to two types of data can be send through video steganography. To overcome the issue of security in proposed work encryption has been introduced.

1. To implement separation approach to separate audio and video data from a video file.
2. To implement MLSB for embedding data to particular frames of video content.
3. To embed text file behind audio file.
4. To reconstruct audio and video to develop stego video.
5. To analyze parameters for performance evaluation.

Video steganography is used for secure transmission of secret data over a communication network. Various approaches have been proposed for the purpose of video steganography. Various phases for video steganography have been described below.

In the first phase of the proposed system the video file separated by using "easy audio video separator" and then video file is read by using video reader. Number of frames has to be extracted using this video reader process. Then audio file is read by using audio reader that defines bits available in audio file.

Secret information is read text and image text information is encrypted using AES algorithm. And a frame no is selected for the embedding of image data to a particular frame. Multiple least significant bits are implemented to that frame for detection of bits available in that frame. Text file is embedded in that audio file bits.

Then audio and video file has been mixed using video mixer and reconstruct the video file and transmit it to user for extraction of secret information.

6. CONCLUSION

Now these days security of information becomes a big issue. We study various papers upon the video Steganography. We decided to improve the video Steganography techniques by using different algorithms. In video Steganography secret data is embedding with different frames available in video files. Then divide that secret data into two different segments and separate the video using separation approach for various separation of audio and video format from video files. Then embed text and images in video file for the purpose of hiding information. Number of approaches has been used for the purpose of the embedding of image and text in video file for the secure transmission type. But there is issue of linkage of data due to signalizes attack. Video composition consumes time for embedding of data.

REFERENCES

[1] S. K. Moon "Data Security Using Data Hiding", Conference on Computational Intelligence and Multimedia Applications, 2007, 247 – 251.
[2] B. Mehboob "A steganography implementation" IEEE Conf. on Biometrics and Security Technologies, 2008, pp. 1 – 5.
[3] S. D. Hu "A Novel Video Steganography Based on Non-uniform Rectangular Partition", IEEE Conf. on Computational Science and Engineering (CSE), 2011, pp 57 – 61.
[4] X. Xu "Universal spatial feature set for video steganalysis" Image Processing (ICIP), 2012, pp 245 – 248.
[5] P. Yadav "A secure video steganography with encryption based on LSB technique", IEEE Conf. on Computational Intelligence and Computing Research (ICCIC), 2013, pp 1 – 5.
[6] K. Patel "Lazy Wavelet Transform Based Steganography in Video", Communication Systems and Network Technologies (CSNT), 2013, pp 497 – 500.
[7] X. Xu "Video steganalysis based on the constraints of motion vectors", IEEE Conf. on Image Processing (ICIP), 2013, pp 4422 – 4426.
[8] S. K. Moon "Application of data hiding in audio-video using anti forensics technique for authentication and data security", IEEE Conf. on Advance Computing Conference (IACC), 2014, pp 1110 – 1115.
[9] Y. Kakde "Audio-video steganography", IEEE Conf. on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015, pp 1 – 6.
[10] R. J. Mstafa "A New Video Steganography Algorithm Based on the Multiple Object Tracking and Hamming Codes", International Conference on Machine Learning and Applications (ICMLA), 2015, pp 335 – 340.
[11] https://goo.gl/TIBwiJ