IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 12, December 2015

A Review on Secure Video Steganography Technique using LSB & ISB

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

Research scholar (M.Tech), Rayat Bahra University, Mohali, India [1]

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

Abstract: Due to the high speed of internet and advances in technology, people are turning out to be more stressed over data being hacked by hackers. Recently, numerous algorithms of steganography and information hiding have been proposed. Steganography is a procedure of inserting the secret data inside the host medium (content, sound, picture and feature). Simultaneously, a large portion of steganography software programs have been given to unauthorized clients to retrieve the secret data that was installed in the embedded files. Some steganography calculations can be effectively recognized by steganalytical detectors due to absence of security and embedded efficiency. In this paper the current steganography strategies are examined.

Keywords: Steganography, Video steganography, Security.

I. INTRODUCTION

The Steganography, Cryptography and Digital Watermarking techniques can be used to obtain security and privacy of data. The steganography is the art of hiding data inside another data such as cover medium by applying different steganography techniques. While cryptography results in making the data human unreadable form called as cipher thus cryptography is scrambling of messages. Whereas the steganography results in exploitation of human awareness so it remains unobserved and undetected or intact. It is possible to use all file medium, digital data, or files as a cover medium in steganography.

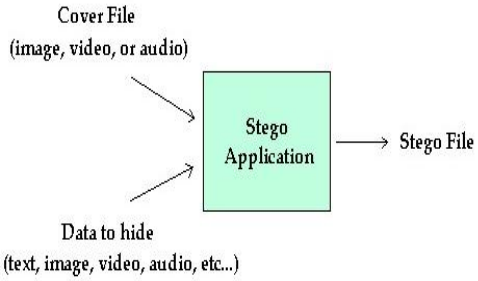

Fig 1: Video Steganography [16]

Generally steganography technique is applied where the cryptography is ineffective. The steganography system consists of the cover file (image, audio, video etc) and the secret message that is hidden inside the cover file by applying steganography the secret message is hidden and stego file is generated which is same as cover image and go undetected or unaltered. Although BMP files are perfect for stenographic use, they are able to carry only small files. So there is a problem, how to get much enough files to hide our message, and what to do to read them in a correct order? Good way out is to hide information in a video file, because as we know, AVI files are created out of bitmaps, combined into one piece, which are played in correct order and with appropriate time gap.

Keeping that in mind all we have to do is to get out is file single frames and save them as BMP files. If we'll use algorithm for hiding data in digital pictures, we can hide our message in bitmap obtained in this way, and then save it into new AVI file.

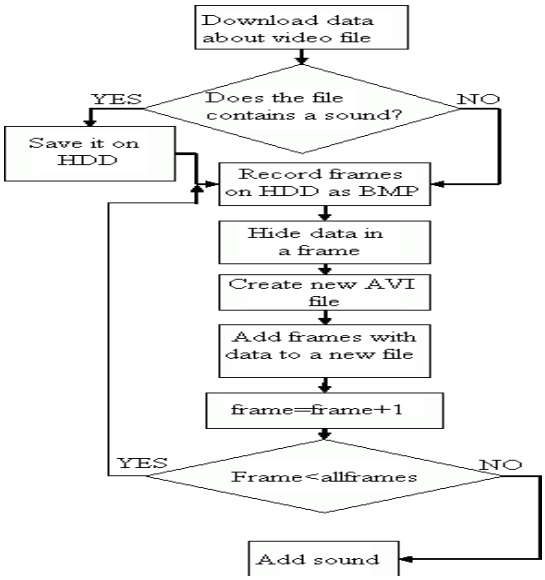

Fig 2: Algorithm of hiding messages in video files.

We'll analyze only uncompressed AVI file, because if any compression is executed files loses its data. AVI files are created out of couple streams. Basic file stream is a video stream and audio stream, which can be file of any extension, for example WAVE. Because of existence of those streams, it is possible to hide data not only in file's frames but also in mentioned audio stream. Thanks to this we can combine opportunities of hiding data in digital pictures and in audio files.

1.1 Cryptography

Cryptography or cryptology; is the practice and study of techniques for secure communication in the presence of third parties. These adversaries are often referred to as Eve in cryptography, while the sender and recipient of messages are called Alice and Bob respectively. More generally, cryptography is about constructing and

DOI 10.17148/IJIREEICE.2015.31222

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 12, December 2015

analyzing protocols that block Eve (or adversaries); various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

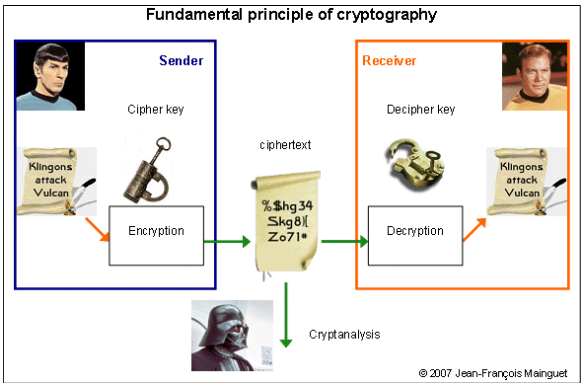

Fig 3: Cryptography

PARAMETERS USED

Peak signal-to-noise ratio: The term peak signal-to-noise ratio (PSNR) is an expression for the ratio between the maximum possible value of a signal and the power of distorting noise that affects the quality of its representation.

Because many signals have a very wide dynamic range, (ratio between the largest and smallest possible values of a changeable quantity) the PSNR is usually expressed in terms of the logarithmic decibel scale. Image enhancement or improving the visual quality of a digital image can be subjective. Saying that one method provides a better quality image could vary from person to person.

For this reason, it is necessary to establish quantitative/empirical measures to compare the effects of image enhancement algorithms on image quality. Using the same set of tests images, different image enhancement algorithms can be compared systematically to identify whether a particular algorithm produces better results.

The metric under investigation is the peak-signal-to-noise ratio. If we can show that an algorithm or set of algorithms can enhance a degraded known image to more closely resemble the original, then we can more accurately conclude that it is a better algorithm.

Mean Squared Error: mean squared error (MSE) of an estimator measures the average of the squares of the "errors", that is, the difference between the estimator and what is estimated. MSE is a risk function, corresponding to the expected value of the squared error loss or quadratic loss. The difference occurs because of randomness or because the estimator doesn't account for information that could produce a more accurate estimate. The MSE is the second moment (about the origin) of the error, and thus incorporates both the variance of the estimator and its bias. For an unbiased estimator, the MSE is the variance of the estimator. Like the variance, MSE has the same units of measurement as the square of the quantity being estimated. In an analogy to standard deviation, taking the square root of MSE yields the root-mean-square error or root-mean-square deviation (RMSE or RMSD), which has the same units as the quantity being estimated; for an unbiased estimator, the RMSE is the square root of the variance, known as the standard deviation.

2. RELATED WORK

Chengdu Hub 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-streams" 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 [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.

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 codecs, 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 codecs.

Tasdemir, K et al [6] "Video steganalysis of LSB based motion vector steganography" his paper proposes a novel flatness measure for video steganalysis targeting LSB based motion vector steganography. The proposed method has introduced two major improvements. Firstly, unlike previous approaches, it takes into account the anchor frame and current frame distances and directions, which significantly affect the correlation strength of adjacent motion vectors. Secondly, it defines a cover model that does not require a training based machine learning system.

Dehkordi, A.B. et al [7] "Robust LSB watermarking optimized for local structural similarity", Digital watermark is an invisible or maybe visible structure added to the original media (known as asset). Images are considered as communication channels when they are subject to a watermark embedding procedure so in the case of embedding a digital watermark in an image, the capacity of the channel should be considered. There is a trade-off between imperceptibility, robustness and capacity for embedding a watermark in an asset. In the case of image watermarks, it is reasonable that the watermarking algorithm should depend on the content and structure of the image. Conventionally, mean squared error (MSE) has been used as a common distortion measure to assess the quality of the images.

Islam, M.R. et al [8] "An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography" In this paper, the proposed technique has focused on Bitmap image as it is uncompressed and convenient than any other image format to implement LSB Steganography method. For better security AES cryptography technique has also been used in the proposed method. Before applying the Steganography technique, AES cryptography will change the secret message into cipher text to ensure two layer security of the message. In the proposed technique, a new Steganography technique is being developed to hide large data in Bitmap image using filtering based algorithm, which uses MSB bits for filtering purpose.

Yi-Chun Liao et al [8] "Data hiding in video using adaptive LSB", Author discuss whether there is any possibility of hiding data in video. Testing our theory, we propose a novel video hiding scheme based on LSB, and we use three-dimensional array to auxiliary our scheme, adaptive LSB data hiding technique, which is a typical method used to achieve information hiding in images, and three-dimensional array used to storage pixels' information of the cover image and the secret image. From the experimental results, we found that our scheme can be easily achieved and hided data into video with imperceptibility. We also implemented a video player with extracting and pasting functions in real-time.

3. PROBLEM FORMULATION

Steganography is an excellent means of conversing covertly if there are guarantees on the integrity of the channel of communication[1]. It is not even necessary for the two parties to agree to a specific hiding format. 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. 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.

4. PROPOSED WORK

Video Steganography is used to transmit different information securely to the receiver. In this the secret information has to be transmitted by embedding secret information behind the different frames of video files. In this process the frames from video files have to be extracted and the frame that is extracted from video is used as cover object. The least significant bit of the video frame has to be computed. After computation of these bits the secret message that has to be embedded behind the cover object is selected & the bit of secret message is embedded behind bits of cover object using XOR operation.

5. APPROACHES USED

New Data Hiding Algorithm in MATLAB utilizing Encrypted secret message.

In this work they have attempted to insert some secret message inside any spread record in encoded shape so that nobody will have the capacity to concentrate real secret message. The system grew in MATLAB.

IJIREEICE
ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526
INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 12, December 2015

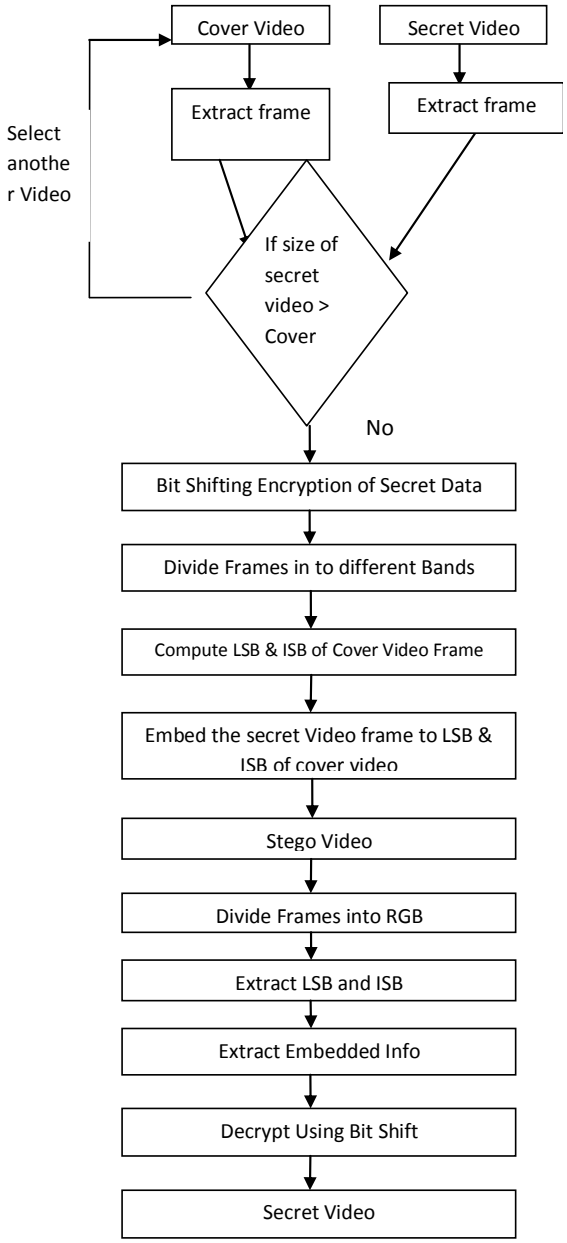

Fig 4: Flow of Proposed Work

They install LSB and LSB+3 bits of the spread record in every other byte position.The encryption of the secret message document here they have taken 5 times however one can go up as far as possible. Anyhow, on the off chance that they expand the encryption number then the procedure turns out to be moderate yet the encryption will be extremely solid.

On a basic level it will be troublesome for anybody to decode the scrambled message without knowing the precise encryption system. Their technique is basically stream figure strategy and it may take colossal measure of time if the records size is expansive and the encryption number is additionally huge.

This present system might most suitable for water stamping. The steganography system may be further secured on the off chance that they pack the secret message first and afterward scramble it and after that at long last install inside the spread record.

Improved LSB method for Video Steganography: As Steganography turns out to be all the more broadly utilized as a part of registering there are a few issues that not to be resolve. Each strategy has a few limits however a few preferences too. The proposed framework is to insert message in sound document and recouped effectively at the collector end. A strategy for inserting content information in sound file utilizing minimum huge bit is been finished. The header part is forgotten as it can make debasement in sound record. This system does not influence the record size of the sound.

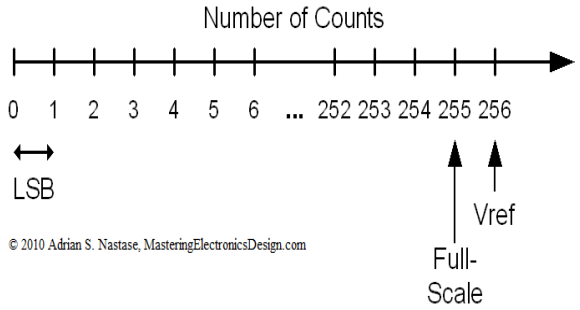

Fig 5: LSB

One count is 1 LSB, and is defined as follows:

$$LSB = \frac{Vref}{2^N} \quad (1)$$

Where N is the ADC's or DAC's number of bits.

For ADCs that have a differential voltage reference, the LSB is

$$LSB = \frac{Vref}{2^N} \quad (2)$$

Where V ref (+) and V ref (-) are the non-inverting and the inverting inputs of the differential voltage reference respectively.

The ADC outputs a digital word that shows how many counts are in its input voltage level. As the ADC counts the input level, it never reaches the voltage reference. Its full scale (FS) is calculated with the following formula:

$$LSB = \frac{Vref}{2^N} \quad (3)$$

After replacing the LSB in equation (3),the ADC full-scale results as in equation (4).

$$LSB = \frac{Vref}{2^N} \quad (4)$$

n our 8-bit ADC example, if the voltage reference is V ref = 5V, then the LSB and FS are:

$$LSB = \frac{Vref}{2^N} \quad (5)$$

As you can see, and ADC can never reach its V ref but, as the number of bits is higher, it gets very close to its reference voltage. The same can be said about a DAC. Moreover, from equation (1), we can write the mathematical relation between V ref and LSB as follows:

$$LSB = \frac{Vref}{2^N} \quad (6)$$

If we replace Vref in equation (3), and after calculations, we can write the definition of the LSB as a function of the ADC's full-scale, as in equation (7).

$$LSB = \frac{Vref}{2^N} \quad (7)$$

This is the trouble, as the LSB has two definitions, equations (1) and (7). Both of them are valid, and some authors are ambiguous or confused about them. I have seen articles in which Vref is considered the component full-scale, which is the premise that generates subsequent wrong definitions.

An Approach of Video Steganography: They proposed the LSB coding with XORing technique in which the information inserting is finished by XORing the LSB's One of the secret signal (information to be installed) utilized as a part of XORing system then secret sign recovered from the stego at the beneficiary side. It is seen from this that there is no distinction between the first and recovered message, that implies the recuperation is 100%.The message recovered when the LSB's of the stego sign are extricated specifically. This shows that the immediate extraction of LSB's will just result in commotion if inserting is done utilizing XORing technique. Along these lines it builds the security.

6. CONCLUSION

As Steganography turns out to be all the more broadly utilized as a part of figuring there are a few issues that not to be resolve. Each strategy has a few restrictions yet a few preferences moreover. Sound steganography is more difficult than picture steganography on the grounds that the has more accuracy than human visual framework (HVS). As steganography proceeds on its developmental way specialists have uncovered new stages where steganographic systems could be utilized to conceal data flawlessly. Such research endeavors have revived the innovative work endeavors situated towards steganography stages and steganalysis and various.

REFERENCES

[1]. Nedeljko Cvejic ,Tapio Seppben " Increasing the capacity of LSB Based audio Steganography", IEEE Conf. on LSB Method, 2002.
[2]. Chengdu Hub "A Novel Video Steganography Based on Non-uniform Rectangular Partition" International Conference on Intelligence and multimedia Application. IEEE 2007
[3]. Bin Liu "Secure Steganography in Compressed Video Bit-streams", IEEE Conf. on Pervasive Computing (JCPC), 2009, pp 185 – 190
[4]. Balaji, R. "Secure data transmission using video Steganography", National Conference on emerging computing , 2010.
[5]. Keren Wang "Video Steganalysis Against Motion Vector-Based Steganography by Adding or Subtracting One Motion Vector Value", IEEE Conf. on Electrical Engineering (ICEE), 2011, pp 1.
[6]. Tasdemir, K "Video steganalysis of LSB based motion vector steganography", International Conference on Communication Systems and Network Technologies, 2011.
[7]. Dehkordi, A.B. "Robust LSB watermarking optimized for local structural similarity", International conference, 2011.
[8]. Islam, M.R. "An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography", International Journal of Computer Applications (0975 - 8887) Volume 7- No.9, October2011.
[9]. Yi-Chun Liao "Data hiding in video using adaptive LSB", IEEE Conf. on Coimbatore, India IEEE-20180, 2012.
[10]. Prof. Samir Kumar Bandyopadhyay and Barnali Gupta Banik "Multi-Level Steganographic Algorithm for Audio Steganography using LSB Modification and Parity Encoding Technique" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 2012.
[11]. Ramadhan J. Mstafa and Khaled M. Elleithy "A Highly Secure Video Steganography using Hamming Code (7, 4)" Senior Member, IEEE Department of Computer Science and Engineering University of Bridgeport, 2012.
[12]. Pooja P. Balgurgi, Prof. Sonal K. Jagtap "Intelligent Processing: An Approach of Audio Steganography" International Conference on Communication, Information & Computing Technology (ICCICT), Oct. 19-20, Mumbai, 2012.
[13]. Tasdemir, K "Video steganalysis of LSB based motion vector steganography", IEEE Conf on Visual Information Processing (EUVIP), 2013, pp 260 – 264.
[14]. NehaGupta, Ms. Nidhi Sharma "Dwt and Lsb Based Audio Steganography" 2014 International Conference on Reliability, Optimization and Information Technology ICROIT 2014, India, Feb 6-8 2014.
[15]. 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