ISSN No. 0976-5697

Volume 7, No. 6(Special Issue), November 2016

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Modified Data Hiding Approach for Audio and Video Data

Neha Singla
M.Tech Regular Scholar
Computer Science Section
Yadvindra College of Engineering,
Talwandi Sabo,Bathinda,Punjab.
singlaneha564@gmail.com

Raj bhupinder Kaur
Assistant Professer,
Computer Engineering Dept.
Yadvindra College of Engineering
Talwandi Sabo,Bathinda,Punjab
er.rajbhupinder@gmail.com

Abstract*-Video Steganography is emerging area of research for secure transmission of data. In the process of video data hiding frames of the video file have been used. Due to utilization of frames large amount of data can be easily embedded behind the frames of file. In this paper secure video data hiding approach has been purposed that use multiple bits of the pixels for embedding of secret information. By using multiple bits stagnalysis cannot be easily implemented on the stego video file for extraction of secret information. This paper comprises text and video data hiding behind a single video file components that are audio and video.*

Keywords:LSB& ISB, audio and video, text file performance evaluation.

1 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.

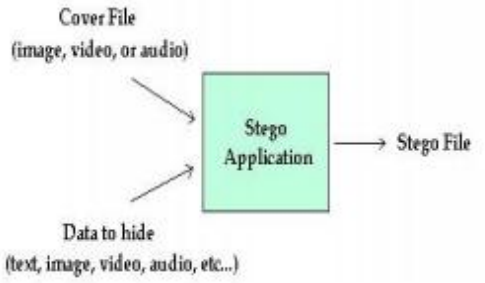

Fig 1: Video Steganography [16]

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.

1.1HISTORY OF STEGANOGRAPHY

It is believed that steganography was first practiced during the Golden Age in Greece. An ancient Greek record describes the practice of melting wax off wax tablets used for writing messages and then inscribing a message in the underlying wood. The wax was then reapplied to the wood, giving the appearance of a new, unused tablet. The resulting tablets could be innocently transported without anyone suspecting the presence of a message beneath the wax. An ancient Greek record describes the practice of melting wax off wax tablets used for writing messages and then inscribing a message in the underlying wood. The wax was then reapplied to the wood, giving the appearance of a new, unused tablet. The resulting tablets could be innocently transported without anyone suspecting the presence of a message beneath the wax. Later on Germans developed microdot technology which FBI Director J. Edgar Hoover referred to as "the enemy's masterpiece of espionage. Microdots are photographs the size of a printed period having the clarity of standard-sized typewritten pages. The first microdots were discovered masquerading as a period on a typed envelope carried by a German agent in 1941. The message was not hidden, nor encrypted. It was just so small as to not draw attention to itself. Besides being so small, microdots permitted the transmission of large amounts of data including drawings and photographs. Another common form of invisible writing is through the use of Invisible inks. Such inks were used with much success as recently as WW-II. An innocent letter may contain a very different message written between the lines. Early in WW-II steganographic technology consisted almost exclusively of invisible inks. Common sources for invisible inks are milk, vinegar, fruit juices and urine. All of these darken when heated.

1.2 USES OF STEGANOGRAPHY

1. 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.
2. 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 steganographic 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, steganographic methods can be used to hide this.
4. 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.
5. 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.

2. REVIEW OF LITERATURE

Hamad A. Al-Korbi et al[2015] "High-capacity image steganography based on Haar DWT for hiding miscellaneous data" Steganography can be defined as the art and science of concealing private data within a carrier that could be a video, an image, an audio or a text that acts as a cover medium. Many steganography techniques exist; each has its own advantages and limitations. Capacity, robustness and the overall level of security are among the main factors to assess the performance of steganography algorithms. Also, the level of the stego-image distortion should be acceptable This paper aims at proposing a high capacity and efficient steganography technique, where binary images, color images, and large text files can be all concealed within a single cover image at the same time using Haar Wavelet transform. A high capacity of about 99% has been achieved using the proposed algorithm, with low mean square error (MSE) and high power signal-to-noise ratio (PSNR). This algorithm is developed with the aid of MATLAB environment. The obtained results from the proposed algorithm have been promising in terms of efficiency, performance, and capacity.

Md. Rashedul Islam et al[2014] "An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography" In Steganography, the total message will be invisible into a cover media such as text, audio, video, and image in which attackers don't have any idea about the original message that the media contain and which algorithm use to embed or extract it. 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. This method uses the concept of status checking for insertion and retrieval of message. This method is an improvement of Least Significant Bit (LSB) method for hiding information in images. It is being predicted that the proposed method will able to hide large data in a single image retaining the advantages and discarding the disadvantages of the traditional LSB method. Various sizes of data are stored inside the images and the PSNR are also calculated for each of the images tested. Based on the PSNR value, the Stego image has higher PSNR value as compared to other method. Hence the proposed Steganography technique is very efficient to hide the secret information inside an image.

Ratnakirti Roy et al[2014] "Image steganography with block entropy based segmentation and variable rate embedding"
Steganography is the art and science of concealing information inside apparently innocuous covers like images, audio and video such that the very existence of the hidden message remains imperceptible toan adversary. Image steganography has numerous implementations developed over time. It is evident that certain areas in the image are more efficient for hiding data than the others. Such regions are called Regions of Interest. This paper proposes an object based image steganography technique that utilizes image entropy to segment smooth and textured areas in a cover image and then embed data with a variable data rate high efficiency embedding scheme.

P. M. Siva Raja et al[2013] "An efficient data embedding scheme for digital images based on Particle Swarm Optimization with LSBMR" As an important component of multimedia information security, information hiding has received wide attention in recent years. In fact, intellectual properties are becoming harder to protect and so are original contents, that's why we need techniques to be developed such as Image Steganography. Steganography is a technique for information hiding. It aims to embed secret data in to digital cover media, such as Images, Audio and Video without being suspicious. Evolutionary algorithms are stochastic search methods that mimic the natural bio logical evolution and the social behaviour of species. Such algorithms have been developed to arrive at near optimum solutions to large-scale optimization problems. For which traditional mathematical techniques may fail. In this paper, a novel stenographic method, based on Particle Swarm Optimization algorithm (PSO) is proposed, PSO is an evolutionary computational model based on Swarm intelligence. Kennedy and Elbe hart developed PSO through simulating social behavior. In PSO, each individual is called a "particle" and the

978-93-85670-72-5 © 2016 (RTCSIT)

position of each particle is a candidate solution to a problem. LSB Matching Revisited (LSBMR) image steganography using Particle Swarm Optimization algorithm (PSO) is proposed, in Particle Swarm Optimization algorithm (PSO) is used to select the embedding regions according to the size of the secret message and to optimize the threshold value of the selected image regions. In order to improve the quality of stego images, an optimal substitution matrix for transforming the secret messages is first derived by means of the PSO algorithm. The experimental results show that our proposed method has larger message capacity and better image quality then the existing method.

Jian Huang et al[2012] "Implementation of the RTMP server based on embedded system" Based on embedded Linux operating system, the major control messages and streaming media service functions of the RTMP server is analyzed in detail, and the powerful streaming media function of adoble company's flash media server is simplified to transplant the services of the live and VOD streaming media to embedded system. The experimental results shows the transplanted services can be successfully run on TMS320DM6467T chip evaluation boards, and support the service of real-time or on demand publish of video and audio.

3. METHDOLOGY

• Video Data Hiding

Video data hiding is the process for hiding information behind the frames of a video file. Frame of a video contain information about different true colors. True colors are RED, GREEN and BLUE. These three colors are used for development of different pixels in a file. In the purposed work video and audio data has been used for embedding behind a single video file. Audio signal has been extracted from the image and used for hiding text message behind audio. Secret video has been used for embedding behind frames of cover video from which audio signal has been extracted.

In the purposed work cover video has been used for extraction of audio signal using easy audio video converter. After extraction of audio video file has been loaded to the system and frames from the video file has been extracted. After frame extraction frames have been divided into three different true colors bands.

After division of the true color band pixels of red, green and blue region has been divided into binary format for extraction of LSB, ISB and MSB. 240 is the pixel value that has been divided into 8 bit format for detection LSB, ISB and MSB.

Table 3.1 LSB, ISB and MSB of a pixel

Value	128	64	32	16	8	4	2	1
Bits	1	1	1	1	0	0	0	0
	MSB		ISB			LSB		

This table represents binary division of pixel value 240. On the basis of binary division most significant bits are identified that can change whole pixel value during a single modification. Least significant bits are those bits that do not affect too much the quality of the pixel during change.

After extraction of LSB and ISB pixels secret information that has been converted into binary format has been embedded behind pixel LSB and ISB based on intensity value of the single pixel. If the pixel intensity is much higher then LSB can be used if a pixel having low intensity then ISB and LSB can be used for data hiding.

To embed pixel information behind the cover pixel XOR operation has been used that set the value of pixel at a particular bit using XOR operation.

Table 3.2 XOR operation for data embedding

Cover Bit	Secret Bit	Output
0	0	0
0	1	1
1	0	1
1	1	0

This table represents data embedding that has been done by using different bits of the cover and secret data. On the basis of these bits embedding output bit has been executed.

After embedding whole secret information behind cover frame all the frames have been reconstructed to from a stego video that contains secret information behind pixels.

• Audio Data Hiding

After video audio data has been hiding behind spectrums of the audio file. Audio wav file has been read by the system and different frequency bands have been extracted from the signal. These bands have been used for data embedding. To embed secret message has been encrypted using blowfish encryption scheme that use a key for conversion of data into different cipher text so that originality of data can be changed. After these bits of the cipher text has been added to the phases of the audio signal. If a secret bit that has to be embed is 0 then old phase of audio signal is subtracted by pi/2 and if secret information bit is 1 then audio old phase has been added by pi/2.

After embedding the secret information behind the phase of audio signal all the bands are merged to form a stego audio signal. These signals can be transmit along with stego video data to receive end for secure data transmission.

4. RESULTS

In experimental setup of purposed work different videos have been used for embedding of secret video and text information. In this setup video has been selected that are compressed free. Due to use of codec in video file data cannot be embedded easily. In the purposed work MP4, AVI format videos have been used for data embedding.

Video file format has been represented in the described table that represents different parameters of a video file. These video files have been used for data embedding.

Table 4.1 video parameters

Parameters	Description
Format	AVI, Mp4

978-93-85670-72-5 © 2016 (RTCSIT)

Duration	In seconds
Bits/ pixel	24
Frame Rate	25
Height	360
Width	640
No. of frames	299

This table represents different video parameters that have been used for data embedding. These parameters provide information about components of a video file.

After extraction of video parameters from video file parameters have been used for embedding of secret information. Secret information has been embedded behind LSB, ISB on the basis of pixel intensity.

In the purposed work various parameters have been analyzed for performance evaluation of purposed system. These parameters provide information about distortion occurred in the video file after embedding secret information. These performance evaluation parameters are PSNR and MSE.

a. PSNR (Peak Signal to Noise Ratio)

PSNR stands for 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. PSNR is usually expressed in terms of the logarithmic decimal scale. PSNR is used to measure the quality of image (stego-image). The signal or input in this case is the original data, and the noise is the error introduced by compression. The PSNR is defined as:

$$\text{PSNR} = 10.\log_{10}\left(\frac{\text{MAX}_1^2}{\text{MSE}}\right)$$

$$= 20.\log_{10}\left(\frac{\text{MAX}_1}{\sqrt{\text{MSE}}}\right)$$

$$= 20.\log_{10}(\text{MAX}_1) - 10.\log_{10}(\text{MSE})$$

Although a higher PSNR generally indicates that the good quality of image. PSNR is most easily defined via the mean squared error (MSE). Here, MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. In this expression, PSNR is inversely proportional to the MSE, if the PSNR is high then MSE is low and if the PSNR is low then MSE is high.

b. MSE (Mean Square 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. It is basically a difference between the cover image and stego image. If the value of MSE is low, then the quality of the stego image is better. 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 MSE is defined as:

$$\text{MSE} = \frac{1}{\text{mn}}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Table 5.3 PSNR for

Video	LSB+ISB (in dB)	LSB(in dB)
Video1	45.18	34.79
Video2	45.30	35.45
Video3	44.56	33.56
Video4	44.90	36.76

Table 5.1 PSNR value for cover and stego video

This table represents comparison of purposed work with previous approach on the basis of parameter peak signal noise ratio.

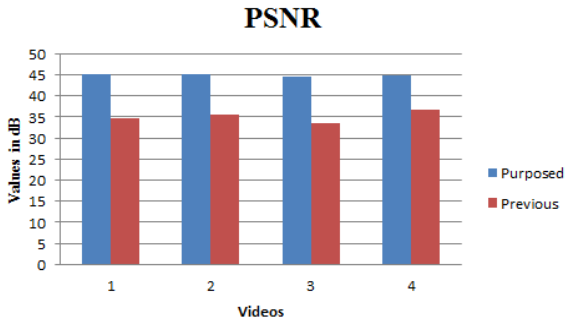

Fig 4.2 Graphical represention of PSNR

This graph represnets the comparision between the PSNR value obtained by previous and proposed approach. proposed approach attain much higher PSNR than previous approaches.

Table 5.2 PSNR value for cover and stego video

Video	LSB+ISB	LSB
Video1	0.065	0.45
Video2	0.07	2.06
Video3	0.063	0.67
Video4	0.074	1.79

This table represents comparison of proposed work with previous approach on the basis of parameter mean square error.

978-93-85670-72-5 © 2016 (RTCSIT)

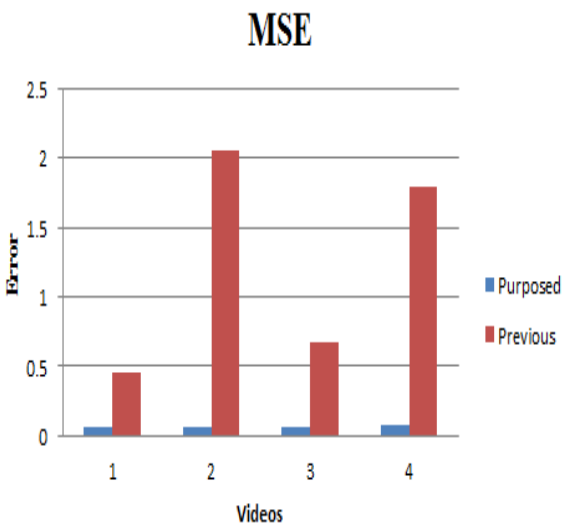

Fig 4.3 Graphical represention of MSE

This graph represnets the comparision between the MSE value obtained by previous and proposed approach. proposed approach attain much lower MSE than previous approaches.

5. CONCLUSION & FUTURE SCOPE

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.

In this first issue that due to embedding behind least significant bits of video frames steganalysis can be one easily on these frames to retrieved data. Second issue is that on embedding the data size of data gets increases which are not easy to transmit over the network. We removed this problem by using various types of approaches i.e. LSB+ISB.

In the future reference video steganography can be used for high secure transmission of secret information by using a onetime password embedding approach. This may validate accessibility of guaranteed receiver that can extract hidden information. In the second way detection of ISB sometimes cause problem to high value pixels for embedding of secret information. One can be research to remove of this effect.

6. REFRENCES

[1] Bin Liu, "Secure Steganography in Compressed Video Bit streams", *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 IslandSystemsApplications and Technology Conference (LISAT), 2014*, pp. 1–6

[5] Marwaha, P. "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 conference on Visual Information Processing (EUVIP), 2013, pp. 260–264.

[10] Hamad A. Al-Korbi "High-capacity image steganography based on Haar DWT for hiding miscellaneous data" IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies,pp. 1–6,2015.

[11] Md. Rashedul Islam "An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography" IEEE International Conference on Informatics, Electronics & Vision,pp. 1–6,2014.

[12] Ratnakirti Roy "Image steganography with block entropy based segmentation and variable rate embedding" IEEE International Conference on Business and Information Management,pp- 75–80,2014.

[13] P. M. Siva Raja "An efficient data embedding scheme for digital images based on Particle Swarm Optimization with LSBMR" IEEE International Conference on Computational Intelligence and Information Technology,pp. 17–24,2013.

978-93-85670-72-5 © 2016 (RTCSIT)

[14] Jian Huang, "Implementation of the RTMP server based on embedded system" IEEE International Conference on Computer Science and Information Processing,pp. 160 – 162,2012.

978-93-85670-72-5 © 2016 (RTCSIT)