Multimedia based Steganography using PMM and M4M

Souvik Bhattacharyya
Department of CSE
University Institute of Technology,
The University of Burdwan
West Bengal, India

Indradip Banerjee
Department of CSE
University Institute of Technology,
The University of Burdwan
West Bengal, India

Gautam Sanyal
Department of CSE
National Institute of Technology,
Durgapur
West Bengal, India

ABSTRACT
In today's highly digitalized world maintaining the secrecy of the secret data is a vital problem. Steganography is an emerging area which may be used for secure transmission of the digital data. It is the art and science of embedding data into different covers such that the data embedded is imperceptible. The covers that can be used cover all forms of digital multimedia object namely text, image, audio and video. This paper proposes a novel multimedia based steganography technique for an un-compressed movie. This proposed work hides the data both in audio and video signal part of the movie. In video part data hiding operations are executed entirely in the discrete integer wavelet domain by converting the gray level version of each frame of the video in to transform domain using discrete integer wavelet technique through 2-D lifting scheme through Haar lifted wavelet. For providing an imperceptible stego-frame/stego-video for human vision, a novel image based steganographic approach called pixel mapping method (PMM) is used for data hiding in the wavelet coefficients. To enlarge the embedding capacity the secret information also has been embedded in the audio portion of the movie with the help of M4M technique**.** Experimental results demonstrate that the proposed algorithm has high imperceptibility and capacity and produces satisfactory results.

General Terms
Steganography, Cover Image, Cover Audio, Stego Image, Stego Audio***.***

Keywords
PMM (Pixel Mapping Method), M4M (Mod 4 Method),Integer Wavelet Transform.

1. INTRODUCTION
The majority of today's steganographic systems uses multimedia objects like image, audio, video etc as cover media. In modern approach, depending on the nature of cover object, steganography can be divided into four types: Text Steganography, Image Steganography, Audio Steganography and Video Steganography [1]. Encoding secret messages in text can be a very challenging task. This is because text files have a very small amount of redundant data to replace with a secret message. There are numerous methods by which to accomplish text based Steganography [3-6].Coding secret messages in digital images is the most widely used amongst the all digital methods. This is because it can take advantage of limited power of the Human Visual System (HVS). Almost any plain text, cipher text, image and any other media that can be encoded into a bit of stream can be hidden in a digital image [7-9]. Encoding secret messages in audio is the most challenging techniques to use when dealing with Steganography [11]. This is because the Human Auditory System (HAS) has such a dynamic range that it can listen over. When information is hidden inside video [10, 12] the program or person hiding the information will usually use the DCT (Discrete Cosine Transform) method. Steganography in Videos is similar to that of Steganography in Images, apart from information is hidden in each frame of video.

This paper has been organized as following sections: - Section 2 discusses about some of the related works done based on image steganography where as Section 3 and section 4 describes some related works on audio steganography and video steganography respectively. Section 5 deals with proposed method on multimedia based video steganography. Section 6 describes different algorithms for different functions used at both at sender side and receiver side. Experimental results are discussed in Section 7 and Section 8 draws the conclusion.

2. REVIEW OF RELATED WORKS ON IMAGE STEGANOGRAPHY
In this section various image based steganography method namely LSB (least-significant-bit), PVD (pixel-value differencing), GLM (gray level modification) and the method proposed by Ahmed et al. has been presented.

2.1 Data Hiding by LSB
Various techniques about data hiding have been proposed in literatures. One of the common techniques is based on manipulating the least-significant-bit (LSB) [8], [13] and [14] planes by directly replacing the LSBs of the cover-image with the message bits. LSB methods typically achieve high capacity but unfortunately LSB insertion is vulnerable to slight image manipulation such as cropping and compression.

2.2 Data Hiding by PVD
The pixel-value differencing (PVD) method proposed by Wu and Tsai [17] can successfully provide both high embedding capacity and outstanding imperceptibility for the stego image. Based on PVD method, various approaches have also been proposed. Among them Chang et al. [11] proposes a new method using tri-way pixel-value differencing.

2.3 Data Hiding by GLM

In 2004, Potdar et al. [10] proposes GLM (Gray level modification) technique which is used to map data by modifying the gray level of the image pixels. Gray level modification Steganography is a technique to map data (not embed or hide it) by modifying the gray level values of the image pixels.

2.4 Data Hiding by the method proposed by AHMAD et al.

In this work [1] a novel Steganographic method for hiding information within the spatial domain of the gray scale image has been proposed. The proposed approach works by dividing the cover into blocks of equal sizes and then embeds the message in the edge of the block depending on the number of ones in left four bits of the pixel.

3. REVIEW OF RELATED WORKS ON AUDIO STEGANOGRAPHY

This section presents some existing techniques of audio data hiding namely Least Significant Bit Encoding, Phase Coding Echo Hiding and Spread Spectrum techniques. There are two main areas of modification in an audio for data embedding. First, the storage environment, or digital representation of the signal that will be used, and second the transmission pathway the signal might travel [4, 11].

3.1 Least Significant Bit Encoding

By substituting the least significant bit of each sampling point with a binary message bit, LSB coding allows a data to be encoded in to the cover audio and produces the stego audio. In LSB coding, the ideal data transmission rate is 1 kbps per 1 kHz. The main disadvantage of LSB coding is its low embedding capacity. A novel method of LSB coding which increases the limit up to four bits is proposed by Nedeljko Cvejic Et al. [28, 29]. There is other two disadvantages also associated LSB coding. The first one is that human ear is very sensitive and can often detect the presence of single bit of noise into an audio file. Second disadvantage however, is that LSB coding is not very robust.

3.2 Phase Coding

Phase coding [29, 30] overcomes the disadvantages of noise induction method of audio steganography. Phase coding designed based on the fact that the phase components of sound are not as perceptible to the human ear as noise is. This method encodes the message bits as phase shifts in the phase spectrum of a digital signal, achieving an inaudible encoding in terms of signal-to-noise ratio.

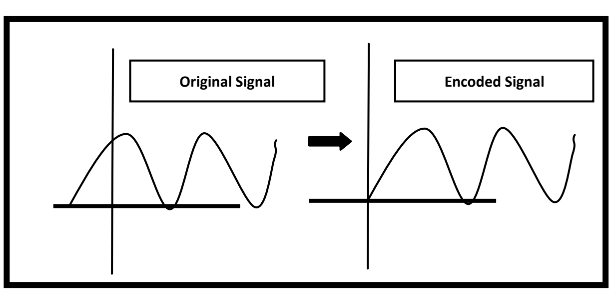

Fig 1: The original signal and encoded signal of phase coding

The disadvantage associated with phase coding is that it has a low data embedding rate due to the fact that the secret message is encoded in the first signal segment only.

3.3 Echo Hiding

In echo hiding [29, 31, 32] method information is embedded into an audio file by inducing an echo into the discrete signal. Like the spread spectrum method, Echo Hiding method also has the advantage of having high embedding capacity with superior robustness compared to the noise inducing methods. To extract the secret message from the final stego audio signal, the receiver must be able to break up the signal into the same block sequence used during the encoding process.

3.4 Spread Spectrum

Spread Spectrum (SS) [29] methodology attempts to spread the secret information across the audio signal's frequency spectrum as much as possible. This is equivalent to a system using the LSB coding method which randomly spreads the message bits over the entire audio file. The difference is that unlike LSB coding, the SS method spreads the secret message over the audio file's frequency spectrum, using a code which is independent of the actual signal. As a result, the final signal occupies a more bandwidth than actual requirement for embedding. The Spread Spectrum method has a more embedding capacity compared to LSB coding and phase coding techniques with maintaining a high level of robustness. However, the SS method shares a disadvantage common with LSB and parity coding that it can introduce noise into the audio file at the time of embedding

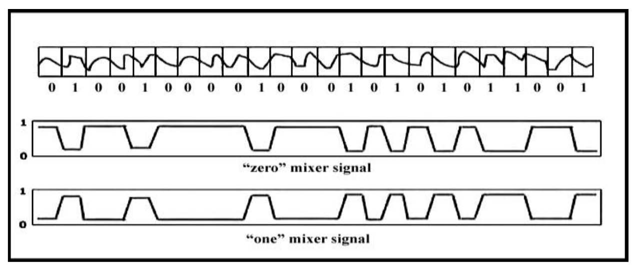

Fig 2: Echo Hiding Methodology

4. REVIEW OF RELATED WORKS ON VIDEO STEGANOGRAPHY

Several approaches are studied in video data steganography literature. In this section, some of the most well-known approaches have been discussed.

4.1 Data Hiding in Video by LSB

The most common method is Least Significant Bit method (LBS) which hide secret data into the least significant bits of the host video [18], [19] and [20]. This method is simple and can hide large data but the hidden data could be lost after some file transformations.

4.2 Data Hiding in Video by Spread Spectrum Methodology

Another well-known method which has been still researching is called Spread Spectrum [20], [21]. This method satisfies the robustness criterion. The amount of hidden data lost after applying some geometric transformations is very little. The amount of hidden lost is also little even though the file is compressed with low bit-rate. This method satisfies another criterion is security.

4.3 Data Hiding in Video by DCT

Wang et. al. presented a technique for high capacity data hiding [24] using the Discrete Cosine Transform (DCT) transformation. Its main objective is to maximize the payload while keeping robustness and simplicity. Here, secret data is embedded in the host signal by modulating the quantized block DCT coefficients of I- frames.

4.4 Data Hiding in Video by Some Other Methods

There are also some introduced methods that base on multi-dimensional lattice structure [22] or enable high quantity of hidden data and high quantity of host data by varying the number of quantization levels for data embedding [24]. Lane proposed a vector embedding method [25] that uses a robust algorithm with video codec standard (MPEG-I and MPEG-II). This method embeds audio information to pixels of frames in host video. Moreover, a robust against rotation, scaling and translation (RST) method was also proposed for video watermarking [23]. In this method, secret information is embedded into pixels along the temporal axis within a Watermark Minimum Segment (WMS).

5. PROPOSED METHOD FOR MULTIMEDIA BASED VIDEO STEGANOGRAPHY

Multimedia is media and content that uses a combination of different content forms. The term is used in contrast to media which only use traditional forms of printed or hand-produced material. Multimedia includes a combination of text, audio, still images, animation, video, and interactivity content forms. Multimedia is usually recorded and played, displayed or accessed by information content processing devices, such as computerized and electronic devices, but can also be part of a live performance. Multimedia is distinguished from mixed media in fine art; by including audio, for example, it has a broader scope. The term "rich media" is synonymous for interactive multimedia. Hypermedia can be considered one particular multimedia application.

Multimedia steganography is a method of hiding the message in multimedia files of any formats e.g. if suppose the cover medium is a video file which is a combination of Images (image frames) and an audio file, steganographic techniques can be implemented on both the image sequence and the audio to hide some data.

In this paper a new approach towards Multimedia Steganography (Video which includes new image and audio steganographic techniques) has been proposed which comes with the following challenges:

- **Video Format Selection:** Different video formats have different way of packing data into itself. So it's quite a challenging task to design a general algorithm which work's for all/most of the video formats.
- **Lack of References:** Very less of work has been done in this field, so the approach towards the goal to obtain a Multimedia Steganographic system is a very challenging task.
- **Disintegrating and integrating the Image Sequence and Audio:** Obtain the Stego Video with no/unrecognizable distortion and at the same time maintaining the properties of the Stego Video with respect to the original cover video file.

5.1 The Problem Abstract

The idea is to develop a new technique for data hiding in a video that would enable hiding data in the image frame sequence of the video and in the audio part extracted from the video. The method should be robust enough so that the secret message in the video cannot be detected easily/at all.

Image Steganography: Pixel Mapping Method (PMM) [26-27] is used on the image sequence generated from the video rather than embedding the message bit directly image a mapping is done so that it cannot be easily detected and become hard to obtain the secret message even if it is detected.

Audio Steganography: An approach based on the **Mod 16 Method (M16M) [33]** named **Mod 4 Method (M4M) [36]** along with a **Number Sequence Generator Algorithm** to avoid embedding data in the consecutive indexes of the audio, which will eventually help in avoiding distortion in the audio quality, has been used to embed data in the audio extracted from the video.

Video Steganography: The above two developed techniques are incorporated in a single algorithm in the ***Wavelet domain*** to embed data in the Video (= Image Sequence + Audio) as a whole.

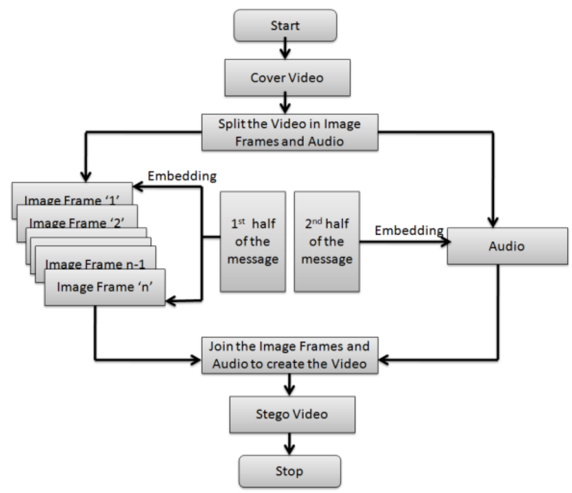

Fig 3: Sender Side System Overview

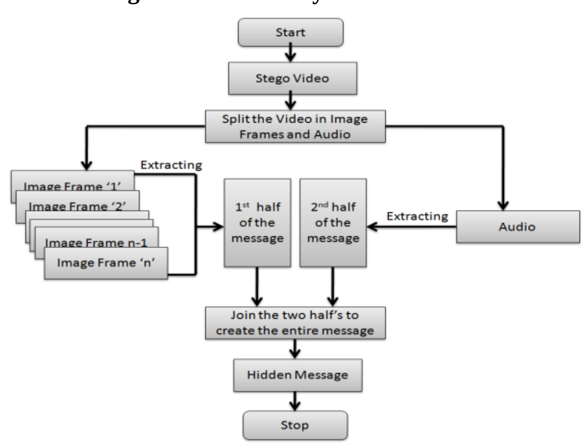

Fig 4: Receiver Side System Overview

6. ALGORITHMS FOR MULTIMEDIA BASED VIDEO STEGANOGRAPHY

6.1 Data Hiding in Image using PMM:

Pixel Mapping Method (PMM) [26-27] is a method for data hiding within the spatial domain of any gray scale image. The input messages can be in any digital form and are often treated as a bit stream. Embedding pixels are selected based on some mathematical function which depends on the pixel intensity value of the seed pixel and its 8 neighbors are selected in counter clockwise direction. Before embedding a checking has been done to find out whether the randomly selected pixel or its neighbor lies at the boundary of the image or not. Data embedding are done by mapping each two bit of the secret message in each of the neighbor pixel based on the intensity value and no of ones (in binary) present in that pixel. In Fig.5 mapping information has been shown. Extraction process starts again by selecting the same pixels required during embedding. At the receiver side other different reverse operation has been carried out to get back the original information.

PAIR OF MSG BIT	PIXEL INTENSITY VALUE	NO OF ONES (BIN)
01	EVEN	ODD
10	ODD	EVEN
00	EVEN	EVEN
11	ODD	ODD

Fig 5: Mapping Technique for embedding of two bits

Data Embedding through PMM

a) Select a cover image and a secret message.
b) Select the Embedding Seed Pixels and its 8 neighbours in counter clockwise direction based on a mathematical function.
c) Check whether the selected seed pixel or its neighbour lies at the boundary of the image or not.
d) Map each two bit of the secret message in each of the neighbour pixel based on the intensity value and no of one's (in binary) present in that pixel to obtain a stego image.

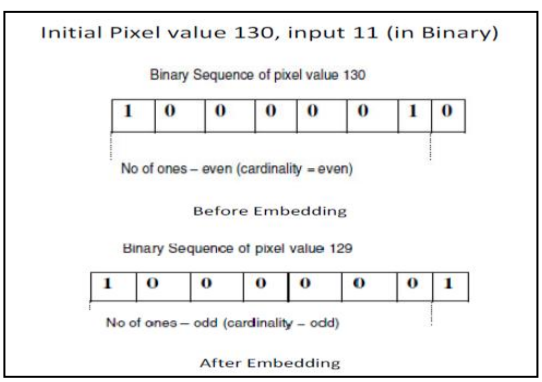

Fig 6: A snapshot of data embedding process of PMM.

Data Extraction through PMM

Extraction process starts again by selecting the same pixels required during embedding. At the receiver side other different reverse operation has been carried out to get back the original information.

6.2 Data Hiding in Audio using M4M

Mod 4 Method (M4M) [36] is a technique for imperceptible audio data hiding in an audio file of wav or mp3 format. This approach based on the Mod 16 Method (M16M) [33] designed for image named Mod 4 Method (M4M) along with a Number Sequence Generator Algorithm to avoid embedding data in the consecutive indexes of the audio, which will eventually help in avoiding distortion in the audio quality. The input messages can be in any digital form, and are often treated as a bit stream. Embedding positions are selected based on some mathematical function which de-ends on the data value of the digital audio stream. Data embedding is performed by mapping each two bit of the secret message in each of the seed position, based on the remainder of the intensity value when divided by 4. Extraction process starts by selecting those seed positions required during embedding. At the receiver side other different reverse operation has been carried out to get back the original information.

6.3 Data Embedding Method

Mod 4 Method (M4M) Sending Algorithm is described as:

- Input: Sampled Audio Data Matrix (a), Message.
- msg = Message converted to binary ;
- Initialize m = n = cnt = x =1 and l=cnt;
- Begin for loop starting with i=1, incrementing 2 and till msize;
- Increment cnt and l by 1 and assign i to count;
- msg0=0; msg1=1;
- let cvr contains the value at a(m,n);
- if cvr is negative then sgn = -1 else sgn = 1;
- R is the absolute remainder after dividing cvr by 4;
- msgx1=binmsg(count) and increment count by 1;
- msgx2=binmsg(count) and increment count by 1;
- If(msgx1=msg0 and msgx2=msg0) cvr = cvr - R;
- Else if (msgx1=msg0 and msgx2=msg1)
- cvr = cvr - R + 1;
- Else if (msgx1=msg1 and msgx2=msg0)
- cvr = cvr - R+ 2;
- Else if (msgx1=msg1 and msgx2=msg1)
- cvr = cvr - R +3;Divide cvr by 1000;
- If sgn = -1 then cvr = cvr * -1;
- Set the value of cvr at a(m,n);
- Let r be the remainder after dividing x by 4;
- If r = val then m = m + r+1; where val = 0, 1 , 2 and 3;
- x = x + 1;
- End For loop

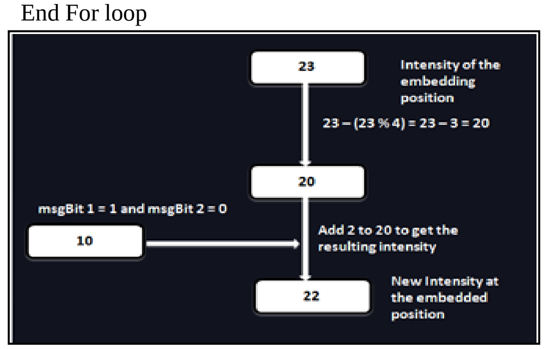

Fig 7: A snapshot of data embedding process using M4M.

6.4 Data Extraction Method

Mod 4 Method (M4M) Receiving Algorithm is described as: Input: Sampled Audio Matrix (a), Message size

- Initialize m = n = x = count =1;
- binmsg1='';
- Begin for loop starting with i=1, incrementing 2 and till msg size
- V = value of a(m,n) ;
- let R be the remainder after dividing V by 4;
- if(R==0)
- binmsg1(count)=char (0);count=count+1;
- binmsg1(count)=char (1);count=count+1;
- else if(R==1) binmsg1(count)= char(0);
- count=count+1;binmsg1(count)= char(1);
- count=count+1;
- else if(R==2)
- binmsg1(count)= char(0);count=count+1;
- binmsg1(count)= char (1);count=count+1;
- else if(R==3)
- binmsg1(count)= char(0);count=count+1;
- binmsg1(count)= char (1);count=count+1;
- End if
- Let R1 be the remainder after dividing x by 4;
- If R1 = val then m = m + R1 +1; where val = 0, 1 , 2 and 3;
- x = x + 1;
- Initialize msgx=msg1=''and k=0;
- Begin for Loop with incrementing i by 1 and till Message size
- Begin for Loop with incrementing j by 1 and till 8
- Increment k by 1;msgx(j) = char(binmsg1(k));
- End For loop

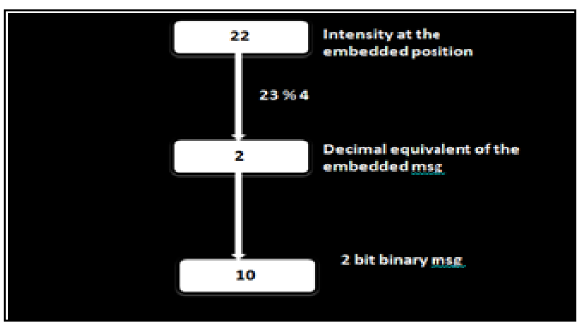

Fig 8: A snapshot of data extraction process using M4M.

A. Wavelet DPCS (Division- PMM-Combination-Sending) Algorithm:

a) Input: Height and width of a particular frame, and the Message to be embedded.
b) Divide the msg into 4 parts viz msg1, msg2, msg3, msg4.
c) Let 'els' be an array of elementary lifting steps which has a format {type, coefficients, max_degree} where Type is 'p' = primal coefficient is a vector of real no.'s, and max_degree is the highest degree of the polynomials of 'p'.
d) lshaarInt = Integer to Integer wavelet transform in Haar lifting scheme.
e) lsnewInt = New Lifting Scheme obtained by appending the elementary lifting step 'els' to the lifting scheme' lshaarInt'.
f) 2D lifting wavelet decomposition w.r.t the existing wavelet and store it in parts viz. CA, CH, CV and CD.
g) Call the **Pixel Mapping Method** for mapping data in the four above mentioned parts.
h) Return the 2D lifted and reconstructed wavelet;

B. Wavelet DPCR (Division-PMM-Combination-Receiving) Algorithm:

a) Input height and width of a particular frame and the length of the message.
b) Divide the length of the message by 4 and store it in 'l'.
c) Let 'els' be an array of elementary lifting steps which has a format {type, coefficients, max_degree} where Type is 'p' = primal coefficient is a vector of real no.'s, and max_degree is the highest degree of the polynomials of 'p'.
d) lshaarInt = Integer to Integer wavelet transform in haar lifting scheme.
e) lsnewInt = New Lifting Scheme obtained by appending the elementary lifting step 'els' to the lifting scheme' lshaarInt'.
f) 2D lifting wavelet decomposition w.r.t the existing wavelet and store it in parts viz. A, H, V, D.
g) Call the **Pixel Mapping Method** Receiving to extract the data in the four above mentioned parts.
h) Return the 2D lifted and reconstructed wavelet.

C. Data Hiding in Video using PMM and M4M:

The idea as discussed earlier is to hide a message in a cover video i.e. in the image sequence extracted from the cover video and send the stego video to the receiver end, where in the receiver end the message is extracted.

Sender side

a) Select a cover video and a message.
b) Divide the Video in Two parts: Visual Image Sequence and the Audio.
c) Embed the first part of the secret message in the Visual Image Sequence using the Pixel Mapping Method in the Wavelet Domain and regenerate the original Image Sequence.
d) Embed the next part of the secret message in to the audio part using M4M embedding technique.
e) Recombine the Visual and the Audio part to generate the Stego Video.
f) Send the stego video to the receiver part.

Receiver side

a) Select the Stego video.
b) Divide the Video in Two parts: Visual Image Sequence and the Audio.
c) Extract the first part of the secret message from Visual Image Sequence using the Pixel Mapping Method in the Wavelet Domain.
d) Extract the next part of the secret message from the audio part using M4M extraction method.

7. ALGORITHMS FOR MULTIMEDIA BASED VIDEO STEGANOGRAPHY

In this section the experimental result of the proposed method has been based on two benchmarks techniques to evaluate the hiding performance. First one is the capacity of hiding data and another one is the imperceptibility of the stego image or stego audio, also called the quality of stego image or audio. The quality of stego-objects should be acceptable by human eyes for image and by human ears for audio. The authors also present a comparative study of the PMM with the existing methods like PVD, GLM and the methods proposed by Ahmad T et al. by computing embedding capacity, mean square error (MSE) and peak signal-to noise ratio (PSNR).The authors also compute the normalized cross correlation coefficient for computing the similarity measure between the cover image and stego image. In this section experimental result of stego image are shown based on two well known images: Lena and Pepper. A comparative study of the embedding capacity with other methods has been illustrated in Figure 9.The experimental result of stego audio are shown based on two audio formats viz. wav and mp3, having a total of different six audio files, three of each format. Fig. 11 shows the length and maximum embedding capacity of each of the audio files.

IMAGE	IMAGE SIZE	PVD	GLM	AHMAD ET ALL.	PMM
LENA	128x128	**	2048	2493	2393
	256x256	**	8192	10007	10012
	512x512	50960	32768	40017	45340
PEPPER	128x128	**	2048	2443	2860
	256x256	**	8192	9767	11694
	512x512	50685	32768	39034	46592

Fig 9: Comparison of embedding capacity

Fig 10: A) Cover Image B) Stego Image of Lena after embedding "I am an Indian and I feel proud to an Indian."

Audio file	Length	Maximum Embedding Capacity
chimes.wav	00:00:07	8498
heartbeat.wav	00:00:13	31583
johncena.wav	00:01:51	38850
gaanwala.mp3	00:02:45	139308
jagorone.mp3	00:03:46	188440
yaaron.mp3	00:04:25	212901

Fig 11: Maximum Embedding Capacity varying with format and size of the audio.

7.1 Peak Signal to Noise Ratio (PSNR) and Mean Squared Error (MSE) of a signal

The peak signal-to-noise ratio (PSNR) is the ratio between a signal's maximum power and the power of the signal's noise. Engineers commonly use the PSNR to measure the quality of reconstructed signals that have been compressed. Signals can have a wide dynamic range, so PSNR is usually expressed in decibels, which is a logarithmic scale. In statistics, the **mean squared error (MSE)** of an estimator is one of many ways to quantify the difference between values implied by an estimator and the true values of the quantity being estimated. MSE is a risk function, corresponding to the expected value of the **squared error loss** or **quadratic loss**. MSE measures the average of the squares of the "errors." The error is the amount by which the value implied by the estimator differs from the quantity to be estimated.

Audio		Data Size					
		100	500	1000	2500	5000	10000
chimes.wav	PSNR	67.1593	60.8245	57.9941	54.0638	51.0484	N.A
	MSE	0.0125	0.0538	0.0538	0.2551	0.5108	
heartbeat.wav	PSNR	74.0891	66.8539	63.7689	59.6869	56.7102	53.6966
	MSE	0.0025	0.0134	0.0273	0.0699	0.1387	0.2776
johncena.wav	PSNR	73.1188	67.0395	64.2669	60.3983	57.4135	54.4213
	MSE	0.0032	0.0129	0.0243	0.0593	0.1180	0.2349
gaanwala.mp3	PSNR	79.3587	72.9449	70.0694	66.1954	63.1914	60.1326
	MSE	7.5372e-004	0.0033	0.0064	0.0156	0.0312	0.0631
jagorone.mp3	PSNR	80.6707	74.2569	71.3813	67.5074	64.5033	61.4194
	MSE	5.5721e-004	0.0024	0.0047	0.0115	0.0231	0.0469
yaaron.mp3	PSNR	80.4089	74.1413	71.5498	67.7883	64.8967	61.9353
	MSE	5.9182e-004	0.0025	0.0046	0.0108	0.0211	0.0416

Fig 12: PSNR and MSE values of six audio files at different message sizes.

IMAGE	IMAGE SIZE	PVD	GLM	AHMAD ET ALL.	PMM
LENA	128x128	36.20	30.5	44.30	49.0296
	256x256	35.00	33.20	46.80	50.3489
	512x512	41.79	35.50	55.00	54.1515
PEPPER	128x128	38.70	38.00	43.50	47.9468
	256x256	35.00	37.20	47.50	48.3668
	512x512	40.97	34.00	52.50	54.1521

Fig 13: PSNR for various Image Steganography methods

7.2 Similarity Measure between Cover Image and Stego Image

For comparing the similarity between cover image and the stego image, the normalized cross correlation coefficient (r) has been computed. Similarity measure of two images can be done with the help of normalized cross correlation generated from the above concept using the following formula:

$$r = \frac{\sum_{(C(i,j)-m_1)(S(i,j)-m_2)}}{\sqrt{(\sum_{C(i,j)-m_1})^2}\sqrt{(\sum_{S(i,j)-m_2})^2}}$$

Here C is the cover image, S is the stego image, m_1 is the mean pixel value of the cover image and m_2 is the mean pixel value of stego image.

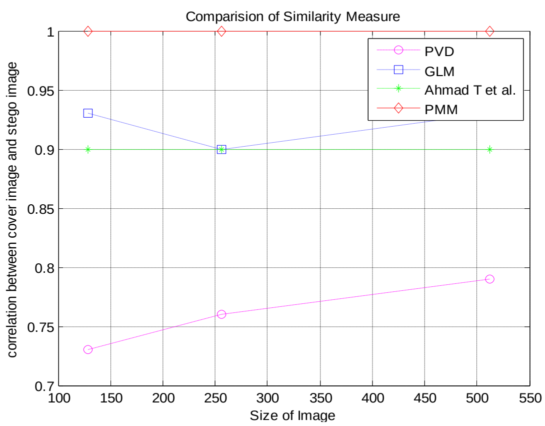

Fig 14: Comparison of Similarity Measure for Lena Image

7.3 Similarity Measure of the Cover Audio and Stego Audio through Correlation

The most familiar measure of dependence between two quantities is the Pearson product-moment correlation coefficient [34-35], or "Pearson's correlation." It is obtained by dividing the covariance of the two variables by the product of their standard deviations. Karl Pearson developed the coefficient from a similar but slightly different idea by Francis Galton. The Pearson correlation is +1 in the case of a perfect positive (increasing) linear relationship (correlation), -1 in the case of a perfect decreasing (negative) linear relationship (anti correlation) , and some value between -1 and 1in all other cases, indicating the degree of linear dependence between the variables. As it approaches zero there is less of a relationship (closer to uncorrelated). The closer the coefficient is to either -1 or 1, the stronger the correlation between the variables. If the variables are independent, Pearson's correlation coefficient is 0, but the converse is not true because the correlation coefficient detects only linear dependencies between two variables. If there is a series of n measurements of X and Y written as x_i and y_i where i = 1, 2 …., n then the sample correlation coefficient can be used in Pearson correlation r between X and Y. The sample correlation coefficient is written as

$$r_{xy} = \frac{\sum_{i=1}^{n}(x_i - \bar{X})(y_i - \bar{Y})}{(n-1)S_x S_y}$$

where $\bar{X}$ and $\bar{Y}$ are the sample means of X and Y, S_x and S_y are the sample standard deviations of X and Y.

Secret Message Size(in char)	Cover Audio	Correlation-Coefficient
100	Chimes.wav	1.000
500	Chimes.wav	0.9999
1000	Chimes.wav	0.9994
2500	Chimes.wav	0.9980
5000	Chimes.wav	0.9976
8000	Chimes.wav	0.9970
10000	heartbit.wav	0.9951
10000	gaanwala.mp3	0.9950

Fig 15: Similarity Measure of the Cover and Stego through Correlation

7.4 Case study of Video Steganographic Technique in terms of MSE and PSNR

Case Study1:

Video name : **baby.avi**
Total Message : "University Institute of Technology"
The data is inserted in the frame number 1, 3,6,10 and 11.

Frame No.	PSNR	MSE
1	**61.6923**	**0.0440**
3	**61.4383**	**0.0467**
6	**61.4190**	**0.0469**
10	**34.2765**	**24.2902**
11	**34.3523**	**23.8698**

Case Study 2:

Video name : **movie.avi**
Total Message : "University Institute of Technology"
The data is inserted in the frame number 1, 3,6,10 and 11.

Frame No.	PSNR	MSE
1	**31.2860**	**48.3595**
3	**31.2099**	**49.2139**
6	**31.2318**	**48.9665**
10	**31.3008**	**48.1945**
11	**31.2535**	**48.7224**

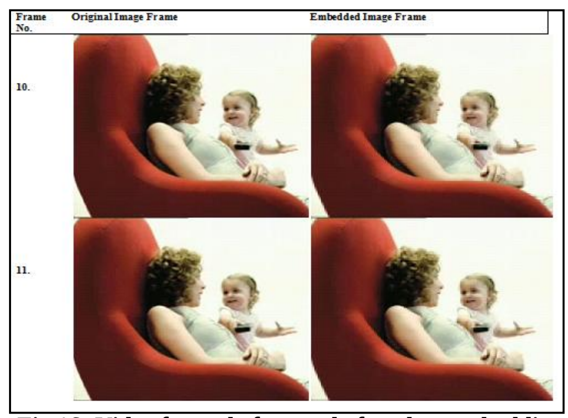

Fig 16: Video frame before and after data embedding for Case 1

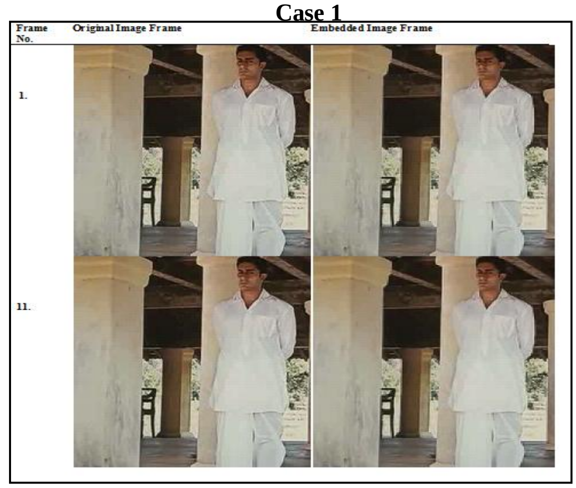

Fig 17: Video frame before and after data embedding for Case 2

7.5 Similarity Measure between Cover Video frame and Stego Video frame using by relative entropy distance (Kulback Leibler distance)

Kullback Leibler distance (KL-distance) [37] (also **information divergence**, **information gain**, **relative entropy**, or **KLIC**) is a natural distance function from a "true" probability distribution, P, to a "target" probability distribution, Q. It can be interpreted as the expected extra message-length per datum due to using a code based on the wrong (target) distribution compared to using a code based on the true distribution. For discrete (not necessarily finite) probability distributions, P= $\{p_1, ..., p_n\}$ and Q=$\{q_1, ..., q_n\}$, the KL-distance is defined to be KL(P, Q) = $\Sigma_i\, p_i\, .\, \log_2({}^{p}{}_{i} / {}_{qi})$. For continuous probability densities, the sum is replaced by an integral.

In steganography security of the hidden data is represented numerically by relative entropy distance (Kulback Leibler distance)

Video	Frame No		Data Size 100	Data Size 500	Data Size 1000	Data Size 2500	Data Size 5000	Data Size 10000
baby.avi	1	security of the hidden data	0.0001	0.0004	0.0010	0.0022	0.0038	0.008
	3	security of the hidden data	0.0001	0.0003	0.0011	0.002	0.0036	0.0077
	6	security of the hidden data	0.0001	0.0004	0.0010	0.0021	0.004	0.0078
	10	security of the hidden data	0.0001	0.0004	0.0012	0.002	0.0041	0.0082
	11	security of the hidden data	0.0001	0.0003	0.0013	0.0025	0.0039	0.008
movie.avi	1	security of the hidden data	0.0001	0.0003	0.0010	0.0019	0.0032	0.0075
	3	security of the hidden data	0.0001	0.0004	0.0011	0.0022	0.0035	0.008
	6	security of the hidden data	0.0001	0.0003	0.0010	0.0021	0.0038	0.008
	10	security of the hidden data	0.0001	0.0003	0.0015	0.0027	0.004	0.0081
	11	security of the hidden data	0.0001	0.0004	0.0011	0.0022	0.0036	0.008

Fig 18: Security value of hidden data in various video frames

8. MATHEMATICAL ANALYSIS OF SECURITY OF HIDDEN DATA

Kullback–Leibler divergence is a non-symmetric measure of the difference between two probability distributions *P* and *Q*. KL measures the expected number of extra bits required to code samples from *P* when using a code based on *Q*, rather than using a code based on *P*. Typically *P* represents the "true" distribution of data, observations, or a precisely calculated theoretical distribution. The measure *Q* typically represents a theory, model, description, or approximation of *P*. KL divergence is a special case of a broader class of divergences called f-divergences. For probability distributions *P* and *Q* of a discrete random variable their K–L divergence is defined to be

$$D_{KL}(P \| Q) = \sum P(i) \log \frac{P(i)}{Q(i)}$$

In words, it is the average of the logarithmic difference between the probabilities *P* and *Q*, where the average is taken using the probabilities *P*. The K-L divergence is only defined if *P* and *Q* both sum to 1 and if *Q* (*i*) > 0 for any *i* such that *P*(*i*) > 0. If the quantity 0log0 appears in the formula, it is interpreted as zero. For distributions *P* and *Q* of a continuous random variable, KL-divergence is defined to be the integral

$$D_{KL}(P \| Q) = \int_{-\infty}^{\infty} p(x) \log \frac{p(x)}{q(x)} dx$$

where *p* and *q* denote the densities of *P* and *Q*. More generally, if *P* and *Q* are probability measures over a set *X*, and *Q* is absolutely continuous with respect to *P*, then the Kullback–Leibler divergence from *P* to *Q* is defined as

$$D_{KL}(P \| Q) = -\int_x \log \frac{dQ}{dP} dP$$

where $\frac{dQ}{dP}$ is the Radon–Nikodym derivative of *Q* with respect to *P*, and provided the expression on the right-hand side exists. Likewise, if *P* is absolutely continuous with respect to *Q*, then

$$D_{KL}(P \| Q) = \int_x \log \frac{dP}{dQ} dP = \int_x \frac{dP}{dQ} \log \frac{dP}{dQ} dQ$$

which we recognize as the entropy of *P* relative to *Q*. Continuing in this case, if μ is any measure on *X* for which $p = \frac{dP}{d\mu}$ and $q = \frac{dQ}{d\mu}$ exist, then the Kullback–Leibler divergence from *P* to *Q* is given as

$$D_{KL}(P \| Q) = \int_x p \log \frac{p}{q} d\mu$$

The logarithms in these formulae are taken to base 2 if information is measured in units of bits, or to base *e* if information is measured in nats.

9. ANALYSIS OF EXPERIMENTAL RESULTS

From the experimental results in can be seen that the embedding capacity of the PMM method is better in most cases compared to the other method except the PVD technique and also the similarity measures proves that the proposed method is best among these four methods which ensures that cover image and the stego image is almost identical. Also as the message bits are not directly embedded at the pixels of the cover image, steganalysis may be able to find out the embedded bits but cannot be able to extract the original message bits. PSNR value of the proposed method for various size of the image is moderate among various other methods. From the comparison results of the existing audio steganography method with M4M method it can be seen that the embedding capacity of M4M method is much better that the other existing audio steganography methods because it can map two bits at a time instead of one for embedding. M4M is also capable of producing stego audio with minimum or zero degradation. Thus the integrated effect of PMM along with M4M technique for a multimedia based video steganography produces a good quality stego video with high embedding capacity and moderate PSNR. From the security aspects the relative entropy distance is very low between the cover frame and stego frame which yields a very high security value. However the proposed scheme of video steganography has been tested on two sets of video frames for measuring performance. However this may be extended for more number of video frames.

10. CONCLUSION

A new multimedia based un-compressed video steganographic scheme has been proposed in this paper, which works through the integrated approach of image steganography technique via PMM and audio steganography technique via M4M approach. Both PMM and M4M provide high embedding capacity and imperceptible stego-objects. The performance of the steganographic algorithm is studied and experimental results conclude that this scheme can be applied on un-compressed videos with no noticeable degradation in visual and audible qualities.

11. REFERENCES

[1] T Mrkel, JHP Eloff and MS Olivier."An Overview of Image Steganography," in proceedings of the fifth annual Information Security South Africa Conference, 2005.

[2] Kahn, The Code breakers - the comprehensive history of secret communication from ancient times to the Internet, Scribner, New York (1996).

[3] J.T. Brassil, S. Low, N.F. Maxemchuk, and L. O'Gorman, "Electronic Marking and Identification Techniques to Discourage Document Copying", IEEE Journal on Selected Areas in Communications, vol. 13, Issue. 8, October 1995, pp. 1495-1504.

[4] L.Y. Por and B. Delina, "Information Hiding: A New Approach in Text Steganography", 7th WSEAS International Conference on Applied Computer & Applied Computational Science, April 2008, pp- 689-695.

[5] A.M. Alattar and O.M. Alattar, "Watermarking electronic text documents containing justified paragraphs and irregular line spacing ", Proceedings of SPIE - Volume5306, Security, Steganography, and Watermarking of Multimedia Contents VI, June 2004, pp- 685-695.

[6] M.H. Shirali-Shahreza and M. Shirali-Shahreza, "Text Steganography in Chat", Proceedings of the Third IEEE/IFIP International Conference in Central Asia on Internet the Next Generation of Mobile, Wireless and Optical Communications Networks (ICI 2007), Tashkent, Uzbekistan, September 26-28, 2007.

[7] L. M. Marvel, C. G. Boncelet, Jr. and C. T. Retter, "Spread spectrum image steganography," IEEE Trans. on Image Processing, 8(8), 1075-1083 (1999).

[8] Analysis of LSB Based Image Steganography Techniques ,R. Chandramouli, Nasir Memon, Proc. IEEE ICIP, 2001.

[9] An Evaluation of Image Based Steganography Methods,Kevin Curran, Kran Bailey, International Journal of Digital Evidence,Fall 2003.

[10] Doërr and J.L. Dugelay, "A Guide Tour of Video Watermarking", Signal Processing: Image Communication, vol. 18, Issue 4, 2003, pp. 263-282.

[11] K. Gopalan, "Audio steganography using bit modification", Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, (ICASSP '03), vol. 2, 6-10 April 2003, pp. 421-424.

[12] Doërr and J.L. Dugelay, "Security Pitfalls of Frameby-Frame Approaches to Video Watermarking", IEEE Transactions on Signal Processing, Supplement on Secure Media, vol. 52, Issue 10, 2004, pp. 2955-2964.

[13] J.Y. Hsiao. C.C. Chang. and C.-S. Chan. Finding optimal least significant- bit substitution in image hiding by dynamic programming strategy. Pattern Recognition, 36:1583–1595, 2003.

[14] C.K. Chan. and L. M. Cheng. Hiding data in images by simple lsb substitution. Pattern Recognition, 37:469–474, 2004.

[15] P Huang. K.C. Chang., C.P Chang. and T.M Tu. A novel image steganography method using tri-way pixel value differencing. Journal of Multimedia, 3, 2008.

[16] Ahmad T. Al-Taani. and Abdullah M. AL-Issa. A novel steganographic method for gray-level images. International Journal of Computer, Information, and Systems Science, and Engineering, 3, 2009.

[17] Potdar V.and Chang E. Gray level modification steganography for secret communication. In IEEE International Conference on Industria lInformatics, pages 355–368, Berlin, Germany, 2004.

[18] C.S. Lu: Multimedia security: steganography and digital watermarking techniques for protection of intellectual property. Artech House, Inc (2003).

[19] J.J. Chae and B.S. Manjunath: Data hiding in Video. Proceedings of the 6th IEEE International Conference on Image Processing, Kobe, Japan (1999).

[20] Provos, N., Honeyman, P.: Hide and Seek: An Introduction to Steganography. IEEE Security & Privacy Magazine 1 (2003).

[21] I.J.Cox, J. Kilian, T. Leighton, T.Shamoon: Secure spread spectrum watermarking for multimedia. Proceedings of IEEE Image processing (1997).

[22] J.J. Chae, D. Mukherjee and B.S. Manjunath: A Robust Data Hiding Technique using Multidimensional Lattices. Proceedings of the IEEE Forum on Research and Technology Advances in Digital Libraries, Santa Barbara, USA (1998).

[23] X. Niu, M. Schmucker and C. Busch: Video watermarking resisting to rotation, scaling, and translation. Proceedings of SPIE Security and Watermarking of Multimedia Contents IV (2002).

[24] Y. Wang, E. Izquierdo, "High-Capacity Data Hiding in MPEG-2 Compressed Video", 9th International Workshop on Systems, Signals and Image Processing, UK, 2002.

[25] D.E. Lane "Video-in-Video Data Hiding", 2007.

[26] "Hiding Data in Images Using Pixel Mapping Method (PMM) by Souvik Bhattacharyya and Gautam Sanyal at SAM'10 - 9th annual Conference on Security and Management under The 2010 World Congress in Computer Science, Computer Engineering, and Applied Computing held on July 12-15, 2010, USA.

[27] A Novel approach of Data Hiding Using Pixel Mapping Method (PMM) by Souvik Bhattacharyya, Lalan Kumar and Gautam Sanyal at International Journal of Computer Science and Information Security (IJCSIS-ISSN 1947-5500) , Volume. 8 , N0. 4 , JULY 2010,Page No -207-214.

[28] Nedeljko Cvejic and Tapio Seppben, Increasing the capacity of LSB-based audio steganography, in IEEE 2002, (2002).

[29] Natarajan Meghanathan and Lopamudra Nayak, Steganalysis Algorithms for Detecting the Hidden Information in Image, Audio and Video Cover Media, in at International Journal of Network Security & Its Application (IJNSA), Vol.2, No.1, January 2010.

[30] W. Bender. and D. Gruhl, Steganography: Techniques for data hiding, in IBM SYSTEMS JOURNAL, 35(1996).

[31] Samir Kumar Bandyopadhyay, Debnath Bhattacharyya, Poulami Das, Debashis Ganguly and Swarnendu Mukherjee,A tutorial review on Steganography, in In the Proceedings of International Conference on Contemporary Computing, (2008).

[32] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal,A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier, in Journal of Global Research in Computer Science (JGRCS) VOL 2, NO 4 (2011),APRIL-2011.

[33] Arko Kundu, Kaushik Chakraborty and Souvik Bhattacharyya,Data Hiding in Images Using Mod 16 Method, in In the Proceedings of ETECE 2011,(2011)

[34] S. Dowdy and S. Wearden. Statistics for research. Wiley. ISBN 0471086029, page 230, 1983.

[35] W. E. Winkler. The state of record linkage and current research problems. Statistics of Income Division, Internal Revenue Service Publication R99/04., 1999.

[36] Audio Steganography Using Mod 4 Method (M4M) by Souvik Bhattacharyya, Arko Kundu, Kaushik Chakraborty and Gautam Sanyal at JOURNAL OF COMPUTING, VOLUME 3, ISSUE 8, AUGUST 2011

[37] C. Cachin, An information theoretic model for steganography, Proceedings of 2nd Workshop on Information Hiding. D. Aucsmith (Eds.). Lecture Notes in Computer Sciences, Springer-verlag, USA, **1525,** (1998).