Info Hide – A Cluster Cover Approach

R. Amirtharajan
Assistant Professor ECE / SEEE
SASTRA University
Thanjavur 613402

Krishnendra Nathella
ECE / SEEE
SASTRA University
Thanjavur 613402

J Harish
ECE / SEEE
SASTRA University
Thanjavur 613402

ABSTRACT

In a highly digitalized world we live today, the data to be transmitted are confidential at times, and in such cases there are many malicious intruders who try to access this information. Steganography is one recent method to provide reliable security. Steganography is the science of embedding data into different covers such that the data embedded is imperceptible; the aim is to embed and deliver secret messages in digital objects without suspicion. The covers that can be used cover all forms of digital multimedia. This paper deals with "Multimedia Steganography" in the most common forms of multimedia- Image, Video and Audio.

Categories and Subject Descriptors

D.2.11 Information hiding
D.4.6 Security and Protection

General Terms

Data Security

Keywords

Audio steganography, LSB steganography, Information hiding, video steganography.

1. INTRODUCTION

Research is being carried out on multimedia objects such as images, videos, audios etc for data hiding and there has been a significant advancement within the past decade. Information hiding also plays a significant role in modern internet era as information is constantly exchanged over unsecure public networks. In order to enhance the security there exist various encryption techniques. Encryption has a disadvantage that the message can be easily tracked as they resemble a stream of meaningless codes. This problem could be overcome by the technique called "Steganography". Steganography is a science of hiding data in the cover media in order to make it innocuous to any unintended user. Here, the message is embedded in a cover which could be an image, audio, video etc...This makes the message imperceptible to any intruder, thus it increases the security.

There are different approaches in steganography. The various techniques in data hiding have been explained by W. Bender et al [1] in their paper-'Techniques for data hiding'. One of the most common methods is simple LSB substitution. In this method secret data is embedded in LSBs of the pixels present in the image.LSB steganography has low computation complexity and high embedding capacity, in which a secret binary sequence is used to replace the least significant bits of the host medium (Bender et al., 1996).

Generally steganography can be implemented either in spatial domain or in frequency domain. The fore mentioned simple LSB substitution method comes under spatial domain where the pixels in the image are modified directly to hide the data. Among the different approaches in steganography one using the pixel value differencing is Chih-Ching Thien, Ja-Chen Lin's [2] 'A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function' which uses the basic concept of modulus operation. Their method has the following advantages: their technique achieves good image vision quality without the need for post-processing; the smaller error advantage over the simple LSB substitution method the proposed method has high-hiding capacity.

Chung-Ming Wang [3] has proposed in his paper 'A high quality steganographic method with pixel-value differencing and modulus function' a technique which avoids the falling-off-boundary problem by using pixel-value differencing and the modulus function. The hiding capacity of the two consecutive pixels depends on the difference value. Smoother the area is, lesser the secret data can be hidden; on the contrary, more the edges an area has, more the secret data can be embedded. This way, the stego-image quality degradation is more imperceptible to the human eye. `

A loophole exists in the PVD method. Unusual steps in the histogram of pixel differences reveal the presence of a secret message. An analyst can even estimate the length of hidden bits from the histogram. To enhance security, a modified scheme was proposed by Xinpeng Zhang, Shuozhong Wang [4]-'Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security' which avoids occurrence of the above-mentioned steps in the pixel difference histogram while preserving the advantage of low visual distortion of the PVD.

In frequency domain jpeg steganography is widely prevalent with the most common methods being DCT and DWT. Hideki Noda et al's [5] 'High-performance JPEG steganography using quantization index modulation in DCT domain' presents a novel, reversible steganographic method, which can reconstruct an original image effectively after extracting the embedded secret data. The proposed reversible hiding method aims at BTC (block truncation coding) compressed color images. The secret data then are embedded in the common bitmap and the quantization levels of each block use the properties of side matching and the order of these quantization levels to achieve reversibility.

An important branch that's closely related to steganography is-Steganalysis. The steganalytic approach is complementary to steganography where the person tries to detect and decode the secret data embedded in the cover object. Many of the steganographic methods are designed to be resistant to the steganalytic attacks. However many steganalysis approaches have been developed to successfully attack the LSB techniques. The chi-square method [6] (Westfield and Pfitzmann, 1999) detects the presence of hidden data based on the fact that the occurrence probabilities of adjacent gray values tend to become equal after the LSB embedding. The technique can also be used against other steganographic schemes such as J-Steg in which pairs of values (PoVs) are swapped into each other to embed message bits.

Another powerful method, RS Steganalysis [7](Fridrich and Goljan, 2002; Fridrich et al., 2001) proposed by Fridrich et al[7], utilizes a pair of mutually complementary flipping, to test the received image. If the change of smoothness is asymmetric, the image is judged as containing secret message. The JPEG decoding process also comprises three major steps: entropy decoding, de-quantization, and inverse DCT (IDCT). Each step in decoding process performs essentially the inverse of its corresponding step in encoding procedure. The entropy decoding step decodes the compressed code to the quantized DCT coefficients. The de-quantization step then converts each quantized DCT coefficient to its approximate value by multiplying with its quantization value. DCT is then used to convert the de-quantized coefficients to their spatial value. As mentioned above, the entropy encoding step in the JPEG encoding process is lossless. It means that if the secret bits are embedded in the quantized DCT coefficients, they will not be destroyed by the follow-up encoding steps. Lisa marvel et al [8] implemented spread spectrum based image steganography describes the uses of spread spectrum in steganography. Petitcolas et al [9, 10] briefly explain about the information hiding schemes and their classifications.

In video, watermarking has gained the world's imagination more than Steganography. There are many watermarking techniques and Gwena.el Do.err, Jean-Luc Dugelay's [11] "A guide tour of video watermarking" provides a overview of the existing watermarking techniques. This paper provides basic information regarding video watermarking. Digital watermarking has recently been extended from still images to video content. Further research in this area is strongly motivated by an increasing need from the copyright owners to reliably protect their rights. Because of the large economic stakes, digital watermarking is promised to a great future. New applications are likely to emerge and may combine existing approaches. For example, a watermark can be separated into two parts: one for copyright protection and the other for customer fingerprinting. However many challenges have to be taken up. Robustness has to be considered attentively. There are indeed many hostile video processing which might alter the watermark signal. It might not even be possible to be immune against all those attacks and detailed constraints has to be defined according to the targeted application. Since collusion is far more critical in the context of video, it must be seriously considered. Finally the real-time constraint has to be met in many applications. In spite of all those challenges, many algorithms have already been proposed in the literature. It goes from the simple adaptation of a watermarking algorithm for still images to the really video specific watermarking Scheme. Open paths still remains in video watermarking. This technology is indeed in its infancy and is far from being as mature as for still images. Quite all possible image processing have been investigated for still images watermarking. On their side, the proposed algorithms for video have remained relatively simple. Many video processing have not been tried and the line is consequently not exhausted. Moreover, introduction of perceptual measures have significantly improved the performances of algorithms for still images. This approach has not been fully extended to video yet. Perceptual measures for video exist but the major challenge consists in being able to exploit them in real-time. Finally, the second generation of watermarking algorithms has only given its first results. Future discoveries in this domain are likely to be of great help for digital video watermarking.

Very few techniques have been proposed for audio steganography, while many have been proposed for audio watermarking. One of the more popular ones is "Robust audio watermarking using improved TS echo hiding" by Yousof Erfani, Shadi Siahpoush [12]. Here the author proposes a novel and content based improved time spread echo hiding method (ITS). Here the system decoder relies upon distinguishing a watermarked bit based on a correlation amount quantity and also the echo kernel embeds the watermark bit into the whole signal. The presented system is cepstral content based in which the original signal cepstral portion of error at the decoder is removed and thus the performance of the decoder detection rate is improved considerably. Experimental results show the good results for the system robustness against the common signal processing attacks through calculating error detection rates in comparison with conventional echo hiding methods. Also good results were obtained for watermark inaudibility through mean opinion test (MOS) test and SNR value comparisons.

Usually audio steganographic techniques are highly susceptible steganalytic attacks but here the " INFORMATION HIDING SYSTEM STEGOWAVEK FOR IMPROVING CAPACITY" technique proposed by, Young-Shil Kim Young-Mi et al[13]make the it more resistant to steganalytic attacks. Here the technique involves Low bit encoding where one bit of Mask is inserted into the last bit. Attacker has the disadvantage where attack was able to do the Mask which was easily concealed in case of Low bit Encoding. Also capacity of Stego-data is low. To improve low capacity, more than one bit is embedded in every sixteen bits. But the attacker easily filters Mask when inserted bit is equally distributed in every sixteen bits. It is proposed that the Mask should be inserted in forms of sign curve with changing the number of bits.

In this paper multimedia steganography has been implemented as available in the literature in matlab and the results are discussed. To start with image where it is the most popular form of cover used in steganography. Steganography in images can be done in two domains: Spatial and Transform. This paper involves work in both the domains, in the spatial domain "LSB substitution" technique has been implemented and in the frequency domain the "DWT technique have been implemented. LSB substitution technique involves substituting the LSB bits in each pixel of the image with the secret data bits. It is simple, highly efficient and provides high embedding capacity. The DWT based steganography divides the images into 4 frequency sub bands and data is embedded in the specific sub bands based on a rule. Its advantages include robustness towards noise and steganalytic attacks and retrieval of original Cover image. PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error) are the parameters used here to evaluate the proposed techniques.

The Audio steganography is at its inception. Here the aim is to embed data such that it is least perceptible to the listeners with an optimum trade-off between capacity and quality. In this proposed scheme, the audio is read as frequency coefficients and secret data is converted into its digital form. For every N sample of frequency coefficients, these bits are embedded by following the proposed algorithm. SNR (Signal to Noise Ratio) is used to evaluate the audio quality after embedding.

Video Steganography is a novel technique where embedding capacity can be increased manifold. The video consists of number of frames and each frame contains video related information such as map and index. The frame can be treated as an image and further processing can be done. In Video Steganography, the algorithm used for embedding is OPAP (Optimal Pixel Adjustment Process).This involves embedding the message bits using LSB (least significant bit) substitution method and OPAP is done to enhance the stego video quality. This method can increase the PSNR by 6 % thereby improving the video quality significantly.

This paper is organized as follows -section 2 reviews about the simple LSB substitution and OPAP ; section 3 reviews the DWT based steganography; section 4 Reviews audio and video steganography techniques ; section 5 discuss the finding and conclusion

2. Spatial domain techniques in image steganography

2.1 Simple LSB substitution:

Consider a 8-bit gray scale image matrix consisting m x n pixels and a secret message consisting of ‘k’ bits. The first bit of message is embedded into the LSB of the first pixel and the second bit of message is embedded into the second pixel and so on. The resultant stego-image which holds the secret message is also a 8-bit gray scale image and difference between the cover image and the stego-image is not visually perceptible. This can be further extended, and any number of LSB’s can be modified in a pixel but the quality of the image degrades with the increase in number of LSB’s. Usually up to 4 LSB’s can be modified without significant degradation in the message. The peak signal to noise ratio (PSNR) of this method is low.

$$\text{PSNR=10 log } \frac{2^8 - 1}{MSE}$$

$$\text{MSE= } \frac{1}{m} \sum_{0}^{m-1} Z_i - H_i$$

One method to improve the quality of the LSB substitution is Optimal Pixel Adjustment Process (OPAP).

2.2 OPAP:

In order to improve image quality obtained by simple LSB substitution we go for OPAP technique[14]. Here embedding error between stego image and cover image is found and reduced significantly. Let Pi, Pi’, Pi’’ be the ith pixel value of the cover image, stego image obtained by LSB substitution and enhanced stego image obtained by OPAP technique respectively. The embedding error ∂i=Pi-Pi’. ∂i lies in the range $-2^k <= ∂i <= 2^k$.

Now this methods divides ∂i into three intervals and modify the value of Pi’ to reduce the error.

CASE 1:

$2^{k-1} < ∂i < 2^k$, if Pi’>=2^k then Pi”=Pi’-2^k otherwise Pi”=Pi’.

CASE 2:

$-2^{k-1} < ∂i < 2^{k-1}$, Pi” =Pi’.

CASE 3:

$-2^k < ∂i < -2^{k-1}$, if Pi’ <256-2^k, then Pi”=Pi’+2^k

Otherwise Pi’’=Pi’.

Thus OPAP technique enhances the image quality significantly. PSNR tends increase by about 5%.

2.3 INVERTED PATTERN APPROACH:

The image will be divided into blocks of uniform size. Suppose if the image consists of G pixels and if each block consists of j pixels, then there will be a total of G/j blocks. In this scheme [15], the aim is to reduce the MSE and also to increase the security by introducing a sort of cryptic effect in the technique.

Since MSE is based on the difference in pixel values between the cover image and stego image, we can obtain minimum MSE (=0) if we find a way to convert the data to a form that is perfectly compatible with the cover image, i.e. there is minimum change in the cover image, hence we’ll need a key to note down the change in the data when we make it compatible. One of the simplest methods will be to embed one bit of data in each pixel, and in order to make the data compatible we can invert the bit before embedding the data in the image, hence for each bit we’ll need a key to note whether we use the inverted form of bit or the bit itself. But here the key size will be equal to the size of the data itself; hence it is not of much use.

Our approach is also similar to the one discussed above. Here the image is divided into blocks of size, let us say J. In each block if one bit of data is embedded in the LSB of each pixel, then each block can contain up to J bits of data. Here we can reduce the MSE by checking if the inverted form of J bits of data has a reduced MSE when compared to the original data itself, and then choose those J bits which give minimum MSE. Hence we can achieve lower overall MSE and also introduce a sort of cryptic effect into the embedding technique. This technique can be further extended by increasing k (no. of LSBs modified) to up to 4.

Algorithm for Inverted pattern scheme:

2.3.1 EMBEDDING Algorithm:

INPUT:
A) Image-IMG
B) No. of blocks into which the image must be divided into-H
C) no. of bits to be embedded into each pixel-k
OUTPUT:
A) Key

Steps to embed:

Let IMG contain G pixels, it’ll be divided into H blocks of size G/H=J.

Let the total no. of bits in the data to be embedded be B, since each pixel is embedded with k bits, the B bits are grouped into k bits each, hence we have B/k=r groups of bits, we'll need only r/j blocks of image to embed the entire data.

1. Divide the G pixels in the IMG into H blocks.
2. Read the B bits of data and group them into K bits each using the formula given below-
3. Consider the first block of image. Embed j groups of bits in the block and calculate the MSE. Let the MSE be M.
4. Repeat step 3 for the inverted form of j groups of bits. Let this MSE be M1
5. Compare M and M1

If M<M1

- Embed the j group of bits into the pixels in the block.
- Assign the key for the block as 0.

Else

- Embed the inverted form of j group of bits into the pixels in the block.
- And assign the key for the block as 1.
- Generate the key as the output.

We have discussed about the algorithm involved in embedding the data in a cover image based on our technique, now we'll be seeing about the retrieval process of the data embedded in the image.

2.3.2 Extraction Algorithm:-

Let the stego image be called SIMG, it'll have G pixels. In the retrieval process, the SIMG is divided into G blocks of j pixels each (similar to the process in the embedding of data in the cover image). The k LSB from each pixel is retrieved similar to the process involved in the extraction of data in the simple LSB substitution method. Once the required LSBs from the pixels have been extracted by using the key to invert certain portion the actual data can be obtained. The exact algorithm involved in this procedure is explained below:

1. Divide the G pixels in the SIMG into H blocks of j bits each.
2. Extract the k bits of LSB in each pixel using the formula given below (similar to extraction process in simple LSB substitution)
3. Group the B bits into groups of size j*k. so, we'll have B/(k*j) groups (which will be equal to the size of the key). Let B/(k*j)=P.
4. Use key to invert the required portions of data and retain the rest. i.e. we have 1 bit in the key for each of the P groups of bits. The extraction process is as below:

```
    1. for i starting from 1 up to P
    2. Check key. If key(i) =1,
          If true, then invert the ith group of bits in the P groups of retrieved bits.
          Else, retain the bits as they are.
```

5. Group the extracted bits obtained from the previous step into 8 or 7 bits (as followed in the embedding process) and convert them into corresponding characters based on their decimal (ASCII) values. Thus we have obtained the data that was embedded into the cover image.

2.3.3 EXPERIMENTAL RESULTS:

In this section we show the experimental results of our scheme. We used Sony VAIO laptop with INTEL centrino duo processor,1.73 GHz ,1 Gb ram .we developed our program in MATLAB version 7.4.0 running on WINDOWS VISTA operating system. We derived our results by working on three sample images with 256 graylevels-LENA.tif (256x256), BIRD.tif (560x400). We found that the image quality improved on using OPAP and inverted pattern scheme. We have implemented the simple LSB substitution, OPAP and inverted pattern technique in all sample images and tabulated the results in tables 1,2,3 as follows. we have chosen constant block size of 8 for our approach for easy comparison and analysis. Our quality of stego image improves with decrease in the block size. The running time of our implementation on all our images for varying data sizes was very short usually under 2 seconds. Our key size depends on the size of the data to be embedded and gives excellent results up to 1024.we have clearly shown this in our tabular analysis. In each pixel we will be embedding 2 bits(k=2) of the data in the LSBs for all cases.

TABULAR REPRESENTATION OF EXPERIMENTAL RESULTS:

Fig: Bird.tif Lena.tif

Table1: image under consideration- LENA.tif

LENA	**Simple LSB substitution with OPAP**	**Using IP scheme with OPAP**				
		Block size				
		1	**2**	**4**	**8**	**16**
No of characters embedded	24000	24000	24000	24000	24000	24000
MSE	15.9	7.59	11.75	12.97	13.94	14.5
PSNR	36.11	39.32	37.5	36.99	36.68	36.51
TIME	-	9.9	7.080	5.75	5.19	4.92
No of bits inverted	0	23924	11689	5954	3012	1486
% decrease In MSE	-	52.2	26.1	18.42	12.32	8.8

Table 2: image under consideration- BIRD.tif

BIRD	**Simple LSB substitution with**	**Using IP scheme with OPAP**				
		Block size				
		1	**2**	**4**	**8**	**16**

	OPAP					
No of characters embedded	24000	24000	24000	24000	24000	24000
MSE	4.5	2.17	3.36	3.70	3.92	4.13
PSNR	41.52	44.15	42.85	42.44	42.19	41.96
TIME	-	10.01	7.27	6.022	5.47	5.16
No of bits inverted	0	23930	11448	5973	2984	1488
%decrease In MSE	-	51.77	25.33	17.77	12.88	8.22

3. Frequency domain Techniques in image steganography:

In spatial domain embedding is carried out by changing the pixel values directly but they have an inherent disadvantage of being prone to steg-analysis and histogram detection. So in order to increase the robustness, we are going for frequency domain techniques. The most common methods are DCT based techniques .The DWT based techniques can also be used in steganography.

3.1 Algorithm for embedding in DWT technique:

1. Apply DWT on the cover image and the four sub bands will be obtained.
2. For the first $M_c \times N_c$ where $M_c \times N_c$ are the size of the image. The 2 consecutive bits of the secret data will be combined to form a value ranging between 0 and 3.then two consecutive numbers are subtracted to form a differential sequence. For example If combined value is 1203 then differential sequence will be -1 2 -3 so there are only 4 absolute values which are embedded in HH band and their subtraction pairs will be stored in LH or HH band.
3. The remaining bits are embedded in unused LSBs of HL and LH bands. The embedding pattern is shown in the image.
4. Perform the inverse DWT and generate the key matrix to store the non integer values (0.25,0.5,0.75)

3.1.2 Retrieval procedure:

1. Obtain the key and Perform DWT on the stego image.
2. Extract the absolute values HH band and according to the values extracted the differential pair can be obtained.
3. Obtain the other embedded bits.

3.1.3 Experimental results:

In this section we show our experimental results on DWT technique. We used 4 cover images to test the proposed algorithm. They are Lena, Mahatma Gandhi, Airplane, and Baboon.

File format-tiff,

Image resolution-256 x 256

Image type-Gray (if color image is converted to Gray image)

No of bits embedded-25000

Table 3: DWT results

Image	**MSE**	**PSNR**
Lena	0.4424	51.67
Airplane	0.4706	51.40
Baboon	0.4909	51.22
Mahatma Gandhi	0.3975	52.14

From the experimental results shown in the above table it is evident that MSE and PSNR is better for this DWT based technique. When the secret data is 25000 ,the spatial domain techniques has PSNR value which is less than 45 but in DWT technique MSE is very low .More over the key size of the DWT technique will be almost equal to the data size but it can be tagged in the image. Even if the key is known data cannot be extracted since it will be meaningless codes. This has the advantage that even if LSBs are extracted correct data cannot be obtained unless mapping rules are known. So this provides Robustness not only against noise but also against intruders.

Fig: Baboon.tif Airplane.tif MahatmaGandhi.tif

4. Video Steganography

We have worked on implementing video steganography using OPAP with distributed data embedding. Prior to getting into the OPAP method we had implemented the same using other spatial and frequency domain techniques. We have chosen OPAP technique after proper deliberation for the following reasons: it offers very high data embedding capacity, it is very simple and easier to implement and takes relatively less time to embed the data when compared to the other existing algorithms.

The OPAP (Optimal Pixel Adjustment Process) which is usually used in conjunction with simple LSB substitution has been discussed in detail in the spatial domain sections in of the project. In short the OPAP is generally used to increase the PSNR of the stego object (image) so that embedded data is made more imperceptible to the HVS. We have focussed on decreasing the time required to embed the data and simultaneously improve upon the already high embedding capacity of the Video Cover Object.

We have used uncompressed video with .avi extension to embed our data. The video usually has about 100-150 frames and a resolution of 100x100 to 200x200 pixels and runs at 10-15 frames per second.

4.1 Methodology:

As discussed earlier Digital video comprises a series of orthogonal bitmap digital images displayed in rapid succession at a constant rate. These images are called frames. The frames in a video are nothing but normal images with some extra information such as the index and other Meta data related to the video. Each frame can be extracted individually from the video and can be converted into an image. This can then be treated as the cover object and the data can be embedded in it using one of the usual techniques used for data hiding in images. The stego-image then obtained can then be converted back into frames and arranged in sequence to obtain the stego-video. This video contains the embedded data which can be obtained by extracting each frame and extracting the data from it.

Our technique spreads the data evenly over the entire video instead of concentrating it in into one single frame, thereby making the detection of the data even more impossible. For example if there are 4 bits of data to be embedded into a video with more than four frames then each bit will be embedded in one of the four frames in the video. This approach gives a huge advantage in the aspect of increasing the imperceptibility of the data embedded into the video. Our methodology is quite simple and unsophisticated and hence very fast when compared to other existing techniques.

4.2 The Algorithm for embedding is as follows:

1. Read the cover video with .avi extension.
2. Let the Cover video consist of **N** number of frames. Each of these frames are extracted from the video for the purpose of embedding the data in them.
3. Read the data to be embedded and convert it into binary form containing B bits.
4. Considering the amount of data to be embedded and the capacity of video calculate the value of k(no. of LSB's to be modified in each pixel), using the following formula. **K=(MAXDATA/B).** Where **MAXDATA**=**N*Height*Width.** (K should not exceed 4 in order to maintain satisfactory video quality).
5. Divide the B into N number of blocks of data. Let these blocks be called **BL_i**.
6. Divide each block into groups of K bits.
7. Consider one frame at a time and embed the K groups of bits in blocks **BL_i** into the Pixels in the corresponding frame. For example block **BL_i** is embedded into the ith frame. For embedding OPAP (Optimal Pixel adjustment process) is used which has been explained in the previous sections of the paper.
8. The frames with embedded data are again combined together to obtain the Stego-video.

4.3 The algorithm for retrieving the embedded data is as follows:

1. Read the Stego- video with .avi extension.
2. Let the Stego video consist of **N** number of frames. Each of these frames are extracted from the video for the purpose of retrieving the data from them.
3. Calculate the value of **K** using the following formula. **K= (MAXDATA/CHARBITS).**Where **CHARBITS** = (number of characters that have been embedded in the video)* 8.
4. Calculate the size of block of data to be extracted from each frame of the video using the formula

   BL_i= CHARBIT/ (K *N).
5. Extract the **BL_i** bits of data from the ith frame using the OPAP technique as described in the previous sections of paper.
6. The Extracted data which is a stream of bits should be grouped into groups of 8 bits each and converted back into the character format in order to retrieve the data embedded in the video.

4.4 Experimental Results:

This section shows the experimental results of the proposed scheme. This experiment was carried out using Sony VAIO laptop with INTEL centrino duo processor, 1.73 GHz, 1 GB RAM. The program has been developed in MATLAB version 7.4.0 running on WINDOWS VISTA operating system.

The MSE and PSNR values are generally used to estimate the effectiveness of a technique in steganography; hence we have also provided our results based on the same parameters. Since MSE and PSNR value cannot be calculated for the video as a whole, the values have been calculated for each frame and plotted in the form of a graph shown below.

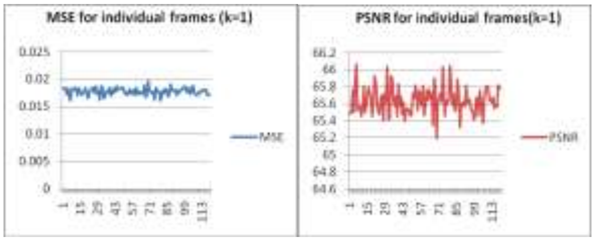
The algorithm was tested using various uncompressed video samples and similar results were obtained. We have tabulated the results obtained from a 13 second video in the .avi format with 120 frames displayed at 15 frames per second having a resolution of 120x180 pixels. Some of the frames of the stego and cover video have been provided later on in order show the effectiveness of our algorithm.

We have plotted the results obtained from our experimental results on the .avi uncompressed video in three pairs of graphs each showing the MSE and PSNR values obtained in three different cases. The three cases are:

Low data payload (k=1, not all frames are used for embedding)
Optimal Payload (k lies in the range of 1 to 4, all frames are used for embedding)
Extreme payload (k=4, All frames are packed with data to the maximum capacity).
The effectiveness of our algorithm in all the three cases has been expatiated in depth in this section.

Low Data Payload:

About 100-10000 characters are embedded in this case. In particular the results were obtained for embedding 100 characters (800 bits) into the video. Both the MSE and PSNR values have been calculated and plotted for each of the 120 frames available in the stego-video.



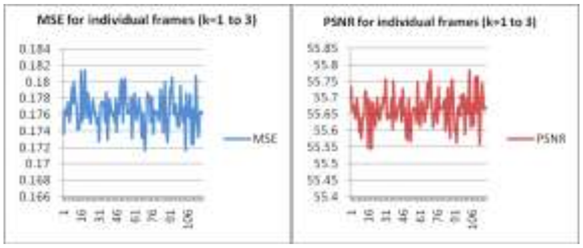
Time Taken=3.22 seconds

The most significant aspect of our technique is the spreading of the data to be embedded evenly over all the available frames. As the data to be embedded is far lesser than the payload capacity of the video a value of K=1 is used. K represents the number of LSBs that are modified in each pixel. Hence the MSE is very low and correspondingly the PSNR values are also high. It has been clearly enunciated in the graphs that have been plotted.

It can be seen that the MSE lies between 0.02 to 0.015 offering very high quality stego video and it is literally resistant to all steganalytic attacks, as the MSE value is even for all the frames and is also extremely small. It is clearly evident for this case that the technique performs equally well or better than the existing techniques.

Optimum Data Payload:

As stated before here the K values will in the range of 1 and 3 and about 10000 to 3lakh characters can be embedded. Here too since the data is evenly spread across all the frames MSE and PSNR values and relatively low and limited to a very small range. Thus it avoids the MSE value peaking for a few frames and being very less for others. This aspect again makes this technique more robust against steganalytic attacks. The Graph plotted below has been obtained for embedding 1 lakh characters in the video that we have considered. A value of K=3 has been used for embedding the data.



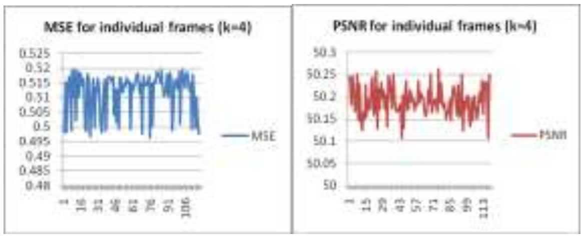
Time Taken=3.760 seconds

It is quite clearly evident from the graph that the MSE and PSNR values for all the frames are limited to within the range of 0.172 to 0.182 and 55.5 to 55.8 respectively. This value is well within the accepted limits of steganographic techniques and is performed very fast. There is only negligible time difference in the time taken to embed an optimal data payload when compared to low data payload.

Extreme data payload:

Based on our technique and the object we have chosen a maximum of 1316667 (120*120*160*4/7) characters can be embedded in the video. (Here the values have been obtained as follows: - frame resolution: 120x160; video has 120 frames; each pixel can hold up to 4 bits ; each character is represented with 7 bits). Obviously the K value will be 4, though the value of K can be increased to accommodate more data payload it is not done as it will affect the video quality adversely.

The graphs have been plotted for embedding 10 lakh characters at k=4.



Time Taken=4.02 seconds

It can be seen that the MSE and PSNR value lie in the range of 0.49 to 0.52 and 50.1 to 50.5 respectively. Thus the technique operates very fast and has MSE and PSNR value well within the normal range.

5 Audio Steganography:

5.1 Proposed Algorithm:

There are many existing algorithms which provide different methods for embedding. This paper discusses a novel algorithm which involves the following steps.

1. The first step involves the selection of the carrier which in this case is an audio file. The user can choose any audio file with .wav format.

2. After choosing the appropriate cover the information to be embedded is chosen from a file location in the local system. The information must then be embedded into the appropriate locations in the carrier. In order to perform this, specific properties of both the audio file and the message like binary equivalent or frequency components are extracted. The carrier frequency coefficients are divided into equal length blocks of size ‘n’ and one location from each block is chosen and one bit of the information is embedded into it. Thus the rate of embedding into the cover is 1 in n coefficients.

3. The ‘n’ is chosen based on the “***Hearing Threshold***”. The hearing threshold is the rate of embedding which determines the quality of the audio file after the information has been embedded. If the rate of embedding is greater than the Hearing threshold the quality is degraded and a smaller rate does not have a great impact on the quality but sets a limit to the payload of the data that can be embedded. So the tradeoff between quality and capacity has to be dealt with properly to meet the requirements. The hearing threshold is set a value of 1 in 1000 and an appropriate embedding rate is chosen.

4. The embedded frequency coefficients are then combined to create the stego audio file.

Normally any audio file has three main parameters the sampling rate in hertz, no. of bits per samples and the sampled data. There will be very large number of samples even in a small wave file. Hence the proposed technique works effectively on all forms of audio files.

Embedding can be done either by mere substitution or some conditions can be introduced. For example a threshold value is considered as the parameter. The sample value where the data is to be embedded is compared with this threshold value. If the sample value is greater, then data bit ‘1’ is embedded and if this condition fails ‘0’ is embedded. Employing such conditions greatly increases the SNR.

An appropriate embedding rate is selected such that there is no conflict with the constraints set on stego audio quality and embedding capacity set by the hearing threshold.

The retrieval process is complementary to the embedding procedure. Retrieve the data from the corresponding sample coefficients of the audio file into which they have been embedded.

5.2 SNR Analysis:

Signal-to-noise ratio [1] is defined as the ratio of signal power to the noise power corrupting the signal. We introduce an estimation formula for the proposed algorithm. The SNR between the original audio $F = \{f_i\}$, and the stego audio $F^* = \{f_i^*\}$, can be expressed as $\mathrm{SNR}=-10 \log_{10}\{(f-f^*)/f\}$ (dB)

4. Conclusion

Image steganography in spatial and frequency has been implemented and results are discussed. According to the simulation results for DWT, the PSNR is still a satisfactory value even the highest capacity case is applied. This is due to the different characteristics of DWT coefficients in different sub-bands. Since the most essential portion (the low frequency part) is kept unchanged while the secret messages are embedded in the high frequency sub-bands (corresponding to the edges portion of the original image), better PSNR is not a surprising result. Furthermore, expectable security is maintained as well since no message can be extracted without the knowledge of mapping rules.

The video technique is faster than those existing for video embedding techniques especially in the first and second cases as discussed earlier. It has very high data payload and is thus more suited than image steganography where large data payload is required. The MSE and PSNR values obtained also conform to those normally expected from steganographic techniques. But it must be noted that this technique cannot withstand any sort of compression and other data redundancy removal operations hence it is not as robust as other complex and slower frequency domain techniques such as DCT and DWT. This technique is also applicable for raw video formats and cannot be used for compressed video and other file formats. The future scope of this work lies in further decreasing the MSE of the stego-Video and making this technique more resistant to steganalytic attacks.

The performance of the proposed audio steganography scheme in terms of SNR is analyzed. The audio steganography technique discussed in this paper is very simple and least consuming technique. The choice of optimal sampling rate will result in an optimal trade off between Capacity and quality, thereby achieving the best results.

5. Acknowledgement

The authors wish to thank Dr. John Bosco Balaguru Dean Research SEEE and Dr K.Thenmozhi Associate Dean ECE SEEE/SASTRA University for their valuable guidance and support.

6. References

[1] Bender, W., Gruhl, D., Morimoto, N., Lu, A. Techniques for data hiding. IBM systems Journal (1996) 35 (3–4), 313–336.

[2] Ching-Chiuan Lin∗, Nien-Lin Hsueh, lossless data hiding scheme based on three-pixel block differences.(2007),vol 81,581-595

[3] Chung-Ming Wang., Nan-I Wu., Chwei-Shyong Tsai., Min-Shiang Hwang., A high quality steganographic method with pixel-value differencing and modulus function The Journal of Systems and Software (2008) 81, 150–158

[4] Xinpeng Zhang , Shuozhong Wang.,Vulnerability of pixel-value differencing steganographyto histogram analysis and modification for enhanced security (2003) 331-339

[5] Hideki Noda a, Michiharu Niimi a, Eiji Kawaguchi, High-performance JPEG steganography using quantization index modulation in DCT domain (2004) 455-461

[6] A. Westfeld, A. Pfitzmann, Attacks on steganographic systems, in:Proceedings of the Third International Workshop on Information Hiding(2000) pp. 61–76.

[7] J. Fridrich, M. Goljan, D. Hogea, New methodology for breaking steganographic techniques for JPEGs, in: Proceedings of SPIE: Security and Watermarking of Multimedia Contents, vol. 5020, (2003), pp. 143–155.

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

[9] S. Katzenbeisser, F.A.P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Norwood, MA, 2000,97-98

[10] F.A.P. Petitcolas, R.J. Anderson, M.G. Kuhn, Information hiding—a survey, Proc. IEEE 87 (7) (1999) 1062–1078.

[11] Gwena.el Do.err, Jean-Luc Dugelay. A guide tour of video watermarking” Signal Processing: Image Communication 18 (2003) 263–282.

[12]Yousof Erfani , Shadi Siahpoush.,“Robust audio watermarking using improved TS echo hiding” ,Digital Signal Processing 19 (2009) 809–814.

[13] Young-Shil Kim,Young-Mi Kim , Jin-Yong Choi, Doo-Kwon Baik ,2004, ” Information Hiding System Stegowavek For Improving Capacity**”** , Springer journal,(2004) 174-188

[14] Chi-Kwong Chan, L.M. Cheng, “Hiding data in images by simple LSB substitution “, Pattern Recognition 37 (2004) 469 – 474.

[15] Cheng-HsingYang, “Inverted pattern approach to improve image quality of information hiding by LSB substitution” , Pattern Recognition 41 (2008) 2674 – 2683.

[16] Po-Yueh Chen Hung-Ju Lin, “A DWT Based Approach for Image Steganography**”,** International Journal of Applied Science and Engineering (2006) 4, 3: 275-290.