New Steganography approach using encrypted secret message inside Audio and Video media

1P.L.RAJESWARI, DR. ASOKE NATH2

1DEPARTMENT OF ECE,IFET COLLEGE OF ENGG.
2Department of Computer Science St. Xavier's College(Autonomous) Kolkata, India

Abstract

Steganography is the technique of hiding any secret information like password, data and image behind any cover file.This paper proposes a method which is an audio-video crypto steganography system which is the combination of audio steganography and video steganography using advanced chaotic algorithm as the secure encryption method. The aim is to hide secret information behind image and audio of video file. Since video is the application of many audio and video frames, we can select a particular frame for image hiding and audio for hiding our secret data.4LSB substitution can be used for image steganography and LSB substitution algorithm with location selection for audio steganography. Suitable parameter of security and authentication such as PSNR value, histograms are obtained at both the receiver side and transmitter sides which are found to be identical at both ends. Reversible data hiding methods for both video and audio are also being mentioned. Hence the security of the data and image can be enhanced. This method can be used in fields such as medical and defense which requires real time processing. Here, we propose a data hiding and extraction procedure for high resolution AVI (Audio Video Interleave) videos. Although AVI videos are large in size but it can be transmitted from source to target over network after processing the source video by using these Data Hiding and Extraction procedure securely. There are two different procedures, which are used here at the sender's end and receiver's end respectively. The procedures are used here as the key of Data Hiding and Extraction.

Keywords: Steganography, Audio Steganography, Video Steganography, AVI, LSB

I.INTRODUCTION

The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level. Hiding information into a media requires following elements [2] :

1. The cover media(C) that will hold the hidden data
2. The secret message (M), may be plain text, cipher text or any type of data
3. The stego function (Fe) and its inverse (Fe-1)
4. An optional stego-key (K) or password may be used to hide and unhide the message.

The stego function operates over cover media and the message (to be hidden) along with a stego-key (optionally) to produce a stego media (*S*). The schematic of steganographic operation is shown below.

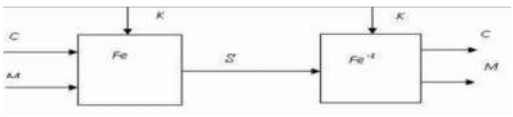

Fig 1: The Steganographic operation

Steganography and Cryptography are great partners in spite of functional difference. The steganography is the art of hiding data inside another data such as cover medium by applying different steganographic 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. Generally steganography technique is applied where the cryptography is ineffective.

Modern techniques of steganography

The common modern technique of steganography exploits the property of the media itself to convey a message. The following media are the candidate for digitally embedding message: -

» Plaintext
» Still imagery
» Audio and Video
» IP datagram

a)Audio Steganography

The basic model of Audio steganography consists of Carrier (Audio file), Message and Password. Carrier is also known as a cover-file, which conceals the secret information. Basically, the model for steganography is shown in Fig 2. Message is the data that the sender wishes to remain it confidential. Message can be plain text, image, audio or any type of file. Password is known as a stego-key, which ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-file. The cover-file with the secret information is known as a stego-file.

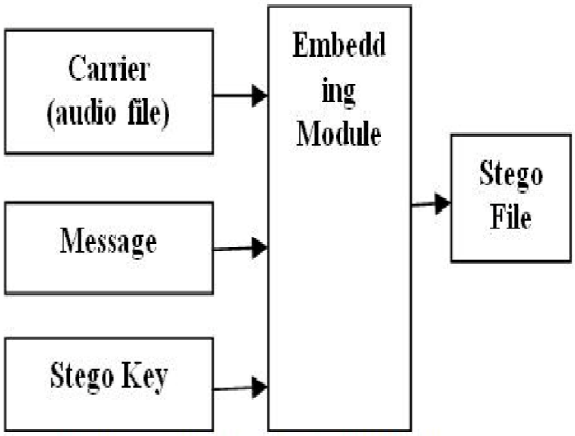

Fig 2: Basic Audio Steganographic Model

The information hiding process consists of following two steps.

- »Identification of redundant bits in a cover-file. Redundant bits are those bits that can be modified without corrupting the quality or destroying the integrity of the cover-file.
- »To embed the secret information in the cover file, the redundant bits in the cover file is replaced by the bits of the secret information.

In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file. There are several methods are available for audio steganography. Some of them are as follows:

1. ***LSB CODING:*** Sampling technique followed by Quantization converts analog audio signal to digital binary sequence.

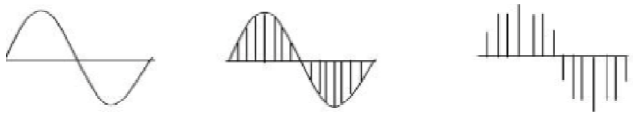

Fig 3: Sampling of the Sine Wave followed by Quantization process.

In this technique LSB of binary sequence of each sample of digitized audio file is replaced with binary equivalent of secret message. For example if we want to hide the letter 'A' (binary equivalent **01100101**) to an digitized audio file where each sample is represented with 16 bits, then LSB of 8 consecutive samples (each of 16 bit size) is replaced with each bit of binary equivalent of the letter 'A'.

Sampled Audio Stream (16 bit)	'A' in binary	Audio stream with encoded message
1001 1000 0011 1100	**0**	1001 1000 0011 110**0**
1101 1011 0011 1000	**1**	1101 1011 0011 100**1**
1011 1100 0011 1101	**1**	1011 1100 0011 110**1**
1011 1111 0011 1100	**0**	1011 1111 0011 110**0**
1011 1010 0111 1111	**0**	1011 1010 0111 111**0**
1111 1000 0011 1100	**1**	1111 1000 0011 110**1**
1101 1100 0111 1000	**0**	1101 1100 0111 100**0**
1000 1000 0001 1111	**1**	1000 1000 0001 111**1**

1) ***PARITY CODING:***

Parity coding is one of the robust audio steganographictechnique. Instead of breaking a signal into individual samples, this method breaks a signal into separate samples and embeds each bit of the secret message from a parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process inverts the LSB of one of the samples in the region. Thus, the sender has more of a choice in encoding the secret bit. Figure 4, shows the parity coding procedure.

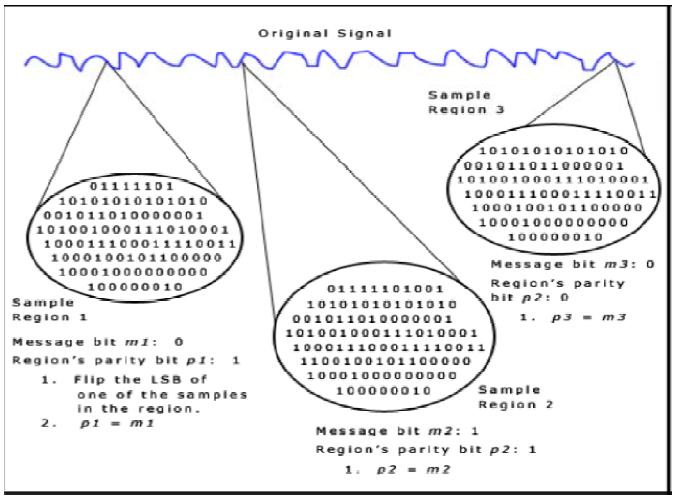

Fig 4. Parity coding

2) ***PHASE CODING:***

The phase coding technique works by replacing the phase of an initial audio segment with a reference phase that represents the secret information. The remaining segments phase is adjusted in order to preserve the relative phase between segments. In terms of signal to noise ratio, Phase coding is one of the most effective coding methods. When there is a drastic change in the phase relation between each frequency component, noticeable phase dispersion will occur. However, as long as the modification of the phase is sufficiently small, an inaudible coding can be achieved . This method relies on the fact that the phase components of sound are not as per the human ear as noise is. Phase coding is explained in the following procedure:

1 Divide an original sound signal into smaller segments such that lengths are of the same size as the size of the message to be encoded.
2. Matrix of the phases is created by applying Discrete Fourier Transform (DFT).
3. Calculate the Phase differences between adjacent segments.
4. Phase shifts between adjacent segments are easily detectable. It means, we can change the absolute phases of the segments but the relative phase differences between adjacent segments must be preserved.
5. Using the new phase of the first segment a new phase matrix is created and the original phase differences.
6. The sound signal is reconstructed by applying the inverse Discrete Fourier Transform using the new phase matrix and original magnitude matrix and then concatenating the sound segments back together.

The receiver must know the segment length to extract the secret information from the sound file. Then the receiver can use the DFT to get the phases and extract the secret information .

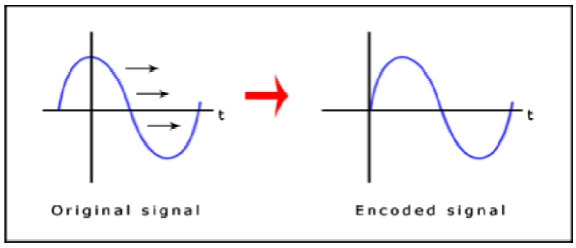

Fig 5. Phase coding

4) SPREAD SPECTRUM:

In audio steganography, the basic spread spectrum (SS) method attempts to spread secret information across the frequency spectrum of the audio signal. This is similar to a system which uses an implementation of the LSB that spreads the message bits randomly over the entire sound file. However, unlike LSB coding, the Spread Spectrum method spreads the secret information over the frequency spectrum of the sound file using a code which is independent of the actual signal . As a result, the final signal occupies a bandwidth which is more than what is actually required for transmission. The Spread Spectrum method is capable of contributing a better performance in some areas compared to LSB coding, phase coding, and parity coding techniques in that it offers a moderate data transmission rate and high level of robustness against removal techniques. However, the Spread Spectrum method has one main disadvantage that it can introduce noise into a sound file. The Spread Spectrum steps are shown in Figure 6.

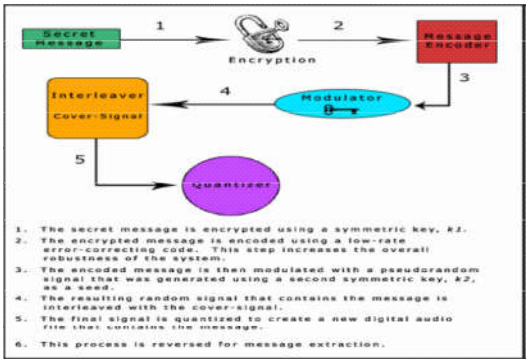

Fig 6. Spread Spectrum

5) ECHO HIDING

Echo hiding technique embeds secret information in a sound file by introducing an echo into the discrete signal. Echo hiding has advantages of providing a high data transmission rate and superior robustness when compared to other methods. Only one bit of secret information could be encoded if only one echo was produced from the original signal. Hence, before the encoding process begins the original signal is broken down into blocks. Once the encoding process is done, the blocks are concatenated back together to create the final signal [5, 20]. Echo Hiding is shown in Figure 7.

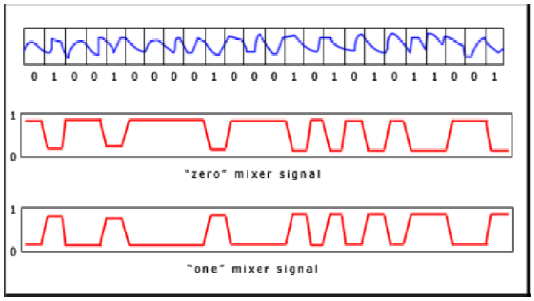

Fig 7. Echo hiding

b)Video Steganography

Digital video is a very promising host candidate that can carry a large amount of data (payload) and its potential for secret communications is largely unexplored. Since a video is formed from a sequence of frames, it presents the data hider with the possibility to embed and send a large amount of data. The requirements of any data hiding system can be categorized into security, capacity and robustness Cox et al. (1996). All these factors are inversely proportional to each other creating the so called data hiding dilemma. The focus of this paper aims at maximizing the first two factors of data hiding i.e. security and capacity coupled with alteration detection. The proposed scheme is a data-hiding method that uses high resolution digital video as a cover signal. The proposed scheme provides the ability to hide a significant quality of information making it different from typical data hiding mechanisms because here application that require significantly larger payloads like video-in-video and picture-in-video is considered. Data hiding requirements include the following:

1) **Imperceptibility**- The video with data and original data source should be perceptually identical.
2) **Robustness**- The embedded data should survive any processing operation the host signal goes through and preserve its fidelity.
3) **Capacity**-Maximize data embedding payload.
4) **Security**- Security is in the key.

Data Hiding is the different concept than cryptography, but uses some of its basic principles .In this paper, some important features of data hiding have been considered. The consideration is that of embedding information into video, which could survive attacks on the network. Some important video Steganography methods are:

1)Least Significant Bit Modifications:

The most widely used technique to hide data, is the usage of the LSB. Although there are several disadvantages to this approach, the relative easiness to implement it, makes it a popular method. To hide a secret message inside a image, a proper cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm. When using a 24 bit color image, a bit of each of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel. Thus, a 800 ×600 pixel image can contain a total amount of 1.440.000 bits (180.000 bytes) of secret data.

For example, the following grid can be considered as 3 pixels of a 24 bit color image, using 9 bytes of memory:

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

When the character A, which binary value equals 10000001, is inserted, the following grid results:

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

In this case, only three bits needed to be changed to insert the character successfully. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximal cover size. The resulting changes that are made to the least significant bits are too small to be recognized by the human eye, so the message is effectively hidden. While using a 24 bit image gives a relatively large amount of space to hide messages,it is also possible to use a 8 bit image as a cover source. Because of the smaller space and different properties, 8 bit images require a more careful approach. Where 24 bit images use three bytes to represent a pixel, an 8 bit image uses only one. Changing the LSB of that byte will result in a visible change of color, as another color in the available palette will be displayed. Therefore, the cover image needs to be selected more carefully and preferably be in grayscale, as the human eye will not detect the difference between different gray values as easy as with different colors.

2) Masking And Filtering:

Masking and filtering techniques, usually restricted to 24 bits or grayscale images, take a different approach to hiding a message. These methods are effectively similar to paper watermarks, creating markings in an image. This can be achieved for example by modifying the luminance of parts of the image. While masking does change the visible Properties of an image, it can be done in such a way that the human eye will not notice the anomalies.Since masking uses visible aspects of the image, it is more robust than LSB modification with respect to compression, cropping and different kinds of image processing. The information is not hidden at the ”noise” level but is inside the visible part of the image, which makes it more suitable than LSB modifications in case a lossy compression algorithm like JPEG is being used .

3) Transformations:

A more complex way of hiding a secret inside an image comes with the use and modifications of discrete cosine transformations. Discrete cosine transformations (DST)), are used by the JPEG compression algorithm to transform successive 8 x 8 pixel blocks of the image, into 64 DCT coefficients each. A simple pseudo-code algorithm to hide a message inside a JPEG image could look like this:

```
Input: Message, cover image
Output: steganographic image containing message
While data left to embed do
 Get next DCT coefficient from cover image
       If DCT not equal to 0 and DCT not equal to 1 then
                  Get next LSB from message
                  Replace DCT LSB with message bit
   End if
Insert DCT into steganographic image
End while
```

Although a modification of a single DCT will affect all 64 image pixels, the LSB of the quantized DCT coefficient can be used to hide information. Lossless compressed images will be suspect able to visual alterations when the LSB are modified. This is not the case with the above described method, as it takes place in the frequency domain inside the image, instead of the spatial domain and therefore there will be no visible changes to the cover image. When information is hidden inside video the program or person hiding the information will usually use the DCT (Discrete Cosine Transform) method. DCT works by altering values of certain parts of the images, it usually rounds them up. For example if part of an image has a value of 6.667 it will round it up to 7. Data Hiding in Videos is similar to that of Data Hiding in Images, apart from information is hidden in each frame of the video.

II.PROPOSED METHOD

a) For Audio Steganography

Here we will discuss the disadvantages of the previous procedure and how those are different with present method. The main disadvantages associated with the use of existing methods like echo hiding, spread spectrum and parity coding are, human ear is very sensitive to noise and it can often detect even the slightest bit of noise introduced into a sound file and another problem is robustness. Phase coding has main disadvantage of low data transmission rate because of the fact that the secret message is encoded only in the first signal segment. Hence this method is used only when a small amount of data needs to be transferred. Among different information hiding techniques proposed to embed secret information within audio file, ***LeastSignificant Bit (LSB)*** coding method is the simplest way to embed secret information in a digital audio file by replacing the least significant bit of audio file with a binary message. Hence LSB method allows large amount of secret information to be encoded in an audio file.

Figure 8 and figure 9 represents the complete working of the audio stegnography process of embedding the encrypted secret message using public key cryptographic algorithm, RSA into the 4th and 5th layers of the audio file. In the sender side, the text file which has to be embedded into an audio file is encrypted using public key cryptographic algorithm, RSA. The cipher text obtained is then embedded in the 4th AND 5th LSB bit using one of the Steganographic algorithms, LSB algorithm. The resultant audio file contains the secret message embedded into it. On the receiver side, the embedded audio file is selected to extract the secret message. The secret message is decrypted using RSA decryption method and the secret messages are compared before embedding and after embedding. Also, comparisons are made based on PSNR of both original audio file and embedded audio file, to indicate that less noise intrusion even after changing the 4th and 5th LSB bit of the original wave.

SENDER

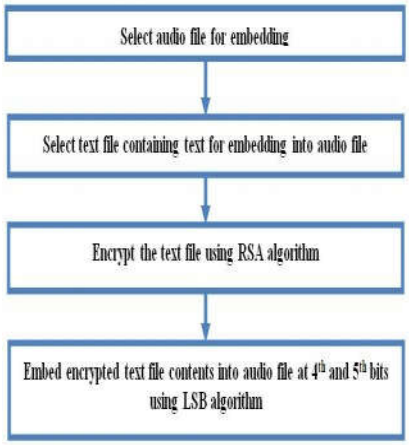

Fig .8: Sender

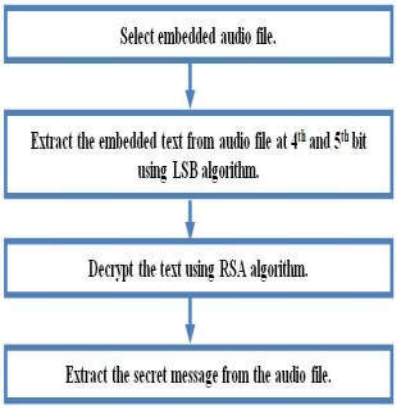

Fig.9: Receiver

Algorithm For Embedding Text File Content Into Audio File At The Sender Side.
Step1: Select the audio file for embedding the secret message.
Step2: Play the audio file so that it sounds clear to the end user.
Step3: Select the text file containing the secret message.
Step4: Encrypt the text file contents.
Step5: Compare text file and audio file size. If text file size > audio file contents Error message displayed indicating cannot embed secret message. Else
Embed secret message in the audio file in the 4th and 5th LSB bit of every sample.
Step6: Display message to user of the new audio file created after embedding secret message.

Algorithm For Extracting The Embedded Text From Audio File At The Receiver Side.

Step 1: Select the new audio file for extracting the secret message.
Step 2: Extract the secret message from the audio file from the 4th and 5th LSB bit of every sample.
Step 3: If secret message present in audio file Then
Display message to end user after extracting message.
Else
Display that no hidden data is present in the text.
Step 4: Decrypt the secret message.
Step 5: Display message to end user after decrypting the message.

b) For Video Steganography

The main high resolution AVI fie is nothing but a sequence of high resolution image called frames. Initially stream the video and collect all the frames in bitmap format (Figure 1). And also collect the following information:

1 **Starting frame**: It indicates the frame from which the algorithm starts message embedding.
2 **Starting macro block**: It indicates the macro block within the chosen frame from which the algorithm starts message embedding.
3 **Number of macro blocks**: It indicates how many macro blocks within a frame are going to be used for data hiding. These macro blocks may be consecutive frame according to a predefined pattern. Apparently, the more the macro blocks we use, the higher the embedding capacity we get. Moreover, if the size of the message is fixed, this number will be fixed, too. Otherwise it can be dynamically changed.
4 **Frame period**: It indicates the number of the inter frames, which must pass, before the algorithm repeats the embedding. However, if the frame period is too small and the algorithm repeats the message very often, that might have an impact onto the coding efficiency of the encoder. Apparently, if the video sequence is large enough, the frame period can be accordingly large. The encoder reads these parameters from a file. The same file is read by the software that extracts the message, so as both of the two codes to be synchronized. After streaming the AVI video file into AVI frames the conventional LSB replacement method is used. Recently it has been claimed that LSB replacement involving more than one least significant bit planes is less detectable than single bit plane LSB replacement. Hence the use of multiple bit planes for embedding has been encouraged. But the direct use of 3 or more bit planes leads to addition of considerable amount of noise in the cover image. Still as the work is in high resolution video so get a RGB combination of each pixel as in Figure 2 hence if one LSB is considered there is a choice of 3 bits for each pixel. This will give a higher security of the Data Hiding method.

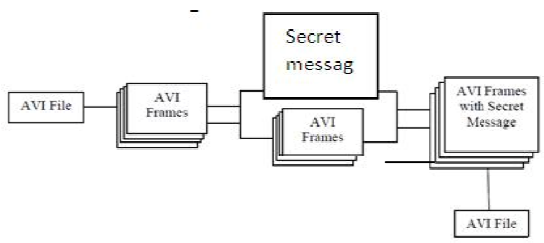

Fig1. AVI video Streaming and Data Hiding

III.RESULTS AND DISCUSSION

a) For Audio Steganography

Different experiments were conducted to prove that the proposed method of embedding audio file. The following experiments were conducted by modifying the 4th and 5th bit LSB with same data and different data.

1. Same audio file is embedded with different text file with varying text content sizes.
2. Different audio files of different time durations are taken and embedded with same text content.
3. Different categories of audio file are considered and embedded with same text content.

In all the cases, SNR (Signal to Noise Ratio) and PSNR (Peak; Signal to Noise Ratio) area calculated. Figure 10 shows the original audio file before embedding the text content and Figure 11 shows the audio file after embedding the text content. The results show that the size of the audio file remains same even after embedding the secret message.

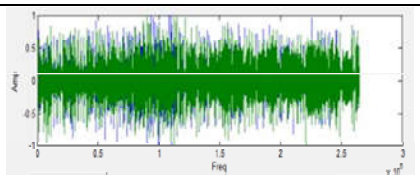

Fig.10. original audio file

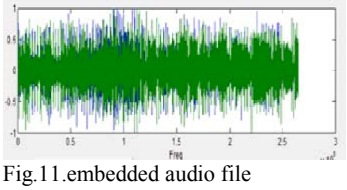

Fig.11.embedded audio file

b) For Video Steganography

Data size estimation: Each frame of the Video is taken a data source for Data Hiding. First the maximum size of the hiding data is calculated as shown in Figure 3. The size of the image is 2000 × 1000 and modified it to 2048 × 1024. On further calculations we get 786,432,000 chars that can be embedded. The following equation mentioned below have been followed:(((Width × height) × 3 bits)/8 bits)/3 bytes × 3000 frames = char/video
And the image Bitmap size = 2048 × 1024

Step of calculations the maximum of hiding information:

1. Each frame consist = 2048 × 1024 = 2, 097, 152 Pixels.
2. Each pixel include 3 bytes (One byte we use single bit for encode data hiding) R = 1 bit, G = 1 bit and B = 1 bit.
3. Each frame = Pixels ×3 = 2, 097, 152 × 3 = 62, 915, 456 bits.
4. Each frame we can maximum hiding data is 62, 915, 456 bits/8 bits = 786, 432 bytes.
5. If this video 3000 frames = 786, 432 × 3000 = 2, 359.296, 000 bytes (1 bytes = 1Character).
6. For 1 Character of Unicode we need 3 bytes/1 character of Unicode = 2, 359.296,000 bytes/3 =786, 432, 000 chars.

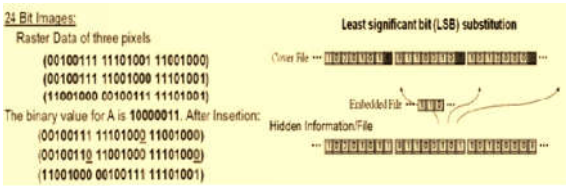

Fig 3

IV. AUTHENTICATION

Authentication is mainly done to confirm the real identity of the data or image or whatever entities. It is mainly done to ensure that it came from the real user. Here authentication is mainly done for the security purpose at both the transmitter as well as the receiver for secure communication. The data hiding key provided at the transmitter side act as the authentication key in audio steganography. In case of video hiding the frame number and the triple key provided as the encryption key acts as the tool for authentication. The strength of the key used decides the strength of authentication.

V. CONCLUSION

The proposed systems are considered to be an efficient method for hiding message in audio and video files such that data can reach the destination in a safe manner without being modified. Using the method of embedding text in the 4th and 5th layer with same data and different data along with the encryption and decryption of the secret message using public key cryptographic algorithm, makes data more secure and transparency is minimized. In this paper a data hiding technique is proposed for high resolution video. The intension is to provide proper protection on data during transmission. For the accuracy of the correct message output that extract from source tools for comparison can be used and statistical analysis can be done. Its main advantage is that it is a blind scheme and its affect on video quality or coding efficiency is almost negligible. It is highly configurable, thus it may result in high data capacities. Finally, it can be easily extended, resulting in better robustness, better data security and higher embedding capacity.

References

1. Arup Kumar Bhaumik, Minkyu Choi, RosslinJ.Robles, and MaricelO.Balitanas ," Data Hiding in Video", International Journal of Database Theory and Application Vol. 2, No. 2, June 2009.
2. Padmashree G, Venugopala P S," Audio Stegnography and Cryptography: Using LSB algorithm at 4th and 5th LSB layers", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 4, October 2012.
3. Jayaram P, Ranganatha H R, Anupama H S," INFORMATION HIDING USING AUDIO STEGANOGRAPHY – A SURVEY", The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011.
4. AsokeNath, Sankar Das, AmlanChakraborti, **"**Data Hiding and Retrieval" published in IEEE "Proceedings of International Conference on Computational Intelligence and Communication Networks (CICN 2010)" held from 26-28 NOV'2010 at Bhupal, Page: 392-397(2010).
5. JoyshreeNath, Sankar Das, ShalabhAgarwal and AsokeNath, "Advanced steganographic approach for hiding encrypted secret message in LSB, LSB+1, LSB+2 and LSB+3 bits in non standard cover files", International Journal of Computer Applications, Vol14-No.7,Page-31-35, Feb(2011).
6. JoyshreeNath, Sankar Das, ShalabhAgarwal and AsokeNath, " Advanced Steganography Algorithm using encrypted secret message", International Journal of Advanced Computer Science and Applications, Vol-2, No-3, Page-19-24, March(2011).
7. JoyshreeNath, Sankar Das, ShalabhAgarwal and AsokeNath, "A Challenge in hiding encrypted message in LSB and LSB+1 bit positions in any cover files : executable files, Microsoft office files and database files, image files, audio files and video files ",JGRCS, Vol-2,No.4,Page:180-185,April (2011)