ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 8, August 2014

A Secured Communication Based on Adaptive Steganography

Parlapelly Anusha[1], V. Sudarshini Kataksham[2], C.V.Keerthi Latha[3]

Department of Electronics and Communication Engineering, Stanley College of Engineering and Technology for Women, Hyderabad, India[1,2,3]

Abstract: Steganography is an art of sending hidden data or secret messages over a public channel so that a third party cannot detect the presence of the secret messages. The goal of steganography is different from classical encryption, which seeks to conceal the content of secret messages; steganography is about hiding the very existence of the secret messages. Modern steganography is generally understood to deal with electronic media rather than physical objects. There have been numerous proposals for protocols to hide data in channels containing pictures, video, audio and even typeset text. A steganographic method of embedding textual information in an audio image and then to the audio file is presented in this project. In the proposed technique, first an image is selected after that we have to take the secret text and by using Adaptive LSB algorithm have to hide the secret text in that image. This stego image again hidden into the audio file. Based on LSB algorithm has to hide the stego image into the audio file. This audio file is sampled and then an appropriate bit of each alternate sample is altered to embed the textual information as well as an image. As a steganographic approach the perceptual quality of the host audio signal and host image was not to be degraded.

Keywords: Steganography, Embedding, LSB algorithm.

I. INTRODUCTION

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret.

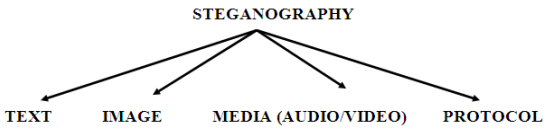


Fig 1: Different Types STEGANOGRAPHY

The technique used to implement this, is called steganography. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, Steganography focuses on keeping the existence of a message secret. In Our Project we are going to implement hiding information inside images the LSB (Least Significant Byte) method is usually used. To a computer an image file is simply a file that shows different colours and intensities of light on different areas of an image. The best type of image file to hide information inside of is a 24 Bit BMP (Bitmap) image. The reason being is this is the largest type of file and it normally is of the highest quality. When an image is of high quality and resolution it is a lot easier to hide and mask information inside of. Although 24 Bit images are best for hiding information inside of due to their size some people may choose to use 8 Bit BMP's or possibly another image format such as GIF, the reason being is that posting of large images on the internet may arouse suspicion. When hiding information inside Audio files the technique usually used is low bit encoding which is somewhat similar to LSB that is generally used in Images. The problem with low bit encoding is that it is usually noticeable to the human ear, so it is a rather risky method for someone to use if they are trying to mask information inside of an audio file. Spread Spectrum is another method used to conceal information inside of an audio file. This method works by adding random noises to the signal the information is conceal inside a carrier and spread across the frequency spectrum. Echo data hiding is yet another method of hiding information inside an audio file This method uses the echoes in sound files in order to try and hide information By simply adding extra sound to an echo inside an audio file, information can be concealed The thing that makes this method of concealing information inside of audio files better than other methods is that it can actually improve the sound of the audio inside an audio file.

II. RELATED WORKS

Audio Steganography

Audio steganography works by slightly changing the binary sequence and concealing with the secret message. Several methods are proposed such as Least Significant Bit (LSB) replacing last digit of carrier file. Parity coding involves breaking down of signal and then hiding the message in parity bits of each sample. Phase coding involves encoding of secret data to phase shifts. Spread spectrum distributes secret data into frequency spectrum, in which direct sequence and frequency hopping is used. The Echo method generates echo for insertion of secret data into signal.

Video Steganography

The separation of video into audio and images or frames results in the efficient method for data hiding. The use of

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 8, August 2014

video files as a carrier medium for steganography is more eligible as compared to other techniques. As a result of this technique is discussed and proposed in this paper.

Network Steganography

The approach for hiding data is to use network steganography by sending data with the help of network protocol. Network or transport layer such as IP/TCP or ICMP and UDP protocols are used for sending messages

IMAGE STEGANOGRAPHY (Text Hide in Image):-

The implementation of system will only focus on Least Significant Bit (LSB) as one of the steganography techniques as mentioned in below.

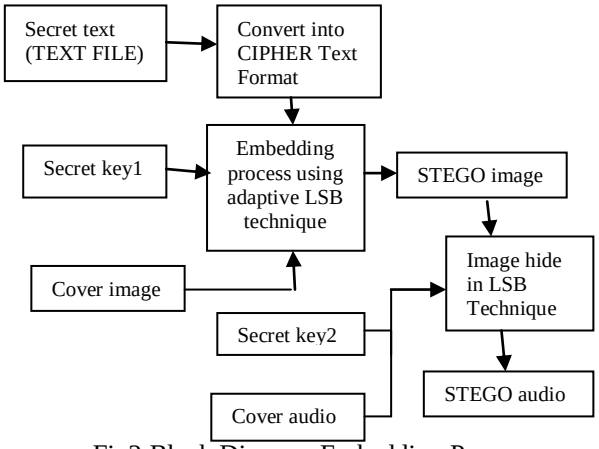


Fig2:Block Diagram Embedding Process

III. LEAST-SIGNIFICANT BIT (LSB) TECHNIQUE

The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. Digital images are mainly of two types (i) 24 bit images and (ii) 8 bit images. In 24 bit images we can embed three bits of information in each pixel, one in each LSB position of the three eight bit values. Increasing or decreasing the value by changing the LSB does not change the appearance of the image; much so the resultant stego image looks almost same as the cover image. In 8 bit images, one bit of information can be hidden. A stego-image is obtained by applying LSB algorithm on both the cover and hidden images. The hidden image is extracted from the stego-image by applying the reverse process. If the LSB of the pixel value of cover image C(i,j) is equal to the message bit m of secret massage to be embedded, C(i,j) remain unchanged; if not, set the LSB of C(i, j) to m. The message embedding procedure is given below-

S(i,j) = C(i,j) - 1, if LSB(C(i,j)) = 1 and m = 0
S(i.j) = C(i,j), if LSB(C(i,j)) = m
S(i,j) = C(i,j) + 1, if LSB(C(i,j)) = 0 and m = 1

Data Encryption: Chaos Crypto system

1) This method is one of the advanced encryption standard to encrypt the text data for secure transmission.
2) It encrypts the original text message with encryption key value generated from chaotic sequence with threshold function by bit xor operation
3) Here logistic map is used for generation of chaotic map sequence.
4) It is very useful to transmit the secret text data through unsecure channel securely which prevents data hacking.
5) The chaotic systems are defined on a complex or real number space called as boundary continuous space.
6) Chaos theory generally aims that to recognize the asymptotic activities of the iterative progression

Input Text: - Shiva ram

Chaos's Encrypt Text: - ¦bÁªIS9¸Þ

where LSB(C(i, j)) stands for the LSB of cover image C(i,j) and m is the next message bit to be embedded.= S(i,j) is the stego image As we already know each pixel is made up of three bytes consisting of either a 1 or a 0.

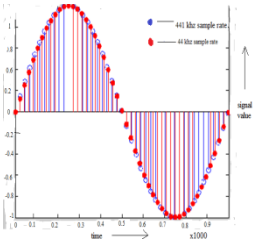
For example, suppose one can hide a message in three pixels of an image (24-bit colours). Suppose the original 3 pixels are:
(11101010 11101000 11001011)
(01100110 11001010 11101000)
(11001001 00100101 11101001)

A steganographic program could hide the letter "J" which has a position 74 into ASCII character set and has a binary representation "01001010", by altering the channel bits of pixels.
(11101010 11101001 11001010)
(01100110 11001011 11101000)
(11001001 00100100 11101001)

In this case, only four bits needed to be changed to insert the character successfully. The resulting changes that are made to the least significant bits are too small to be recognised by the human eye, so the message is effectively hidden. The advantage of LSB embedding is its simplicity and many techniques use these methods. LSB embedding also allows high perceptual transparency.

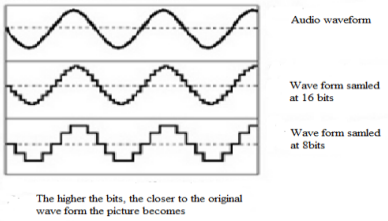
AUDIO STEGANOGRAPHY (STEGO Image Hide in AUDIO):-

Steganography techniques are used to hide secret information in the most common audio/video formats. There are three main different kinds of audio/video steganography:
1) Insertion steganography, where the secret message is inserted in the cover object;
2) Substitution steganography, where some bits of the cover object are substituted with the bits of the secret message;
3) Constructing steganography, where an ad hoc cover object is generated to contain the secret message.



ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 8, August 2014



Least significant bit (LSB) coding is the simplest way to embed information in a digital audio file. By substituting the least significant bit of each sampling point with a binary message, LSB coding allows for a large amount of data to be encoded.

Standard LSB-Encoding ALGORITHM:

It performs bit level manipulation to encode the message. The following steps are

a. Receives the audio file in the form of bytes and converted in to bit pattern.

b. Each character in the message is converted in bit pattern.

c. Replaces the LSB bit from audio with LSB bit from character in the message.

Algorithm: Improved/ Modified LSB Encoding

```
        if  host sample a>0
if bit 0 is to be embedded
            if ai-1=0 then ai-1ai-2.....a0=11.....1
            if ai-1=1 then ai-1ai-2.....a0=00.....0and
                        if ai-1=0 then ai-1=1
                        else if ai-2=0 then ai-2=1
                        .....
                        else if a15=0 then a15=1
           else if bit 1 is to be enbedded
            if ai-1=1 then ai-1ai-2.....a0=00.....0
           if ai-1=0 then ai-1ai-2.....a0=11.....1 and
                        if ai-1=1 then ai-1=0
                        else if ai-2=1 then ai-2=0
                        ........
                        else if a15=1 then a15=0
        if  host sample a<=0
           if bit 0 is to be embedded
           if ai-1=0 then ai-1ai-2.....a0=11.....1
           if ai-1=1 then ai-1ai-2.....a0=00.....0 and
                        if ai-1=1 then ai-1=0
                        else if ai-2=1 then ai-2=0
                        .........
                        else if a15=1 then a15=0
else if bit 1 is to be embedded
            if ai-1=1 then ai-1ai-2.....a0=00.....0
            if ai-1=0 then ai-1ai-2.....a0=11.....1and
                        if ai-1=1 then ai-1=0
                        else if ai=2=1 then ai-2=0
                        ........
                        Else if a15=1 then a15=0.
```

The phase coding method breaks down the sound file into a series of N segments. A Discrete Fourier Transform (DFT) is applied to each segment to create a matrix of the phase and magnitude. The phase difference between each segment is calculated, the first segment (s0) has an artificial absolute phase of p0 created, and all other segments have newly created phase frames. The new phase and original magnitude are combined to get the new segment, Sn. These new segments are then concatenated to create the encoded output and the frequency remains preserved. In order to decode the hidden information the receiver must know the length of the segments and the data interval used. The first segment is detected as a 0 or a 1 and this indicates where the message starts. This method has many advantages over Low Bit Encoding, the most important being that it is undetectable to the human ear. Like all of the techniques described so far though, its weakness is still in its lack of robustness to changes in the audio data. Any single sound operation or change to the data would distort the information and prevent its retrieval.

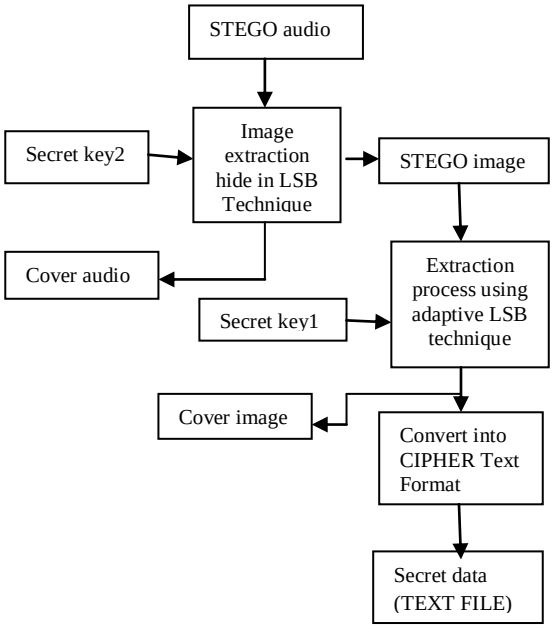


Fig3:Block Diagram of Extraction Process

Receiver Decrypt Text: - Shiva ram

Advantages:-

a) This algorithm use random size of key.
b) Because of this random size the middle person can't predict the size of key and data**.**
c) The number of times execution of loop is not fixed so that more secure algorithm.
d) This is more secure and easy to implement.

Quality Measurement:-

The Quality of the reconstructed image is measured in-terms of mean square error (MSE) and peak signal to noise ratio (PSNR) ratio. The MSE is often called reconstruction error variance σ_q^2. The MSE between the original image f and the reconstructed image g at decoder is defined as:

$$\mathbf{MSE} = \sigma_q^2 = \frac{1}{N} \sum_{j,k} (f[j,k] - g[j,k])$$

Where the sum over j, k denotes the sum over all pixels in the image and N is the number of pixels in each image. From that the peak signal-to-noise ratio is defined as the ratio between signal variance and reconstruction error variance. The PSNR between two images having 8 bits per pixel in terms of decibels (dB) is given by:

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 8, August 2014

$$\textbf{PSNR} = 10 \log_{10} \left(\frac{255^2}{MSE} \right)$$

Generally when PSNR is 20 dB or greater, then the original and the reconstructed images are virtually in-distinguishable by human eyes.

IV. CONCLUSION

In this research, I presented an efficient technique for hiding data in an image and an audio file. The basic idea of our technique is to hide data in an image file and that image which contains data is hided in to an audio file.

Cover image	Existing method		Modified method With audio signal		
	MSE	PSNR	MSE	PSNR	Correlation coeffient
Lena	81.9474	28.9955	0.4166	51.9396	0.9999
Nehru-Gandhi	86.4408	28.4408	0.2177	54.7524	0.9999
Gandhi	88.8853	28.6425	0.4559	51.5420	0.9999
Temple	88.4879	28.6620	0.4134	51.5967	0.9999
Baboon	86.7836	28.7464	0.6261	50.1645	0.9995

From the experimental results, it is found that the hidden secret data creates minimal changes in the cover audio and without altering its quality. Moreover, the secret data itself is successfully hidden and extracted with minimal distortion.

V. FUTURE SCOPE

For video, a combination of sound and image techniques can be used. This is due to the fact that video generally has separate inner files for the video (consisting of many images) and the sound. So techniques can be applied in both areas to hide data. Due to the size of video files, the scope for adding lots of data is much greater and therefore the chances of hidden data being detected is quite low.

REFERENCES

[1] Siva Janakiraman , Pixel Bit Manipulation for Encoded Hiding -An Inherent stego,2012 IEEE,978-1-4577.
[2] Bruice Schneier, Applied Cryptography Protocols, Algorithm and Source Code in C. 2nd ed. Wiley India edition, 2007.
[3] C.K. Chan, L.M. Chen, Hiding data in images by simple LSB substitution, Pattern Recognition. 37 (3) (2004) 469–474.
[4] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt Digital Image Steganography:Survey and Analysis of Current Methods.
[5] Hiding data in images by simple LSB substitutionChi-Kwong Chan⁎, L.M. Cheng Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong Kong Received 17 May 2002; received in revised form 11 July 2003; accepted 11 August 2003.
[6] Information Hiding Using Least Significant Bit Steganography and Cryptography Shailender Gupta Department of Electrical & Electronics Engineering, YMCAUST,
[7] Marvel, L., M., Boncelet Jr., C.G. & Retter, C.,"Spread Spectrum Steganography", IEEE Transactions on Image Processing, 1999.
[8] Waugh & Wang, S,"Cyber Warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004.
[9] Stefan Katznbeisser, Fabien. A., P.Petitcolas editors, Information Hiding Techniques for Steganography and Digital Watermarking,Artech House, Boston.London,2000.
[10] Jamil,T., "Steganography: The art of Hiding Information is Plain Sight", IEEE Potentials,18:01,1999.
[11] B.Pfitzmann ,"Information Hiding Terminology," proc.First Int'l Workshop Information Hiding, Lecturer Notes in Computer Science No.1,174,Spring –Verlag,Berlin,1996,pp.347-356.
[12] Yean- Kuhn Lea and Ling-Hew Cheng,"High capacity steganographic model" ,IEEE Proc.Visual Image Signal Process.,Vol.147,No.3,June 2000.
[13] Ross J.Anderson, Fabien A.P.Petitcols, on The limits of steganography, IEEE Journal of Selected Areas in Communication, 16(4);474-481,May 1998.
[14] M.Ashourian, R.C. Mainland Y.H.Ho, DitheredQuantization for Image Data Hiding In DCT domain, Proc.of IST2003, 2003, 171-175.
[15] C.C.lin, P.F.Shiu, High Capacity Data hiding scheme for DCT-based images. Journal of Information Hiding and Multimedia Signal Processing,1(3),2010,314-323.

BIOGRAPHIES

P.Anusha received the B-Tech degree in Electronic and Communication Engineering from Trinity College of Engineering, India. She is pursuing Masters in Embedded Systems from Stanley College of Engineering and Technology for Woman, Hyderabad, India. Her research interest includes MATLAB, Embedded systems, Digital signal processing.

V.SUDARSHANI KATAKSHAM received the Bachelor of Engineeing degree in Electronics and communication Engineering from Jawaharlal Nehru Technological University, Hyderabad in 2009 and pursued her M.TECH in VLSI SYSTEM DESIGN from CVSR college of Engineering and Technoogy JNTU, Hyderabad. She is currently working as a Asst Professor in Electronics and communication Engineering Department at Stanley College of Engineering And Technology For Women ,Abids, Hyd. And she has three years of Teaching experience and attended various seminars. His areas of interest include High performance VLSI Design and VHDL based system design.

C.V.Keerthi Latha received B.E. degree in Electronic & Communication Engineering from J.N.T.U. and M.E degree with digital systems specialization from Osmania University. Since 2004 she has been working with department of ECE as an Assistant professor and completed 7 years of experience .