ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering (ICIET'14)

On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Audio Based Steganography for Hiding Secret Data

V. Nithya poorani[#1], L.Jawagar[#2]
Final Year ME, Communication Systems, Mount Zion College of Engineering and Technology, India

ABSTRACT—Watermarking has been proposed as a solution to the problem of resolving Copyright ownership of multimedia data (image, audio, video). The work presented in this thesis is concerned with the design of robust digital image watermarking algorithms of least significant bit (LSB) algorithm for copyright protection and similarly the voice is compressed by using linear predictive code (LPC) algorithm, It is one of the most powerful speech analysis techniques, and one of the most useful methods for encoding good quality speech at a low bit rate and provides extremely accurate estimates of speech parameters. Finally hide the watermarked image and compressed voice by using Steganographic method. Steganography is an art of sending hidden data or a secret message over a public channel so that a third party cannot detect the presence of the secret message. Firstly, an overview of the watermarking system, applications of watermarking and attacks, are given. The robustness of the data is very important issue in watermarking. The watermarking algorithm which requires the presence of original image for watermark detection.

KEYWORDS—Steganography, watermarking, compression, least significant bit, linear predictive coding

I.INTRODUCTION

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It secures the network, as well as protecting and overseeing operations being done.

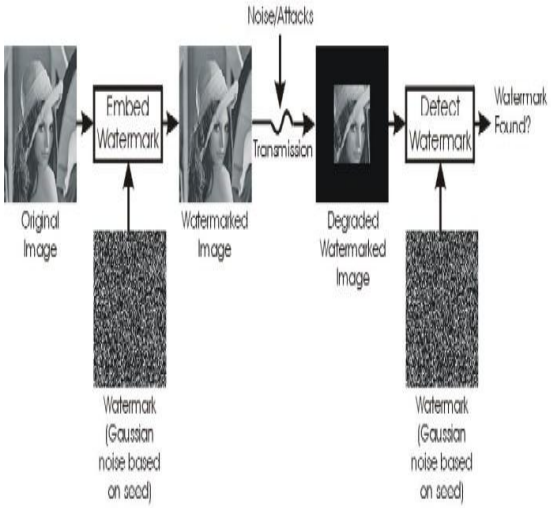

Fig. 1 General process of watermarking an image

When the watermark is still perceivable after some attacks, the process is referred as robust watermarking. Robust watermarking is usually used for copyright control. In the opposite, fragile watermarking is the case where the watermark is

embedded to an image in such a way, that the slightest alteration of the image, due to an attack, would make the watermark unperceivable.

II. STEGANOGRAPHY

Steganography is one important technique in data hiding area. With the invention of multimedia and similar technological area the need for such a counter attack measure has become even more important. Information present in internet and other digital media allows duplication and reproduction of material without the knowledge of the owner of the data. Hence increase in easy reaches of data means easy hacking of data. Thus there must be surveillance and protection systems to analyze techniques for hiding and recovering data.

A. Steganographic Technique

There have been numerous techniques for hiding information and are still in research. Various such methods are communication via invisible inks, microdots and spread spectrum channels. All these techniques involve embedding information within digital media, specifically digital images.

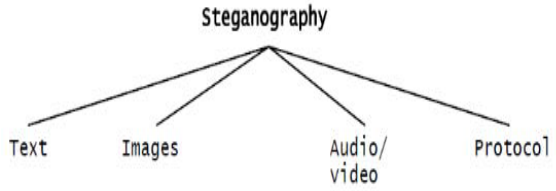

Fig. 2 Different technique in steganography

Spatial transform techniques embed the information into the bits of image directly without use of transformation. Generally the file's non-significant bits (containing the message) are altered such that the file does not show any sign of alteration. Steganography relies on some form of carrier or information. They are also called us 'dummy data'. Digital images are widely used as carriers. Secret information is embedded within an image such that the image looks unchanged to human eye.Steganography means covered writing. It includes a vast array of methods of secret communications that conceal the very existence of the message. Steganography is the art of concealing the existence of information. Steganography might sound similar to cryptography. Cryptographic techniques "scramble" messages so if intercepted, the messages cannot be understood. Steganography aims to take a selection of plaintext and complete conceal its existence within some arbitrary.

B. Segmentation

Segmentation means to divide the marketplace into parts, or segments, which are definable, accessible, actionable, and profitable and have a growth potential. In other words, a company would find it impossible to target the entire market, because of time, cost and effort restrictions. It needs to have a 'definable' segment - a mass of people who can be identified and targeted with reasonable effort, cost and time. Segmentation allows a seller to closely tailor his product to the needs, desires, uses and paying ability of customers. It allows sellers to concentrate on their resources, money, time and effort on a profitable market, which will grow in numbers, usage and value.

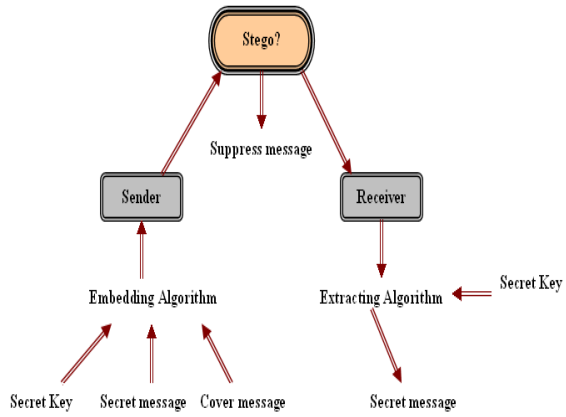

Fig. 3 Steganographictechniquescenaro

III. PROPOSED SYSTEM of AUDIO BASED STEGANORAPHY

A. Watermarking

There are few approaches designed for protecting data securing systems.one is cryptography and another is watermarking.by using cryptanalysis the cipher text can be easily tracked by the unauthorized person,so we use another method of securing data called watermarking.The invisibly watermarked document should satisfy several criteria:

- The watermark must be difficult or impossible to remove, at least without visibly degrading the original image, The watermark must survive image modifications that are common to typical image-processing applications (e.g., scaling, color requantization, dithering, cropping, and image compression)
- For some invisible watermarking applications, watermarks should be readily detectable by the proper authorities, even if imperceptible to the average observer. Such decidability without requiring the original, un-watermarked image would be necessary for efficient recovery of property and subsequent prosecution.

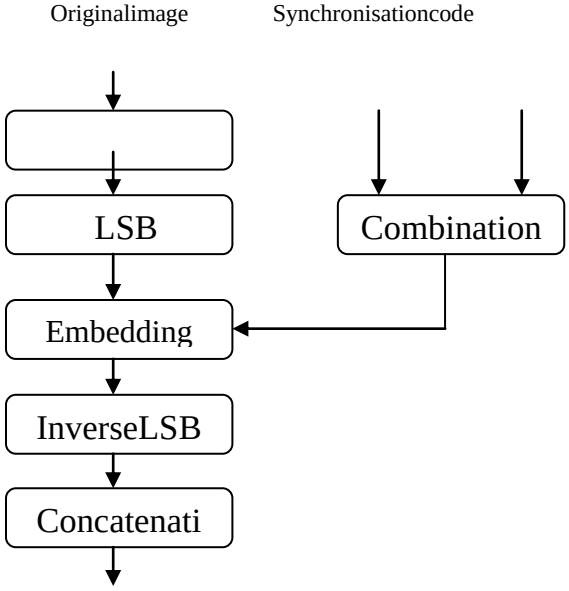

Fig. 4 Watermarking embedding

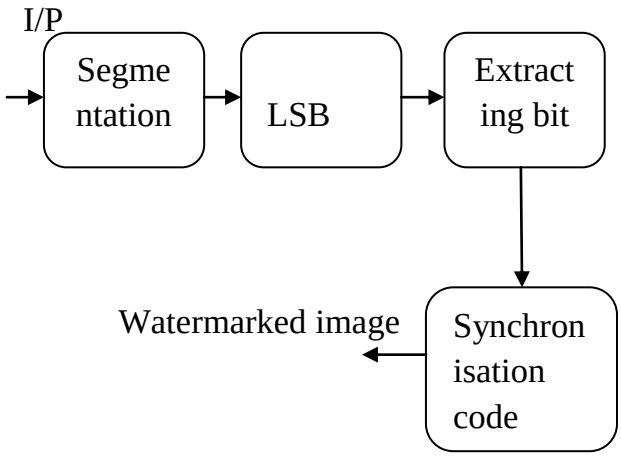

Fig. 5 Watermark Extraction

B. Voice compression

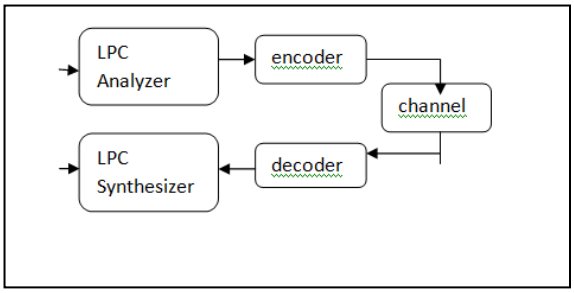

Fig.6 : Voice Compression

Voice compression may mean different things:

- Speech encoding refers to compression for transmission or storage, possibly to an unintelligible state, with decompression used prior to playback.
- Time-compressed speech refers to voice compression for immediate playback, without any decompression (so that the final speech sounds faster to the listener).
- Audio level compression refers to a sound recording effect which increases the perceived volume of a sound.

Linear predictive coding (LPC) is a tool used mostly in audio signal processing and speech processing for representing the spectral envelope of a digital signal of speech in compressed form, using the information of a linear predictive model. It is one of the most powerful speech analysis techniques, and one of the most useful methods for encoding good quality speech at a low bit rate and provides extremely accurate estimates of speech parameters. Linear predictive coding (LPC) is a tool used mostly in audio signal processing and speech processing for representing the spectral envelope of a digital signal of speech in compressed form, using the information of a linear predictive model. It is one of the most powerful speech analysis techniques, and one of the most useful methods for encoding good quality speech at a low bit rate and provides extremely accurate estimates of speech parameters.

IV. Results and Discussions

The watermarked image and compressed voice data is hide using the steganographic method in an audio file. The output is follows as Compression

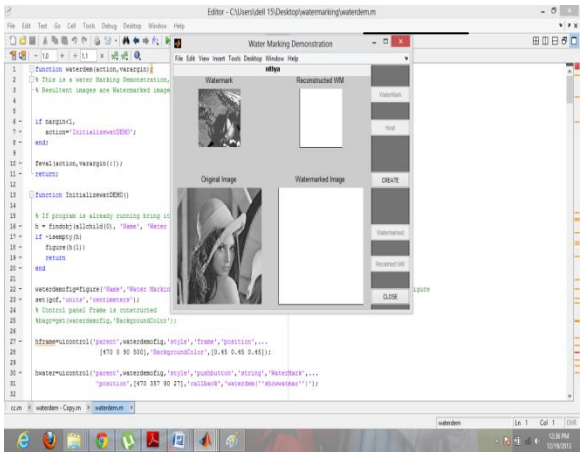

Fig. 7 Screen shot of original image

This figure represents the screen shot of the original image by selecting the host option in the output screen. The image which is to be watermark is hide inside the original image. The hiding image is more secret, so that only sender and receive an able to retrieve the secret image.

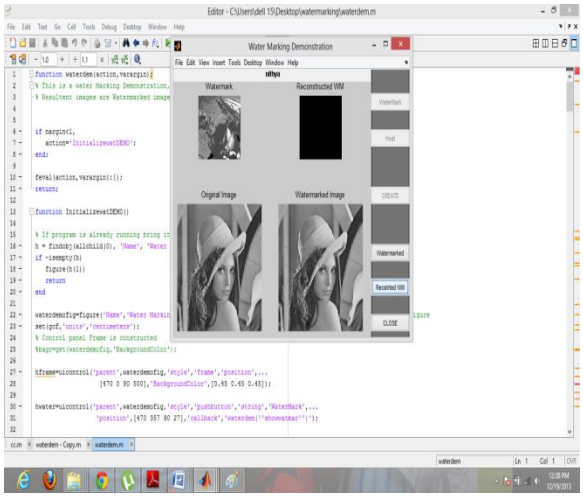

Fig. 8 Screen shot of watermarking demonstration

The figure 5.5 Represents the reconstructed image. The reconstructed image is create by selecting the reconstruct watermark option in the screen shot. After the reconstruction process the watermark image can be retrieve by the sender from the receiver.

.

Fig. 9 Screen shot ofVoice compression

The figure Represents the output of voice compression data. The voice which is to be compressed is given as an input. And by using linear predictive code algorithm the voice is compressed. So that large amount of data can be store.

V. CONCLUSIONS

Watermarking scheme based on the Least significant bit algorithm is proposed. Watermark is embedded in very low frequency mode, thus achieving good performance against various attacks. Watermark is associated with synchronization codes and thus the synchronized watermark has the ability to resist shifting and cropping. Extensive simulations over different audio signals indicate that the proposed watermarking scheme has greater robustness against common attacks than other watermarking algorithms. Experiments demonstrate that the watermarked data are indistinguishable from original one. The proposed scheme achieves very low false positive and false negative error probability rates. And similarly voice compression process is performed by using the linear predictive code algorithm. Finally the secret information like watermarking image and compressed voice is hides in an audio file by using Steganographic method. This process is used in many applications.

REFERENCES

[1] Bhat.V, Sengupta.K.I, and Das.A, (2010)"An adaptive audio watermarking based on the singular value decomposition in the wavelet domain,"Digital Signal Process., no. 20, pp. 1547–1558.

[2] Cox.I.J, and Miller.M.L,(2002) "The First 50 years of electronic watermarking,"J.Appl.SignalProcess.vol.2, pp. 126 132.

[3] N. E. Huang et al.(1998), "The empirical mode decomposition and Hilbert spectrum for nonlinear and non-stationary time series analysis," Proc. R. Soc., vol. 454, no. 1971, pp. 903–995, 1998.

[4] kiroveski.D and Malvar.S,(2001) "Robust spread-spectrum audio Watermarking," in Proc. ICASSP, pp. 1345–1348
[5] Khaldi.K,Boudraa.A.O,Turki.M, Chavel.T, and Samaali.I,(2009) "Audio encoding based on the EMD," in Proc. EUSIPCO,pp. 924.
[6] Khaldi.K and Boudraa,A.O,(2012) "On signals compression by EMD," Electron. Lett., vol. 48, no. 21, pp. 1329–1331.
[7] Khaldi.K,Alouane.M.T.H,andBoudraa.A.O (2010), "Voiced speech enhancement based on adaptive filtering of selected intrinsic mode functions,"J. Adv. in Adapt. Data Anal., vol. 2, no. 1, pp. 65–80.
[8] Swanson.M.D,Zhu.B,and Tewfik.A.H,(1998) "Robust audiowatermarking using perceptual masking,"Signal Process., vol. 66, no. 3, pp. 337–355.
[9] Wang.L,Emmanuel.S,andKankanhalli.M.S,(2010) "EMD andpsychoacoustic model based watermarkingfor audio," in Proc. IEEE ICME, pp. 1427–1432.
[10] Wu.S, Huang.J, Huang.D, andShi.Y.Q,(2005) "Efficiently self-Synchronized audio watermarking forassured audio datatransmission," *IEE*E Trans. Broadcasting,vol. 51, no. 1, pp. 69–76, Mar.