A MULTILEVEL SECURITY SCHEME USING CHAOS BASED ENCRYPTION AND STEGANOGRAPHY FOR SECURE AUDIO COMMUNICATION

Bhaskar Mondal[1], Tarni Mandal[2]

[1]Assistant Professor, Department of Computer Science and Engineering, [2]Associate Professor, Mathematics, National Institute of Technology Jamshedpur, Jharkhand, India
bhaskar.cse@nitjsr.ac.in, tmandal.math@ nitjsr.ac.in

Abstract

Steganography is the practice of encoding secret information in indiscernible way. Audio steganography is the science of hiding some secret text or audio information in a host audio. This paper contains audio stegnography using bit modification of time domain audio samples which is a well known simple technique for multimedia data embedding with potential for large payload But before applying stegnography or hiding secret audio in cover audio a chaos based encryption is performed on secret audio data in order to increase the security against steganalysis.

And the bit modification technique is also not the simple LSB (least significant bit) modification technique. It contains two approaches which make the steganalysis more difficult as compare to simple LSB technique.

First approach is with selection of bits of sample for embedding secret audio while the other approach is to use the compliment of the secret audio before hiding it in the host message. The improvised proposed approach works against steganalysis and decreases the probability of secret audio being extracted by an intruder. Chaos based encryption is used to secure secret audio in case the stegnography technique breaks.

Keywords: *Audio steganography, Chaos based encryption, steganalysis, and LSB modification technique*

----------***----------

1. INTRODUCTION

In this present era, electronic communication has become an integral and significant part of everyone's life because it is simpler and faster. With adoption of electronic communication on such a large scale, the issue of security of information has gained special significance. So to transmit information secretly it has become necessary to devise ways to transmit.

One of the concerns in the area of Information security is the concept of hidden exchange of information. Steganography is a sub-discipline of Information hiding that focuses on concealing the existence of messages. The term hiding refers to the process of making the information imperceptible or keeping the existence of the information secret. Steganography[1] is a word derived from the ancient Greek words steganos, which means covered and graphia, which in turn means writing .In the process of steganography secret message is hide in some cover file which result in the stego file.

Any steganography technique has to satisfy two basic requirements. The first requirement is perceptual transparency, i.e. cover object (object not containing any additional data) and stego object (object containing secret message) must be perceptually indiscernible. The second constraint is high data rate of the embedded data.

Steganography is often mixed up with cryptography[10]. Cryptography changes representation of secret message being transmitted while steganography hides presence of secret message.

Modern advances in computer, communication and signal processing have enabled the discovery of sophisticated techniques of steganography[9]. These advances have broadened steganography's use to include various types of medium and various forms of information. Steganography can be applied to different type of media including text, audio and video. Audio and video files are considered to be excellent carriers for the purpose of steganography due to presence of redundancy. [3][6]Audio steganography requires a secret message to be embedded within a cover audio message. Due to availability of redundancy, the cover audio message before steganography and stego message after steganography remains

same. Another secutity schemr used for secure audio communication and authentication of audio is digital water marking[2][4][5].

In Audio Steganography, the weakness of the Human Auditory System (HAS) is used to hide information in the audio. That is, while using digital images as cover files the difficulty of the human eye to distinguish colors is taken advantage of, while using digital audio one can count on the different sensitivity of the human ear when it comes to sounds of low and high intensity; usually, higher sounds are perceived better than lower ones and it is thus easier to hide data among low sounds without the human ear noticing the alteration. However audio Steganography is more challenging than Image Steganography because the human Auditory System (HAS) has more precision than Human Visual System (HVS).

To perform audio steganography successfully, the adopted technique should work against HAS. For any audio steganography technique to be implementable, it needs to satisfy three conditions; capability (high data rate), transparency and robustness (ability to withstand attacks).
The objective of this paper is to come up with a steganography technique which can satisfy the above conditions up to large extend. The technique consist of two level of security-(i) Chaos based encryption of the secret message (ii) By applying steganography using LSB technique with improved way of data hiding.

2. CHAOS BASED ENCRYPTION

The Works on chaos in cryptography were connected with encrypting messages through modulation of chaotic orbits of continuous-time dynamical systems.

Chaos is a ubiquitous phenomenon existing in deterministic nonlinear systems that exhibit extreme sensitivity to initial conditions and have random like behaviours.

Chaotic maps[8] and cryptographic algorithms have some similar properties: both are sensitive to tiny changes in initial conditions and parameters; both have random like behaviours; and cryptographic algorithms shuffle and diffuse data by rounds of encryption, while chaotic maps spread a small region of data over the entire phase space via iterations. The only difference in this regard is that encryption operations are defined on finite sets of integers while chaos is defined on real numbers.

It is natural to apply the discrete chaos[7] theory to cryptography for the following reasons. The property of sensitive dependence of orbits on initial conditions makes the nature of encryption very complicated.

Table-1. Similarity between Chaotic system and Cryptographic algorithms

Chaotic systems	Cryptographic algorithms
Phase space: set of real numbers	Phase space: finite set of integers
Iterations	rounds
Parameters	Key
Sensitivity to initial conditions and parameters	Diffusion

2.1 Chaos Algorithm

Step1. Load some speech
Step2. Shuffle 25 ms windows over a 250ms radius
Step 3. Listen back
Step 4. Set up filterbank with 64 bands from Nyquist to 50 Hz
Step 5.Scale bandwidths to be 1.5 x normal, so the effect of filtering both forward and backwards is approximately the bandwidth of a single forward pass, at least in the top 10 dB.
Step 6. Break the speech into sub bands using the filters; Pass each sub band signal back through the same filter, but backwards in time, and then flip them again
Step 7.Each row of dsub is one of the 64 band-passed signals sum up scrambled sub bands to get a full-band signal
Step 8. take a listen.
function Y = shufflewins(X,W,R)
X is a waveform, which is chopped into W-point windows which are then hamming-windowed and 50%-overlapped. These windows are shuffled over a radius of R points and overlap-added to construct Y, a version of X with approximately the same average spectrum over R point windows, but scrambled structure over a W-point timescale.
Step 9.The approach is to build an index matrix, where each row pulls in successive, non-overlapping windows from the original data.
This matrix then has as many rows as needed to get all the overlapping windows. We can then index the input with it, and simply sum up.
Step10. Upper bound on the the number of windows that overlap for eachpoint = the number of rows we'll need in our index matrix
Step11. Unravel Y, then add a zero on the end. Any indices we don't needin our index will point here, so they have no contribution to the final sum
Step12. Create one row of the final index matrix that pulls out every ovf'th window from the original matrix in its unravelled form. Pad any gaps with the zero index.
Step13. Add in the following rows, which are offset by H points, and with indices that are shifted to pick up the interleaving windows
Now, the big payoff - index by the rows, including pulling in the zeros, in such a way that it's all ready to sum up to get OLA
function output = ERBFilterBank(x, fcoefs)

This function takes a single sound vector, and returns an array of filter outputs, one channel per row.
function cfArray = ERBSpace(lowFreq, highFreq, N)
This function computes an array of N frequencies uniformly spaced between highFreq and lowFreq on an ERB scale.
Step14. Now this cover chaos encrypted audio can be embedded into host audio using modified lsb technique.
Step15. This cover audio can be extracted on other side using lsb extraction technique.
Step16. Now this audio can be decrypted using reverse chaos technique and original audio can be listened back
Step17. Plot the results

3. LSB SUBTITUTION TECHNIQUE

Out of all known techniques for steganography LSB modification is one of the simplest techniques providing high capacity. In this technique, data is being hidden in least significant bit(s) of cover samples. The weight age of LSBs in comparison with the combined weight age of whole sample is very small.

However, changing the LSBs of cover file will induce some noise but as long as the noise induced is below detectable threshold, this technique is possible and useful. Increasing the number of altered LSBs will induce more noise. If noise increases above the threshold and becomes detectable through any of the steganalysis methods, audio steganography technique fails. Using more LSBs per sample increases the capacity and decreases the transparency. On the other hand, using less LSBs per sample will decrease the capacity and increase the transparency. So, there is always a trade-off between both these parameters.

3.1 LSB Modification Encoder

In this first the host message is converted from analog to digital form through analog-to-digital converter (ADC). Then the secret message is embedded in the LSB(s) of host message samples. The modified host message which is called as stego message is passed through digital-to-analog converter (DAC) to produce analog stego message.

3.2 LSB Decoder

The decoder passes analog stego message through analog-to-digital converter to obtain samples of the stego message.

While decoding process bits from different samples are extracted to retrieve complete secret message which is embedded during encoding.

3.3 Improved LSB Technique

The simple LSB modification technique is vulnerable to steganalysis. Any intruder analyzing the samples of stego message could easily retrieve the secret message by analysing the LSB of the each sample. In this paper proposed methodology is called as improved LSB modification technique. Through experimentation it has been observed that modifying lower LSB (first or second) of a sample with secret message bit doesn't produce a detectable change or noise.

And the new technique proposed is named as Smart Bit Selection and inverted bit placement technique.

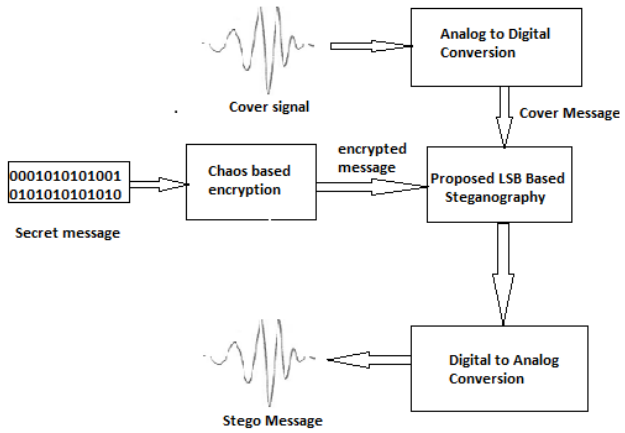

Fig. 1. Enhanced LSB embedding is being performed on the basis of as Smart Bit Selection and inverted bit placement technique.

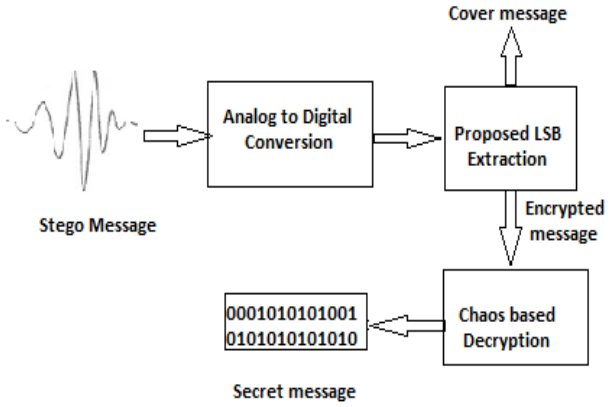

Fig. 2. Decoder which extracts the encrypted secret message

Above figure shows the proposed methodology encoder where enhanced LSB embedding is being performed on the basis of as Smart Bit Selection and inverted bit placement technique. Encryption is also being included. In case the steganography algorithm breaks, the use of chaos based encryption technique will make the encrypted secret message to be exposed to the intruder instead of the actual secret message.

Above figure shows the proposed methodology decoder which extracts the encrypted secret message. The encrypted secret message is then decrypted to obtain the actual secret message.

3.4 Smart Bit Selection and Inverted Bit Placement Technique

To confuse the intruder, same bit of a sample is never used to embed the secret message. Randomness is produced by selecting a different bit in every sample to hide secret message. First three Most Significant Bits (MSBs) of a sample will decide which bit of the sample would contain the secret message bit. Table II shows a possible Bit Selection mapping. To decide the LSB position we are checking parity of the first three MSB of each sample. Samples which produce 0 as parity, in those samples first LSB will be used to hide secret data and those samples which produce parity 1 second LSB will be used.

Table-2: A possible bit selection mapping

MSB value	Parity	LSB Position
000	0	first
001	1	second
010	1	second
011	0	first
100	1	second
101	0	first
110	0	first
111	1	second

And to further confuse intruder, instead of placing bits exact value, inverted value of the secret message will be placed in the cover message.

CONCLUSIONS

We have presented some results of a study on the conflicting requirements of encryption and data robustness in bit modification audio steganography. The study demonstrated the capability of the technique for hiding a potentially large payload of data with robustness using high bit indices for embedding. A tradeoff between noise tolerance and payload, both of which depend on higher bit indices, is needed for a reasonably imperceptible embedding of audio signal. The chaos based encryption thus providing the more stronger steganography technique in audio media. It has extended the conventional LSB modification technique for audio steganography to make it more secure against steganalysis.

REFERENCES

[1] R.J. Anderson, F. A. P. Petit colas, “On the limits of the steganography,” *IEEE Journal Selected Areas in Communications*, Vol. 16, No. 4, 1998, pp. 474-481.

[2] I. Cox, M. Miller "Electronic watermarking: the first 50 years", Proc. 4th IEEE Workshop on Multimedia Signal Processing, Cannes, France, October 2001, pp. 225-230.

[3] F. Hartung, M. Kutter "Multimedia Watermarking Techniques", *Proceedings of the IEEE*, Vol. 87, No. 7, July 1999, pp. 1709-1107.

[4] C. Yeh, C. Kuo "Digital Watermarking through Quasi m-Arrays", Proc. IEEE Workshop on Signal Processing Systems, Taipei, Taiwan, October 1999, pp. 456-461.

[5] W. Jonker, J.-P. Linnartz, "Digital Rights Management in Consumer Electronics Products", IEEE Signal Processing Magazine, Vol. 21, No. 2, pp.82-91, 2004.

[6] D. Pan, “A tutorial on MPEG/Audio compression”,IEEE Multimedia, 2(2), pp. 60-74, 1995.modifieddiscrete cosine transform of MPEG/Audio Layer III”,Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control,pp.984-989,2004.

[7] Chen G (2003) Chaotification via feedback: the discrete case. In: Chen G, Yu X (eds) Chaos Control: Theory and Applications, Spriner, Berlin Heidelberg New York, 159 – 177

[8] Chen G, Dong X (198) From Chaos to Order: Methodologies, Perspectives and Applications. World Scientific, Singapore

[9] Bhaskar Mondal, S. K. Singh “A Highly Secure Steganography Scheme For Secure Communication”, Proc International Conference of Computation and Communication Advancement (IC3A)-2013, JIS College of Engineering, January, 2013.

[10] Bhaskar Mondal and et. al. “An Improved Cryptography Scheme for Secure Image Communication”, International Journal of Computer Applications (0975 – 8887) Number 18 (ISBN: 973-93-80874-18-3) April 2013 Issue. Volume 67(18) pages 23-27.

BIOGRAPHIES

Bhaskar Mondal was born in West Bengal, India on in 1986. He received B. Tech. degree in Computer Science and Engineering from West Bengal University of Technology in 2008 and M. Tech. degree in Computer Science and Engineering from Kalyani Government Engineering College, West Bengal, India in the year of 2010. He became a member of IEEE in 2013.

He is working at National Institute of Technology, Jamshedpur as Assistant Professor in the department of Computer Science and Engineering since January 2011. His research interest includes Secret Image Sharing, Security and NLP.

Dr. Tarni Mandal was born in Bihar, India in 1956. He received Bachelor of Science (Hons.) in Statistics in 1977 followed by Master of Science in Statistics in 1980 from Bhagalpur University. He received Master of Science in Applied Mathematics from Ranchi University in 1995. He awarded PhD by Ranchi University in 2001.

He is working at National Institute of Technology, Jamshedpur as Associate Professor in the department of Mathematics. His research interest includes Secret Image S Operations Research, Security and Fractional Functional Programming Problem.