Audio Steganography using ZDT: Encryption using Indexed Based Chaotic Sequence

[1]Shivani Sharma, [2]Virendra Kumar Yadav, [3]Munesh Chandra Trivedi, [4] Avadesh Gupta
[1,2,3,4]Computer Science & Engineering
[1,2,3]ABES Engineering College, [4] IMS College
Ghaziabad, Uttar Pradesh, India
[1]+91-8800764073
shivanisharma2804@gmail.com, virendrashines@gmail.com, muneshtrivedi@gmail.com, avadesh.gupta@imsgzb.com

ABSTRACT
Steganography is an art and branch of science of hiding data secretly. Steganography can be applied to various digital mediums such as image, text, audio, video, protocols, radio waves, floppy disk, hard drive, network packet etc. Audio steganography uses audio file as the cover medium. It is more difficult to implement than image steganography as Human Visual System (HVS) is less sensitive then Human audio system. ZDT enables to achieve this task and ensures no distortion in the cover audio file. Along with steganography this approach uses cryptography for security concern. Indexed Based Chaotic Sequence is used as an encryption technique. This technique is applied on several audio files and the obtained results shows efficiency, robustness, better complexity (time and space) in terms of performance analysis matrix.

General Terms
Security.

Keywords
ZDT; echo-hiding; decay; matrix of locations; distortion

1. INTRODUCTION

1.1 Information Hiding

It is a domain which deals with hiding data in any digital medium to establish a covert channel between sender and receiver [2]. It is used in various domains like cyber security, steganography, web security etc.

1.2 Steganography

Secret communication has become the backbone while sending confidential data from sender's end to receiver's end.

To achieve this secret communication steganography is used. It is one of the sub-disciplines of information hiding which is widely used to conceal the existence of secret data [2]. Steganography enables a user to hide data such that only intended receipt can access the secret data. Since ancient times it is been used to hide data by using invisible ink, microdots, wax, bald head etc. Success of any steganography technique depends on several parameters which includes amount of distortion, complexity in terms of time and space, memory overhead, fidelity, hidden bpp (bits per pixel) etc. While applying steganography, the main focus is to have minimum distortion in the cover medium. If the distortion exceeds the limit then changes can be detected easily.

ICTCS '16, March 04-05, 2016, Udaipur, India
 ISBN 978-1-4503-3962-9/16/03…$15.00
DOI: http://dx.doi.org/10.1145/2905055.2905272

1.3 Cryptography

It is the complementary of steganography. It is used to mould the data by applying encryption technique, so that only intended user can read the data secret data [3]. The proposed technique uses combination of both i.e. steganography for data hiding and cryptography to enhance security.

1.4 Audio Steganography

Audio Steganography hide data in an audio file, data can be image, audio, video, text etc. Data should be embedded in an imperceptible manner. The success of audio steganography is established if cover and stego audio file is indistinguishable. Audio steganography techniques defined by three parameters mainly i.e. transparency, robustness and capacity.

2. RELATED WORK

2.1 Zero Distortion Technique

ZDT is an acronym of Zero Distortion Technique. It is a novel approach which hides data in any digital medium and as the name suggests, its implementation gives zero distortion in the cover image. For security purpose Indexed Based Chaotic Sequence is used for encryption. This technique does not embed data in any digital medium instead uses it as a reference only. This technique depends on matrix of locations [4].Matching of the binary bits of the cover image and secret data is carried out.

2.2 ZDT on gray images

Zero distortion technique has been applied to gray images, color images and on text file. On gray images [4] experimental results shows good performance in terms of time complexity but less amount of data is hidden in comparison to color images.

2.3 ZDT on color images

To overcome this demerit of less amount of data and to obtain better results ZDT is applied on color images [5].Large amount of data can be hidden in a color image as it contains RGB bands. Firstly data is hidden in red band, if data left then if will be hidden in green and blue band respectively.

2.4 ZDT on text file

We extend our work by applying ZDT on a text file [6], in order to improve ZDT's efficiency. For text steganography abbreviation method is used, which is used to reduce the size of the secret text. In abbreviation method a database of abbreviated word is created which is used to replace the target word with its abbreviated form also known as acronym .Table I shows abbreviated form of some sample words.

2.5 Indexed Based Chaotic Sequence

It is a non-linear technique with generates a random sequence that shows chaotic behavior [7]. Chaos means irregular pattern or behavior. Matrix of location contains the locations of the cover audio file where secret text file is being hidden [4][5][6]. It is then randomized using Indexed Based Chaotic Sequence formula using eq(1),

$$X_{n+1} = \mu * X_n * (1 - X_n) \qquad (1)$$

The value of X0 and μ is initialized at sender's end and same is used at other end [8].Value of X0 lies in the range [0, 1] and μ in between 3.57 to 4 as it shows chaotic behavior in this range [9].

2.6 Low Bit Encoding

Low Bit Encoding is a classical method of performing audio steganography in spatial domain. It is also known as LSB (Least Significant Bit) encoding. In this method least significant bit is used to hide secret data in an audio file. It is a popular and simple technique and guarantees minimum amount of distortion in the cover audio file. Using this technique a large amount of data can be hidden but is less robust to noise which affects the security. High imperceptibility is achieved while robustness and security is compromised [10][11][12].It is easy to implement but noticeable to human ear and can hide 16 kbps [13].

2.7 Echo Hiding

In this method short echo is inserted in the host signal and then data is being embedded in it. After inserting echo in the carrier channel, the stego signal and the cover signal should possess same properties. Echo signal's three parameters are manipulated for hiding data : the decay rate (for the inaudible echo) initial amplitude and the offset (delay). Up to 1ms delay the effect is indistinguishable between echo and original signal. Imperceptibility is ensured as decay rates and amplitude can be set to values according to the audible threshold of human ear [11][13-14].

3. PROPOSED WORK

Zero Distortion Technique (ZDT) is a novel approach of performing steganography in spatial domain. It has already been applied on gray images [4], color images [5], text file [6].Now we had extended our previous work by applying it on audio file. Text file of various sizes is hidden in different audio files having no distortion, as audio file is used only as a reference and data is hidden in matrix of locations. It is then randomized using Indexed Based Chaotic Sequence.

3.1 Algorithm for Implementing ZDT on Audio File at Sender's End

3.1.1 Embedding data using ZDT

embedding_using_ZDT ()

Input: Audio File (AF), Secret Text File (STF).
Output: Matrix of locations (MLOC).

1) Load Audio File (AF) as cover file.
2) Load Secret Text File (STF) i.e. data to be hidden.
3) Convert Audio File (AF) and Secret Text File (STF) into decimal format, then into binary format.
4) Match the binary bits of Audio File (AF) and Secret Text File (STF).
5) If matched then save the location into a matrix known as Matrix of Locations (MLOC) of dimension m x n.
6) Repeat step 4 and 5 till all the binary values of Secret Text File (STF) is matched.
7) Pass Matrix of Locations (MLOC) to encryption_function () for randomization.

3.1.2 Encryption using Indexed Based Chaotic Sequence

encryption_function ()

Input: Matrix of locations (MLOC).
Output: Chaotic Sequence Matrix (CSEQ).

1) Initialize the value of a in the range [0, 1] and μ between 3.57 and 4.
2) Apply formula of Indexed Based Chaotic Sequence using eq (1),

$$Xn+1 = \mu * Xn * (1-Xn) \qquad (1)$$

3) Random values of dimension Matrix of Locations (MLOC) are generated in the range of [0,1] but in row vector form.
4) Sort the values in increasing order and also compute index values.
5) Substituting values of Matrix of Locations (MLOC) in sorted index values.
6) Reshape values obtained in step 5 in m x n dimension, the resultant is Chaotic Sequence Matrix (CSEQ).This CSEQ is passed to the decryption function at receiver's end.

3.2 Algorithm for Implementing ZDT on Audio File at Receiver's End

3.2.1 Decryption using Indexed BASED Chaotic Sequence

decryption_function ()

Input: Chaotic Sequence Matrix (C_{SEQ}).
Output: Matrix of locations (M_{LOC}).

1) Random values are generated by using Eq (1), values of X_0 and μ are same as fixed at sender's end.

$$Xn+1 = \mu * Xn * (1-Xn)$$

2) Sort the values in increasing order and compute index value also.
3) Reshape values obtained in step 3 into m x n dimension, the resultant is Matrix of locations (M_{LOC}).

3.2.2Extraction of Data Using ZDT

Input: Matrix of locations (M_{LOC}), Audio File (A_F).
Output: Secret Text File (S_{TF}).

1) Audio File (AF) is converted into decimal, then into binary format

2) Location value of binary format of Audio File (AF) is matched with Matrix of locations (MLOC).

3) If location matches then put the binary value of Audio File (AF) in a new matrix of dimension m x n.

3) Repeat step 2 and 3 till all the values of Matrix of locations (MLOC) is matched.

4) Convert the obtained matrix in decimal format and then into character format.

5) Transpose the matrix obtained Secret Text File (STF).

IV. Figures and Tables

A. *Figures shows the schematic diagram of implementation of ZDT on an Audio File at Sender's and Receiver's End*

1) *Sender's End*

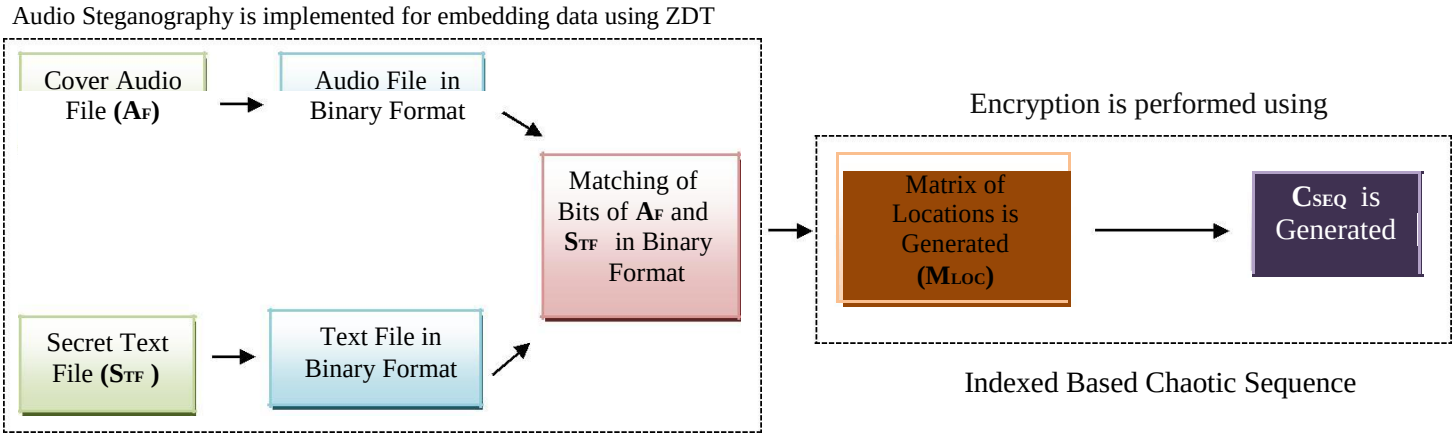

Fig. 1. Schematic Diagram for Embedding Text

2) *Receiver's End*

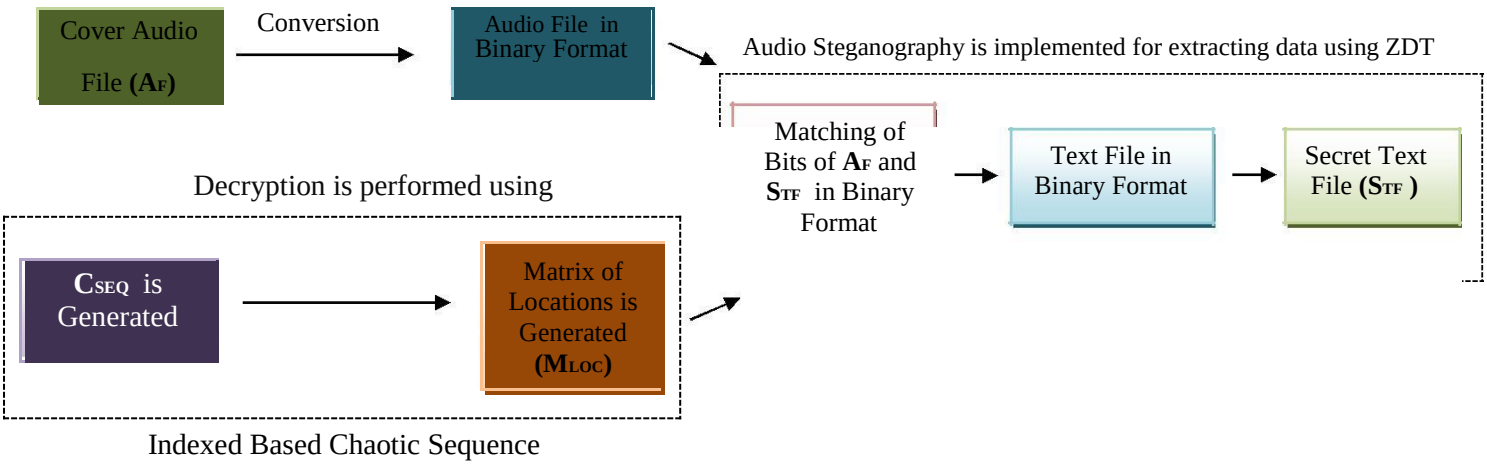

Fig. 2. Schematic Diagram For Extracting Text

B. Comparison of Zero Distortion Technique(ZDT) on Gray Images, Color Images, Text File and Audio File

TABLE I. IMPLEMENTATION OF ZERO DISTORTION TECHNIQUE (ZDT) ON GRAY IMAGES

IMAGE	ORIGINAL SIZE	FORMAT	ROWS X COLUMNS	IMAGE DIMENSION	TEXT LENGTH	STEGO-IMAGE SIZE	TIME(SECONDS)
tire	41.7 KB	tif	205 X 232	47560 X 8	11856	41.9 KB	1.008306
cameraman	52.6 KB	jpg	256 X 256	65536 X 8	200338	52.8 KB	2.684668
rice	59.4 KB	png	256 X 256	65536 X 8	22905	59.5 KB	3.064316
coins	51.5 KB	jpg	246 X 300	73800 X 8	19552	52.5 KB	4.878285
moon	114 KB	tif	537 X 358	192246 X 8	41922	117 KB	146.803198

TABLE II. IMPLEMENTATION OF ZERO DISTORTION TECHNIQUE (ZDT) ON COLOR IMAGES

IMAGE	ORIGINAL SIZE	FORMAT	ROWS X COLUMNS	IMAGE DIMENSION	TEXT LENGTH	STEGO-IMAGE SIZE	TIME(SECONDS)
football	27 KB	jpg	256 X 320 X 3	81920 X 8	86049	27 KB	105.96
autumn	44 KB	Tif	204 X 345 X3	71070 X 8	67872	44 KB	65.72
onion	44 KB	png	135 X 198 X 3	26730 X 8	25387	44 KB	12
peppers	281 KB	Png	194 X 320 X3	49859 X 8	34418	281 KB	16.68

TABLE III. IMPLEMENTATION OF ZERO DISTORTION TECHNIQUE (ZDT) ON TEXT FILE

TEXT FILE	COVER TEXT FILE SIZE	FORMAT	MESSAGE TEXT SIZE(BYTES)	STEGO TEXT FILE SIZE	TIME(SECONDS)
cover_data	2640 bytes	txt	800	2640 bytes	29806
cover_data	3564 bytes	txt	1000	3564 bytes	27602

TABLE IV. IMPLEMENTATION OF ZERO DISTORTION TECHNIQUE (ZDT) ON AUDIO FILE

Audio file	Cover Audio Size	Format	Text File Length	Text File Size	Stego Audio Size	Time (seconds)
handel	143 KB	wav	1,44,455 bytes	142 KB	143 KB	563
laughter	121 KB	wav	102904 bytes	101 KB	121 KB	325.283373
gong	83 KB	wav	81001 bytes	81 KB	234 KB	205.131562
chirp	28 KB	wav	22510 bytes	22 KB	28 KB	17.292585

4. CONCLUSION

In this paper we had extended our previous work by applying ZDT on audio file. The suggested technique is novel and powerful in comparison to existing techniques. It ensures zero distortion in the cover audio file. A large amount of data can be hidden and security is ensured by using Indexed Based Chaotic Sequence.

5. ACKNOWLEDGMENT

We would to thank our family members and Saumya for their constant support and motivation.

6. REFERENCES

[1] Westfeld A, J. Camenisch et al., "Steganography for Radio Amateurs— A DSSS Based Approach for Slow Scan Television", Springer-Verlag Berlin Heidelberg, pp. 201-215.

[2] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding", IBM Systems Journal, vol. 35, Issues 3&4, 1996, pp. 313-336.

[3] William Stalling, Cryptography and network security: Principles and Practices (4th edition), Prentice 2006, ISBN – 978-81-775-8774-6.

[4] Shivani, Yadav. V. K., Batham.S, "An Approach to Image Steganography using Strength of Indexed Based Chaotic Sequence", SSCC-2014 (Springer).

[5] Shivani , Yadav.V , Batham.S ,"Zero Distortion Technique: An approach to image steganography on color images using strength of Chaotic Sequence", accepted in ACM ICTCS 2014.

[6] Shivani , Yadav.V , Batham.S ," A Novel Approach of Bulk Data Hiding using Text Steganography",accepted in Elsevier ICRTC 2015 , in press.

[7] Aradhana Soni and Anuja Kumar Acharya , "A Novel Image Encryption Approach Using An Index Based Chaos And DNA Encoding and Its Performance Analysis" , IJCA (0975-8887) Volume 47-No. 23,June 2012.

[8] S.Batham, A. Acharya, V.K. Yadav, R.Paul."A New Video Encryption Algorithm Based on Indexed Based Chaotic Sequence".CONFLUENCE-2013, IET digital library.

[9] Anuja Kumar Acharya , "Image Encryption Using A Chaos Base Encryption Algorithm", International Conference On Commmunication,Computing and Security(ICCCS 2011) .

[10] Ashima Wadhwa, "A survey on audio steganography techniques for digital data security", International journal of advanced research in computer science and software engineering, vol. 4, issue 4, April 2014.

[11] Jayaram P, Ranganatha HR, Anupama HS, "Information hiding using audio steganography---A survey", The International journal of multimedia and its applications IJMA, vol. 3, No. 3, August 2011.

[12] Ankit Chadha, Neha Satam, Rakshak Sood, Dattatray Bade, " An efficient method for image and audio steganography using least significant bit substitution", International journal of computer applications, vol. 77, September 2013.

[13] Fatiha Djebbar, Beghdad Ayad, Karim Abed Meraim, Habib Hamam, "Comparative study of digital audio steganography techniques", springer open journal,January 2012.

[14] Masoud Nosrati, Ronak Karimi, Mehdi Harari, "Audio steganography: A survey on recent approaches", world applied programming, vol. (2), No. (3), pp. 202-205,March 2012.