International Journal of Engineering & Technology, 7 (4.19) (2018) 727-731

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Using Magic Cube and a Modified LSB for Audio Steganography

Nuha Salim Mohammed[1*], Ziyad Tariq Mustafa Al-Ta'I[2]

[1,2]Department of Computer Science
College of Science, University of Diyala,
[*]Corresponding Author E-mail: nuhasalim89@gmail.com

Abstract

This paper introduces randomness-based audio steganography with magic square and magic cube cryptography methods that are respectively based on (LSB) or Least Significant, with National institute of Standards and Technology(NIST)and enhancement of LSB audio steganography.This enhancement is based on the mathematical foundations of the magic squareby using three algorithms with any order or any size. Magic square is a branch of mathematical combinatorics. It is one of the different arrays in magic number arrangements. The new proposed technique focuses on normal magic cubes of order from (3to n). The values inside the designed magic cube are used as an index to audio cover locations. These scrambled locations (according to the keys of magic cube) in audio cover are used to LSB embed secret text message. In order to increase the security of the proposed system, the starting number, the difference value, the dimension, and the values inside the magic cube are kept as a secret key. The National institute of Standards and technology (NIST) package is successfully used to test the randomness of the magic cube's keys values. peak signal to noise ratio (PSNR) of audio stegocovers are(62.65743352-79.57336476) dB in which the size of secret text message (256-16) bits.

Keywords: *Magic cube, audio steganography, Magic Square, Least Significant Bit, steganography, NIST tests.*

1. Introduction

In this modern world, protecting the secrecy of the communication is not only the aim of the connected communication, but also the privacy of the communicators [1]. Therefore, information hiding gets its way in this growing world. Information hiding is the process of hiding amount of data called secret massage into a cover media that may be audio, video or image in an imperceptible way to build a covert channel [2]. The two main branches of information hiding are steganography and watermarking. However, many techniques are proposed for steganography [3]. Since an audio and voice are the most common way of communication, it is convenient to develop an audio hiding systems, specifically an audio steganography systems [4]. A number of steganography techniques [5] are available for embedding information in an audio. These can be broadly classified as spatial domain techniques and transform domain techniques. In the spatial domain [6], the simplest technique is to embed the data in the Least Significant Bits (LSBs) of each byte in an audio cover. Recently magic square is presented as a branch of mathematical combinatorics [7]. Therefore, this research presents an audio stenographic scheme using magic cube.

2. Related Work

The following are some studies associated to the proposed work:
In 2015, Kaziwa Saleh et.al [8] proposed aggregation method between a improved LSB and Rubik's cube principle, LSB used to data hide and Rubik's cube to data scramble. In this work, improve LSB hiding secure data in the lowest sample among two sequent samples of the cover audio. The utilized method make the secret message retrieval harder due it adds two protection levels (hiding in the lowest sample, scrambling) that produces the encrypted data imperceptible.
In (2015), Omar A. Dawood et.al, proposed a new Public-Key algorithm are improved that based on magic square and magic cube and the Diffie Hellman (key exchange protocol)[9]. Diffie-Hellman utilize to detect the magic cube's dimension with any kind of cubes(double even, single even, and odd) .The magic cube technique depend on the folding six of series magic squares with sequential or non-sequential numbers of N dimensions, which symbolized the dimensions or faces of magic cube.
In 2016, Omar A. Dawood et.al [10], a new approach has improved for constructing magic cube by utilizing the folded magic square. The proposed approach generalized the design of magic cube with any order regardless the kind of magic square whether, odd, single even, or double even order.This model is the construction of magic cube of six surfaces and any order also with variable starting value, which makes the strategy generalized.

3. Magic Cube

Magic Cubes are widely used in cryptography, steganography, watermarking, computer games, and error correcting codes, statistics and mathematical field [10].A magic cube is a cube matrix drawn as a checkerboard filled with numbers or letters in particular arrangements. It consists (N^3) boxes, called cells, filled with integers that are all different [10]. Such an array of numbers is called a magic cube if the sums of the numbers in the horizontal rows, vertical columns, and main diagonals are all equal. If the

integers in a magic cube are the consecutive numbers from 1 to n3, the cube is said to be of the n th order, and the magic number, or sum of each row, is a constant symbolized as magic constant (MC). Where MC is given in equation (1).

$$MC = \frac{n(n^3+1)}{2} \quad (1)$$

Where n is the order of the magic cube. A magic cube of order (3) is a regular magic cube, such as the example in Fig. (1). this magic cube should have MC values (row, columns, or diagonals) is equal to MC $=\frac{3(3^3+1)}{2}=\frac{84}{2}=42$ [10].

21	0	15
6	12	18
9	24	3

48	27	42
33	39	45
36	51	30

75	54	69
60	66	72
63	78	57

102	81	96
87	93	99
90	105	84

129	108	123
114	120	123
117	132	111

156	135	150
141	147	153
144	159	138

Fig. 1: Example of Magic Cube of order-3

Magic cube sum (MS) can be calculated by equation (2) [11].

$$MS = \frac{n^2(n^3+1)}{2} \quad (2)$$

The MS for magic cube of order (3) is 126, and MS for magic cube of order (4) is 520. Another method for accounting MS is by multiply MC with the dimension of the magic cube [11].The pivot element (center element) (P) for any magic cube of odd-order can be accounted as shown in equation (3) [11].

$$p = \frac{2A+D(n^2-1)}{2} \quad (3)$$

Where n= magic cube order, A=start value and D=difference value that represents the difference between successive and previous numbers. Fig. (2). shows three examples a, b and c respectively that explain the formula.

75	54	69
60	66	72
63	78	57

(a): N=3, A=54 and D=3

52	17	42
27	37	47
32	57	22

(c): N=3, A=17 and D=5

17	3	13
7	11	15
9	19	5

(c): N=3, A=3 and D=2

Fig. 2: Magic Cube forthree order by Different P Elements.

Depending on eq. (3), p elements for this example are 66, 37, and 11, respectively.
The construction of the magic Cubes includes: an odd order magic squares; a single even order magic Cubes, and double even order magic Cubes [12].

3.1. Magic Cubes as Odd-Order

Magic cube have One of the simplest three types where the degree or order (n) is of formula (2*n + 1), where (n) might be any whole number for example, (1, 2, 3, 4 etc.).This type includes and explains De la Loubère's strategy. The dimension of magic cube will be (3x3), (5x5), and (7x7) and so on[6].

3.2. Magic Cubes as DoubleEven Order

Double even order cube where the order (determine type of magic cube) or degree (n) is of the formula (4*n), for example, (4, 8, 12, 16, 32, etc.). The magic square that rank is double even can be divided by 2 and 4. The example explains the Albrecht Durer's strategy. Dimension of cube matrix will be (4x4), (8x8), and (12x12) and so on[6].

3.3. Magic Cubes as Single Even Order

Single even order cube where the order (type of magic cube) or degree (n) is of the formula 2(2n+1) = 4n+2, for example, (2, 6, 10, 14, 18, 22, etc.). The order of a single even cube can be divided by 2 but not 4. The example explains Philippe de la Hire's technique. Dimension of matrix will be (6x6), (10x10), and (14x14) and so on [12].

4. The Proposed System

4.1. Transmitter Side

The transmitter side of the proposed system is shown in Fig. (3).

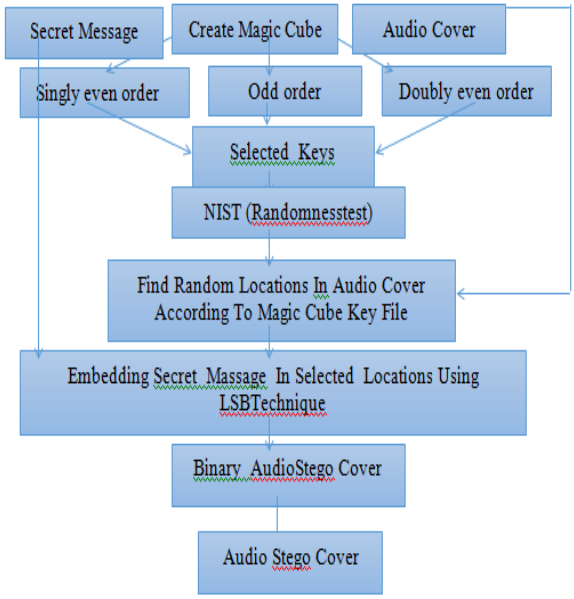

Fig. 3: Flow Chart of transmitter side of proposal

In the transmitter side of the proposed system:
First secret text message must be chosen as $(\frac{1}{8})$ of the audio cover. Second, is converting each character in secret text message to binary form, and audio cover is converted to stream of numbers. Third, create no. of cubes with any size (determines type of cube) according to size secret message with audio cover, and the selection of those keys is a sequential number from each face. Four, the random keys file is created using the magic cube by Siamese Algorithm for (odd order) [13] or Strachney Method (single-even order) [13] or Albrecht Durer's Method (Doubly-even order)[13]. Five then we test those keys by NIST package. Six, is embedding binary secret message in audio cover using LSB technique. The LSB algorithm changes the least bit in each byte of the audio cover which is selected by random keys. An Embedding algorithm isdescribed in algorithm (1).

Algorithm (1): Embedding of Secret Message Using LSB

Input: Binary secret message file, Audio cover file, Random keys file.
Output: Audio Stego Cover .

{
While not end of binary secret file
{
Take bits from Secret message sequentially
While not (end of secret message bits)
{
Take byte from audio cover file according to selected location
Convert the byte to binary form
Take one bit sequentially from secret message file
Modify least bit of audio cover byte according to secret message bit
Combine audio cover byte after modifying
Put audio cover byte in audio stego cover
} (end of while loop)
} (end of while loop)
}
Lastly, is converting the format of the stegocover that is obtained from step fourth, in order to become audio stegocover.

4.2. Receiver Side

The receiver side of the proposed system is shown in figure (4).

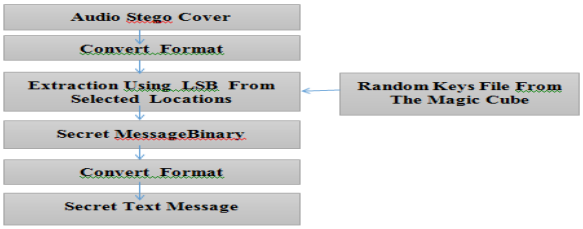

Fig. 4: Flow Chart of receiver side of proposal

Inthe receiver side of the proposed system, firstly audio stegocover is converted to stream of numbers. Secondly, an extraction of secret message is done from selected locations according to the random keys file which is previously created in transmitter side as shown in an algorithm (2).

Algorithm (2): Extraction of Secret Audio using LSB

Input: Audio stego cover file, selected locations (from random keys file)
Output: Secret text file
{
While not end of Stego cover file
{
Take a key (location) according to selected location
Convert to binary form
Take the least bit of byte from the stegocover file
Put the least bits into extracted secret message file sequentially
} (end of while loop)
}

Lastly, is converting extracted secret message into characters format in order to be read.

5. Results

Table (1) shows the creation of (60) keys from magic cube by using (10) iterations.

Table 1. Details of One Magic Cube Creation for 10 Iterations, Starting Numberand Difference value are Random

Iteration Number	Magic Cube Order	First Key	Second Key	Third Key	four key	five key	Six key
1	3	230	302	374	446	518	590
2	4	8288	8960	9632	10304	10976	11648
3	5	18256	20531	22806	25081	27356	29631
4	6	15702	18294	20886	23478	26070	28662
5	7	13608	16744	19880	23016	26152	29288
6	8	200	264	328	392	456	520
7	9	3641	4937	6233	7529	8825	10121
8	10	23106	31506	39906	48306	56706	65106
9	11	21862	32389	42916	53443	63970	74497
10	12	3829	5557	7285	9013	10741	12469

The used audio covers are shown in Fig. (5). The resulted audio stegocovers are shown in Fig. (6).

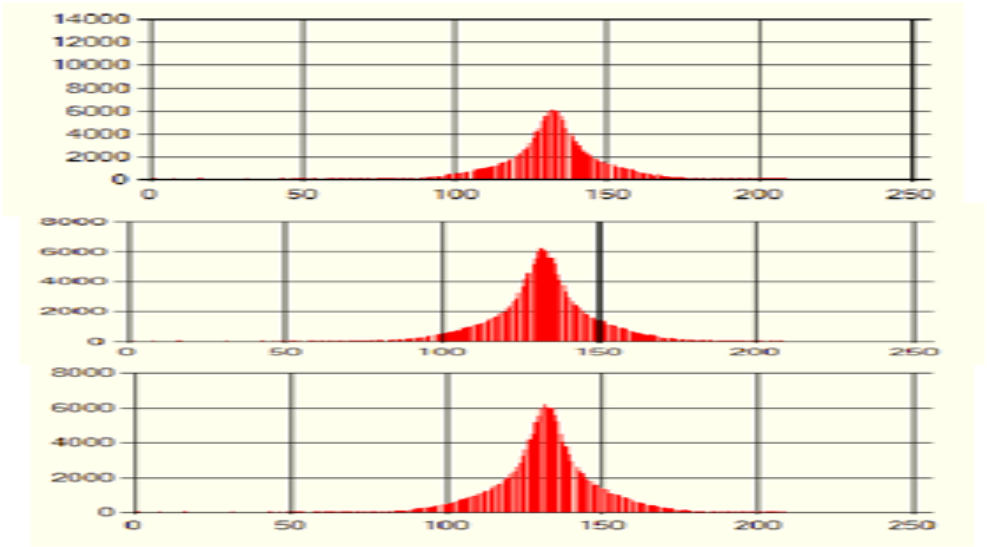

Fig.5: Samples of Audio Covers

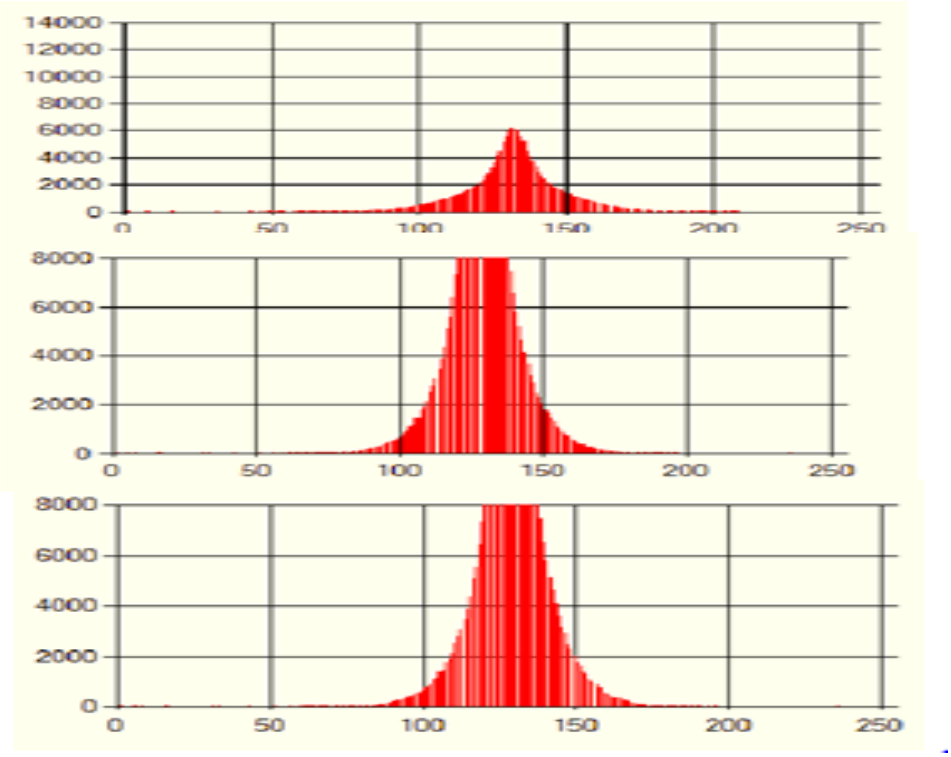

Fig.6: Samples of Audio Stego-covers

Table 2: Evaluation of Audio Stegocovers

Audio Files	Size of Secret message	16 bits	32 bits	64 bits	128 bits	256 bits
Sample1 (14 sec)	SNR	75.67398584	77.87268729	70.25886189	67.19754891	64.78408219
	PSNR	79.57336476	81.7720666	74.1582562	71.09696218	68.68351327
	MSE	0.000481899	0.00029046	0.001676745	0.003393098	0.005914816
Sample2 (23 sec)	SNR	77.82440982	75.25188979	75.66582475	69.53797467	66.3801262
	PSNR	83.01604649	80.44353577	80.85746263	74.72962406	71.57179731
	MSE	0.000292433	0.000528783	0.000480711	0.001970917	0.004078035
Sample3 (5 sec)	SNR	72.40257093	69.2606675	66.07564866	63.28885275	59.23425251
	PSNR	78.08175304	74.93983862	71.75484458	68.96812791	62.65743352
	MSE	0.001011358	0.002084954	0.004341061	0.00824646	0.01345622
Sample4 (3 sec)	SNR	71.12314422	69.120909	65.7539621	62.51552723	58.3455661
	PSNR	76.9384497	74.93620031	71.56925967	68.33079298	62.9842756
	MSE	0.001315938	0.002086702	0.004530586	0.009549949	0.01895342

The proposed method was tested for perceptibility and capacity. For testing the perceptibility, 4 stereo audio files of different sizes (bit rate = 1411Kb/s and sampling frequency = 44100 Hz). Table (2) shows four measurement factor that are used to evaluate the audio stegocovers with different sizes of secret messages.

6. Statistical Tests

In table (3).show different statistical tests that are used to measure the randomness quality of the generated keys by the magic cube.

Table 3: Statistical Tests for the Keys of Magic Cube

Test Name	Number of Tests	Number of Successes	Number of Failures	Lowest success ratio	P-Value >0.01
Block Frequency Test	181	181	0	100%	0.859684
Cumulative Sums (Forward) Test	362	362	0	100%	0.592517
FFT Test	181	181	0	100%	0.638173
Frequency Test	181	180	1	99%	0.710156
Lempel-Ziv Compression Test	181	181	0	100%	1
Linear Complexity Test	181	181	0	100%	1
Longest Runs of One's Test	181	181	0	100%	1
Non- OverlappingTemplates Test	26788	21429	5359	79%	0.003496
Overlapping Template Test	181	181	0	100%	1
Random Excursions Test	0	0	0	0%	0
Random Excursions Variant Test	0	0	0	0%	0
Rank Test	181	181	0	100%	0
Runs Test	181	178	3	98%	0.609751

Serial Test	362	357	5	98%	0.498961
Universal Statistical Test	0	0	0	0%	0

7. Steganographic Tests

7.1. Audio Conversion Test

The audio stegocover is converted from 8-bit to 16-bit audio. The hidden text message has not detected, but it could not be recovered.

7.2. Audio Processing Tests

The audio stegocover is resampled to (22.100 kHz). The hidden text message has not detected, and it could be recovered.

8. Conclusion

Magic cube is a promising field in cryptography, however in this work it is used as a promising technique in audio steganography. The keys of magic cube are used to improve the security of LSB steganography method. The statistical tests have been proved that the generated keys by the proposed magic cube are random enough to be used as a secure key. The steganographic tests showed that the proposed steganographic system is a successful secure system because the secret text message couldn't be detected or at least it couldn't be recovered if it is detected. Also use of more than an algorithm to generate the cube with the size of variable and non-specific and with the way to choose the keys more security and use the magic cube with start number and difference value are random.It is very difficult to follow and predicate these values because of theirrandomness.These are all increase the security suggested system.

References

[1] Musrrat Ali, Chang WookAhn, and Millie Pant, " Data Hiding Schemes: A survey", Embodying Intelligence in Multimedia Data Hiding, The authors; licensee Science Gate Publishing P.C. - CC BY-NC 4.0 International License DOI: 10.15579/gcsr., GCSR Vol. 5 ch.1, pp. 1-19, 2016.

[2] Ziyad Tariq Mustafa Al-Ta'i, " Development of Multilayer New Covert Audio Cryptographic Model ", International Journal of Machine Learning and Computing, Vol. 1, No. 2, June 2011.

[3] Ziyad Tariq Mustafa Al-Ta'i, " Comparison Between PSO and HPSO In Image Steganography ", International Journal of Computer Science and Information Security, Vol. 15, No. 8, August 2017.

[4] Ziyad Tariq Mustafa Al-Ta'i, " Simulation of New Covert Audio CryptographicModel", 3rd International Conference on Machine Learning and Computing(ICMLC 2011), Singapore, 26-28 February 2011.

[5] Abbas Cheddad , Joan Condell, Kevin Curran, and Paul Mc Kevitt, " Digital image steganography: Survey and analysis of current methods", Elsevier Journals- Signal Processing, Contents lists available at ScienceDirect, journal homepage: www.elsevier.com/locate/sigpro, Signal Processing 90 (727–752), 2010.

[6] Chang CC, Lin MH, and Hu YCm,"A fast and secure image hiding scheme based on LSB substitution", International Journal of Pattern Recognition and Artificial Intelligence, Volume 16, Issue 04, June 2002.

[7] Clifford A. Pickover, " The Zen of Magic Squares, Circles, and Stars:
An Exhibition of Surprising Structures across Dimensions", Princeton University Press, 400 pp., ISBN 0-691-07041-5. 2002.

[8] Saleh, K., Muhammad, M. and Ahmed, K., 2015. Using Rubik's Cube and a Modified LSB for Audio Steganography. J. Zankoi Sulaimani, 4, pp.187-194.

[9] Dawood, O.A., Rahma, A.M.S. and Hossen, A.M.J.A., 2015. New Variant of Public Key Based on Diffie-Hellman with Magic Cube of Six-Dimensions. International Journal of Computer Science and Information Security, 13(10), p.31.

[10] Dawood, O.A., Rahma, A.M.S. and Hossen, A.M.J.A., 2016. Generalized Method for Constructing Magic Cube by Folded Magic Squares. International Journal of Intelligent Systems and Applications, 8(1), p.1.

[11] Harvey D. Heinz and John R. Hendricks, " Magic Square Lexicon: Illustrated", Copyright by Harvey D. Heinz ,Published in small quantities by HDH as demand indicates, ISBN 0-9687985-0-0, Binding courtesy of Pacific Bindery Services Ltd., 2000.

[12] D.I. George, J.Sai Geetha and K.Mani, "Add-on Security Level for Public Key Cryptosystem using Magic Rectangle with Column/Row Shifting", International Journal of Computer Applications (0975 – 8887) Volume 96– No.14, pp. 38-43, June 2014.

[13] Tang, Leeming. Breaking the Magician's Code: Magic Squares. Diss. University of Leeds, School of Computing, 2004.