# An Enhancement of LSB Audio Steganography Using Magic Cube

**Nuha Salim Mohammed*, Ziyad Tariq Mustafa Al-Ta'I and Saja Salim Mohammed**

*nuhasalim89@gmail.com

Department of Computer Science – College of Science – University of Diyala

**Received: 18 September 2018 Accepted: 13 February 2019**

## Abstract

In this paper, an enhancement of LSB audio steganography is presented. This enhancement is based on the mathematical foundations of the magic cube and magic square. Magic cube is a branch of mathematical combinatorics. It is one of the different arrays in magic number arrangements. The proposed technique focuses on normal magic cubes of order (3, 4, … 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 the magic cube) in the 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 NIST package is successfully used to test the randomness of the magic cube's keys values. The PSNR values of audio stego-covers are (62.65743352-79.57336476) dB in which the size of secret text message (256-16) bits.

**Keywords:** Magic cube, Magic Square, Audio Steganography, Randomness test.

# تحسين الاخفاء بالبت الاقل اهمية باستخدام المكعب السحري

**نهى سالم محمد محمود، زياد طارق مصطفى الطائي و سجى سالم محمد محمود**

قسم علوم الحاسبات – كلية العلوم – جامعة ديالى

## الخلاصة

في هذا البحث، تم تقديم تحسين لاخفاء الصوت بالبت الأقل اهمية. هذا التحسين يعتمد على الاسس الرياضية للمكعب السحري. المكعب السحري هو فرع من الرياضيات التوافيقية. وهو واحد من المصفوفات المختلفة في ترتيبات الأرقام السحرية. تركز التقنية المقترحة على المكعبات السحرية العادية من الترتيب (3، 4، ...n). تستخدم القيم الموجودة داخل المكعب السحري المصمم كفهرس لمواقع الغطاء الصوتي. تستخدم هذه المواقع المبعثرة (وفقًا لمفاتيح المكعب السحري) في الغلاف الصوتي المستخدم لتضمين الرسالة النصية السرية. من أجل زيادة أمنية النظام المقترح ،حيث يتم الاحتفاظ برقم البداية وقيمة الفرق والأبعاد والقيم داخل المكعب السحري كمفتاح سري. تم استخدام الاختبارات العشوائية (NIST) بنجاح لاختبار عشوائية قيم مفاتيح المكعب السحري. نسبة قمة الاشارة الى الضوضاء في الغطاء الصوتي المضمن الرسالة السرية هو 62.6574-79.5733) ) dB بينما حجم الرسالة النصية ( 256-16) بت.

**الكلمات المفتاحية:** المكعب السحري، المربع السحري، الاخفاء في الصوت، الاختبارات العشوائية.

## Introduction

In this modern world, protecting the secrecy of 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 the amount of data called secret message 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 audio and voice are the most common way of communication, it is convenient to develop audio hiding systems, specifically audio steganographic systems [4]. A number of steganography techniques [5] are available for embedding information in 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 a magic square is presented as a branch of mathematical combinatorics [7]. Therefore, this paper presents an audio steganographic scheme using a magic cube.

**Related Work**

The following are some studies associated to the proposed work:

Kaziwa Saleh et.al. (2015) [8] proposed a mixture between Rubik's cube principle to scramble the audio data, and a modified LSB technique to hide the secret data. The modified LSB technique includes embedding using only irredundant bits of the binary representation of each character in the secret message and hiding in the lowest sample between two consecutive samples of the cover audio. The used technique makes the retrieval of secret message harder because it adds two levels of protection (scrambling, and hiding in the lowest sample) against the attempts of obtaining data, and makes the embedded data imperceptible.

Omar A. Dawood et. al. (2015) [9] developed a new variant of asymmetric cipher (Public Key) algorithm that based on the Diffie-Hellman key exchange protocol and the mathematical foundations of the magic square and magic cub. The proposed model uses the Diffie-Hellman algorithm just to determine the dimension of magic cube's construction. The magic cube is based on the folding six of series magic squares with sequential or with period numbers of n-dimensions that represent the faces or dimensions of the magic.

Omar A. Dawood et.al. (2016) [10] presented a new method for constructing magic cube by using the folded magic square technique. This method generalizes the design of magic cube with N order regardless the type of magic square whether odd order, singly even order or doubly even order, since it has depended mainly on the magic square construction methods, and all what the designer need is just how to builds six magic square sequentially or with constant difference value between each pair of the numbers in the square matrix

## 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 $n^3$, 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 MC, Where MC is given in equation (1).

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

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 figure (1). This magic cube should have MC values of (row, columns, or diagonals) is equal to

$$\mathbf{MC} = \frac{\mathbf{3(3^3+1)}}{\mathbf{2}} = \frac{\mathbf{84}}{\mathbf{2}} = \mathbf{42\ [10].}$$

| | | |
|---|---|---|
| 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 | 126 |
| 117 | 132 | 111 |

| | | |
|---|---|---|
| 156 | 135 | 150 |
| 141 | 147 | 153 |
| 144 | 159 | 138 |

**Figure 1:** Example of Magic Cube of order 3

The magic cube sum can be calculated by equation (2) [11].

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

The MS for a magic cube of order (3) is 126, and MS for a magic cube of order (4) is 520, and so on. Another method for calculating MS is by multiplying MC by the size of the magic cube [11].

The pivot element (center element) (P) for any magic cube of odd order can be calculated as shown in equation (3) [11].

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

Where n= cube order, A=start number and D=difference number that represents the difference between the numbers. Figure (2) shows three examples a, b, and c respectively that explain the notation.

| | | |
|---|---|---|
| 75 | 54 | 69 |
| 60 | 66 | 72 |
| 63 | 78 | 57 |

| | | |
|---|---|---|
| 52 | 17 | 42 |
| 27 | 37 | 47 |
| 32 | 57 | 22 |

| | | |
|---|---|---|
| 17 | 3 | 13 |
| 7 | 11 | 15 |
| 9 | 19 | 5 |

(a) N=3, A=54 and D=3 (b): N=3, A=17, D=5 (c): N=3, A=3 and D=2

Depending on eq. (3), p elements for this example are 66, 37, and 11, respectively.

**Figure 2:** Magic Cube of Order 3 with Different Pivot Elements

The construction of the magic Cubes includes three types: an odd order magic squares; a singly even order magic Cubes, and the doubly even order magic Cubes [12].

### 1- Magic Cubes of Odd Order

One of the three types of the magic cube where the order n is of the form (2m+1), where m may be any positive integer (1, 2, 3, etc.). This type includes De la Loubère's method. The cube size will be (3*3), (5*5), and (7*7) and so on.

### 2- Magic Cubes of Doubly Even Order

The Doubly even order magic Cubes where the order n is of the form (4m), where m may be any positive integer (1, 2, 3, etc.). The order of doubly even square can be divided by 2 and 4. This type includes Albrecht Durer's method. The cube dimension will be (4*4), (8*8), and (12*12), and so on.

### 3- Magic Cubes of Singly Even Order

Magic Cubes of singly even order Cubes where n is of the form (2 (2m+1)), where m may be any positive integer (1, 2, 3, etc.). The order of a singly even square can be divided by 2 but not 4. This type includes the Philippe de la Hire's method. The cube size will be (6*6), (10*10), and (14*14) and so on [12].

### The Proposed System

The proposed system consists of

**Transmitter Side**

The transmitter side of thproposed system is shown in figure 3.

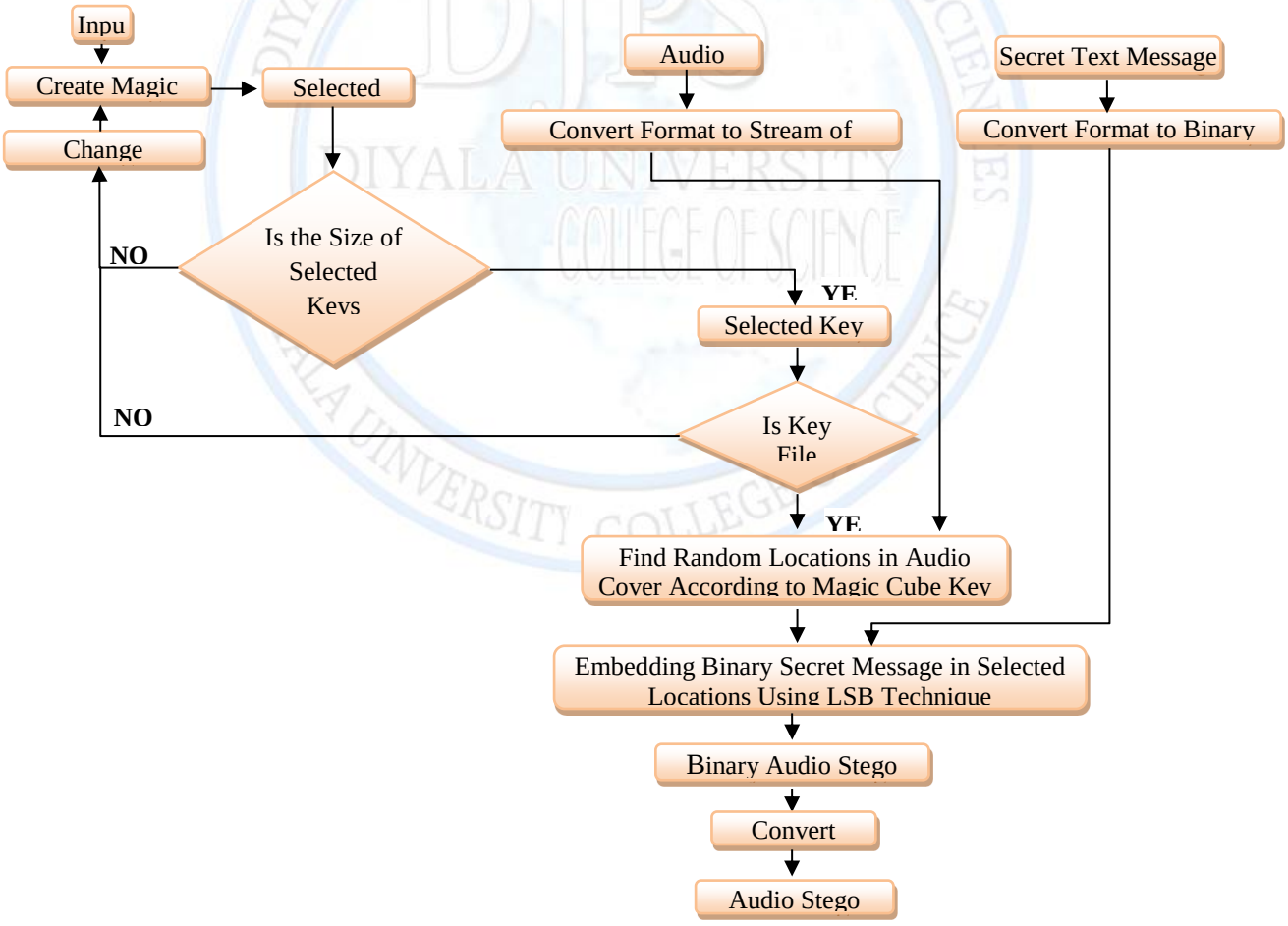


**Figure 3:** Block Diagram of the transmitter side of the proposed system

In the transmitter side of the proposed system, firstly secret text message must be chosen as $(\frac{1}{8})$ of the audio cover. Secondly, is converting each character in secret text message to binary form, and the audio cover is converted to a stream of numbers. Thirdly, the random keys file is created using the magic cube as described in algorithms (1, 2, and 3).

**Algorithm 1:** Siamese Method (odd order) Magic cube Creation

Input: Order of magic cube (n), starting value, magic difference, filling manner.
Output: Magic cube.
step1: start at the top center cell with starting value;
step2: for each broken diagonal do
step3: for each cell in diagonal do
step4: assign value to cell; if value $\in$ x then continues else start=start+1 if value $\notin$ x then start=0;
step5: increment by magic difference;
step6: move onto next diagonal cell (if not $(n-1)^{th}$ increment);
End for;
step7: move one cell down onto next broken diagonal;
End for;

**Algorithm 2:** Strachney Method (single-even order) Magic cube Creation

Input: Order of magic cube(n), starting value, magic difference, filling manner.
Output: Magic cube.
Step1: start in top center cell of top-left sub-square with starting value;
Step2: m = ¼(n-2);
Step3: for each broken diagonal in sub-square do
Step4: for each cell in broken diagonal do
Step5: assign value to cell; if value $\in$ x then continue else start=start+1 if value $\notin$ x then start=0;
Step6: assign (value + (½n) ²) to bottom-right sub-square cell;
Step7: assign (value + 2(½n) ²) to top-right sub-square cell;
Step8: assign (value + 3(½n) ²) to bottom-left sub-square cell;
Step9: increment by magic difference;
Step10: if center cell OR (1colm -(except column 1)) then
Step11: swap cell with ½ n cell below it else if ((½n-(m-2)) column ½n) then

Step12: swap (row, cow+½n) with (row+½n, col+½n) cell;
Step13: move onto next diagonal cell (if not ½n-1 increment);
End for;
Step14: move one cell down onto next broken diagonal;
End for;

**Algorithm 3:** Albrecht Durer's Method (Doubly-even order) Magic cube Creation

Input: Order of the magic cube (n), starting value, magic difference, filling manner.
Output: Magic cube.
Step1: start at top left corner cell by starting value;
Step2: for each row do
Step3: for each column do
Step4: assign a value to cell; if value $\in$ x then continue else start=start+1; if value $\notin$ x then start=0 and increment by magic difference;
Step5: if the cell is complement then assign complement value to the cell;
end for;
end for;

Fourthly, is embedding the 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 of the third step. An Embedding algorithm is described in the algorithm (4).

**Algorithm 4:** 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 a byte from an audio cover file according to a selected location
Convert the byte to binary form
Take one bit sequentially from the secret message file
Modify the least bit of audio cover byte according to the 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 stego-cover that is obtained from step fourth, in order to become audio stego-cover.

**Receiver Side**

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

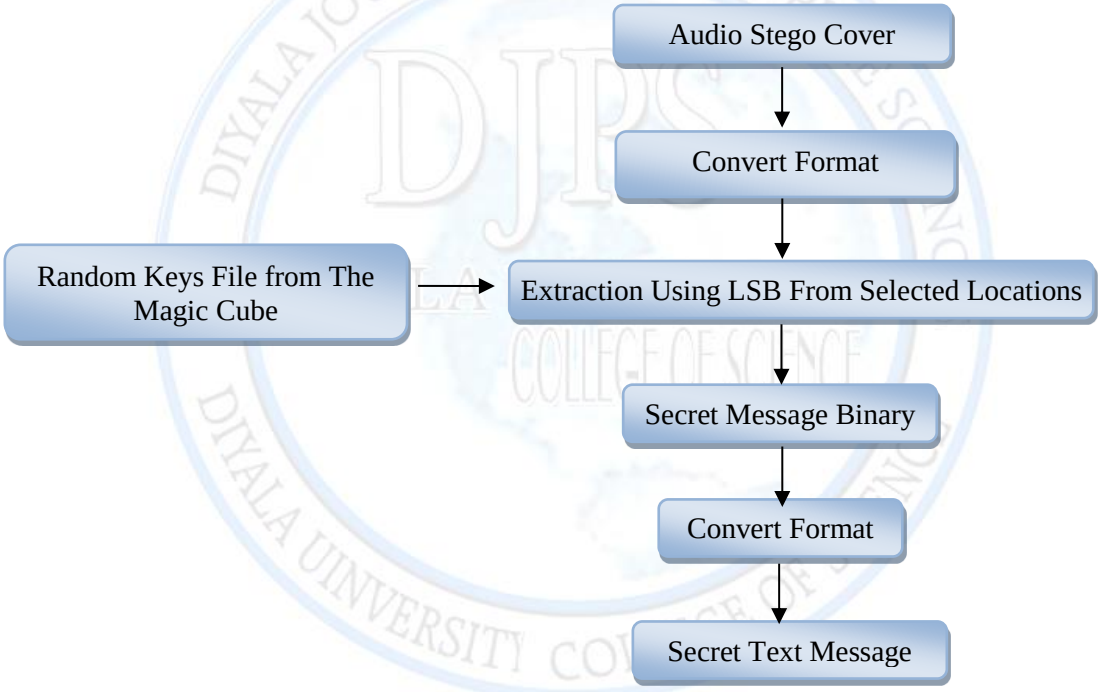


**Figure 4:** Block Diagram of the receiver side of the proposed system

In the receiver side of the proposed system, firstly audio stego-cover is converted to a stream of numbers. Secondly, an extraction of the secret message is done from selected locations according to the random keys file which is previously created in the transmitter side as shown in an algorithm 5.

**Algorithm 5:** 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 a selected location
Convert to binary form
Take the least bit of byte from the stego-cover file
Put the least bits into extracted secret message file sequentially
} (end of while loop)
}
```

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

## Results

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

**Table 1:** the details of One Magic Cube Creation for 10 Iterations

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

The used audio covers are shown in figure 5. The resulted audio stego-covers are shown in figure 6.

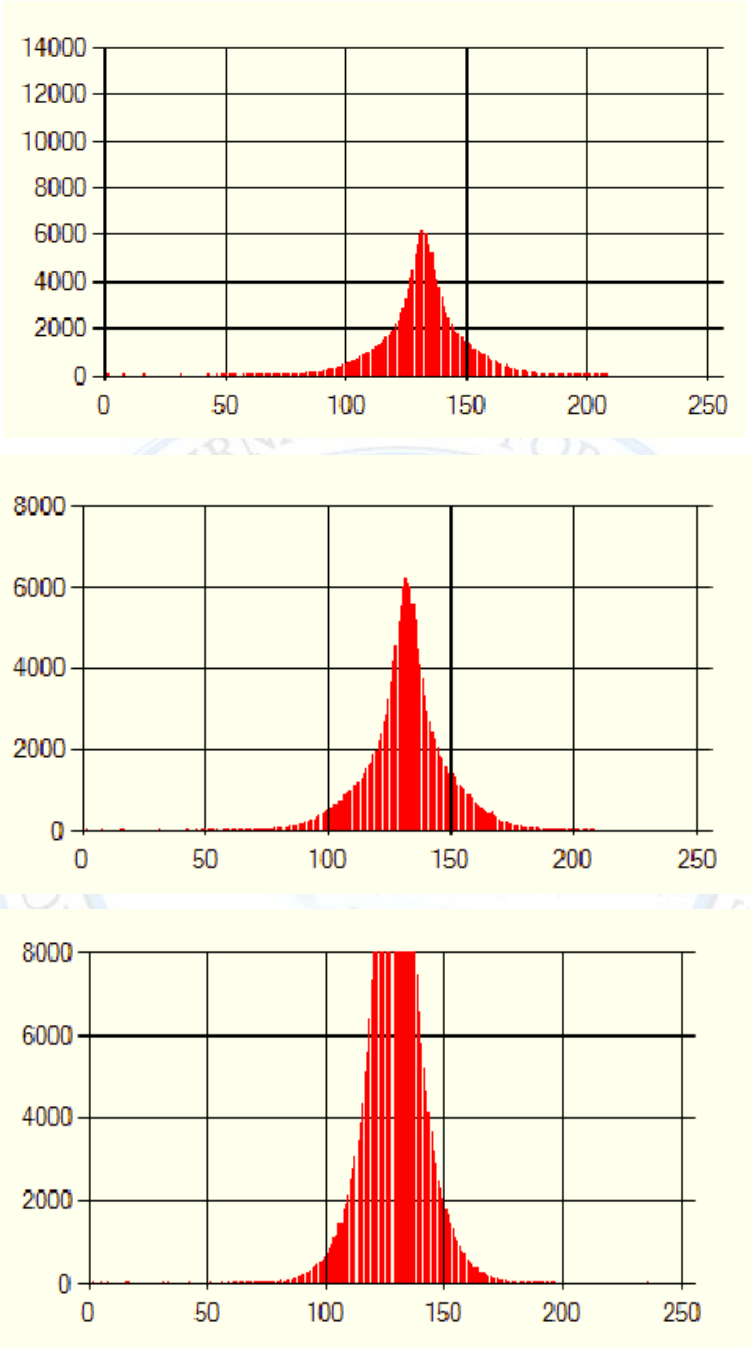


**Figure 5:** Samples of Audio Covers

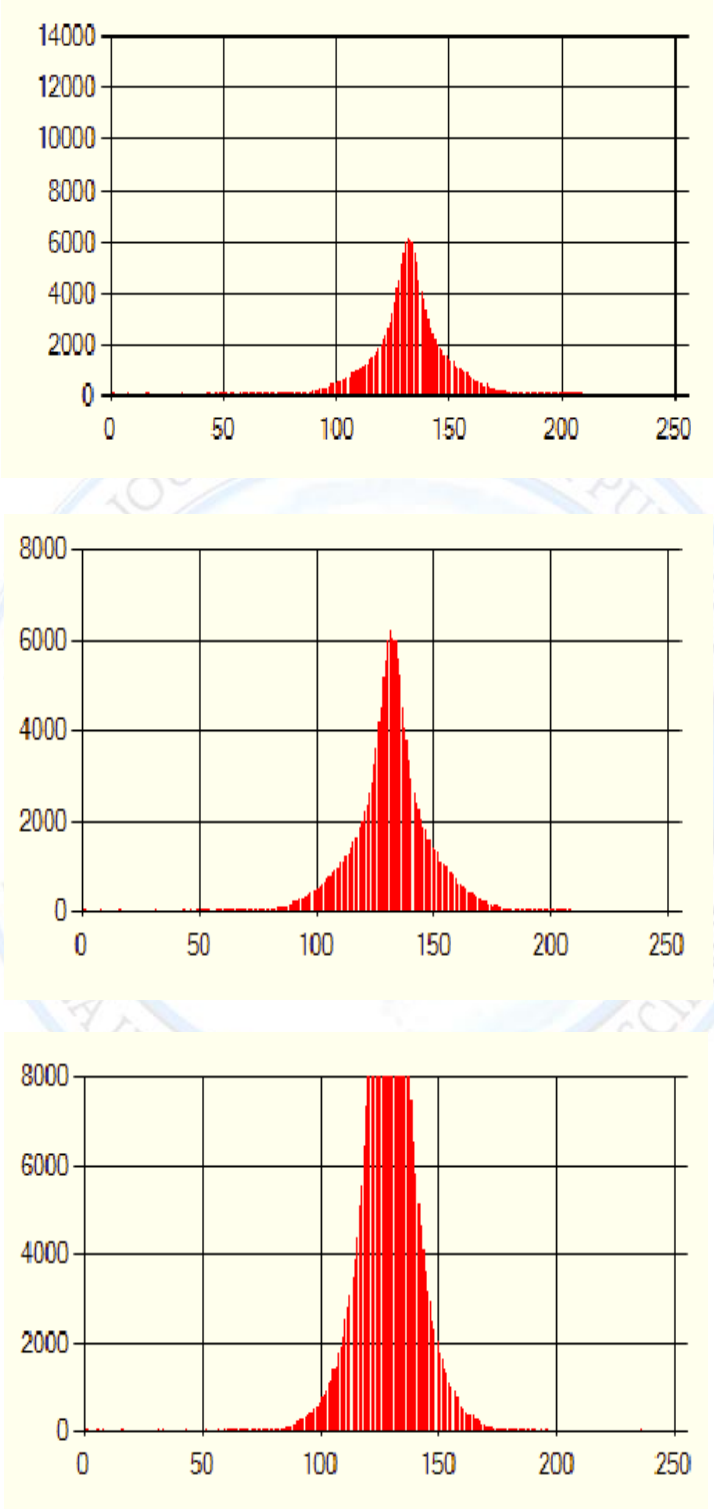


**Figure 6:** Samples of Audio Stegocovers

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 factors that are used to evaluate the audio stego-covers with different sizes of secret messages.

**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 |

## Statistical Tests

Table 3 shows different statistical tests that are used to measure the randomness quality of the generated keys by the magic cube.

**Table 3:** The Statistical Tests on the Keys of the 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- Overlapping Templates 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 |

**Steganographic Tests**

**1- Audio Conversion Test**

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

**2- Audio Processing Tests**

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

## 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 the 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 secure keys. 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.

## References

1. Z. T. M. Al-Ta'I, International Journal of Machine Learning and Computing, June, 1(2),1(2011).
2. M. Ali, C. W. Ahn, M. Pant, Data Hiding Schemes: A survey, Embodying Intelligence in Multimedia Data Hiding, vol5, ch1, (Science Gate Publishing, Greece,2016) pp.1-19.
3. Z. T. M. Al-Ta'I, E. R Mohammad, International Journal of Computer Science and Information Security ,15(8), 2017
4. Z. T. M. Al-Ta'I, Simulation of New Covert Audio Cryptographic Model, In: International Conference on Machine Learning and Computing (ICMLC 2011), 26-28 February (2011), Singapore, pp.132-136
5. A. Cheddad, J. Condell K. Curran, P. Mc. Kevitt , Elsevier Journal of Signal Processing, 90(3), 727-752(2010).

**6.** C. C. Chang, M. H. Lin,Y. C. Hu, International Journal of Pattern Recognition and Artificial Intelligence, June, 16(4), 399-416(2002).

**7.** C. A.Pickover, The Zen of Magic Squares, Circles, and Stars: An Exhibition of Surprising Structures across Dimensions, (Princeton University Press, Princeton, New Jersey, 2002), pp. 1-65.

**8.** K. Saleh, M. Muhammad, K. Ahmed, Journal of Zankoi Sulaimani, 4, 187-194(2015).

**9.** O. A. Dawood, A. M. S. Rahma, A. M. J. A. Hossen, International Journal of Computer Science and Information Security,13( 10), 34-37(2015).

**10.** O. A. Dawood, A. M. S. Rahma, A. M. J. A. Hossen, International Journal of Intelligent Systems and Applications, 8(1),1(2016).

**11.** H. D. Heinz, J. R. Hendricks, Magic square lexicon: Illustrated, (HDH, Canada, 2000), pp.7-11.

**12.** D. I George, J. Sai Geetha, K.Mani ,International Journal of Computer Applications June, 96(14),38-43(2014).