Journal of Engineering and Applied Sciences 12 (8): 2164-2169, 2017
ISSN: 1816-949X

Triangular Coordinate Extraction (TCE) for Hybrid Cubes

Muhammad Faheem Mushtaq, Sapiee Jamel and Mustafa Mat Deris
Faculty of Computer Science and Information Technology,
University Tun Hussein Onn Malaysia, 86400 Johor, Malaysia

Abstract: Hybrid Cube (HC) is generated from a combination and permutation of integers. All possible combinations of hybrid cube layers are the source for the generation of encryption and decryption keys in the non-binary block cipher. This study extends the hybrid cube encryption algorithm (HiSea) and analyzing their security issues by increasing the complexity in mathematical approaches. Based on existing HC technique, this research proposed a new coordinate extraction technique for data security. For this purpose, four key matrices generated from HiSea of order 4. Each key matrix generates one row of a new matrix based on our proposed Triangular Coordinate Extraction (TCE) technique. The proposed technique undergoes the following phases; selecting the surface of HC, intersection of diagonals, TCE for Hybrid Cube surface (HCs) stages and extraction of coordinates during the rotation of HCs. The rotation has been needed in the development of ciphertext by rotating the plaintext and to obtaining the original plaintext from ciphertext.

Key words: Hybrid cube, TCE technique, diagonals, hybrid cube surface, HiSea

INTRODUCTION

Cryptography plays an important role in information security where it used to store sensitive information and transmit it across undefined networks like the internet where information are no longer protected by physical boundaries. Hence, secure communication is a fundamental requirement for all transactions. Recently, the encryption technology comprises of different mathematical processes for the development of complex algorithms. These algorithms were conventionally designed to secure discretion of military and diplomatic communications. Selection of right algorithms or techniques results in a highly immune cryptographic components to cryptanalysis.

The magic cube is 3-Dimensional (3D) coordinates consisting of six faces are used to propose encryption and decryption techniques. The construction of magic cubes using the concept of a magic square and two orthogonal Latin squares is described by Trenkler (2000, 2005). Furthermore, the magic cube based technique used to achieved information hiding in grayscale image proposed by Wu *et al.* (2016). This technique translates the sensitive information into the spatial coordinates and changed the LSBs of the cover image regarding these coordinates.

Adoption of scientific mathematical properties such as magic cube transformation and natural chaotic sequence in an image encryption algorithm is considered by Shen *et al.* (2005) and Zhang *et al.* (2005). The concept of confusion and diffusion in these encryption algorithms are used to enhance the complexity of overall algorithm. Moreover, hybrid cubes are generated on the basis of Latin squares, Orthogonal Latin Squares, Magic Squares and Magic Cubes which displayed good diffusive characteristics (Jamel *et al.*, 2010). Their research opens up a new way for creating a key scheduling algorithm based on permutation and combination of integer numbers.

The hybrid cube encryption algorithm (HiSea) was proposed by Jamel *et al.* (2011). HiSea is a non binary block cipher because the message, ciphertext, encryption and decryption key and internal operations of the cipher are based on integer numbers (Jamel *et al.*, 2011). The limitation of HiSea is that the encryption and decryption process is represented in 2-Dimensional (2D) so, a cryptanalyst addresses the original message easily with minimum number of possibilities. Furthermore, Rajavel are generating cubical key and encryption algorithm using cube rotation and HC generation from magic cubes (Rajavel and Shantharajah, 2012a). Later on, they enhance their previous work, by proposing an improved key generation and encryption algorithm (Rajavel and Shantharajah, 2012b). Here, hybridization is based on rotation and generation of HC by randomly shuffled cube. Hybridization was performed with magic cubes which are very time consuming process and need high computation cost. The limitations of HiSea and research by Rajavel are handled by the proposed technique in this research.

Corresponding Author: Muhammad Faheem Mushtaq, Faculty of Computer Science and Information Technology, University Tun Hussein Onn Malaysia, 86400 Johor, Malaysia

In this context, this research is trying to introduce a new technique using mathematical approaches which divert the high security in overall implementation during rotation of HC. To achieve highly encrypting capacity and better computational performance, a new cube structure based on the rotation of HCs of order 4 is proposed where the layer entries are between a set of integers 1-4096. This work illustrated a new TCE technique that is used to extract coordinates from hybrid cube during rotation phase. By dividing the HC like triangular results make it easy to extract coordinates during rotation.

Rotation cube initially used the four key matrices that are generated from hybrid cube encryption algorithm (Jamel, 2012). In the next step, the generated cube from the key matrix is rotated by using the HCs stages. This HCs rotation can increase the probability which enhances the ability of HC to resist against chosen plaintext attack and known plaintext attack. It also increases the difficulty to find plaintext from cryptanalyst and even the single rotation of HCs can reflect all stages of HC. Experimental results show that the proposed technique is suitable for evaluating the non-binary block cipher.

MATERIALS AND METHODS

Preliminaries: We use the following definitions which are used to describe the construction of the TCE technique for hybrid cube.

Hybrid cube: HC is constructed by using inner matrix multiplication of two magic cubes proposed by Jamel *et al.* (2011). The purpose of hybrid cube encryption algorithm used at sender and receiver computer for encrypting the plaintext and also decrypting the ciphertext, respectively. Let us consider HC layers of order 4 {1, 2, 3, 4}: Cube 1 is based on inner matrix multiplication of layer with different coordinates {x =1, 2, 3, 4} of Magic Cube 1 (MC1) and layer {x = 4, 3, 2, 1} of Magic Cube 2 (MC2) and so on. Hybrid Cube 1 (HC1) is formed from above mention Cubes. Hybrid Cube 2 (HC2) is formed by magic Cube 2 and 3 and so on.

Definition 1: Let x be inner matrix multiplication of magic cubes. HC of order 4 is defined by $H_{i,j}$, i in {1, 2, …, n} and j in {1, 2, 3, 4} defined as:

$$H_{i,j} = MC_{i,j} \times MC_{i+1j} \text{ j in } \{4, 3, 2, 1\}$$

where, $MC_{i,j}$ is jth layer in ith magic cubes. The 880 MC are used to generate 879 HC. These hybrid cubes using inner matrix multiplications in each layer between the two adjacent cubes. The entries of a generated HC is belong to the set {1, 2, …, 4096}.

Coordinate geometry: Coordinate geometry is one of the most important ideas of mathematics. It provides a link between geometry and algebra using the graph of lines and curves. This connection allows geometric problems to be explained algebraically. The rectangular system is known as coordinate system used to uniquely determine a point in 2D and 3D spaces by its distance from the origin of the coordinate system. Geometry problems can be solved using the concepts of line and circle in the euclidean plane (Robbin, 2005).

Rotation plane: The 2D rotation is specified around an origin, general rotation around the fixed points and 3D rotation it is specified around a general axis by Aguilera and Aguila (2004). This axis is represented by the supporting line of the directed segment. The rotation in 3D space is essentially considered as rotations parallel to a 2D plane instead of the rotations around an axis. Rotation plane is considered as the set of all rotated points for a specified rotation matrix lies in a single plane.

Proposed technique

TCE technique for HC: The constructions of new TCE technique for HC which can be complement the existing HC encryption algorithm. TCE technique can extract of 2D coordinates during Hybrid Cube Surface (HCs) rotation. This proposed technique consists of three main steps: the first step in the development of TCE technique is the selection of HC surface which is used for the rotation. The rotation of HCs is the main element of construction of encryption and decryption key in the block cipher. The second step calculates the center of selected HCs by using primary and secondary diagonals. The intersection of diagonals divides the HCs into four different stages. The final step includes the extraction of coordinates using triangular stages during counterclockwise rotation of HCs. This technique increases the complexity by rotating HCs and it is computationally secure the encryption and decryption process of HC. More details of these steps are illustrated as follows.

Select a surface of HC: The overall design of 2D rotations of HCs is divided into six faces. At first phase, the 2D rotation of HCs using first face (f = 1) is considered. Later on we will consider remaining five faces of HC. TCE technique for HCs at face 1 is divided into four stages by intersecting two diagonal lines passing through the center of the circle are presented in Fig. 1.

Calculate the center using primary diagonal and secondary diagonal: By using the intersection of primary and secondary diagonal coordinates $HCs_{i,j}$, the center of

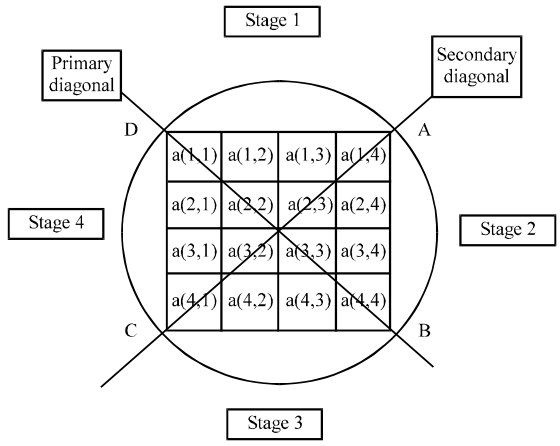

Fig. 1: TCE technique for HCs

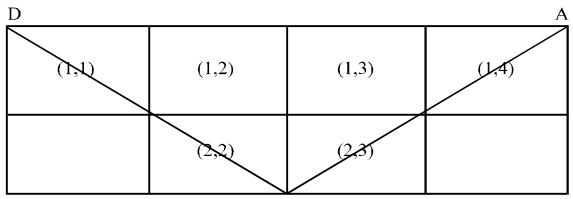

Fig. 2: Coordinates of stage 1 from point D to A in HCs

HCs is calculated. These diagonals are defined below. Moreover, some proposed definitions are also presented.

Primary diagonal: For any square matrix $A = [a_{ij}]_{nxn}$ with n rows and n columns is a primary diagonal where the collection of entries is i = j. The elements of order 4 matrix are a(1,1), a(2,2), a(3,3) and a(4,4).

Secondary diagonal: A square matrix $A = [a_{ij}]_{nxn}$ with n rows and n columns is a secondary diagonal where the collection of entries $a_{i, n-i+1}$ for all $I \in \{1,\ldots,n\}$. The elements of order 4 matrix are a(1,4), a(2,3), a(3,2) and a(3,4).

Definition 2: Let a Hcs be a 4×4 matrix, then we find the symmetric coordinates (i, j) and (j, i) of matrix as follow:

$$= \begin{bmatrix} \{(1,2)(2,1)\}, \{(1,3)(3,1)\}, \{(1,4)(4,1)\} \\ \{(2,3)(3,2)\} \{(3,4)(4,3)\} \{((4,2)(2,4)\} \end{bmatrix}$$

taking 1st mean of each symmetric coordinates:

$$= \left[\{3\}, \{4\}, \{5\}, \{5\}, \{7\}, \{6\}\right]$$

then taking 2nd mean of all terms:

$$\text{Mean: } \frac{3+4+5+5+7+6}{6} = 5 \quad (1)$$

Definition 3: Let the HCs be an order 4 matrix, then we define the properties of diagonal cells in hybrid cube, when:

- Primary diagonal of HCs matrix is the collection of entries HCs(i, j) where i = j
- Secondary diagonal of hybrid cube surface matrix is collection of entries HCs(i, j) where i+j = 5 by using Definition 2

When the value of the diagonals HCs(i, j) is i = j and i+j = 5 then the value of coordinates of particular cell is 1/2HCs(i, j). According to the Definition 3 in case of intersection of diagonals the coordinates satisfy the reflexive and symmetric properties as follows:

$$\{(1,1), (2,2), (3,3), (4,4), (1,4), (2,3), (3,2), (4,1)\}$$

TCE for HCs stages: Extracting the value during rotation of HCs in all four stages by using Eq. 2-5 based on properties discusses in Definition 3. The returned value is taken from the intersection of selected rows and columns.

HCs stage 1: The triangular stage 1 of HCs is the passage from D to A specific to the selected problem as presented in Fig. 2. The formula used for finding the value of coordinates at stage 1 during rotation of HCs is as follows:

$$\sum_{i=0}^{1} \sum_{j=1+i}^{4-i} (i+1, j) = \sum_{i=0} \left(\sum_{j=1}^{4} (i+1, j)\right) + \sum_{i=1} \left(\sum_{j=2}^{3} (i+1, j)\right) \quad (2)$$

If and only if (iff) the triangular coordinates satisfy Definition 3.

HCs stage 2: The triangular stage 2 of HCs is the passage from A to B specific to the selected problem as presented in Fig. 3. The formula used for finding the value of coordinates at stage 2 during rotation of HCs as presented:

$$\sum_{j=0}^{1} \sum_{i=1+j}^{4-j} (i, 4-j) = \sum_{j=0} \left(\sum_{i=1}^{4} (i, 4-j)\right) + \sum_{j=1} \left(\sum_{i=2}^{3} (i, 4-j)\right) \quad (3)$$

If triangular coordinates satisfy Definition 3.

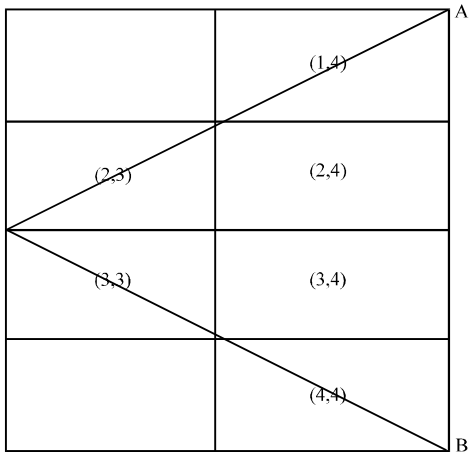

Fig. 3: Coordinates of stage 2 from point A to B in HCs

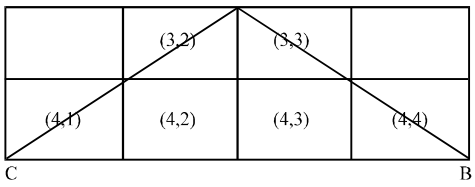

Fig. 4: Coordinates of stage 3 from point B to C in HCs

HCs stage 3: The triangular stage 3 of HCs is the passage from C to B specific to the selected problem as presented in Fig. 4. The formula used for finding the value of coordinates at stage 3 during rotation of HCs is written as:

$$\sum_{i=0}^{1}\sum_{j=1+i}^{4-i}(4\text{-}i, j) = \sum_{i=0}(\sum_{j=1}^{4}(4\text{-}i, j)) + \sum_{i=1}(\sum_{j=2}^{3}(4\text{-}i, j)) \quad (4)$$

if triangular coordinates satisfy Definition 3.

HCs stage 4: The triangular stage 4 of HCs is the passage from D to C specific to the selected problem as presented in Fig. 5. The formula used for finding the value of coordinates at stage 3 during rotation of HCs is illustrated as:

$$\sum_{j=0}^{1}\sum_{i=1+j}^{4-j}(i, j+1) = \sum_{j=0}(\sum_{i=1}^{4}(i, j+1)) + \sum_{j=1}(\sum_{i-2}^{3}(i, j+1)) \quad (5)$$

If triangular coordinates satisfy Definition 3. The rotation of HCs is studied and Triangular coordinate extraction technique analyzed well to promote the performance of the encryption techniques and methods, moreover to ensure the security proceedings.

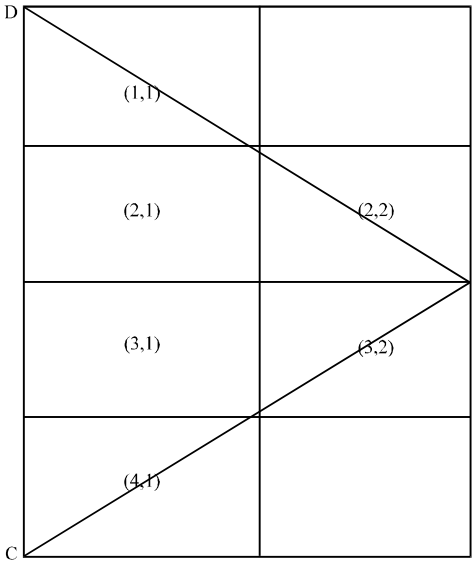

Fig. 5: Coordinates of stage 4 from point C to D in HCs

RESULTS AND DISCUSSION

TCE technique is implemented in HC encryption algorithm. This tends to increase the complexity of HC. In this study, firstly four key matrices (order 4) generated from hybrid cube encryption algorithm the steps in TCE technique are demonstrated. Secondly, the rotation cube is rotated by using TCE technique stages. The rotation matrix provides an invertible matrix that is used in the development of encryption and decryption key in the block cipher. Moreover, some experimental results are presented to prove the validity of the proposed technique.

Selection of four key matrices (A-D) are required to generate one Rotation Cube (RC) matrix based on TCE technique. These key matrices are presented as:

$$A=\begin{bmatrix} 9 & 1620 & 3180 & 768 \\ 486 & 3844 & 1521 & 22 \\ 1786 & 9 & 676 & 3402 \\ 3584 & 580 & 60 & 1353 \end{bmatrix} \quad B=\begin{bmatrix} 682 & 2601 & 1764 & 90 \\ 128 & 1620 & 3180 & 425 \\ 2793 & 580 & 60 & 1920 \\ 1462 & 196 & 529 & 2950 \end{bmatrix}$$

$$C=\begin{bmatrix} 1920 & 52 & 588 & 2793 \\ 3402 & 361 & 100 & 1786 \\ 22 & 2116 & 3025 & 486 \\ 425 & 3172 & 1628 & 128 \end{bmatrix} \quad D=\begin{bmatrix} 2950 & 900 & 49 & 1462 \\ 1353 & 52 & 588 & 3584 \\ 768 & 3172 & 1628 & 9 \\ 90 & 1225 & 3364 & 682 \end{bmatrix}$$

Step 1: The key matrix A is used for the construction of first row in RC:

$$A = \begin{bmatrix} 9 & 1620 & 3180 & 768 \\ 486 & 3844 & 1521 & 22 \\ 1786 & 9 & 676 & 3402 \\ 3584 & 580 & 60 & 1353 \end{bmatrix} = [7871\ 5995\ 3451\ 5583]$$

Step 2: The key matrix B is used for the construction second row in RC:

$$B = \begin{bmatrix} 682 & 2601 & 1764 & 90 \\ 128 & 1620 & 3180 & 425 \\ 2793 & 580 & 60 & 1920 \\ 1462 & 196 & 529 & 2950 \end{bmatrix} = [7151\ 5093\ 3251\ 5485]$$

Step 3: The key matrix C is used for third rows of RC:

$$C = \begin{bmatrix} 1920 & 52 & 588 & 2793 \\ 3402 & 361 & 100 & 1786 \\ 22 & 2116 & 3025 & 486 \\ 425 & 3172 & 1628 & 128 \end{bmatrix} = [3227\ 5835\ 7647\ 5295]$$

Step 4: Finally, key matrix D is used for fourth rows of RC:

$$D = \begin{bmatrix} 2950 & 900 & 49 & 1462 \\ 1353 & 52 & 588 & 3584 \\ 768 & 3172 & 1628 & 9 \\ 90 & 1225 & 3364 & 682 \end{bmatrix} = [3475\ 5253\ 7375\ 5773]$$

Four key matrices are required to generate one matrix based on TCE technique. The RC of order 4 as follows:

$$RC = \begin{bmatrix} 7871 & 5995 & 3451 & 5583 \\ 7151 & 5093 & 3251 & 5485 \\ 3227 & 5835 & 7647 & 5295 \\ 3475 & 5253 & 7375 & 5773 \end{bmatrix}$$

The result of all four steps will produce a matrix order 4 which is invertible. Key matrix RC for rotation phases is considered and TCE for HCs stages are applied. The first rotation of RC is:

$$R1 = \begin{bmatrix} 5583 & 5485 & 5295 & 5773 \\ 3451 & 3251 & 7647 & 7375 \\ 5995 & 5093 & 5835 & 5253 \\ 7871 & 7151 & 3227 & 3475 \end{bmatrix}$$

The second rotation of RC is:

$$R2 = \begin{bmatrix} 5773 & 7375 & 5253 & 3475 \\ 5295 & 7647 & 5835 & 3227 \\ 5485 & 3251 & 5093 & 7151 \\ 5583 & 3451 & 5995 & 7871 \end{bmatrix}$$

The third rotation of RC is:

$$R3 = \begin{bmatrix} 5773 & 7375 & 5253 & 3475 \\ 5295 & 7647 & 5835 & 3227 \\ 5485 & 3251 & 5093 & 7151 \\ 5583 & 3451 & 5995 & 7871 \end{bmatrix}$$

The matrix (R3) after rotating by using the concept of TCE technique for HCs is tested which is also invertible.

Entropy: To estimate the strength of overall implementation of TCE technique, entropy test is used. In this test, entropy for RC matrix is calculated using MATLAB function CalculateEnt(). The entropy test for RC is 0.9862 which is closer to 1 rather than 0. Hence, it is 98.62% random which shows the HC blocks consist of 16 decimal numbers that are almost random.

Brute force attack: The encryption keys are representing in the matrix of order 4 of integer numbers and it contains each entry lies from 1 to 4096 or within 2^{12} bits is an integer number. The key space for encryption and decryption keys are $2^{12}\times2^{12}\times\ldots\times2^{12}=(2^{12})^{16}=2^{512}$ or approximately $10^{51.2}\times10^{51.2}\times10^{51.2}=(10^{3})^{51.2}=10^{153.6}$ keys. TCE is computationally secure and brute force attack on this large key space will make time-consuming and difficult.

This technique of creating new (4×4) matrix layer is used in the design of encryption and decryption key. The rotation of HCs make it difficult for predicting keys and it provides a large key space used in the cipher. Moreover, the number of keys used in the encryption process that can be determines the practical feasibility of conducting a brute-force key. This new combination of layer entries by using TCE technique can be used to add complexity in the overall design of encryption algorithms. Hence, the extraction and rotation of HCs are used as a guide for the development of TCE technique for HC.

CONCLUSION

In this study, the TCE technique for HCs of 4×4 matrices is presented which can be used to extract the coordinates during rotation of HCs. In this technique, the

HiSea encryption algorithm to increase their security parameters is analyzed and introducing the concept of coordinate extraction. The process of generating TCE technique for HCs is the intersection of two diagonal lines which provides the four triangular stages. These stages are helpful for the extraction of coordinates during the rotation of HCs. Rotation of HCs which create different patterns and TCE technique involving to extracting coordinated during rotation is used to ensure that protection of message from cryptanalysts. Security is the primary concern in the design of TCE for HC. This research can be further analyzed in the future by extraction of coordinates using 3 dimensional HC.

ACKNOWLEDGEMENTS

Resaerchers would like to thank the Universiti Tun Hussein Onn Malaysia (UTHM) and Ministry of Higher Education Malaysia for supporting this research under Project Vot No. U493.

REFERENCES

Aguilera, A. and R.P. Aguila, 2004. General N-dimensional rotations. Proceedings of the WSCG 2004 Short Communications the 12th International Conference in Central Europe on Computer Graphics Visualization and Computer Vision, February 2-6, 2004, Vaclav Skala-UNION Agency, Pilsen, Czech Republic, ISBN:80-903100-5-2, pp: 1-8.

Jamel, S., 2012. The hybrid cubes encryption algorithm (HiSea). Ph.D Thesis, Universiti Tun Hussein Onn Malaysia, Parit Raja, Malaysia.

Jamel, S., M.M. Deris, I.T.R. Yanto and T. Herawan, 2011. The Hybrid Cubes Encryption Algorithm (HiSea). In: Advances in Wireless, Mobile Networks and Applications, Salah S.A.M., C.L. Hu and D. Nagamalai (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-21152-2, pp: 191-200.

Jamel, S., T. Herawan and M.M. Deris, 2010. A Cryptographic Algorithm Based on Hybrid Cubes. In: Computational Science and its Applications, David, T., O. Gervasi, B. Murgante, E. Pardede and B.O. Apduhan (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-12188-3, pp: 175-187.

Rajavel, D. and S.P. Shantharajah, 2012a. Cryptography based on combination of hybridization and cube's rotation. Int. J. Comput. Intell. Inf., 4: 294-299.

Rajavel, D. and S.P. Shantharajah, 2012b. Cubical key generation and encryption algorithm based on hybrid cube's rotation. Proceedings of the 2012 International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME), March 21-23, 2012, IEEE, Tamil Nadu, India, ISBN:978-1-4673-1037-6, pp: 183-187.

Robbin, J., 2005. Coordinate Geometry. University of Wisconsin-Madison, Madison, Wisconsin,.

Shen, J., X. Jin and C. Zhou, 2005. A Color Image Encryption Algorithm Based on Magic Cube Transformation and Modular Arithmetic Operation. In: Advances in Multimedia Information Processing-PCM 2005, Sung, Y.H. and H.J. Kim (Eds.). Springer, Berlin, Germany, ISBN:978-3-540-30040-3, pp: 270-280.

Trenkler, M., 2000. A construction of magic cubes. Math. Gazette, 84: 36-41.

Trenkler, M., 2005. An algorithm for making magic cubes. PHI. ME. J., 12: 105-106.

Wu, Q., C. Zhu, J.J. Li, C.C. Chang and Z.H. Wang, 2016. A magic cube based information hiding scheme of large payload. J. Inf. Secur. Appl., 26: 1-7.

Zhang, L., S. Ji, Y. Xie, Q. Yuan and Y. Wan *et al*., 2005. Principle of Image Encrypting Algorithm Based on Magic Cube Transformation. In: Computational and Information Science, Yue, H., J. Liu, Y.P. Wang, Y. Cheung and H. Yin *et al*. (Eds.). Springer, Berlin, Germany, ISBN:978-3-540-30819-5, pp: 977-982.