International Journal of Computational Intelligence and Informatics, Vol. 1 : No. 4, January - March 2012

Cryptography Based on Combination of Hybridization and Cube's Rotation

Rajavel D
Research scholar,
Science and Humanity (Comp. App.)
Anna university of technology, Coimbatore, India
rajaveld@yahoo.co.in,

Shantharajah S.P
Department of Computer Applications
Sona College of Technology
Salem, Tamil Nadu, India.
spshantharaj@gmail.com

Abstract

We propose a new and improved cryptographic algorithm based on combination of cubical data hybridization and rotation. Hybridization was performed with shuffled cubes, which are generated from randomly gained rotation square. The obtained hybrid cube was again shuffled via rotation square, which in turn generated from randomly selected another rotation square. Cubic rotation was performed as same that of simple Rubik's cube shuffling. In general, four phase of rotation was carried out, in which first one involves rotation of cubes which has sequence of number from 1 to n*n*n, the second one involves the rotation of hybrid cube to achieve cubical keys, the third phase of rotation has been carried out in developing the cipher message by rotating the original message and last one involves the rotation of cipher cube to regain the original message. Random selection was performed in generation of rotation square and random selection of cubical encryption key. The generated key was in cubical form and cipher text generated from this encryption algorithm is more secure from cryptanalysis because rotation and hybridization makes data unpredictable.

Keywords: ***Cryptography, Cubical key, Cube rotation, Cube hybridization, Rotation square***.

1. Introduction

Data transfer rate in internet is very high now a day and more sensitive data is transferred. So security is plays main role in data transfer and storing of data in secure place. Cryptography algorithms provide high secure data communication to protect sensitive data in a secure manner. In cryptography, original message is converting into unpredictable pattern using secret key [1]. The secret key is generated based on mathematical model. Very few advanced encryption algorithms like RSA, Quadratic residuosity, Phi-hiding assumption, etc. provides computational hardness [2] and it makes difficult to break a key by an opponent whose objective is to find the original message. Necessity of cryptography was arrived since World War I to protect information from adversary. In addition, every cryptographic algorithm must satisfy the execution time and high level security channel according to selection of Advanced Encryption Standard (AES) [3]. So we have to consider the represent of data and the way of generating key for encryption. Three dimensional represent of data like cubical form could provide more security.

Cube is a three dimensional object which contains six faces. Data in cube are represented in three dimensional matrixes, for example: 3 x 3 x 3 cube which contain 27 values. Cube based problem provide the computational hardness to find the solution, so cryptanalyst find difficult to arrive with a solution because shuffled cube could produce more possibilities in the form of mathematical functions like exponential and factorial [4, 5]. Most recent cryptographic algorithm proposes cubical based encryption and decryption schemes [6-11]. In that most approaches cubical structure is used for image scrambling, in our approach we have used for text scrambling. Feng, Xiao, Tian, Xiaolin, Xia, Shaowei, proposed the cryptographic algorithm for image encryption based on rotation of magic cubes [12]. In this approach, three dimensional cubes are generated from two dimensional image pixel values. By rotating the cube's face value, image is encrypted but this approach involves only changes in the face values of cube. Sapiee Jamel, Tutut Herawan, and Mustafa Mat Deris, proposed the hybrid cube based cryptographic algorithm [13]. In this approach cube is used only for generation of key, but encryption of message is represented in two dimensional, so cryptanalyst can find the original messages with minimum number of possibilities in comparison to our proposed algorithm. The configuration of Rubik's cube contains several subsets which can be solved by factorization problem. Though, factorization problem is very easy in the case of Rubik's cube but finding the shortest route via factorization is NP-hard [2, 14].

In our previous paper [15] hybridization was performed with magic cubes where the generation of magic cube is time consuming process and take more steps to achieve. So here we propose a new way of doing hybridization. In addition to that

ISSN : 2349 - 6363

we have improved the method of rotation and phase of rotation as compared to our previous paper.

In this study, we improve a new way of generating cubical crypto key and encryption technique using cube rotation and generating hybrid cubes from randomly shuffled cube. Shuffling of cube was based on rotation square which was generated from randomly formed random square. Rotation square was generated for each cube, number of cube is depending up on the order of cubes for example: if the cube order was n, the number of shuffled cube was N (n*n*n). Hybridizing N number of shuffled cubes yields N-1 number of hybrid cubes. Then generated Hybrid cube was again rotated based on randomly generated another rotation square. Rotation square have the value in the set {1, 2, 3}, depending on these values cube would be rotated. Number of row and column of rotation square depends on order of shuffled cube. Rotation of cube can increase the protection of the original message from third party by increasing the probability. A single rotation of 3 dimensional cubes could reflect on all the faces of cube which increase the shuffling of data. So the rotation was carried out in key generation (two phases), encryption and decryption.

This paper is organized as follows: Section 2 describes the basic theory which has been used in proposed algorithms. Section 3 describes the proposed key generation algorithm, encryption and decryption algorithm based on rotated hybrid cubes. Section 4 describes the conclusion of this research.

2. Basic Theory

Random Square is a two dimensional n x n matrix in which values are picked randomly from the range 1 to 100 and forms the square.

2.1 Random Square

Random Square is a two dimensional n x n matrix in which values are picked randomly from the range 1 to 100 and forms the square.

Random Square of order n

Rn = [r(i,j): 1≤ i, j ≤ n] where r(i,j) is in a set {1, 2, … 100}

2.2 Rotation Square

Cubes are rotated based on the rotation square which is formed by performing modulo operation on randomly selected random square.

Rotation square of order n

RSn = [rs(i, j): 1≤ i, j ≤ n] where rs(i, j) in {1, 2, 3}

is a n x n two dimensional matrix.

Rotation square is form by using mod 3 operation with randomly generated random square. Rotation is performed on alternative row and column coordinates based on row and column index value of rotation square. First row values are taken for row rotation and last row values are taken for column rotation. Rotation of row was performed starting from right to left whereas column rotation have been performed from top to bottom side of the cube.

$$\begin{bmatrix} 94 & 69 & 14 \\ 3 & 56 & 16 \\ 20 & 1 & 72 \end{bmatrix} \text{Mod } 3 = \begin{bmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \\ 2 & 1 & 3 \end{bmatrix} \quad (1)$$

Fig. 1 Generate Rotation Square from Random Square. The first row and last coloumn of the rotation square is highlighted in bold.

2.3 Cube Shuffling

Shuffled cube is a three dimensional integer's matrices, arranged in n x n x n pattern. The basic feature of shuffled cube is that numeric values 1 to n*n*n are shuffled randomly based on rotation square. Rotation square is generated from randomly formed random square.

Shuffled cube of order n

SCn = [sc(i, j, k): 1 ≤ i, j, k ≤ n]

Where: sc (i, j, k) in a set {1, 2,…, n*n*n}.

2.4 Hybrid Cube Generation

Hybrid cubes are generated by matrix multiplication of layers in between two different shuffled cubes. Let us consider 3 order hybrid cube layers {1, 2, 3}: hybrid 1 is based on inner matrix multiplication of layer in the different coordinate {i = 1,2,3} of "shuffled cube 1" and layer {i = 3, 2, 1} of "shuffled cube 2" and so on. Hybrid cube 2 is formed by shuffled cube 2 and 3, and so on as mentioned above.

Example for 3 order hybrid cube:

Hybrid cube of order 3 is defined by HCi, defined as

HCi = SC1i, x SC2k

where i in {1, 2,… n} and k in {n,…, 2, 1} SCi,j is jth layer in ith shuffled cube.

$$\begin{bmatrix} SC1_{111} & SC1_{112} & SC1_{113} \\ SC1_{121} & SC1_{122} & SC1_{123} \\ SC1_{131} & SC1_{132} & SC1_{133} \end{bmatrix} X \begin{bmatrix} SC2_{311} & SC2_{312} & SC2_{313} \\ SC2_{321} & SC2_{322} & SC2_{323} \\ SC2_{331} & SC2_{332} & SC2_{333} \end{bmatrix}$$

Fig. 2. Multiplication of Hybrid cube's first layer

3. Proposed Algorithms

3.1 Cubical Key Generation Algorithm

Proposed key generation algorithm produces 3 dimensional hybrid cubical structured key, which is rotated based on rotation square of order n. Rotated hybrid cubical key is presented as follows:

Input: Order of the cube i.e., 'n'

Output: Number of rotated hybrid cubical keys

Step 1: Generation of sequence numbered cube

We first generate N (n*n*n) number of three dimensional sequence cubes (number starts from 1 and ends with n*n*n).

Step 2: Shuffle the sequence cubes using rotation square

a) Generate a two dimensional random matrix in which values range in between 1 to 100, the next step is the conversion of random matrix to rotation square using mod 3 operation. Different rotation squares have been generated for each sequence cube.

b) Shuffle the sequence cube based on corresponding rotation square. Row is rotated based on first row of rotation square; column is rotated based on last row of rotation square. Row and column rotation was performed alternatively, first starts with row rotation.

Step 3: Arrange the shuffled cubes

Randomly pick any one of the cube from N number of shuffled cubes, based on that values cube is arranged.

Step 4: Hybridize the shuffled cubes

Pick two consecutive cubes and perform the hybridization. First hybridization has been performed with cube 1 and 2; second one involves 2 and 3; and so on till all N cubes are hybrid, finally we get N-1 hybrid cubes.

Step 5: Rotate the hybrid cubes

Rotate all hybrid cubes based on rotation square as mentioned in step 2(a). Rotated cubes are considered as cubical encryption key.

Step 5: Generate inverse matrix

The resulting rotated hybrid cubes were used to generate the decryption key by the corresponding inverse matrix of rotated hybrid.

Step 5: Key selection

Randomly selected key from rotated hybrid cubes was considered as a cubical key. This key is used to encrypt the original message cube. Repeat the selection of key until all messages have their own key to encrypt.

Model Implementation

Let us consider a 3 order cube in generating a cubical encrypt and decrypt key using hybridization and rotation of cube.

Step 1:

Order 3 sequence cube as follows

$$SQ3=\begin{bmatrix}1&2&3\\4&5&6\\7&8&9\end{bmatrix}\begin{bmatrix}10&11&12\\13&14&15\\16&17&18\end{bmatrix}\begin{bmatrix}19&20&21\\22&23&24\\25&26&27\end{bmatrix} \quad (2)$$

Step 2:

a) Rotation square

Random generation of 3 x 3 matrix

$$R1=\begin{bmatrix}34&26&88\\91&8&14\\62&93&1\end{bmatrix} \quad (3)$$

$$R2=\begin{bmatrix}52&78&21\\23&41&26\\35&97&82\end{bmatrix} \quad (4)$$

Rotation square – RS1 = equation (3) mod 3

$$RS1=\begin{bmatrix}1&2&1\\1&2&1\\2&3&1\end{bmatrix} \quad (5)$$

Rotation square – RS2 = equation (4) mod 3

$$RS2=\begin{bmatrix}1&3&3\\2&2&2\\2&1&1\end{bmatrix} \quad (6)$$

First row is taken for row rotation and last row is taken for column rotation.

b) Cube shuffling

Consider shuffled cube 9 (eqn 7) formed by Equation (2) is rotated based on equation (5)

$$SC9=\begin{bmatrix}25&8&19\\24&17&20\\9&18&21\end{bmatrix}\begin{bmatrix}16&23&22\\15&14&13\\26&5&4\end{bmatrix}\begin{bmatrix}7&12&3\\6&11&10\\1&2&27\end{bmatrix} \quad (7)$$

Consider shuffled cube 18 (eqn 8) formed by Equation (2) is rotated based on equation (6)

$$SC18=\begin{bmatrix}25&10&19\\4&11&20\\3&2&21\end{bmatrix}\begin{bmatrix}16&15&6\\23&14&5\\8&13&22\end{bmatrix}\begin{bmatrix}7&26&9\\24&17&12\\27&18&1\end{bmatrix} \quad (8)$$

Step 3:

Consider the shuffled cube 9 (equation 7) is taken for arranging of shuffled cubes for further hybridization. According to this arrangement SC9 and SC18 is adjacent to each other.

Step 4:

According to above arrangement hybrid cube 8 is formed by combining SC9 and SC18 that is equation 7 and 8.

So, HC8 = SC9 * SC18

$$HC8_{i=1} = \begin{bmatrix} 880 & 1128 & 340 \\ 1116 & 1273 & 440 \\ 1062 & 918 & 318 \end{bmatrix}$$

$$HC8_{i=2} = \begin{bmatrix} 961 & 848 & 695 \\ 666 & 590 & 446 \\ 563 & 521 & 269 \end{bmatrix}$$

$$HC8_{i=3} = \begin{bmatrix} 232 & 208 & 436 \\ 224 & 201 & 544 \\ 114 & 86 & 626 \end{bmatrix} \quad (9)$$

Step 5:

Rotation square from randomly formed random square, first row and last row of rotation square (bolded value) has been considered for row and column rotation of hybrid cube

$$R3 = \begin{bmatrix} 48 & 96 & 39 \\ 84 & 75 & 63 \\ 43 & 87 & 65 \end{bmatrix} \quad (10)$$

$$RC3 = \begin{bmatrix} 3 & 3 & 3 \\ 3 & 3 & 3 \\ 1 & 3 & 2 \end{bmatrix} \quad (11)$$

Hybrid cube (equation 9) was rotated based on rotation square's (equation 11) first row and last row index value to generate cubical encrypt key as follows

$$EK8_{i=1} = \begin{bmatrix} 436 & 918 & 318 \\ 63 & 512 & 440 \\ 1062 & 1116 & 340 \end{bmatrix},$$

$$EK8_{i=2} = \begin{bmatrix} 224 & 666 & 86 \\ 201 & 590 & 1273 \\ 695 & 446 & 1128 \end{bmatrix},$$

$$EK8_{i=3} = \begin{bmatrix} 114 & 961 & 232 \\ 554 & 848 & 208 \\ 626 & 269 & 880 \end{bmatrix} \quad (12)$$

Step 4:

Inverse matrix was generated for all layers in the rotated hybrid cube (12) for decrypt cubical key generation which will be used in decryption of cipher message

$$DK1_{i=1} \begin{bmatrix} -0.002629 & 0.000355 & 0.002000 \\ 0.003698 & -0.001572 & -0.001425 \\ -0.003927 & 0.004051 & 0.001372 \end{bmatrix}$$

$$DK1_{i=2} \begin{bmatrix} 0.000226 & -0.001648 & 0.001843 \\ 0.001521 & 0.000446 & -0.000619 \\ -0.000741 & 0.000839 & -0.000004 \end{bmatrix}$$

$$DK1_{i=3} \begin{bmatrix} -0.001954 & 0.002217 & -0.000009 \\ 0.001011 & 0.000127 & -0.000297 \\ 0.001081 & -0.001616 & 0.001233 \end{bmatrix}$$

(13)

Based on the key generation algorithm, cubical based unpredictable encrypt cubical key and decrypt cubical key was generated.

3.2 Encryption Algorithm based on Cube Rotation

In this encryption technique, the hybrid cubical key (See section III-A) and original message was assorted. The resultant mixed message was rotated to produce the cipher text.

Input: Original message and N-1 number of cubical encryption key

Output: Cipher text in the form of cubical structure

Step 1: Forming 3 dimensional message

Original messages were converted into M number of message cubes (3 dimensional matrixes) with order n and convert each character into integer using ASCII Codes.

Step 2: Generate cipher cube

Message cube 1 was combined with cubical key 1 to create Message cube 1'. Message cube 1' was rotated based on rotation square, which was generated from first layer of cubical key 1 to form cipher cube 1. The rotation was performed by right to left for each row and top to bottom for each column.

Step 3: Generate all cipher

Repeat the Step 2 until all message cubes are converted into cipher cubes.

Model Implementation

Let us consider the original message as "rajavel love his mom & dad.", we are using 3 order cubes. So we consider a message containing 27 characters for encryption and decryption.

Step 1:

The original messages were converted in to 3 x 3 x 3 cubical structure and each character has been converted in the form of ASCII values.

$$M1_{i=1} = \begin{bmatrix} 114 & 97 & 106 \\ 97 & 118 & 101 \\ 108 & 32 & 108 \end{bmatrix},$$

$$M1_{i=2} = \begin{bmatrix} 111 & 118 & 101 \\ 32 & 104 & 105 \\ 115 & 32 & 109 \end{bmatrix},$$

$$M1_{i=3} = \begin{bmatrix} 111 & 109 & 32 \\ 38 & 32 & 100 \\ 97 & 100 & 46 \end{bmatrix} \quad (14)$$

Step 2:

Consider randomly selected cubical key EK8, from which semi-cipher cube was generated based on mixing of (14) and (12), which is the matrix multiplication product of (14) and (12)

$$SCC1_{i=1} = \begin{bmatrix} 168387 & 272612 & 114972 \\ 156988 & 262178 & 117106 \\ 163800 & 236056 & 85144 \end{bmatrix}$$

$$SCC1_{i=2} = \begin{bmatrix} 118777 & 188592 & 273688 \\ 101047 & 129502 & 253584 \\ 107947 & 144084 & 173578 \end{bmatrix}$$

$$SCC1_{i=3} = \begin{bmatrix} 93072 & 207711 & 76584 \\ 84660 & 90554 & 103472 \\ 95254 & 190391 & 83784 \end{bmatrix} \quad (15)$$

Generate the rotation square from first layer of cubical encryption key (12) which is (EK8i=1 % 3)

$$RS4 = \begin{bmatrix} 1 & 3 & 3 \\ 3 & 2 & 2 \\ 3 & 3 & 1 \end{bmatrix} \quad (16)$$

Finally the cipher cube (17) was generated from rotation of semi-cipher cube (15), based on the rotation matrix RS4 (16).

$$CC1_{i=1} = \begin{bmatrix} 163800 & 236056 & 93072 \\ 272612 & 144084 & 207711 \\ 168387 & 84660 & 76584 \end{bmatrix}$$

$$CC1_{i=2} = \begin{bmatrix} 156988 & 101047 & 117106 \\ 90554 & 129502 & 262178 \\ 118777 & 253584 & 107947 \end{bmatrix}$$

$$CC1_{i=3} = \begin{bmatrix} 114972 & 273688 & 85144 \\ 103472 & 188592 & 190391 \\ 83784 & 173578 & 95254 \end{bmatrix} \quad (17)$$

Encryption algorithm generated the unpredictable cubical cipher, which is very difficult to break without cubical key.

3.3 Decryption Algorithm

Decryption technique is based on rotation of cipher cubes and then combined with the inverse matrix to get decrypted original message cube.

Input: Cipher cubes and cubical decryption key

Output: Original message

Step 1: Rotate the cipher cube

Cipher cube 1 was rotated based on the rotation square which was created from first layer of matrix inverse of decryption cube to create Message 1', repeat the same step until all the cipher cubes are rotated based on rotation. Here inverse rotation was performed from left to right for each row and from bottom to top for each column.

Step 2: Decrypt the message

Mixing of Message 1' and decryption key 1 will create original message 1, repeat the same step until all the original message is generated from decrypted cubes.

Step 3: Convert original text from 3 dimensional cubes

All the message cubes were converted in to plain text with ASCII code.

Model Implementation

Step 1:

Rotation square was generated from first layer inverse matrix of decryption cubical key (in equation 13, DK1i=1), will be equal to the rotation matrix (equation 16)

Rotate the cipher cube (17) based on rotation square to generate the Message' which is equal to semi-cipher cube (15), in this rotation process inverse rotation is performed in each row and column

Step 2:

Original message was obtained from the combination of cipher cube after rotation (16) and decryption key cube (13)

$$M1_{i=1} = \begin{bmatrix} 114 & 97 & 106 \\ 97 & 118 & 101 \\ 108 & 32 & 108 \end{bmatrix}$$

$$M1_{i=2} = \begin{bmatrix} 111 & 118 & 101 \\ 32 & 104 & 105 \\ 115 & 32 & 109 \end{bmatrix}$$

$$M1_{i=3} = \begin{bmatrix} 111 & 109 & 32 \\ 38 & 32 & 100 \\ 97 & 100 & 46 \end{bmatrix}$$

"rajavel love his mom & dad."

Finally without loss of any data decryption algorithm reproduce the original message (14) as well.

4. Conclusion

The rotation phase has been done in key generation, encryption, decryption which enable us to shuffle the data resulting in a unpredicted pattern at each stage of the process. We performed random selection in the case of rotation square generation and selection of encryption key which creates different pattern every time which the ensures the protection of data from cryptanlysts.Generated encryption key is in 3D cubical form which can increase the possibilities for picking a solution in comparison to a 2-D key.

References

[1] Stallings William, "Stalling Cryptography And Network Security", 4/E – 2006 Pearson Education, Inc.

[2] Michael R. Garey and David S. Johnson, "Computers and Intractability: A Guide to the Theory of NP-Completeness", W.H. Freeman (1979).

[3] National Institute of Standards(NIST): FIPS Pub 197: Advanced Encryption Standard AES (2001)

[4] David Joyner, "Adventures in group theory: Rubik's Cube, Merlin's machine, and other mathematical toys", JHU Press, 2002

[5] Scott Vaughen, Counting the Permutations of the Rubik's Cube, Miami Dade College, unpublished.

[6] Li Zhang, Xiaolin Tian, Shaowei Xia, "A Scrambling Algorithm of Image Encryption Based on Rubik's Cube Rotation and Logistic Sequence" IEEE Explore Multimedia and Signal Processing (CMSP), International Conference on 14-15 May 2011 On pp. 312–315

[7] Rajdeep Chowdhury & Saikat Ghosh "Normalizer Based Encryption Technique [NBET] Usingthe Proposed Concept Of Rubicryption" International Journal of Information Technology and Knowledge Management January-June 2011, Volume 4, No. 1, pp. 77-80

[8] Zhi-liang ZHU, Chong WANG, Hua CHAI, Hai YU "A Chaotic Image Encryption Scheme Based on Magic Cube Transformation" 2011 Fourth International Workshop on Chaos-Fractals Theories and Applications 978-0-7695-4560-8/11 2011 IEEE

[9] Xiao Feng, Xiaolin Tian, Shaowei Xia, "An Improved Image Scrambling Algorithm Based On Magic Cube Rotation and Chaotic Sequences" 2011 4th International Congress on Image and Signal Processing 978-1-4244-9306-7/11 2011 IEEE

[10] Jianbing Shen, Xiaogang Jin, and Chuan Zhou, "A Color Image Encryption Algorithm Based on Magic Cube Transformation and Modular Arithmetic Operation" In: Ho, Y.-S., Kim, H.-J. (eds.) PCM 2005. LNCS, vol. 3768, pp. 270–280. Springer, Heidelberg (2005)

[11] Zhang, L., Shiming, J., Xie, Y., Yuan, Q., Wan, Y., Bao, G, " Principle of Image Encrypting Algorithm Based on Magic Cube Transformation", In: Hao, Y., Liu, J., Wang, Y.-P., Cheung, Y.-m., Yin, H., Jiao, L., Ma, J., Jiao, Y.-C. (eds.) CIS 2005. LNCS(LNAI), vol. 3802, pp. 977–982. Springer, Heidelberg (2005)

[12] Feng, Xiao, Tian, Xiaolin, Xia, Shaowei, "A novel image encryption algorithm based on fractional fourier transform and magic cube rotation" IEEE Explore Image and Signal Processing (CISP), 4th International Congress on 15-17 Oct. 2011

[13] Sapiee Jamel, Tutut Herawan, and Mustafa Mat Deris, "A Cryptographic Algorithm Based on Hybrid Cubes", ICCSA 2010, Part IV, LNCS 6019, pp. 175–187, 2010

[14] Christophe Petit and Jean-Jacques Quisquater, "Rubik's for Cryptographers", UCL Crypto Group, January 19, 2011.