Image Scrambling Methods for Image Hiding: A Survey

Reema Rhine, Nikhila T Bhuvan
Rajagiri School Of Engineering And Technology Rajagiri School Of Engineering And Technology

Abstract
With the explosive growth of internet and the fast communication techniques in recent years the security and the confidentiality of the sensitive data has become of prime and supreme importance and concern. In order to protect this data from tampering and unauthorized access various methods for data hiding like authentication, hashing, cryptography have been developed and are in practice today.In this paper, a data hiding mechanism based on the application of Rubik's cubic algorithm is proposed. The biggest advantage of using this algorithm is that, a Rubik's cube possesses 6 faces and it can be divided into 54 (6 faces*3*3) elements for scrambling process. This paper also explores the properties of Arnold's cat map, a method for mapping of the pixels of an image. An image is hit with a transformation that apparently randomizes the original organization of its pixels. However, the original image reappears if iterated enough times. The paper also presents a comparative analysis of these techniques.

Keywords
Data Hiding, Rubik's cubic, Information security

1. INTRODUCTION

Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography is a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret.
Information security becomes an important and urgent issue not only for individuals but also for business and governments. Security of image data is very important in many areas, such as copyright protection and privacy, security communication, and also in military applications Trust in digital data is characterized in terms of confidentiality, authenticity, and integrity. Confidentiality is 'the property that information is not made available or disclosed to unauthorized individuals, processes or entities.' Authenticity is defined as 'the corroboration that the source of data received is as claimed.' Integrity is the 'the property that data has not been altered or destroyed in an unauthorized manner.' Image Scrambling (Encryption)[8] is a good method for providing security to image data by making image visually unreadable and also difficult to decrypt it for unauthorized users.
In this paper, the section II is about the Rubik's cubic algorithm and section III deals with the Arnold's cat map. Section IV compares these methods.

Manuscript received February 5, 2015
Manuscript revised February 20, 2015

2. I.ALGORITHM OF RUBIK'S CUBIC DATA HIDING

The application of Rubik's cubic algorithm combined with encipher system for data hiding[14] can be implemented in three different approaches as shown in Figure 1. The detail process is addressed in the following:

(1) First case, the hidden information can be encrypted by an encipher system. After then, the encrypted data is scrambled by performing Rubik's cubic algorithm. Finally, the scrambled data is then embedded into a cover/host image to achieve data hiding and outcome a stego-image.
(2) Second case, the hidden information is first scrambled by applying Rubik's cubic algorithm. After then, an encipher system is applied to encrypt the hidden data in order to enhance the security. Finally, the encrypted scrambled data is embedded into a cover/host image to achieve data hiding and outcome a stego-image.
(3) Third case, the hidden information is firstly scrambled by applying Rubik's cubic algorithm. After then, data hiding is performed. In order to enhance the security, encipher system is finally applied to encrypt the embedded stego-image to obtain cipher data for transmitting.

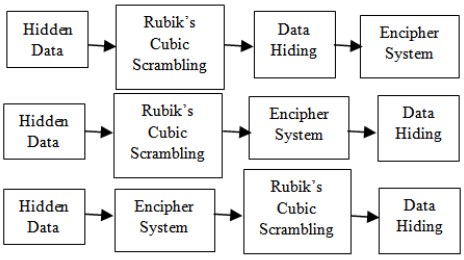

Figure 1: Different data hiding approaches based on the combination of Rubik's cubic algorithm with encipher system.

Rubik's cubic possesses 6 faces and can be divided into 54 (6 faces*3*3) elements. In the beginning, the hidden data (treated similar as an image) will be partitioned into different unit block size such as pixel based, 3*3 pixels based, or other n*n pixels based. Then, 54 units will be selected sequentially and transformed into 6 faces according to the six faces of a Rubik's cubic by designated an index number as shown in Figure 3 and Figure 4.

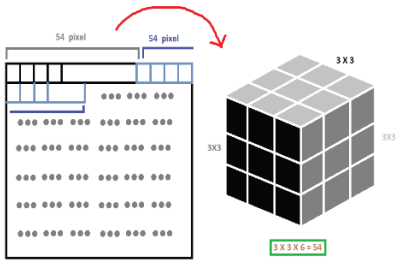

Figure 2 Mapping of Rubik's cubic and image.

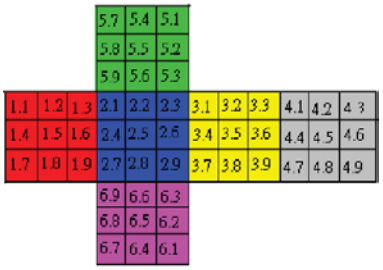

Figure 3 Corresponding Index of a Rubik's Cubic.

Therefore, an image can be partitioned into a lot of different 54 units of blocks and formed a lot of different Rubik's cubic. To apply the Rubik's cubic for image data hiding, the basic process unit can be one pixel, small block, or macro- cell (large block) as compare to the traditional Rubik's Cubic. To restore the original style of a Rubik's Cubic, one can follow the reverse step of rotation or following the decomposition steps of restoring the Rubik's Cubic. Since the application of Rubik's Cubic can scramble the sequence of an original sequence, it can be applied for information encryption or information hiding. In the processing, one can easily find out that the cubic located in the corner, center and sides are transformed only to corner, center and side locations respectively. However, the corner cubic possesses three faces.

In the proposed data hiding, the third case addressed above is adopted. The data hiding process is performed from left to right and then top to bottom in the cover image, i.e., horizontally, with the covert information. In the proposed scheme, some parameters are utilized for controlling the process of data scrambling and data embedding.

(1) Macrocell parameter MP: Two bits length. Options include pixel based and block based. In which, bit pair 00 represents pixel based, i.e., one pixel as a process element. As for pixel based, an image is divided into multiple 54 pixels from the left-most pixel of the top column through the bottom column. As to block based, each of n2 pixels (n row* n column) will form a Macrocell as an element for process. In the proposed scheme, bit pair represents 4*4 (equals 16 pixels) as a process element. Bit pair 10 represents 8*8 (equals 64 pixels) as a process element. Finally, bit pair 11 reserve for further utilization.

(2) Hiding method parameter Hp: Three bits length. In the prototype, LSB data hiding is adopted for spatial domain, DCT data hiding is adopted for frequency domain, and both of LSB and DCT data hiding are adopted for hybrid domain. Therefore, currently there are only three different options are provided.

Table 1. Operation of Hiding method parameter Hp

Bit Pair	**Operation**	
000	spatial	Least Significant Bit, LSB
001	spatial	Generalized LSB, GLSB
010	spatial	Histogram Modification/Differencing
011	frequency	Discrete Cosine Transform, DCT
100	frequency	Discrete Wavelet Transform, DWT
101	hybrid	LSB+DCT
110	hybrid	LSB+DWT
111	reserved	GLSB+DCT

(3) Rotation regulation parameter Rr: One bit length. A value "0" means all of the macrocells use the same rotation parameter for performing scrambling. In addition, value "1" means each macrocell is rotated and scrambled based on different rotation parameters which are all randomly generated.

(4) Rotation parameter Rp: Three bits length. The first bit is used for indicating plus or minus symbol. In which, a value "0" means positive and "1" means negative. The other two bits represent 0 to 3 respectively according to the bit pairs 00, 01, 10, 11. As regarding the rotation of scrambling the sequence of a Rubik's cubic, pseudo random number can be adopted to generate certain number for making scrambling.

In the proposed mechanism, 6 digits are used and formed as "x1x2y1y2z1z2" for rotating and scrambling. Each of the digits will be assigned with one of the numbers from -3 to 3, i.e., $-3 \leq x1, x2, y1, y2, z1, z2 \leq 3$. The operation is summarized as Table II. Digits x1 and x2 represent the rotation direction along the X-axis, y1 and y2 represent the rotation direction along the Yaxis, and z1 and z2 represent the rotation direction along the Z-axis. As performing scrambling, the referred coordination (0,0,0) is fixed, i.e., the cubic that just located on the X-axis, Y-axis, and Z-axis are keep stationary without rotating.

Table II. Operation of Rotation Parameters

Parameters	Operations	
	Digit	**Rotation**
X1,x2,y1,y2, z1,z2	3	Clockwise rotating 270^0 along X-axis, Y-axis, or Z-axis according to the digits
	2	Clockwise rotating 180^0 along X-axis, Y-axis, or Z-axis according to the digits
	1	Clockwise rotating 90^0 along X-axis, Y-axis, or Z-axis according to the digits
	0	No rotation or shift performed
	-1	Counter-clockwise rotating 900 along X-axis, Y-axis, or Z-axis according to the digits
	-2	Counter-clockwise rotating 180^0 along X-axis, Y-axis, or Z-axis according to the digits
	-3	Counter-clockwise rotating 270^0 along X-axis, Y-axis, or Z-axis according to the digits

So, x1 will mapping to the center row of cubic along the X-axis and x2 will mapping to the right most row of cubic along the X-axis. Both of digits y1 and z1 are also mapped to the center row of the cubic along the Y-axis and Z-axis. Digit y2 is mapped to the left most row of the cubic along the Y-axis and z2 is mapped to the bottom most column of the cubic along the Z-axis. If the digit is "0", that means no rotation will be performed. If the digit is "1", that means a counterclockwise rotation of 900 will be performed. If the digit is "-1", that means a clockwise rotation of -900 will be performed.

(4) Encipher parameter Ep: Three bits length. The operations are listed in Table III.

Table III. Operation of Encipher parameter Ep

Bit pair	Operation	Bit pair	Operation
000	Without encryption	100	AES + MD5 (Hash)
001	Triple DES	101	AES + SHA256
010	128 bits AES	110	Reserved
011	AES + RSA (Signature)	111	Reserved

The proposed data hiding approach is implemented by the following procedure:

Step 1: Define the required MP, Hp, Rr, Rp and Ep parameters.

Step 2: Hidden data is encrypted by the cipher system in order to strengthen the data security.

Step 3: The encrypted data is scrambled by applying the Rubik's cubic rotation.

Step 4: The scrambled data is embedded into the cover image to obtain the stego-image [15].

The embedded image is directly utilized to extract the hidden information without the need of estimated or predicted original host image. Hence, the hidden information can be extracted by following the processing procedures.

Step 1: Extract the required parameters from stego-image.

Step 2: Extract embedded data from stego-image to get the hidden scrambled data.

Step 3: Descramble the extract data by applying the Rubik's cubic rotation algorithm reversely.

Step 4: Decrypt the descrambled data to obtain the original hidden data.

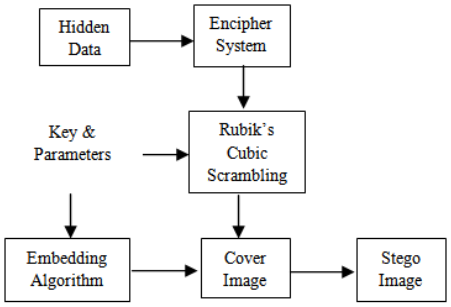

Figure 4. The diagram of proposed data hiding scheme

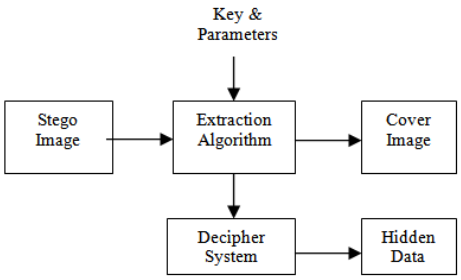

Figure 5. The diagram for hidden data extraction

After the scrambling of the image,it can be embedded into the cover image using any data hiding method

3. Image Scrambling Based Arnold Transformation

Images are composed of discrete units called pixels. A pixel is the basic unit representing some colour value, which when taken together form the image. The image is a m x n matrix, where m represents the number of rows of pixels and n the number of columns of pixels, and each

entry in the matrix being a numeric value that represents a given colour. For example, consider the 175 x 175 image of a caffeine molecule below.

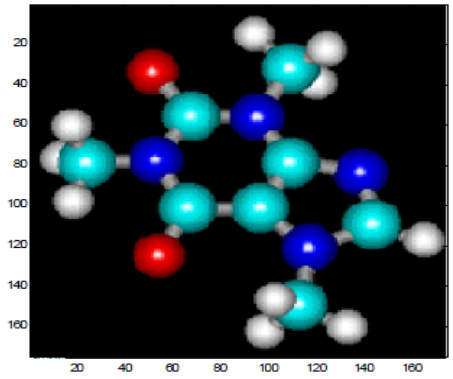

Figure 6. 175 x 175 image of a caffeine molecule

Let X be the image matrix, and we can examine selected entries in X.

$$X = \begin{bmatrix} 217 & 217 & 217 & 217 & \dots & 217 & 217 & 217 & 217 \\ 251 & 251 & 251 & 251 & \dots & 251 & 251 & 251 & 251 \\ 251 & 251 & 251 & 251 & \dots & 251 & 251 & 251 & 251 \\ 251 & 251 & 251 & 251 & \dots & 251 & 251 & 251 & 251 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 251 & 251 & 251 & 251 & \dots & 251 & 251 & 251 & 251 \\ 251 & 251 & 251 & 251 & \dots & 251 & 251 & 251 & 251 \\ 217 & 217 & 217 & 217 & \dots & 217 & 217 & 217 & 217 \end{bmatrix}$$

The numeric entries represent some colour value.

The mapping known as Arnold's Cat Map is named after the mathematician Vladimir I. Arnold, who first illustrated it using a diagram of a cat. It is a simple and elegant demonstration and illustration of some of the principles of chaos – namely, underlying order to an apparently random evolution of a system.

First we need to understand what modular arithmetic is in order to describe Arnold's Cat Map. The expression A mod B evaluates to the number N, such that $0 \le N < B$, and $A - N = k \times B$, where k is an integer. In other words, to find A mod B you add (or subtract) a multiple of B to A so that the result is in the interval [0,B). For example, 3 mod 10 is 3, −2.5 mod 5 is 2.5, and 15 mod 2 is 1. The expression (X, Y) mod N is the same as (X mod N, Y mod N). The effect of Γ is to map any point in the R2 plane to a point (x, y) in the unit square, where $0 \le x < 1$ and $0 \le y < 1$.

If we let

$$X = \begin{bmatrix} x \\ y \end{bmatrix}$$

be a n x n matrix of an image, Arnold's cat map is the transformation

$$\Gamma \begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x+y \\ x+2y \end{bmatrix} \bmod n$$

where mod is the modulo of the

$$\begin{bmatrix} x+y \\ x+2y \end{bmatrix}$$

and n. For example, 3.142mod1 = .142 or 150mod100 = 50 or

$$\begin{bmatrix} 123 \\ 154 \end{bmatrix} \bmod 100 = \begin{bmatrix} 23 \\ 54 \end{bmatrix}$$

Since the signs of both arguments are the same sign here, the modulo will simply be the remainder of the long division of $\begin{bmatrix} x+y \\ x+2y \end{bmatrix}$ and n.

For understanding the mechanism of the transformation Γ better, let us decompose it into its elemental pieces.

1. Shear in the x-diection by a factor of 1.

$$\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x+y \\ y \end{bmatrix}$$

2. Shear in the y-direction by a factor of 1.

$$\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x \\ x+y \end{bmatrix}$$

3. Evaluate the modulo.

$$\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} \bmod n$$

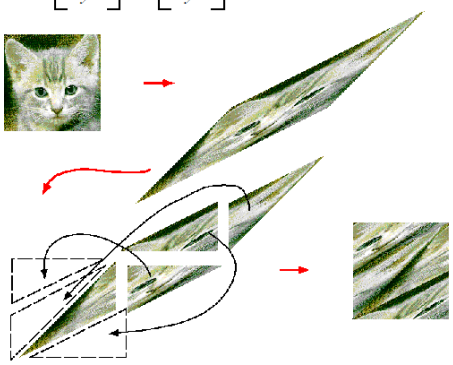

Figure 7. Visuals illustrating the steps

In the figure, the first step shows the shearing in the x and y-directions, followed by evaluation of the modulo operation and then the reassembly of the image.

4. Comparative Analysis of Image Scrambling Techniques

The proposed method is an image scrambling using the Rubik's cube algorithm. This is compared with the Arnold cat map method. In the proposed method the image can be partitioned into a lot of 54 unit blocks and thus form a number of Rubik's cube. To apply this Rubik's cubic algorithm, the basic process unit can be a pixel, small block, or macro cell. For example, if the image is partitioned as pixels, then there will be 54 pixels in that Rubik's cube. An image can also be partitioned based on 3*3, i.e. 9 pixels as a small block. In Arnolds cat method, only the pixel wise scrambling can be done. The shear and modulus operation is applied to each and every pixel.

Rubik's cubic method divides the image into its basic processing units and each of the 54 units are chosen sequentially to form a Rubik's cube for the purpose of scrambling. Here scrambling can be done to images of any shape and size. Arnold cat map method limits the process only to square area images.

In the proposed method the number of scrambling is chosen as desired or can be chosen in random but in Arnold cat map method the number of scrambling depends strictly on the number of pixel of the image. In general, it may be claimed that as the number of pixels increases, the period (number of scrambling) tends to increases. But this is not always true. For example, a 124 x 124 image has a period of fifteen, whereas, a 101 x 101 image has a period of twenty-five.

Table IV. Arnold scrambling algorithm cycle

Size of image (N)	Cycle of scrambling(T)	Size of image (N)	Cycle of scrambling(T)
3	4	25	50
4	3	32	24
5	10	64	49
6	12	100	150
7	8	120	60

To restore the original style of a Rubik's Cubic, one can follow the reverse step of rotation or following the decomposition steps of restoring the Rubik's Cubic. The decomposition steps are based on certain sequence. Since the application of Rubik's Cubic can scramble the sequence of an original sequence, it can be applied for information encryption or information hiding. In the Arnold cat map method, an image is hit with a transformation that apparently randomizes the original organization of its pixels. However, to regenerate the original image, the iteration for scrambling is repeated again until the original image reappears.

The overall security of the image is high in the case of scrambling using Rubik's cube as the scrambling can be done any number of times. Also an image can be partitioned into different number of Rubik's cube and each cube can be applied with different number of scrambling, thus enhancing the security of the image. As compared to the proposed method, the image security is less in the case of Arnold cat map method as here the number of scrambling depends on the number of pixels of the image

Table V. Comparison of image scrambling techniques

Criteria	Rubik's cubic algorithm	Arnold cat map
Basic process unit	Can be pixel or small blocks or macro cells	Pixel
Area	Can be done to image of any shape	Can be done only on square images
Scrambling times	Can be scrambled any number of times.	Depends on the number of pixels of the image
Image reassembly	Can be done by the reversing the scrambling process	Can be done by continuing the same process of scrambling
Security	High, as different number of scrambling can be done on different parts of the image	Low, as the number of scrambling depends on the number of pixels used

5. CONCLUSION

The hiding of confidential data, side information or annotation into host images gradually attracts the attention of researchers due to the emerging of confidential information transmission, digital rights management, digital library, and etc. In this paper, a novel data hiding mechanism based on the application of Rubik's cubic algorithm is proposed to achieve the aforementioned goals. The characteristic of our proposed data hiding mechanism is that it possesses the advantages of reversibility and good visual quality. Arnold cat map method is also studied in this paper. A comparative analysis of both the methods is done in this paper. From the survey it was found that Rubik's cubic algorithm performs better image scrambling than Arnold cat map. It ensures more security and better performance.

REFERENCE

[1] S. E. Chacko, I.T.B. Mary, and W.N.D. Raj, "Embedding invisible watermark in digital image using interpolation and histogram shifting", 3rd International Conference on

Electronics Computer Technology (ICECT), Vol. 4 , pp.89-93, 2011
[2] P. Patil and S. Sonavane, “Fragile Watermarking Scheme for Image Tamper Detection”, International Conference on Communication Systems and Network Technologies (CSNT), pp. 531- 535, 2011
[3] J. W. Lee, T.W. Oh, M.J. Lee, H.Y. Lee, and H.K. Lee, “Video Watermarking on Overlay Layer”, 7th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP), pp. 85-88, 2011
[4] M. Arabzadeh, M.S. Helfroush, H. Danyali, and K. Kasiri, “Reversible watermarking based on generalized histogram shifting”, 18th IEEE International Conference on Image Processing (ICIP), pp.2741-2744, 2011
[5] Dimitri Van De Ville, Wilfried Philips, Rik Van De Walle, Ignace Lemahieu, ―Image Scrambling Without Bandwidth Expansion‖, IEEE On Circuits And Systems For Video Technology, Vol. 14, No. 6, June 2004, pp 892-897.
[6] C. H. Tzeng, Z. F. Yang and W. H. Tsai, “Adaptive Data Hiding in Palette Images by Color Ordering and Mapping with Security Protection”, IEEE Transactions on Communications, Vol. 52, Issue. 5, pp. 791-800, May 2004
[7] Yicong Zhou, Karen Panetta, Sos Agaian, ―An Image Scrambling Algorithm Using Parameter Based M-Sequences‖, In Proc International Conference On Machine Learning And Cybernetics, 2008 (Volume:7), Pp 3695 – 3698, July 2008
[8] S. Li, C. Li, K.-T. Lo, and G. Chen, "Cryptanalysis of an image scrambling scheme without bandwidth expansion," IEEE Transactions on Circuits and Systems for Video Technology, vol. 18, no. 3, pp. 338-349, 2008.
[9] Y. Hu, S. Kwong, and J. Huang, “Using invisible watermarks to protect visibly watermarked images”, International Symposium on Circuits and Systems, Vol. 5, pp. 584-587, 2004
[10] M. H. Lin, Y. C. Hu, and C. C. Chang, “Both Color and Gray Scale Secret Images Hiding in a Color Image”, International Journal of Pattern Recognition and Artificial Intelligence, Vol. 16, No. 16, pp. 697-713, 2002
[11] D. C. Wu and W. H. Tsai, “Spatial-domain image hiding using image differencing”, IEE Proceedings in Vision, Image, and Signal Processing, Vol. 147, Issue 1, pp. 29-37, Feb. 2000
[12] M. Steinder, S. Iren , and P. D. Amer, “Progressively Authenticated Image Transmission,” in Proc. Military Communications Conference, vol.1, 1999, pp.641-645.
[13] F. Mintzer, “Developing digital libraries of cultural content for Internet access”, IEEE Communications Magazine, Vol. 37, pp. 72- 78, 1999
[14] Petitcolas, F.A.P., Anderson, R.J. & Kuhn, M.G., “Information Hiding – A survey”, Proceedings of the IEEE, 87:07, July 1999
[15] Johnson, N.F. & Jajodia, S., “Exploring Steganography: Seeing the Unseen”, Computer Journal, February 1998
[16] Bender, W., Gruhl, D., Morimoto, N. & Lu, A., “Techniques for data hiding”, IBM Systems Journal, Vol 35, 1996
[17] ISO 7498-2:1989, Information Processing Systems, Open Systems Interconnection, Basic Reference Model—Part 2: Security Architecture, http://www.iso.org, International Organization For Standardization; 1989.