ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

Tinkerbell Maps based Image Encryption using Magic Square

Jeena Pappachan[1], Jinu Baby[2]

PG Student [TCE], Dept. of ECE, Mar Baselios College of Engineering and Technology, Trivandrum, Kerala, India[1]

Assistant Professor, Dept. of ECE, Mar Baselios College of Engineering and Technology, Trivandrum, Kerala, India[2]

ABSTRACT:The transmission of data through the internet must be in such a way that it assures the security of data being transmitted. Multimedia data can be effectively transmitted using the technique of encryption. Chaotic maps are being recently used for image encryption and it is an efficient technique. In this paper, a new encryption algorithm is proposed based on Tinkerbell maps and magic square. Tinkerbell maps have excellent chaotic behaviour and its output always depends on the initial conditions. Simulation results shows that this algorithm provides an efficient and secure way for image encryption.

KEYWORDS: Image encryption, Cryptography, Chaotic maps, Tinkerbell maps, Magic square.

I.INTRODUCTION

Increase in the use of electronic communication needs the security of data being transmitted. A large number of digital images are transmitted through the internet and are more vulnerable to abuse now. Applications of digital images not only include internet communication but also in military communication and medical field. Hence it is necessary to encrypt the images thus transforming them to unrecognized noise images to ensure the privacy.
Cryptography is a technique used to encrypt the data and thus prevents the unauthorized access of the secret data. Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Rivest, Shamir and Adleman (RSA) algorithms are some of the conventional cryptographic algorithms. But digital images possess high redundancy and these are not suitable for image encryption. Chaos based encryption is one of the recent effective methods of cryptography for images.

Chaotic system is a deterministic system that shows random behavior. Chaotic outputs are of infinite precision and are sensitive to initial conditions and various control parameters. They are ergodic in nature, and so provide similar properties required for an efficient cryptosystem. Chaotic maps based encryption algorithm thus provides high encryption performance. Tinkerbell maps are real valued, discrete time 2D chaotic maps. The Tinkerbell sequences resemble random noise and hence it can be used for encryption. A magic square is a square matrix of size N*N which consists of all numbers from 1 to N*N exactly once and the sum of any row, column or main diagonal is the same. These two are used for proposing the new image encryption algorithm.

II.RELATED WORK

Many chaotic encryption algorithms are proposed in recent years based on the different types of chaotic maps. Pareek [1] proposed an image encryption algorithm based on chaotic logistic map. In [2], a chaotic shuffle method is proposed. Bao [3] explores three chaotic maps, Logistic map, Tent map and Sine Map for image encryption. Hua [4] used a 2D logistic sine map for image encryption and it provides high security. In [5], Gopalakrishnan performed the image encryption using permutation and diffusion of Tent and logistic chaotic maps. In [6], Chapaneri proposed the algorithm based on Latin rectangle scrambling of 2D Henon map. Hossain [7] used a 3D chaotic map for encryption and Hazarika [9] performed a selective encryption using spatial domain. Sankapal [10] performed stream and block based cryptographic approaches.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

This paper introduces a new encryption algorithm based on Tinkerbell maps and magic square. The content of the paper is organized as follows: Section III explains the new image encryption algorithm. Section IV demonstrates its simulation results and security analysis in Section V. The paper is concluded in Section VI.

III.PROPOSED ALGORITHM

The proposed algorithm for image encryption uses Tinkerbell chaotic maps and magic square. Fig. 1 shows the encryption process. It mainly consists of a secret key, 2D Tinkerbell map generation, row shifting, pixel modification, magic square generation and pixel shuffling. The proposed Tinkerbell map based algorithm uses a 128 bits long secret key. It can be a 16 character length hexadecimal key. It is further divided as 16 sub keys of 8 bits length.

$$K = K_1 K_2 \ldots\ldots K_{16} \quad (1)$$

Here K represents the secret key and $K_1, K_2 \ldots\ldots K_{16}$ represents the sub keys.

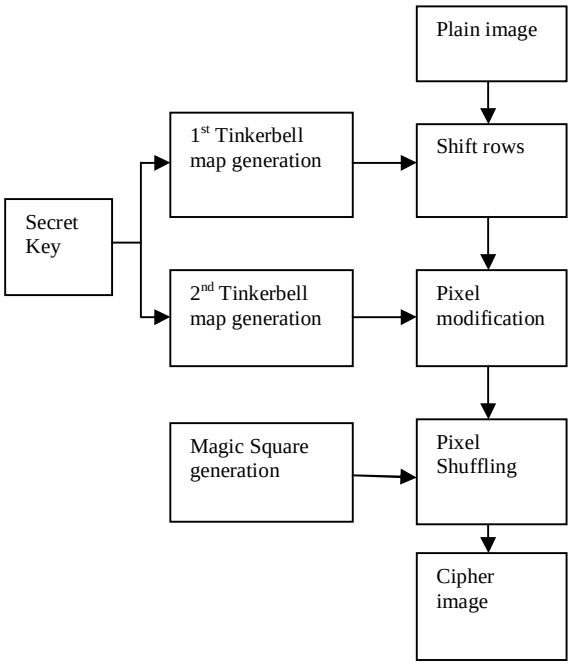

Fig.1Proposed Encryption Algorithm

3.1 2D Tinkerbell Map Generation

Tinkerbell maps are 2D chaotic maps. They are generated using the following equations:

$$p_{n+1} = p_n^2 - q_n^2 + aq_n + bq_n \quad (2)$$

$$q_{n+1} = 2p_n q_n + cp_n + dq_n \quad (3)$$

Here p and q represent the two Tinkerbell sequences and a, b, c and d are constants. The initial conditions of the maps p_0 and q_0 and the various constants affect the generation of the chaotic maps. Fig. 2 shows the Tinkerbell sequences with constants $a = 0.9$, $b = -0.6013$, $c = 2$ and $d = 0.5$ and initial conditions x_0 and y_0 as follows:

$$x_0 = \frac{\sum_n s_1(n) * (2^{n-1})}{2^{32}} \quad (4)$$

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

$$y_0 = \frac{\sum_n s_2(n) * (2^{n-1})}{2^{32}} \tag{5}$$

Where s_1 and s_2 are binary strings of sub keys as follows:

$$s_1 = K_1 K_5 K_3 \tag{6}$$

$$s_2 = K_4 K_2 K_6 \tag{7}$$

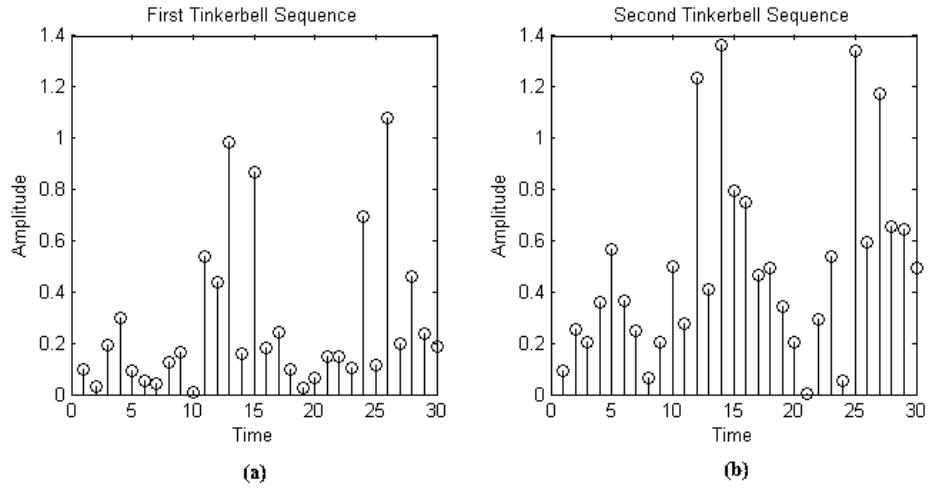

Fig. 2Tinkerbell sequences. (a)First Tinkerbell sequence. (b)Second Tinkerbell sequence.

3.2 Row Shifting

Consider the K_7^{th} number of the first chaotic sequence. If it is greater than 0.5, then downshift the rows of the secret image K_8 times, else downshift the rows K_9 times.

3.3 Pixel Modification

Based on the values of the second Tinkerbell map the pixel values of the image are modified using Table 1. R, G and B represent the red, green and blue levels of image pixels respectively. It can be obtained from the three consecutive bytes of the pixel values. The modification is performed K_{10} times. The decryption process is exactly similar to encryption process. It is the reverse of encryption operation given in the table.

Table 1. Pixel Modification

Values of second Tinkerbell Map	Operations
0 – 0.4	NOT operation
0.4 – 0.8	R XOR K_{11} G XOR K_{12} B XOR K_{13}
>0.8	NOT(R XOR K_{14}) NOT(G XOR K_{15}) NOT(B XOR K_{16})

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

3.4 Magic Square Generation

A magic square of the same size of the secret image is generated. It consists of all the numbers ranging from 1 to N*N where N*N is the size of the secret image. Fig.3(a) shows a magic square of size 5*5.

3.5 Pixel Shuffling

The modified pixels values of the plain image are further shuffled using the magic square. They are rearranged with numbers of magic square. An example of pixel shuffling is shown in Fig. 3. The pixel values of image shown in Fig. 3(b) are shuffled using magic square of same size in Fig. 3(a).

17	24	1	8	15
23	5	7	14	16
4	6	13	20	22
10	12	19	21	3
11	18	25	5	9

(a)

1	96	45	34	55
56	69	99	32	12
11	76	79	90	45
43	23	12	22	90
39	56	77	88	50

(b)

32	90	1	76	77
45	39	69	12	34
43	96	79	88	12
56	99	22	55	11
45	90	50	56	23

(c)

Fig. 3 Pixel shuffling illustration: (a) Magic square. (b) Image Pixels. (c) Shuffled pixels.

IV.SIMULATION RESULTS

The encryption performance is evaluated based on various simulation results. This section deals with the simulation results followed by its security analysis. Fig. 4 shows the encrypted and decrypted images using the proposed algorithm. The encrypted image is extremely different from the original secret image whereas the decrypted image is exactly the same of the plain secret image.

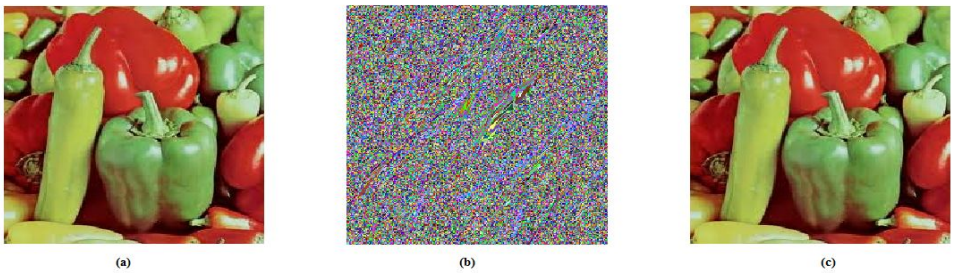

Fig. 4 Encryption: (a) Plain image (b) Encrypted image (c) Decrypted image

V.SECURITY ANALYSIS

5.1 Histogram Analysis

The histogram analysis of the images is shown in Fig.5. The histograms of the red, green and blue channels are shown and are distributed uniformly so that it is difficult for a third person to obtain any secret information from the encrypted image.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

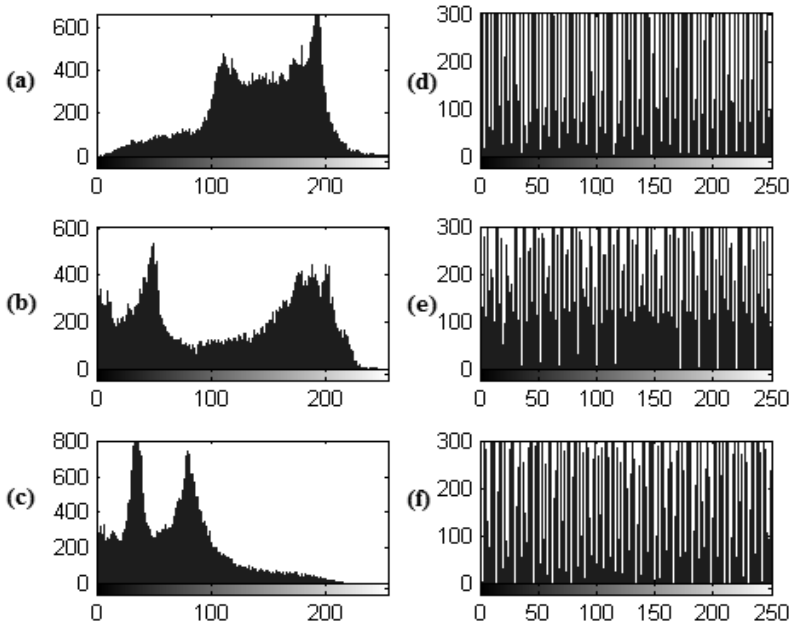

Fig. 5 Histogram analysis: (a) Histogram of red channel of plain image. (b) Histogram of green channel of plain image. (c)Histogram of blue channel of plain image. (d) Histogram of red channel of encrypted image. (e) Histogram of green channel of encrypted image. (f) Histogram of blue channel of encrypted image.

5.2 Key Space Analysis

Key space shows the various combinations of keys that can be used in the encryption process [5]. The key size of the proposed algorithm is 128 bits and there are 2128 key combinations which is sufficiently large to resist brute force attacks.

5.3 Key Sensitivity Analysis

The encryption algorithm must be highly sensitive to even small changes in the secret key. The key sensitivity analysis is performed by encrypting the plain image using key K_1 and decrypting the encrypted image using key K_2. The two keys are such that they are highly similar. The following keys are used for encryption and decryption:

K_1 = *A1B2C3D4E5F6A8B1C2*

K_2 = *A1B2C3D4E5F6A8B1C3*

Fig. 6 shows the encrypted and decrypted images using different encryption and decryption keys. The decrypted image is exactly different from the plain image and it resembles a noise image.Thus even a slight change in the secret key produces a different image and the algorithm is sensitive to the secret key. It is impossible to obtain the secret information without the knowledge of the secret key which makes the encryption algorithm more secure.

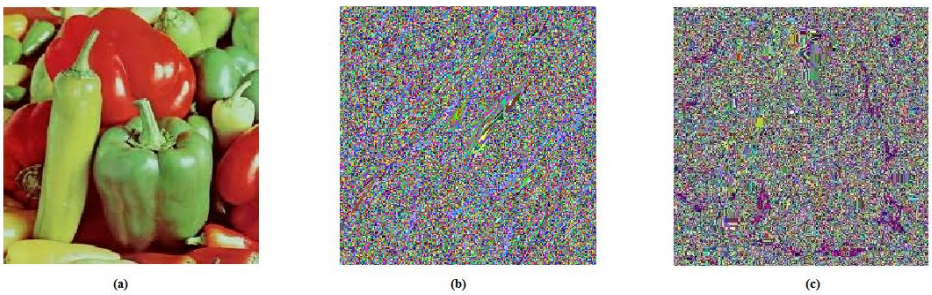

Fig. 6 Key sensitivity analysis. (a)Plain image. (b)Encrypted image using key K_1. (c)Decrypted image using key K_2.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

5.4 Correlation coefficient Analysis

For a plain image, the correlation between the adjacent pixels is usually high either in horizontal, vertical or diagonal directions. The encryption algorithm must be such that the correlation of pixels in decrypted image is reduced. The correlation [8] between a pixel pair x and y can be given as:

$$C = \frac{E[(x - M_x)(y - M_y)]}{S_x S_y} \tag{8}$$

Here *E(.)* represents the expectation and M_x and M_y represents the mean of *x* and *y* respectively. S_x and $S_y$represents the standard deviations of *x* and *y* respectively. Fig. 7 shows the distribution of pixel pairs of the plain and encrypted images along horizontal, vertical and diagonal directions.

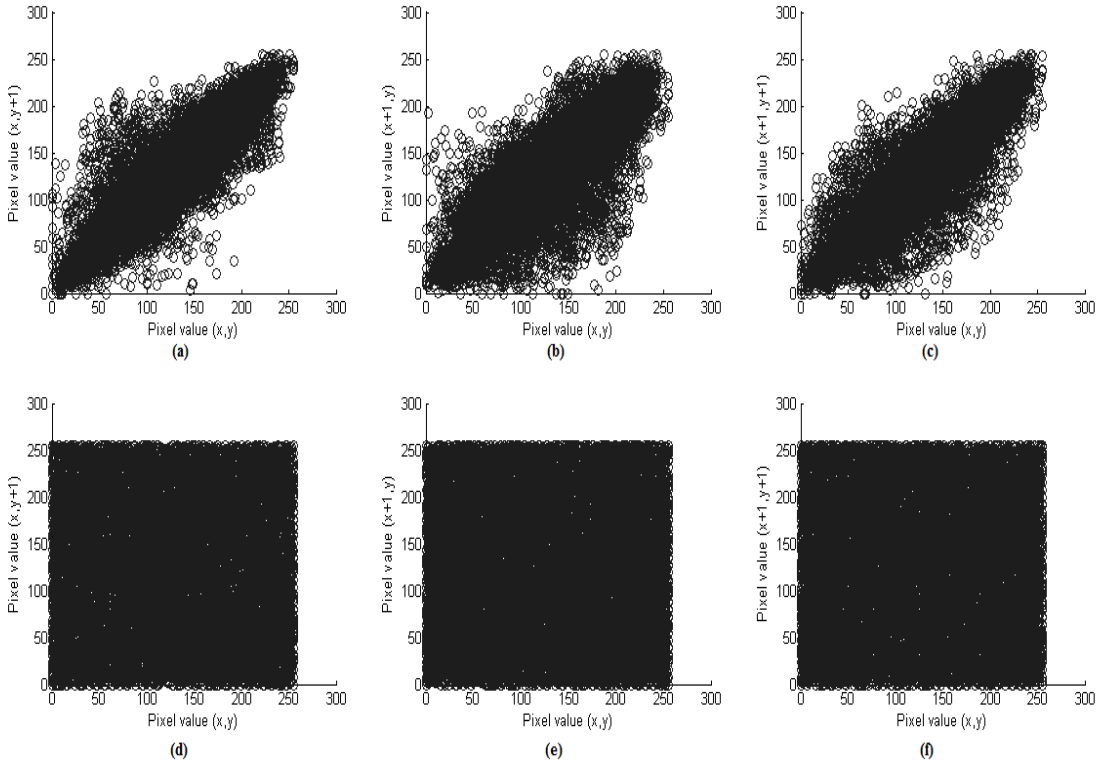

Fig. 7. Correlation of adjacent pixels: (a)Horizontal direction of the plain image. (b)Vertical direction of the plain image. (c)Diagonal direction of the plain image. (d)Horizontal direction of the cipher image. (e)Vertical direction of the cipher image. (f)Diagonal direction of the cipher image.

The neighboring pixels are distributed very close to each other in the plain image whereas in the encrypted image, the pixels are distributed randomly in various directions. This shows that the correlation of pixels is very high in plain image and low in encrypted image. This shows that the proposed encryption algorithm is highly secure. Table 2 shows the correlation coefficients of plain and encrypted images along various directions. The analysis shows that the correlation is nearly zero for the encrypted image by using the proposed encryption algorithm.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

Table 2 Correlation Coefficient

Direction	Plain Image	Cipher Image
Horizontal	0.9534	0.0011
Vertical	0.9207	-0.0046
Diagonal	0.9462	0.0012

VI.CONCLUSION

This paper presents a new image encryption algorithm using Tinkerbell maps and magic square. Based on the 2D Tinkerbell maps, row rotation and pixel modification is performed. Finally a magic square of the same size of the plain image is used for pixel shuffling. Experimental results show that the key space resists brute force attacks and this algorithm is highly sensitive to slight changes in the secret key. The correlation coefficient analysis shows that the encryption process is highly secure. The correlation coefficient values are nearly zero which shows their inability to retrieve secret information from the encrypted image without the knowledge of the secret key. Thus the proposed algorithm is secure and it can be used for real time applications.

REFERENCES

[1] N. K. Pareek, Vinod Patidar and K. K. Sud, "Image Encryption using Chaotic Logistic Map", Image and Vision Computing, pp. 926-934, Feb. 2006.
[2] H. H. Nien, S. K. Changchien, S. Y. Wu and C. K. Huang, "A new Pixel Chaotic Shuffle method for Image Encryption", 10th IEEE International Conference on Control, Automation, Robotics and Vision, Vietnam, pp. 883-887, Dec. 2008.
[3] Long Bao, Yicong Zhuo, C. L. PhilipChen and Hongli Liu, "A New Chaotic System for Image Encryption", International Conference on System Science and Engineering, China, pp. 69-73, July 2012.
[4] Zhongyu Hua, Yicong Zhuo, Chi-Man Pun and C. L. Philip Chen, "Image Encryption using 2D Logistic Sine Chaotic Map", IEEE International Conference on Systems, Man and Cybernetics, USA, pp.3229-3234, Oct. 2014.
[5] T. Goplalakrishnan, S. Ramakrishnan and M. Balakumar, "An Image Encryption using Chaotic Permuatation and Diffusion", IEEE International Conference on Recent trends in Information Technology, 2014.
[6] Santosh Chapaneri and Radhika Chapaneri, "Chaos based Image Encryption using Latin Rectangle Scrambling", Annual IEEE India Conference, INDICON, 2014.
[7] Md. Billal Hossain, Md. Toufikar Rahman, A. B. M. Saadmaan Rahman and Sayeed Islam, "A new approach of Image Encryption using 3D Chaotic map to enhance security of Multimedia component", 3rd IEEE International Conference on Informatics, Electronics and Vision, 2014.
[8] Priya R. Sankpal and P. A. Vijaya, "Image Encryption using Chaotic Map: A survey", 5th IEEE International Conference on Signal and Image Processing, pp. 102-107, 2014.
[9] Nitumoni Hazarika and Monjul Saikia, "A novel Partial Image Encryption using Chaotic Logistic map", IEEE International Conference on Signal Processing and Integrated Networks, 2014.
[10] Minal Goving Avasare and Vishaka Vivek Kelkar, "Image Encryption using Chaos Theory", IEEE International Conference on Communication, Information and Computing Technology, Mumbai, Jan 2015.