An Image Encryption Technique Using Orthonormal Matrices and Chaotic Maps

Animesh Chhotaray, Soumojit Biswas, Sukant Kumar Chhotaray and Girija Sankar Rath

Abstract Many image encryption techniques have been designed based on block based transformation techniques or chaos based algorithms. In this paper, a two stage image encryption technique is proposed. In the first stage, a new method of generating orthonormal matrices is presented and used along with sparse matrices to generate key matrices which are used to transform the original image. Since, chaos based encryption techniques are very efficient due to sensitivity to initial conditions and system parameters, this paper makes an analytical study of some recent chaos based image encryption techniques. In the second stage, the image is encrypted using one of the studied algorithms which has an optimal balance between robustness and execution time. This transformation is very fast and the overall cryptosystem is very robust which can be observed from entropy analysis, resistance to statistical and differential attacks and large key space.

Keywords Image encryption · Orthonormal matrices · Chaotic maps · Asymmetric cryptosystem · Robust · Fast · Statistical and differential attacks

A. Chhotaray (✉)
School of Computer Engineering, Kalinga Institute of Industrial Technology, Bhubaneswar, Odisha, India
e-mail: animesh.chhotaray@gmail.com

S. Biswas
School of Electronics Engineering, Kalinga Institute of Industrial Technology, Bhubaneswar, Odisha, India
e-mail: sbdisaster40@gmail.com

S.K. Chhotaray
Department of Electronics and Communication Engineering, Sardar Vallabhbhai Patel Institute of Technology, Vasad, Gujarat, India
e-mail: sukantchhotaray@gmail.com

G.S. Rath
Department of Electronics and Communication Engineering, C. V. Raman College of Engineering, Bhubaneswar, Odisha, India
e-mail: gsrath2011@gmail.com

A. Nagar et al. (eds.), *Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics*, Smart Innovation, Systems and Technologies 44, DOI 10.1007/978-81-322-2529-4_37

1 Introduction

Transmission of digital images has found its application in military image databases, confidential video conferencing, online personal photograph album etc., that require robust, fast and reliable security system to transmit digital images [1]. Hence, prevention of this image from unauthorized access has become a great security concern.

In recent years, many encryption methods have been proposed. Among them chaotic based encryption methods are considered very efficient due to their sensitivity to initial values and control parameters. Some of the commonly used chaotic maps are logistic map, tent map, sine map, piecewise linear chaotic map etc.

A matrix of integers can be used to represent an image or a part of an image. Transform matrices are used to transform the whole image or a part of it [2–5]. Let $m \times n$ represents an image I and R and S are the transform matrices of dimension $m \times m$ and $n \times n$ respectively. Then a transformed image TI of dimension $m \times n$ can be obtained by the following relation.

$$TI = RIS \tag{1}$$

The original image I can be obtained from T provided inverse of P and Q exists i.e. E can be recovered using the following relation

$$E = (R^{-1})(TI)(S^{-1}) \tag{2}$$

A matrix A is said to be orthogonal if the product of the matrix and the transpose of the matrix results in any scalar multiple of identity matrix I i.e. $A^T \cdot A = kI$, where k is any integer. A will be an orthonormal matrix if $k = 1$. Since, we are using an asymmetric cryptosystem to encrypt the original image, the public key is a product of orthonormal matrix and a sparse matrix whose inverse can be easily calculated [2].

2 Encryption

In the first stage of encryption, the cipher image is obtained using standard block based transformation algorithms. A product of orthonormal matrix and sparse matrix is used as the key matrix. In this stage, all operations are carried out in GF (p).

Sukant et al. proposed an algorithm to generate orthonormal matrices and sparse matrices and their usage in designing an asymmetric block based image encryption technique. In this paper, another algorithm for generating orthonormal matrices is presented and is multiplied with the sparse matrix S obtained using Sukant et al.'s algorithm to get the public key.

2.1 Generation of Orthonormal Matrix

A matrix 'X' generated by the following relation will be orthonormal,

$$X = \begin{bmatrix} n_1 x_{11} & n_2 x_{12} \\ n_2 x_{21} & n_1 x_{22} \end{bmatrix} \tag{3}$$

if x_{11}, x_{12} and x_{22} are orthonormal matrices, $x_{21} = -x_{22} x_{12}^T x_{11}$, $n_1^2 + n_2^2 = 1$. Here, n_1 and n_2 are integers.

With the help of this method, generation of higher order orthonormal matrices becomes very easy. Value of n_1 and n_2 can be generated with help of two integers m_1 and m_2 and using the following relations.

$$n_1 = \frac{m_1^2 - m_2^2}{m_1^2 + m_2^2},\ n_2 = \frac{2m_1 m_2}{m_1^2 + m_2^2}$$

The 8×8 orthonormal matrix (X) used to generate the public key of second stage encryption is mentioned below.

$$X = \begin{bmatrix} 9 & 12 & 234 & 175 & 44 & 102 & 137 & 250 \\ 12 & 242 & 175 & 17 & 102 & 207 & 250 & 114 \\ 151 & 9 & 205 & 165 & 213 & 209 & 188 & 222 \\ 9 & 100 & 165 & 46 & 209 & 38 & 222 & 63 \\ 40 & 24 & 129 & 112 & 177 & 32 & 10 & 106 \\ 24 & 211 & 112 & 122 & 32 & 74 & 106 & 241 \\ 179 & 174 & 46 & 173 & 222 & 188 & 89 & 33 \\ 174 & 72 & 173 & 205 & 188 & 29 & 33 & 162 \end{bmatrix} \tag{4}$$

The public key is generated by

$$key = X \cdot S \cdot X'$$

and its value is given by

$$key = \begin{bmatrix} 188 & 247 & 7 & 239 & 6 & 52 & 201 & 220 \\ 48 & 77 & 154 & 120 & 3 & 250 & 234 & 196 \\ 27 & 58 & 61 & 191 & 15 & 40 & 239 & 14 \\ 81 & 144 & 63 & 136 & 226 & 130 & 129 & 29 \\ 43 & 110 & 221 & 241 & 110 & 166 & 182 & 214 \\ 130 & 81 & 119 & 231 & 199 & 157 & 60 & 215 \\ 84 & 158 & 71 & 105 & 248 & 5 & 169 & 171 \\ 53 & 98 & 170 & 37 & 39 & 90 & 215 & 6 \end{bmatrix} \tag{5}$$

The 8 × 8 sparse matrix (S) generated by using [2] is given as

$$S = \begin{bmatrix} 31 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 7 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 191 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 8 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 47 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 127 \end{bmatrix} \tag{6}$$

The cipher image is further encrypted in the second stage using an efficient chaos based algorithm.

3 Study of Recent Chaos Based Image Encryption Techniques

Khanzadi et al. proposed an encryption algorithm based on Random Bit Sequence Generator (RBSG) using logistic and tent maps. In this algorithm, random ergodic matrices (REM) and random number matrices (RNM) are used to permute the pixels and resulting bitmaps. Random bit matrices (RBM) are used to obtain the substituted bit maps (SBM). The final encrypted image is obtained by combining the SBM's [1].

Zhou et al. proposed an chaotic encryption method using a combination of two chaotic maps. The chaotic system can be a logistic-tent or logistic-sine or tent-sine system. Random pixel insertion is done at the beginning of each row followed by pixel substitution of sub images. Each round is completed with rotation of combined sub-images. The encrypted image is obtained after four such rounds [6].

Fouda et al. proposed an image encryption technique based on piece wise linear chaotic maps (PWLCM). The solutions of Linear Diophantine Equation (LDE) are used to generate the permutation key (PK) and substitution key (SK) which in turn are used to permute and mask the image. PK and SK has new set of initial conditions whose value depend on total encrypted image. The resultant is encrypted image at the end of first round. The whole encryption process is carried out n times [7].

The above algorithms were simulated in Matlab with standard images of different resolutions under identical conditions. Cameraman (C) and lena (L) images of 256 × 256 resolution and baboon (B) image of 512 × 512 resolution with initial entropy values 7.5683, 7.0097 and 7.3579 respectively were used for simulation. The simulation results are shown in Tables 1, 2 and 3. The various metrics used for comparison are entropy (E), 2D correlation coefficient (C), NPCR, UACI, Correlation Coefficients (Horizontal (H), Vertical (V), Diagonal (D), Average (A)) and time (T) in seconds. From the above analysis, it is observed that the degree of randomness of the pixels in the encrypted image is similar in all the three methods

Table 1 Image metrics for cameraman 256 × 256 image

Method	E	C	NPCR	UACI	H	V	D	A	T (s)
Khanzadi	7.9599	0.0051	99.4858	30.4345	0.0385	0.0553	−0.0779	0.0053	156.103
Zhou	7.9970	−0.0041	99.5865	31.1852	−0.0431	0.0225	0.0581	0.0125	2.98
Fouda	7.9968	0.0061	99.5956	31.1804	0.0090	0.0078	0.0279	0.0149	25.875

Table 2 Image metrics for lena 256 × 256 image

Method	E	C	NPCR	UACI	H	V	D	A	T (s)
Khanzadi	7.9877	0.0013	99.6048	29.6489	0.0577	0.0357	0.0489	0.0474	147.48
Zhou	7.9972	0.0054	99.6017	30.4247	−0.0227	−0.0156	−0.0069	−0.0151	2.92
Fouda	7.9971	0.0061	99.6017	30.2863	0.0026	0.0023	−0.0049	0.00004	23.448

Table 3 Image metrics for baboon 512 × 512 image

Method	E	C	NPCR	UACI	H	V	D	A	T (s)
Khanzadi	–	–	–	–	–	–	–	–	Very high
Zhou	7.9993	0.0027	99.5979	27.8237	0.0257	0.0307	−0.0478	0.0029	8.00
Fouda	7.9992	0.0015	99.6124	27.8334	0.0156	−0.0393	0.0804	0.0189	252.388

and all other parameters have nearly similar values except execution time. Since the execution time of method 1 and method 3 is very high compared to method 2, Zhou's method will be used to perform second stage encryption.

4 Results and Security Analysis

The two stage encryption algorithm is tested with the same set of metrics and images used previously to analyse the three chaotic based image encryption algorithms and the results are presented below.

From Tables 1, 2, 3 and 4, it can be observed that the proposed technique's execution time is still substantially less than Khanzadi and Fouda's methods. The image metrics do not show significant deviation.

Table 4 Image metrics for proposed algorithm

Image	E	H	V	D	A	UACI	NPCR	C	T (s)
Cameraman (256)	7.9972	0.0431	0.0147	0.0189	0.0256	31.0643	99.5514	0.0047	2.71
Lena (256)	7.9973	−0.0086	−0.0339	−0.0186	−0.0204	30.5578	99.5880	0.0028	2.76
Baboon (512)	7.9992	−0.0076	−0.0439	0.0292	−0.0074	27.8128	99.6033	0.0022	7.76

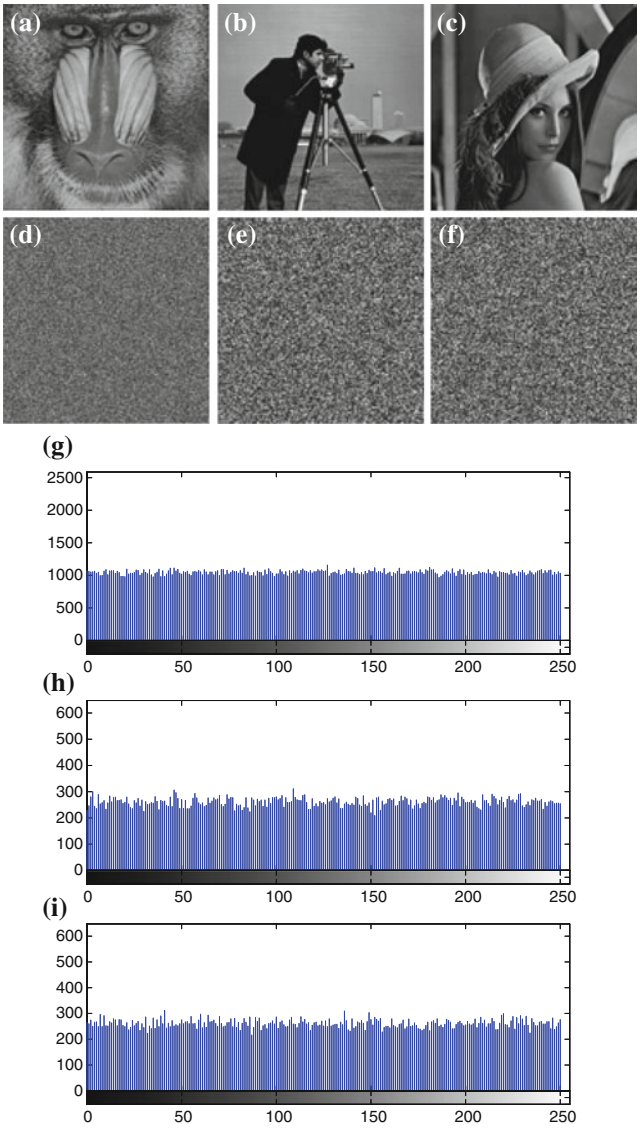

Fig. 1 Simulation results of proposed algorithm. **a** Baboon. **b** Cameraman. **c** Lena. **d** Encrypted baboon. **e** Encrypted cameraman. **f** Encrypted Lena. **g** Encrypted baboon histogram. **h** Encrypted cameraman histogram. **i** Encrypted Lena histogram

4.1 Keyspace

Due to two-stage encryption, brute force attack becomes very difficult as the number of keys becomes very large. In the second stage encryption there are six parameters whose initial value can be between 0 and 4. If 14 decimal places are considered, then number of keys equals 10^{84} [6]. For p = 251, number of 2 × 2 orthonormal matrices are 124,749 [2]. With increase in dimension of matrix and change in value of p the number of orthonormal matrices increases by significant magnitude. For p = 251, around 251^n n × n sparse matrices can be generated. Similar to orthonormal matrices, the number of sparse matrices also increases as value of p changes and alternate representation of sparse matrices are considered. Hence, the key space of the proposed algorithm is huge and can easily thwart any brute force attack.

4.2 Statistical and Differential Analysis

From Fig. 1 it is evident that all the pixels of the final encrypted image are uniformly distributed and hence prevent chosen-cipher text attack. Also, the ciphered images are completely scrambled leaving no trace of original image. The correlation between the pixels of encrypted image and original image is very low which is evident from the correlation coefficients and high entropy value. Differential attack is difficult due to large NPCR and low UACI values. Some of the figures of simulation are shown in the following figure.

4.3 Comparison

The proposed algorithm is compared with AES (128) and algorithms by Khanzadi and Fouda. The former comparison can be done using Tables 4 and 5 whereas the latter can be done using Tables 1, 2, 3 and 4. The proposed algorithm has very small execution time whereas the NPCR, UACI, entropy and correlation coefficient values vary by a non-significant magnitude.

Table 5 Performance metrics with AES (128)

Image	AES (128)				
	E	C	NPCR	UACI	T (s)
Lena (256)	7.9971	0.0023	99.6185	30.5049	69.31
Cameraman (256)	7.9992	0.0077	99.63	31.03	69.93
Baboon (512)	7.9992	0.0037	99.5975	27.8054	283.65

5 Conclusion

In this paper, a two-stage encryption algorithm is proposed. In the first stage, an asymmetric block based encryption technique is used in which the public key is a product of an orthonormal matrix and a sparse matrix. A new method of generating orthonormal matrices is also introduced. The cipher image is further encrypted by a chaos based algorithm proposed by Zhou et al. Since, all operations in the first stage are carried in GF (251), matrix inversion becomes very difficult and hence finding the inverse of the public key is cumbersome. The total number of keys for the entire algorithm is huge which makes brute force attack very difficult. Statistical attack is very difficult since the encrypted images are completely scrambled and correlation coefficients are low. Differential attack is unlikely which is evident from the high NPCR value and low UACI value. Apart from the security aspect, the proposed algorithm has low computational complexity which is evident from the small execution time. Hence, the proposed algorithm is very efficient.

References

1. Khanzadi, H., Eshgi, M., Borujeni, S.E.: Image encryption using random bit sequence based on chaotic maps. Arab. J. Sci. Eng. **39**, 1039–1047 (2014)
2. Chhotaray, S.K., Chhotaray A., Rath, G.S.: Orthonormal matrices and image encryption. In: International Conference on Devices, Circuits and Communication (ICDCCOM), pp. 1–5, BIT Mesra, Ranchi, India (2014). doi:10.1109/ICDCCom.2014.7024732
3. Cui, D., Shu, L., Chen, Y., Wu, X.: Image encryption using block-based transformation with fractional Fourier transform. In: 8th International ICST Conference on Communications and Networking, pp. 552–556 (2013)
4. Younes, M.A.B., Jantan, A.: Image encryption using block-based transformation algorithm. IAENG Int. J. Comput. Sci. **35**, 1 (2008)
5. Karagodin, M.A., Osokin, A.N.: Image compression by means of Walsh transforms. In: IEEE Transactions on Modern Techniques and Technologies (MTT), pp. 173–175 (2002)
6. Zhou, Y., Bao, L., Chen, C.L.P.: A new 1D chaotic system for image encryption. Sig. Process. **97**, 172–182 (2014)
7. Fouda, J.S.A.E., Effa, J.Y., Sabat, S.L., Ali, M.: A fast chaotic block cipher for image encryption. Commun. Nonlinear Sci. Numer. Simul. **19**, 578–588 (2014)