Malaysian Journal of Computing and Applied Mathematics 2020, Vol 3(1): 27-34
©Universiti Sultan Zainal Abidin
(Online)

MALAYSIAN JOURNAL OF COMPUTING AND APPLIED MATHEMATICS

A Novel Image Encryption Approach Using Polar Decomposition and Orthogonal Matrices

***Oussama Noui*[a]*, Amine Barkat*[b]*, Assia Beloucif*[c]**

[a]Department of Physics, Faculty of Sciences of Matter, University of Batna1, Algeria
[b]Department of Electronics, Information, and Bioengineering, Politecnico di Milano, Italy
[c]Institute of Hygiene and Industrial Safety, University of Batna2, Algeria

*Corresponding author: oussama.noui@univ-batna.dz

Received: 13/10/2019, Accepted: 23/02/2020
http://dx.doi.org/10.37231/myjcam.2020.3.1.40

Abstract

Information security is one of the important issues in the information age, image encryption algorithms have been increasingly studied to guarantee the secure image transmission over the internet and through wireless networks. In this article, we propose a new approach for image encryption based on polar decomposition and orthogonal matrices. This scheme offers good confusion and diffusion qualities. The proposed algorithm is shown to be secure against important cryptanalytic attacks (statistical attacks, sensitivity dependence, differential attacks, brute force attacks...), theoretical analysis and computer simulations both confirm that it has a high security level.

Keywords: Encryption, security, digital image, orthogonal matrix, polar decomposition, information

INTRODUCTION

In recent years digital image processing technology and network technologies have been developed rapidly, a vast number of digital images are now transmitted and shared over the Internet; Confidentiality of such content became an important issue nowadays. Furthermore, the conventional encryption methods such as RSA AES, IDEA, DES, 3DES etc. (Singh and Supriya, 2013)., are computationally intensive because they consume more time and are not suitable for images, this is due to the digital image properties like high redundancy, bulk volume and high correlation among adjacent pixels.

To meet this challenge, a variety of encryption schemes have been proposed, (Chen et al. 2004; Wang et al., 2016; Tang et al., 2016; Yang et al., 2010; Fu et al., 2011; Mannai et al., 2015; Chen et al., 2015; Zhao et al., 2015; Kanso & Ghebleh, 2015), recently there has been a growing interest in chaotic based image encryption, because they offer good properties in many concerned aspects regarding speed, security, computing power, complexity and computational overhead. The security of the cryptosystems based on chaotic stands on the used chaotic map and the adopted architecture, some chaotic based methods have security problems which are related to the small size of secret key and to the used chaotic map properties (Bechikh et al., 2015; Akhavan, 2015; Rhouma, 2008; Li, & Xuan, 2002).

In this paper we concentrates on developing of highly robust encryption scheme which offer good confusion by using the polar decomposition and the orthogonal matrices and offers good diffusion qualities based on the polynomial permutation matrix, and to ensure popular security factor, and to prevent statistical, differential and exhaustive attacks, and to be economically in term of time complexity.

Organization of the rest of this paper is as follows: Section II explains the related knowledge, including the polar decomposition, the singular values decomposition and the polynomial permutation, section III presents the encryption and decryption algorithms and the key generation procedure, in section IV we study the performance and the security analysis, including statistical analysis and sensibility analysis, whereas the summary of results and the conclusion is presented in Section V.

RELATED KNOWLEDGE

A. Polar decomposition

Let be a matrix with real entries, the left polar decomposition of is with is orthogonal and is symmetric matrix with non-negative eigenvalues.

B. Singular values decomposition (SVD)

A notion is closely related to the polar decomposition is the singular values decomposition:

Theorem 1 (Golub & Van Loan, 1983).
For any real $n \times n$ matrix A of rank r, we have

$$A = USV^t \qquad (1)$$

where U and V are two orthogonal matrices and S is a $n \times n$ diagonal matrix $S = (\partial_1, \dots, \partial_r, 0, \dots, 0)$ such that $\partial_1 \geq \cdots \geq \partial_r \geq 0$ are the singular values of A.

C. Computation of the polar form from SVD

It is easy to go from the SVD to the polar form:

$$A = USV^t = (USU^t)(UV^t) \qquad (2)$$

Put $P = USU^t$ (P is symmetric matrix with non-negative eigenvalues). And $Q = UV^t$ (Q is the product of two orthogonal matrices then, Q is so). Hence, $A = PQ$ is the polar form of A.

D. Permutation polynomial modulo 2^n

A polynomial $f(x)$ with integral coefficients is said to be a permutation polynomial over a finite ring R if f is one to one map of R onto itself. In Rivest (2001) proved that a polynomial

$$f(x) = a_1 + a_2 + \cdots + a_d x^d \in Z[x]$$

is a permutation polynomial module 2^n, $n > 1$, if and only if a_1 is odd, $(a_2 + a_4 + \cdots\ )$ and $(a_3 + a_5 + \cdots\ )$ are even.

PROPOSED METHOD

Let $A = (a_{ij})$ be a gray scale image of size n, (we take $n = 256$ for tests), the proposed encryption scheme follows these steps:

A. Image encryption

Let A be an image of size 256.
Input: three keys: K_1, K_2, K_3 to generate respectively three matrices:
U_1 is 256×256 orthogonal matrix with real entries.
U_2 is permutation matrix of order 256.
$D = (\pm 1)$ is a diagonal matrix of size 256.

Output: A^*: The encrypted image
1. Apply SVD and polar decomposition to $A = USV^t = PQ$
2. Compute $P^* = P^{U_1} = U_1 P U_1^t$
3. Calculate $Q^* = DU_1 Q U_1 U_2$

4. Calculate the cipher image $A^* = P^*Q^*$

B. *Image decryption*

Input: A^*: The encrypted image, the three keys: K_1, K_2, K_3

1. Apply polar decomposition to $A^* = P^*Q^*$
2. Calculate $P = P^{*U_1^t} = U_1^t P^* = U_1^t P^* U_1$
3. Calculate $Q = U_1^t D Q^* U_2^t U_1^t$
4. Finally, compute the original image $A = PQ$

C. *Generation of U_1*

Using the method in Oussama et al., (2017) to generate an 256×256 orthogonal matrix U_1 from a random sequence
$K_1 = (x_1, \dots, x_{255})$ we put

$$A_0 = \begin{pmatrix} 0 & -x_1 & \dots & -x_{255} \\ x_1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ x_{255} & 0 & \cdots & 0 \end{pmatrix}$$

and $\partial = \sqrt{x_1^2 + \cdots + x_{255}^2}$.

Then,

$$U_1 = I_{256} + \frac{sin\partial}{\partial} A_0 + \frac{1 - cos\partial}{\partial^2} A_0^2$$

is orthogonal.

To obtain a good sensitive dependence, we generate the sequence K_1 from a logistic map $x_{n+1} = \mu x_n(1 - x_n)$ with the initial value $x_0 = [0,1]$ and $\mu = [3.57,4]$ so the first key $K_1 = \{x_0, \mu\}$ is needed to generate the orthogonal matrix U_1.

D. *Generation of permutation matrix U_2*

In order to construct, U_2 we use the permutation polynomial modulo $2^8 = 256$. Indeed, we choose an integer a_0 and an even integer a_2 from $\{1, \dots, 256\}$ then, by (*), the polynomial $P(x) = a_0 + x + a_2 x^2$ define a permutation in the set $\{1, \dots, 256\}$.

Let U_2 the permutation matrix associated to $P(x)$. Hence for the generation of U_2 we need the key $K_2 = \{a_1, a_2\}$.

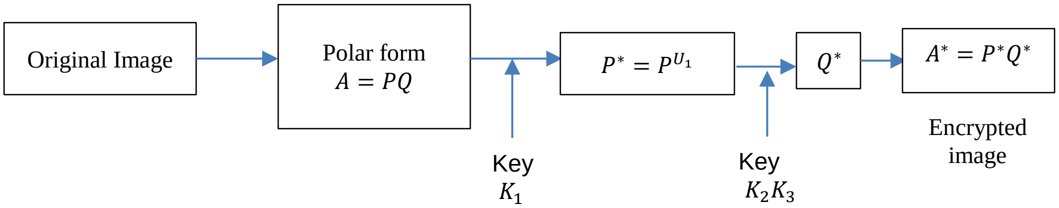


Figure 1. Block diagram of the encryption procedure.

For generation of D we choose randomly a binary sequence K_3 of length 256, we replace the 0 by -1, the obtained sequence forms the diagonal of D. Figure 1 illustrates the block diagram of the proposed algorithm.

PERFORMANCE AND SECURITY ANALYSIS

To study the feasibility of our image encryption scheme, we analyse its security against common cryptanalysis attacks.

A. Key space analysis

Generally, the security of an encryption algorithm mainly stands on its security key design (Beloucif et al., 2016). The proposed method has a sufficiently large key space and high key sensitivity. The secret key in the proposed algorithm consists of three parts: K_1, K_2, K_3.

For the first key, $K_1 = \{x_0, \mu\}$ according to the IEEE floating point standard, the number of possible values of K_1 is about $10^{15} \times 10^{15}$.

For the second key $K_2 = \{a_0, a_2\}, a_0, a_2 \in \{1, \dots, 256\}$ as a_2 is even, we have 256×128 combinations. As the key K_3 is a random binary sequence of length 256 we have 2^{256} combinations to obtain the third key, thus size of key space of our scheme is greater than $10^{30} \times 256 \times 128 \times 2^{256} > 2^{360}$, hence the key space is large enough to resist brute force attack.

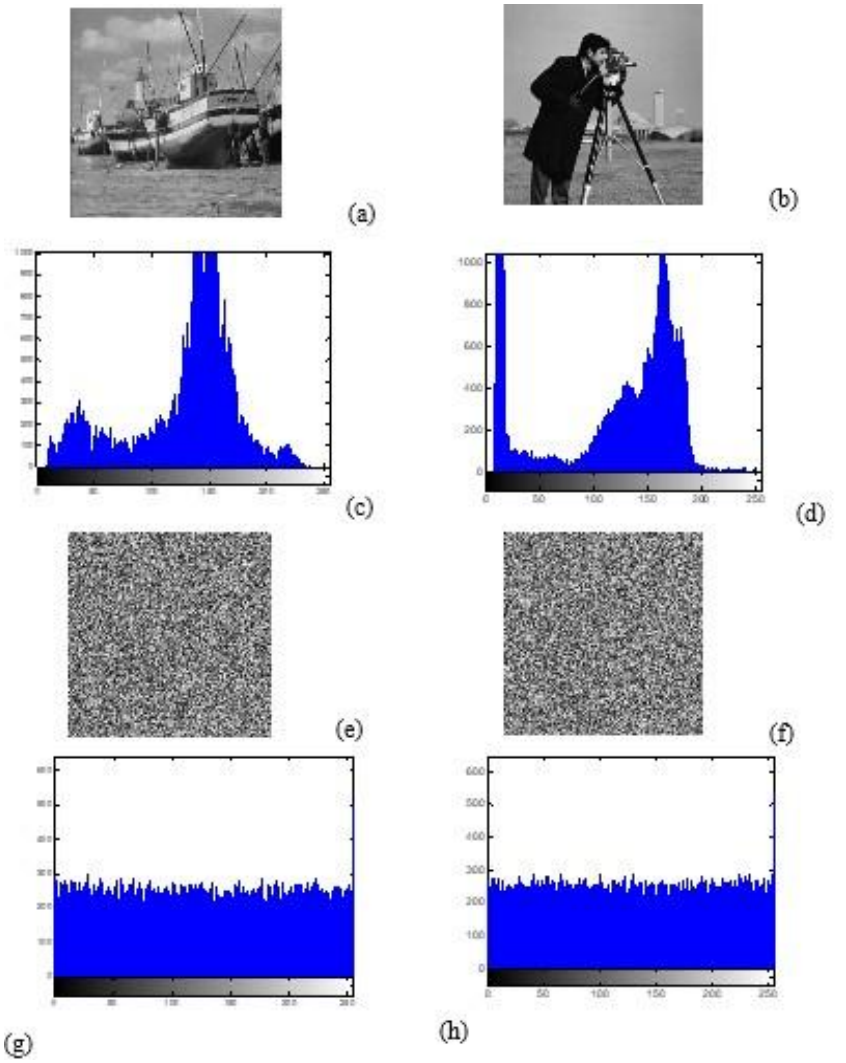


Figure 2. Statistical analysis

B. Cipher image only attack

The illegal user needs to obtain the keys K_1, K_2, K_3 from the cipher image

$$A^* = (U_1 P U_1^t)(D U_1) Q (U_1 U_2) \tag{3}$$

If we encrypt A, on m rounds, we obtain the cipher image

$$A^{(m)} = U_1^m P (U_1^t)^{(m)} (D U_1)^{(m)} Q (U_1 U_2)^{(m)} \tag{4}$$

Hence the calculation of U_1, U_2 and D from (3) or (4) becomes ineffective.

C. Statistical analysis

According to Shannon's theory, a secure cryptographic scheme should be strong enough to resist statistical attack. For the statistical analysis, our image encryption scheme is tested using most known statistical measures which includes histogram, information entropy and adjacent correlation analysis, in the first experiment we encrypted two images of size 256, Figure 2 as (a, b), as its seen in Figure 2, the histogram charts of both encrypted test images (g, h) are uniform which represents the distribution intensity of pixels values in the encrypted image, this results makes statistical attacks difficult.

Table 1. Entropy results for the cipher images

Encrypted image	Cameraman	Boat	Baboon	Lena	Peppers
Entropy	7.9325	7.9520	7.9461	7.9801	7.9932

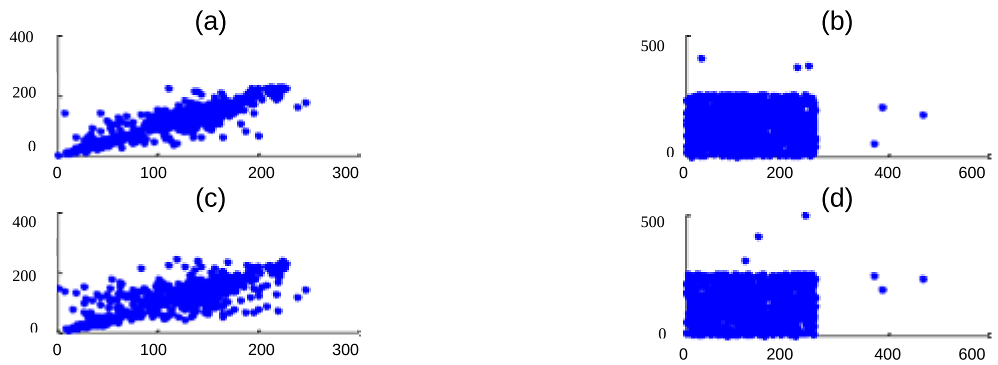
The uniformity is justified by chi-square test, which is described by the following expression

$$x^2 = \sum_{k=1}^{256} \frac{(V_k - 256)^2}{256} \tag{5}$$

where k is the number of gray levels (256), V_k is the observed occurrence frequencies of each gray level (0–255). The lower value of the chi-square value indicates a better uniformity. The second statistical measure is the entropy which is one of the best functions for calculating and measuring the randomness of image encryptions algorithms. The information entropy *H(m)* of a message source *m* can be computed as

$$H(m) = \sum_{k=1}^{2^n-1} p(m_i) \log_2 \frac{1}{p(m_i}. \tag{6}$$

Ideally, the information entropy should be 8 bits for grayscale images. If an encryption scheme generates an output cipher image whose entropy is less than 8 bits, then there would be a possibility of predictability, which may threaten its security. Simulation results for entropy analysis are shown in Table 1. It is clear from Table 1, that the values of entropy of the encrypted test images are very close to theoretical value of 8 bits.



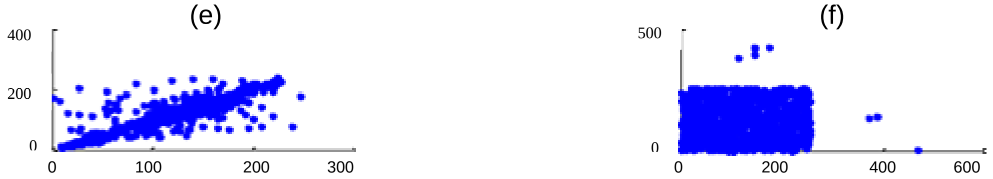


Figure 3. Correlation of two adjacent pixels
(a) Distribution of two horizontally adjacent pixels in the plain image, (b) Distribution of two horizontally adjacent pixels in the cipher-image, (c) Distribution of two diagonally adjacent pixels in the plain-image, (d) Distribution of two diagonally adjacent pixels in the cipher-image, (e) Distribution of two vertically adjacent pixels in the plain-image, (f) Distribution of two vertically adjacent pixels in the cipher-image.

This implies that our encryption algorithm is secure against entropy attack, while the third measure is the correlation analysis, Correlation determines the connection between two variables. In other terms, correlation is a measure that determines level of similarity between two variables. Correlation coefficient is a useful evaluation to judge encryption quality of any cryptosystem. Generally, for any plain image, each pixel is highly correlated with its adjacent pixels in all the three directions: horizontal, vertical and diagonal. A good encryption will erase this correlation between adjacent pixels. The correlation coefficients were calculated using the following equations:

$$C = \frac{\frac{1}{N}\sum_{I=1}^{N}(x_i - \bar{x})\,(y_i - \bar{y})}{\sqrt{\left(\frac{1}{N}\sum_{I=1}^{N}(x_i - \bar{x})^2\right)\left(\frac{1}{N}\sum_{I=1}^{N}(y_i - \bar{y})^2\right)}}$$

with

$$\bar{x} = \frac{1}{N}\sum_{I=1}^{N} x_i\,, \qquad \bar{y} = \frac{1}{N}\sum_{I=1}^{N} y_i$$

where x and y are grey-level values of the two adjacent pixels in the image. The correlation distributions of Cameraman test image are shown in Figure 3.

SENSIBILITY ANALYSIS

A. Chosen plaintext attack.

The attacker has obtained access to the encryption machinery, he makes a minor change of the plain text and examines the obtained cipher text. As the values of NPCR and UACI are larger, the large changes in the cipher text do not give any useful information to the attacker.

NPCR and UACI: number of pixel change rate (NPCR) and unified average change intensity (UACI) are two common measures used to examine the impact of one pixel modify on the whole image, encrypted by an algorithm. NPCR measures the percentage of the number of different pixels to the total number of pixels. In brief NPCR, it means that the number of pixels change rate of ciphered image while one pixel of plaintext image is changed.

Let C_1 and C_2 be two different cipher-images whose corresponding plaintext images are differ by only one bit. Label the grayscale value of the pixel at grid (i, j) in C_1 and C_2 by $C_1(i, j)$ and $C_2(i, j)$ respectively. Define an array, D, the same size as images C_1 and C_2. Then $D(i, j)$ is determined by $C_1(i, j)$ and $C_2(i, j)$ namely, if $C_1(i, j) = C_2(i, j)$ then $D(i, j) = 0$, otherwise, $D(i, j) = 1$. The NPCR is defined as:

$$NPCR = \frac{\sum_{i,j} D(i, j)}{W \times H} \times 100\% \qquad (7)$$

where W and H are the width and height of cipher images C_1 and C_2. To examine the average intensity of differences between the images, UACI is used to check the impact of one-pixel change, UACI is defined as:

$$UACI = \frac{1}{W \times H} = \left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255} \right] \times 100\%$$

Table 2 shows the NPCR and UACI results of our method on a different test images, the obtained results prove that the proposed method can resist differential attack.

Table 2. NPCR and UACI of encrypted-images

Test images	**Lena**	**Cameraman**	**Baboon**	**Boat**	**Peppers**
NPCR	99.5230	99.6902	99.2131	99.6150	99.3874
UACI	31.2013	32.0626	33.1245	32.5132	31.8709

B. Remarks.

1. The key $K = K_1 \| K_2 \| K_3$ of the proposed scheme is flexible, we have the ability to increase the size of the key, for example for K_2, we take a polynomial of degree r, $P(x) = a_0 + a_1 + \cdots + a_r x^r$ and $K_2 = \{a_0, a_1, \dots a_r\}$ such that a_1 is odd $a_2 + a_4 + \cdots$ and $a_3 + a_5 + \cdots$ are even.
2. The key length and the number of rounds are chosen following the desired level of security

CONCLUSION

The security is an essential part of any communication system. This paper proposed an image encryption based on polar decomposition and orthogonal matrices. Permutation matrix is used to achieve the diffusion property; the orthogonal matrix is used to realize the confusion property. Theoretical analysis and experimental results show that the proposed scheme able to resist known attacks, the used algorithm has a flexible key, its length is chosen following the desired security level.

References

Akhavan A, Samsudin A, and Akhshani A. (2015). Cryptanalysis of an improvement over an image encryption method based on total shuffling. *Optics Communications 350,* 77-82.

Bechikh R, et al. (2015). Breaking an image encryption scheme based on a spatiotemporal chaotic system. *Signal Processing: Image Communication 39,* 151-158.

Beloucif A, Oussama N, and Lemnouar N. (2016). Design of a tweakable image encryption algorithm using chaos-based schema. *International Journal of Information and Computer Security 8*(3), 205-220.

Chen G, Mao Y, and Chui C K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons & Fractals 21(3)*, 749-761.

Chen J, et al. (2015). A fast chaos-based image encryption scheme with a dynamic state variable selection mechanism. *Communications in Nonlinear Science and Numerical Simulation* 20(3), 846-860.

Fu C, et al. (2011). A novel chaos-based bitlevel permutation scheme for digital image encryption. *Optics communications, 284*(23), 5415-5423.

Golub G H and Van Loan C F. (1983). *Matrix Computations*, Johns Hopkins University Press, Baltimore, MD.

Kanso A and Ghebleh M. (2015). An efficient and robust image encryption scheme for medical applications. *Communications in Nonlinear Science and Numerical Simulation 24*(1), 98-116.

Mannai O, et al. (2015). A new image encryption scheme based on a simple first-order time-delay system with appropriate nonlinearity. *Nonlinear Dynamics 82*(1-2), 107-117.

Oussama N, Beloucif A, and Noui L. (2017). Secure image encryption scheme based on polar decomposition and chaotic map. I*nternational Journal of Information & Comm Tech 10*(4), 437-453.

Rhouma R. (2008). Cryptanalysis of a new image encryption algorithm based on hyper-chaos. *Physics Letters A 372(38),* 5973-5978.

Rivest R L. (2001). Permutation polynomials modulo 2^n, F*inite fields and their applications, 7,* 287- 292.

Li S and Zheng X. (2002). IEEE International Symposium on Circuits and Systems. Proceedings (Cat. No.02CH37353), Phoenix-Scottsdale, AZ, USA, 2002, pp. II-II.

Singh G and Supriya A. (2013). A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. *International Journal of Computer Applications 67*(19), 33-38.

Tang Z, et al. (2016). Multiple-image encryption with bit-plane decomposition and chaotic maps. *Optics and Lasers in Engineering 80,* 1-11.

Wang B, et al. (2016). Evaluating the permutation and diffusion operations used in image encryption based on chaotic maps. *Optik,* - *Int. J. Light Electron Opt 127*(7), 3541-3545

Yang H, et al. (2010). A fast image encryption and authentication scheme based on chaotic maps. *Communications in Nonlinear Science and Numerical Simulation 15*(11), 3507-3517.

Zhao J, et al. (2015). A novel image encryption scheme based on an improper fractional order chaotic system. *Nonlinear Dynamics 80*(4), 1721-1729.