Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/120414

A New Transformation for Chaotic Image Encryption based on the Arnold Cat Map

V. J. Subashini[1,*] *and S. Poornachandra*[2]

[1] Department of Computer Science and Engineering, Jerusalem College of Engineering, Chennai, India
[2] Department of Electronics and Communicaiton Engineering, Excel Engineering College, Namakkal, India

Received: 7 Nov. 2017, Revised: 14 Jun. 2018, Accepted: 22 Jun. 2018
Published online: 1 Jul. 2018

Abstract: Encryption is a technique used to enhance the security of a file by rendering its contents incomprehensible. The habitual transmission of digital images requires that they are made impervious to unauthorized access. It is, however, tedious to encrypt or decrypt images directly. The Arnold transform, better known as the Arnold cat map, is the most commonly used chaos-based image encryption technique that works by shuffling image pixels. A modified form of the general Arnold cat map is proposed in this article. Arnold cat map uses only shearing, whereas the proposed method utilizes both interweaving and shearing. Like Arnold transform, the proposed method also reconstructs the original image after a certain number of cycles (iterations). The proposed method takes more than twice the number of cycles as Arnold's to bring back the original image.

Keywords: Chaos, image encryption, Arnold cat map, Arnold transform, iterations, period.

1 Introduction

With the rapid advancement of multimedia technology on the Internet, vital information increasingly becomes available in the form of images and videos, with security becoming a serious issue. Images can be secured by means of encryption. Owing to certain intrinsic characteristics of images like high data redundancy, strong correlation among neighbouring pixels and bulk data capacity, however, image encryption differs from that of text. Consequently, algorithms suitable for textual data may not be as appropriate for images. Despite the sizeable number of image encryption algorithms in existence, image scrambling is a common method employed to encrypt image data so as to hide content from unauthorized users. Chaotic maps are useful in ensuring the security of digital images by means of scrambling, because they are easy to generate but deterministic and difficult to predict. The base of these maps is a combination of substitution and diffusion [1]. In the substitution stage, the chaotic map shuffles image pixels and in the diffusion stage, pixel values are altered.

The Arnold transform, a chaotic map, is an effective image scrambling tool used widely in digital image scrambling. The transform is used in watermarking algorithms to scramble watermark images [2,3,4], so as to enhance their privacy and robustness. An image encryption scheme presented in [5] combines shuffling positions and changing the gray values of the image pixels to set off confusion in the relationship between the cipher image and the plain image. Here, the Arnold cat map shuffles the positions of the image pixels in the spatial domain. But the author of [6] found the scheme presented in [5] unable to resist chosen-plaintext attacks and known-plaintext attacks, and based on the scheme in [5], proposed a modified scheme in [6] which can resist both types of attacks. The Arnold transform augments security [7] and scrambles image slices to enhance security [8] so that an authenticated receiver with an appropriate key alone can descramble the images.

The authors of [9] have proposed a fragile watermarking algorithm in which the Arnold cat map scrambles the original image before the watermark is embedded into it. Encryption schemes are proposed, based on the Arnold transform, along with other chaotic maps such as the Henon [10] and quantum [11] chaotic maps. A cryptosystem for RGB images is designed in [12] with the affine hill cipher (AHC) over the $SL_n(F_q)$ and $M_n(F_q)$ domains, along with the Arnold transform. Based on the generalized Arnold transform, an image

[*] Corresponding author e-mail: vjsubashini@yahoo.co.in

zero-watermarking scheme with spread spectrum and de-spreading (SSD) techniques is presented in [13]. An optical multiple-color image security system based on the generalized Arnold map in the gyrator transform domain is investigated by [14]. In [15] a double image encryption algorithm is designed by using Arnold transform and discrete angular transform. The Arnold transform is used to obtain the embedding positions of the watermark in [16]. A quantum realization of the generalized Arnold transform is designed in [17].

In most cases, as exemplified in the literature above, the Arnold transform serves its basic purpose, that of scrambling image pixels. The result is utilized for various purposes like watermarking and enhancing security. A new transformation method proposed in this article is based on the Arnold cat map and mainly deals with increasing the key space by much more than the one offered by the Arnold transform. Also, the proposed transformation shuffles the pixels better at the earliest iterations than the Arnold, thus rendering the proposed transformation eminently appropriate for real-time applications.

The rest of this article is organized as follows. Section 2 describes the Arnold transformation for an image. The proposed new transformation is detailed in Section 3. The investigations undertaken on the proposed method are given in Section 4. The applications of the proposed method are briefly dealt with in Section 5. Finally, the conclusion on the findings is presented in Section 6.

2 General Arnold Transform

The Russian mathematician, Vladimir Arnold, proposed a chaotic transformation termed the Arnold transformation or Arnold cat map [18], while working on the ergodic theory. The implementation of the transformation is very simple: a matrix transforms the coordinate positions in an original image and the image is confused with an increased number of iterations. The original image is restored after reaching a certain number of iterations, and the number of iterations is the key to the transform.

The transformation randomizes the original organization of its pixels. The number of iterations taken to regenerate the original image is called the Arnold period. To encrypt, a number less than the period is chosen as the encryption key. In general, the Arnold transform [4,16] is expressed as

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{1}$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} ab+1 & a \\ b & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{2}$$

where a and b are any positive integers, N is the order of the square image and $x,\ y,\ x',\ y' \in \{1,2,3,\ldots,N\}$. Equations (1) and (2), specifically, [2,5,6] can be represented as

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{3}$$

and

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{4}$$

respectively. In equations (3) and (4), (x,y) represents the position of a pixel in the original image; (x',y'), the position of the pixel in the transformed image; and N the order of the image.

3 The Proposed Transform

The proposed transformation matrix uses the basic principle behind Arnold's transformation matrix. Arnold's transformation matrix is based on the shearing transformation both in the x and y directions, as given below, where the shearing factor is considered to be one.

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \tag{5}$$

The matrices in (5) represent the horizontal (shear parallel to the x-axis) and vertical (shear parallel to the y-axis) shears respectively. In addition to the matrices in (5), the proposed method considers two more shearing transformation matrices given in (6).

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \tag{6}$$

These matrices not only shear but also interweave, i.e., the pixels are laterally shifted in relation to each other and blend closely. The affine transformation matrices shown in (7) are then formed by multiplying the matrices in (5) and (6).

$$\begin{bmatrix} 1 & 4 \\ 1 & 3 \end{bmatrix} \text{ and } \begin{bmatrix} 3 & 1 \\ 4 & 1 \end{bmatrix} \tag{7}$$

Thus the proposed transformation can be stated as in Equations (8) and (9).

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 4 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{8}$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 4 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{9}$$

The matrices in (7) are formed, based on the order in which the shearing occurs. If u and v are the shears along the x-axis and y-axis respectively, then by the order of their first occurrence, (i) the shear along the x-axis and (ii) the shear along the y-axis, and the general transformation matrix for the proposed method can be expressed as in (10) and (11) respectively.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & u+1 \\ 1 & u \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{10}$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} v & 1 \\ v+1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{11}$$

In the equations (10) and (11), the values of u and v are any positive integer $4n+3$, $n \geq 0$, N, the order the image, (x,y), the pixel positions in the original image and (x',y') is the pixel position in the transformed image.

Like the Arnold cat map [20], the proposed transformation is also an automorphism and both one-to-one and onto. The mapping of the transform can be defined as in (12) and (13).

$$\Gamma : (x,y) \rightarrow (x+(u+1)y, x+uy) \bmod N \tag{12}$$

and

$$\Gamma : (x,y) \rightarrow (vx+y, (v+1)x+y) \bmod N \tag{13}$$

Also, the absolute values of the determinant of the transformation matrices are 1.

$$abs\left(\begin{vmatrix} 1 & u+1 \\ 1 & u \end{vmatrix}\right) = abs(u-(u+1)) = abs(-1) = 1$$

$$abs\left(\begin{vmatrix} v & 1 \\ v+1 & 1 \end{vmatrix}\right) = abs(v-(v+1)) = abs(-1) = 1$$

This confirms that the transformation preserves the area [20]. That is, the transformed images are mapped back to the same area.

4 Performance Evaluation

The proposed method is a chaotic transformation for images. That is, on application, if observed, the iterations produce directional streaks and after a certain number of iterations the image returns to its initial state. The number of iterations taken by the image to return to its initial state is referred to as the period [20].

In this article, only square images of size 2^n, $(n \geq 1)$ are considered. Each individual point in an image is referred to as a pixel and the xy-plane where they are laid is called the pixel map. The row number and column number of the map describe the position of each pixel. Matlab is used to produce the experimental results.

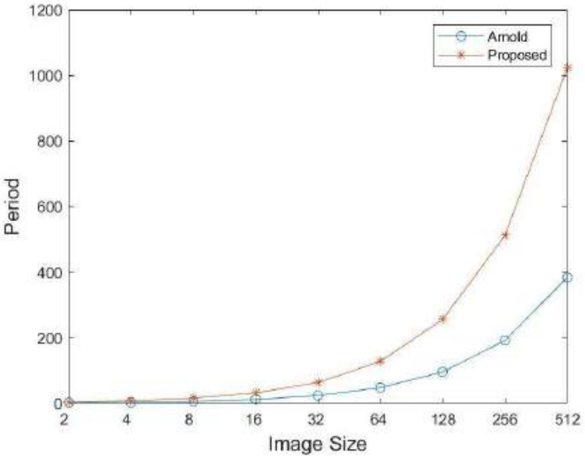


Fig. 1: Periodicity of Arnold's and the proposed method

Consider an image I. Let p be the number of pixels in a row or column, and r and c be the row number and column number respectively within the range $\{1,2,3,\ldots,p\}$. Transforming the image I under the proposed transformation method maps the set of pixel points in I from the current pixel positions (r,c) to another set of pixel positions (r',c') in I. That is,

$$\Gamma\left(\begin{bmatrix} r \\ c \end{bmatrix}\right) = \begin{bmatrix} 1 & u+1 \\ 1 & u \end{bmatrix} \begin{bmatrix} r \\ c \end{bmatrix} \bmod N = \begin{bmatrix} r' \\ c' \end{bmatrix}$$

where r' and c' are the remainders resulting from the application of mod N. Therefore, each pixel position is mapped to a new position within the same pixel map.

Since there is p^2 number of pixels in the pixel map of I, a pixel can take, at most, p^2 iterations to return to its original position. This defines the key space of the transformation. When an image of size 2^n is transformed with the Arnold cat map, it takes $3(2^{n-2})$, $n \geq 2$ iterations for a pixel to return to its original position. The major contribution of the proposed method is to increase this period so that the key space becomes larger. For example, consider $p = 64 = 2^6$. Table 1 shows the traversal of a pixel position (34, 49) in both the Arnold transform and the proposed method. It is observed that the proposed method takes 128 iterations to return the pixel to its original position whereas the Arnold transform takes only 48 iterations, which is less than half taken by the proposed method. The period for $p = 128 = 2^7 = 2^{6+1}$. Thus for an image of size 2^n, $n \geq 1$, the proposed method takes 2^{n+1} iterations for a pixel to return to its initial position.

Table 1: Pixel Traversal

Iterations		Initial position	16	32	48	96	112	128
Pixel position	Proposed method	(35, 49)	(19, 9)	(3, 33)	(35, 17)	(3, 1)	(51, 25)	(35, 49)
	Arnold	(35, 49)	(49, 18)	(44, 58)	(35, 49)	—	—	—

Table 2: Periodicity

N	2	4	8	16	32	64	128	256	512
Arnold's	3	3	6	12	24	48	96	192	384
Proposed method	4	8	16	32	64	128	256	512	1024

(a)
(b)

Fig. 2: (a) Lena image (b) Peppers image

Table 2 presents the iterations needed for a pixel to return to its initial position with Arnold's cat map [14] and the proposed method.

The graph shown in Fig. 1 illustrates the periodicity difference between Arnold's cat map and the proposed method. The periodicity of the proposed method is 8/3 = 2.6667 times greater than Arnold's cat map. Thus, the proposed transfrom is able to offer more key space for encryption.

It is also observed that the proposed method shows better scrambling, compared to Arnold's cat map. Fig. 2 shows the original images considered, Lena and Peppers. Both are bitmap images with dimensions of 512×512 and sized 257 KB. The outputs of eight iterations are listed in Fig. 3.

From Fig. 3, it is observed that the 384^{th} iteration in Arnold's transform reconstructs the original image. But in the proposed method, which seems to be like it, that is not the case, since the iterations following it start scrambling the image again. This lead to confusion in terms of determining the decryption key to crack the encrypted image. The next four iterations of the proposed transform on both the images are listed in Fig. 4.

5 Applications

The proposed method can be applied during the pre-processing of watermark images prior to embedding them into the carrier images in image watermarking algorithms. The method can be used in the confusion stage of image encryption to maximize information security while storing and transporting image information.

5.1 Image Watermarking

The image shown in Fig. 2(a), Lena, is considered the carrier image and Fig. 2(b), Peppers, the watermark. The discrete wavelet transform (DWT) is used to embed the watermark into the carrier image. The results are presented in Fig. 5. The watermark is embedded (i) directly into the carrier image without applying the proposed method, and (ii) after pre-processing with the application of the proposed method. The watermarked images from both (i) and (ii) are presented in Fig. 5(a) and Fig. 5(c) respectively and the extracted watermarks are depicted in Fig. 5(b) and Fig. 5(d) respectively. The unscrambled watermark after the application of the inverse transform of the proposed method is shown in Fig. 5(e).

If the watermark is applied with the proposed method before embedding, changes made on the watermarked image make the watermark indecipherable after extraction. This helps in the secure transmission of the watermarked information. Fig. 6 shows the results after cropping 6.25% of the watermarked image from all the four sides. When the watermark is embedded as such, the cropped watermark can be extracted. However, if it is applied with the proposed method, the pixel scrambling process results in unintelligible watermark extraction. Not even the application of the inverse transformation of the proposed method can help extract the contents of the

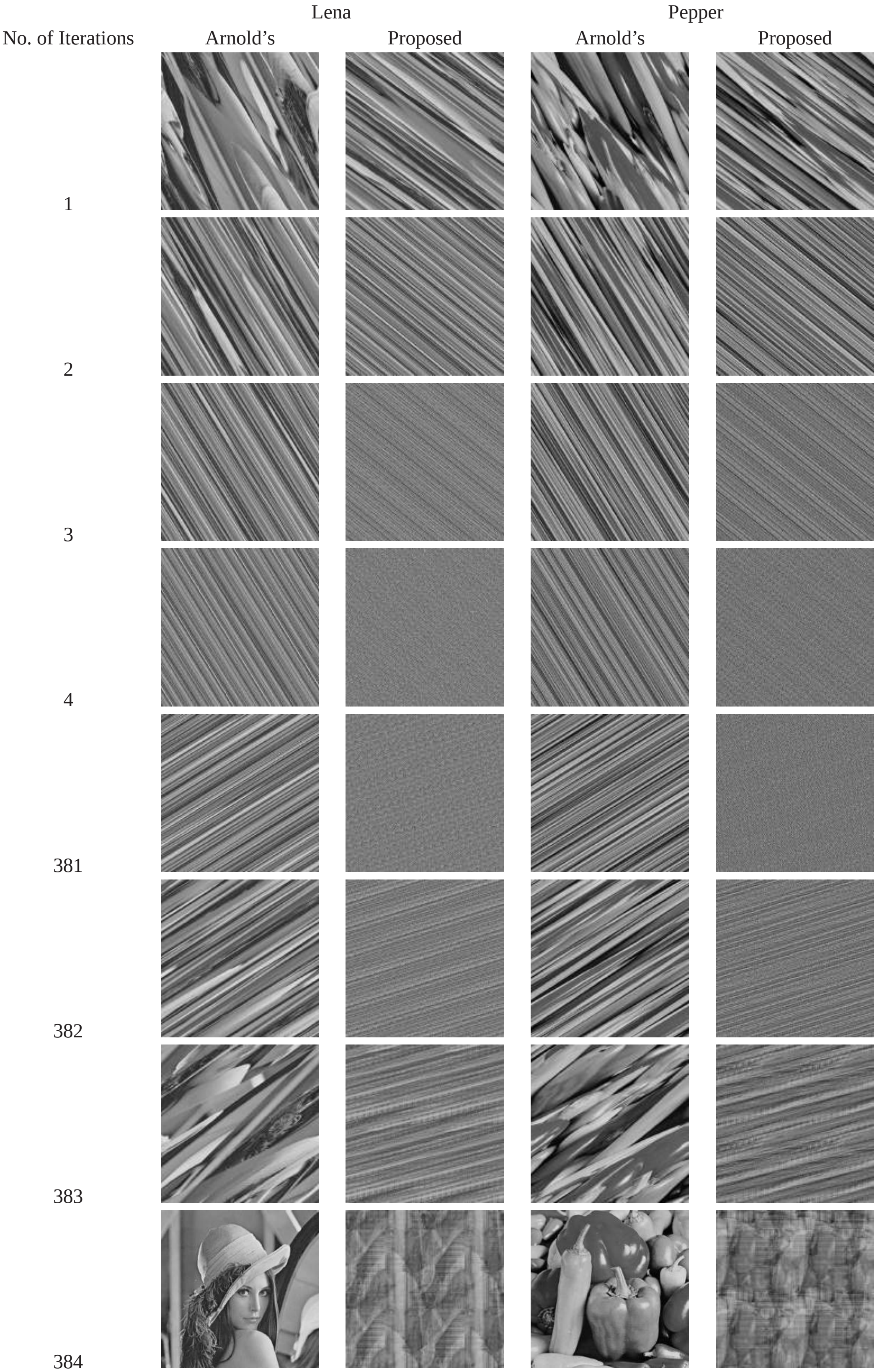


Fig. 3: Comparison of the proposed transform with Arnold transform

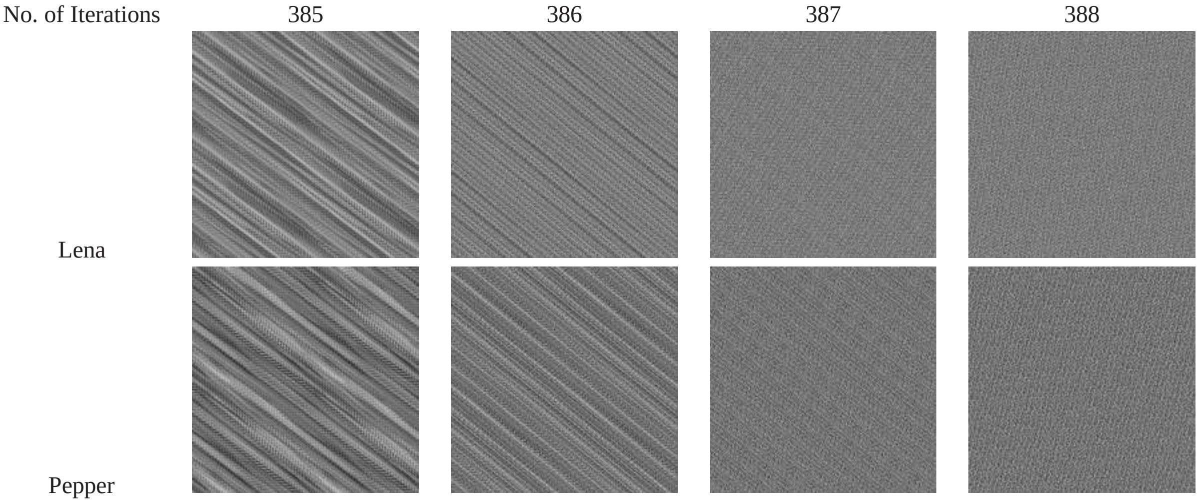


Fig. 4: Transformations using the proposed method

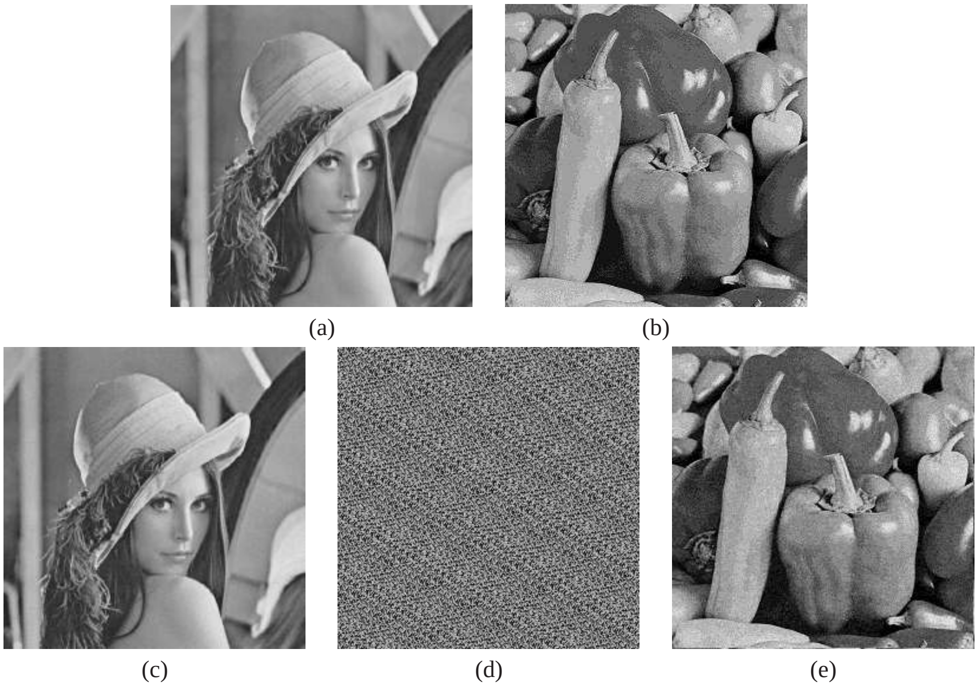
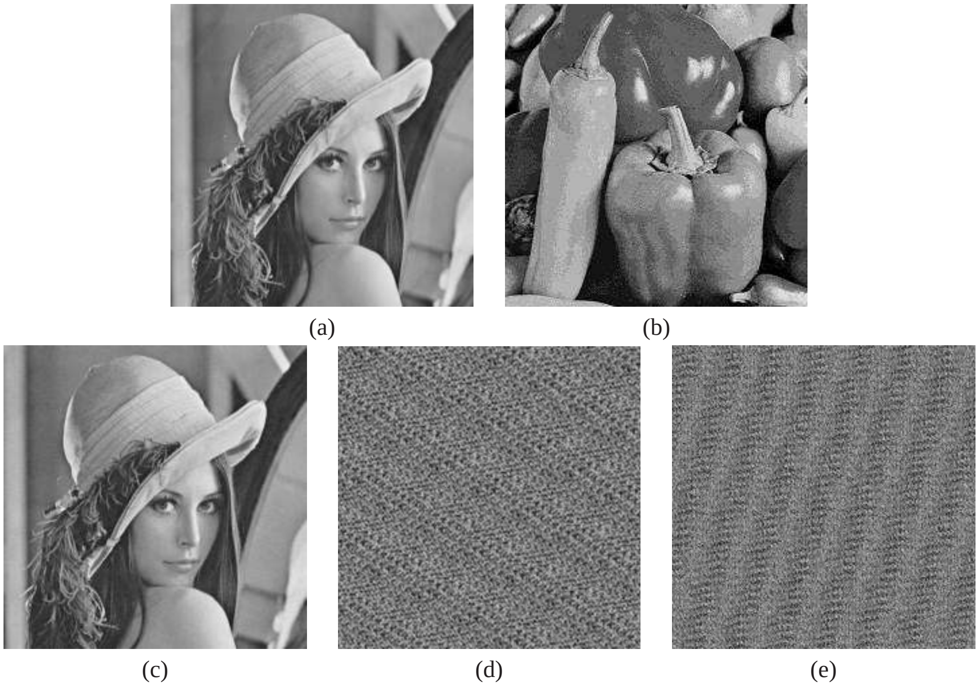

(a)
(b)
(c)
(d)
(e)

Fig. 5: (a) and (c) Watermarked images (b) and (d) Extracted watermarks (e) Unscrambled watermark

information in question. The result of the same is shown in Fig. 6(e).

5.2 Image Encryption

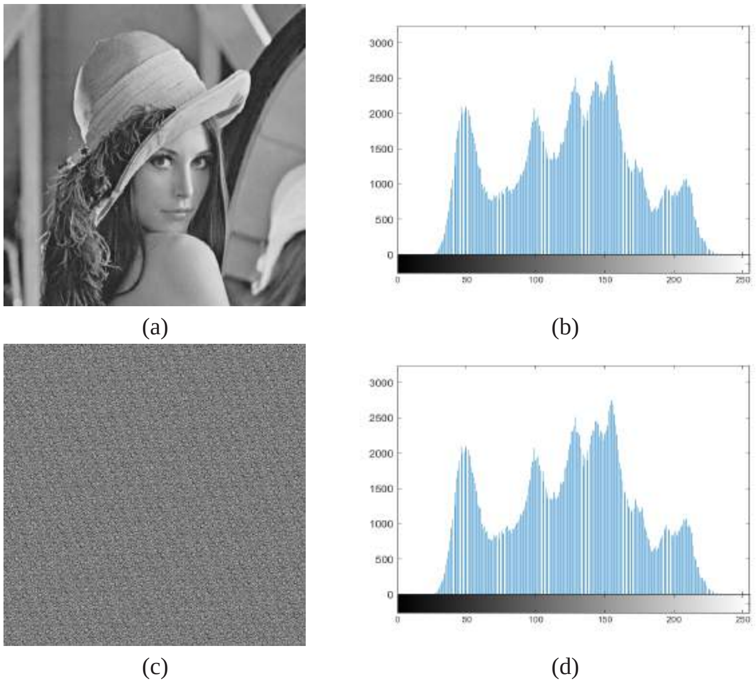
Many image encryption schemes are based on the confusion-diffusion architecture [21]. The encryption process is based on the number of iterations which transposes the image pixels (confusion) and modifies the pixel values (diffusion). The proposed method can be used as a confusion technique as it permutes the position of the pixels and not their values. Fig. 7 presents the original Lena image and its scrambled form, along with their respective histograms. From the figure, it is observed that the scrambled image looks like an encrypted image, owing to the transposition of the image pixels. But the histograms, however, clearly show that the information content in both images is the same. Hence the proposed



(a) (b)

(c) (d) (e)

Fig. 6: (a) and (c) Cropped watermarked images (b) and (d) Extracted watermarks (e) Unscrambled watermark



(a) (b)

(c) (d)

Fig. 7: (a) Original image (b) Histogram of the original image (c) Scrambled image (d) Histogram of the scrambled image

system, along with other diffusion techniques, produces a better encrypted image.

6 Conclusion

Images are widely used in the web, and ensuring their security in terms of unauthorised access is crucial. A new chaotic image encryption method, based on the Arnold cat map, is proposed for the same. It is observed that the proposed method gives greater scrambling choices than the existing Arnold's cat map. This results in more chaos and better encryption by providing a larger key space. The proposed transformation is an automorphism and both one-to-one and onto. Further, it preserves the area as well, given that the pixels lie in the same pixel map, following the transformation. Certain applications of the proposed method are also presented.

References

[1] X. Jun, W. Ying, L. Dengyu, Z. Ying and Z. Li, Security Scheme for Digital Watermarking, Proceedings of the International Conference on Materials Engineering and Information Technology Applications (MEITA), Atlantis Press, pp. 335-339, (2015).

[2] F. Yang, C. Wang, W. Huang and X. Zhou, Embedding Binary Image Watermark in DC Components of All Phase Discrete Cosine Biorthogonal Transform, International Journal of Security and Its Applications, Vol. 9, No. 10, pp. 125-136 (2015).

[3] B.K. Mohammed, H.A.N. Al-taee and A.A.D. Al.magsoosi, 3D Anaglyph Image Watermarking Approach, Journal of AL-Qadisiyah for Computer Science and Mathematics, Vol. 10, No.1, pp. 35-41 (2018).

[4] C. Yu, Steganography of Digital Watermark by Arnold Scrambling Transform with Blind Source Separation Morphological Component Analysis, Multimedia Tools and Applications, Vol. 76, No.5, pp. 6821-6842 (2017).

[5] Z. Guan, F. Huang and W. Guan, Chaos-based Image Encryption Algorithm, Physics Letters A, Vol. 346, No. 1, pp. 153-157 (2005).

[6] M. Xu, A Modified Chaos-based Image Encryption Algorithm, Journal of Software, Vol. 10, No. 8, pp. 931-938 (2015).

[7] M. Dankova and P. Rajmic, Encryption of Messages and Images using Compressed Sensing, Proceedings of the 21st Conference STUDENT EEICT, pp. 500-504 (2015).

[8] L. Agilandeeswari and K. Ganesan, A Robust Color Video Watermarking Scheme based on Hybrid Embedding Techniques, Multimedia Tools and Applications, Vol. 75, No. 14, pp. 8745-8780 (2016).

[9] M. Botta, D. Cavagnino and V. Pomponiu, A Successful Attack and Revision of a Chaotic System based Fragile Watermarking Scheme for Image Tamper Detection, AEU. International Journal of Electronics and Communications, Vol. 69, No. 1, pp. 242-245 (2015).

[10] A. Soleymani, M.J. Nordin and E. Sundararajan, A Chaotic Cryptosystem for Images based on Henon and Arnold Cat Map, The Scientific World Journal, 21 pages (2014).

[11] H. Liu and C. Jin, A Color Image Encryption Scheme based on Arnold Scrambling and Quantum Chaotic, International Journal of Network Security, Vol. 19, No. 3, pp. 347-357 (2017).

[12] D.C. Mishra, R.K. Sharma, R. Ranjan and M. Hanmandlu, Security of RGB Image Data by Affine Hill Cipher over $SL_n(F_q)$ and $M_n(F_q)$ Domains with Arnold Transform, Optik, Vol. 126, No. 23, pp. 3812-3822 (2015).

[13] L. Sun, J. Xu, X. Zhang and Y. Tian, An Image Watermarking Scheme using Arnold Transform and Fuzzy Smooth Support Vector Machine, Mathematical Problems in Engineering, 14 pages (2015).

[14] M.R. Abuturab, Generalized Arnold Map-based Optical Multiple Color-image Encoding in Gyrator Transform Domain, Optics Communications, Vol. 343, pp. 157-171 (2015).

[15] Z. Liu, M. Gong, Y. Dou, F. Liu, M.A. Ahmad, J. Dai and S. Liu, Double Image Encryption by using Arnold Transform and Discrete Fractional Angular Transform, Optics and Lasers in Engineering, Vo. 50, No. 2, pp. 248-255 (2012).

[16] A. Shehab, M. Elhoseny, K. Muhammad, A.K. Sangaiah, P. Yang, H. Huang and G. Hou, Secure and Robust Fragile Watermarking Scheme for Medical Images, IEEE Access, Vol. 6, pp. 10269-10278 (2018).

[17] N.R. Zhou, T.X. Hua, L.H. Gong, D.J. Pei and Q.H. Liao, Quantum Image Encryption based on Generalized Arnold Transform and Double Random-phase Encoding, Quantum Information Processing, Vol. 14, No. 4, pp. 1193-1213 (2015).

[18] D. Qi, J. Zou and X. Han, A New Class of Scrambling Transformation and its Application in the Image Information Covering, Science in China Series E: Technological Sciences, Vol. 43, No. 3, pp. 304-312 (2000).

[19] Y. Chen, H. Yau and G. Yang, A Maximum Entropy-based Chaotic Time-variant Fragile Watermarking Scheme for Image Tampering Detection, Entropy, Vol. 15, No. 8, pp. 3170-3185 (2013).

[20] M.A. Partnof and K. Crum, Chaos and Arnold's Cat Map (2004).

[21] L.Y. Zhang, Y. Liu, K. Wong, F. Preschi, Y. Zhang, R. Rovatti and G. Setti, On the Security of a Class of Diffusion Mechanisms for Image Encryption, IEEE Transactions on Cybernetics, Vol. 48, No. 4, pp. 1163-1175 (2018).

V. J. Subashini is a Senior Assistant Professor at Jerusalem Engineering College, Chennai, India. She earned her MCA from Manonmanium Sundaranar University, Tirunelveli and M.E (CSE) from Anna University, Chennai. Her research interests lie in the field of security and image processing. She is currently pursuing Ph.D at Anna University, Chennai. She has presented and published papers in national and international conferences and co-authored articles published in international journals, and national and international conferences.

S. Poornachandra is the Principal, Excel Engineering College, Namakkal, India. He earned his Ph.D from Anna University. He is expertise in the fields of Biomedical Signal and Image Processing and Medical Instrumentation. He has published 22 articles in leading national and international journals. He has also published 37 papers in national and international conference proceedings, as well as authored 14 books. He has guided 37 short-term projects. He was the Principal Investigator of six funded projects. He serves as the expert peer review member of 19 journals and editorial member in four journals.