

[Egyptian Informatics Journal (2016) 17, 139](http://dx.doi.org/10.1016/j.eij.2015.10.001)–[146](http://dx.doi.org/10.1016/j.eij.2015.10.001)

Cairo University

Egyptian Informatics Journal

[www.elsevier.com/locate/eij](http://www.elsevier.com/locate/eij) [www.sciencedirect.com](http://www.sciencedirect.com/science/journal/11108665)

FULL-LENGTH ARTICLE

Image encryption based on Independent Component Analysis and Arnold’s Cat Map



Nidaa AbdulMohsin Abbas

*University of Babylon, College of IT, Iraq*

Received 27 May 2015; revised 3 October 2015; accepted 16 October 2015

Available online 23 November 2015

Abstract Security of the multimedia data including image and video is one of the basic require- ments for the telecommunications and computer networks. In this paper, a new efficient image encryption technique is presented. It is based on modifying the mixing matrix in Independent Component Analysis (ICA) using the chaotic Arnold’s Cat Map (ACM) for encryption. First, the mixing matrix is generated from the ACM by insert square image of any dimension. Second, the mixing process is implemented using the mixing matrix and the image sources the result is the encryption images that depend on the number of sources. Third, images decrypted using ICA algorithms. We use the Joint Approximate Diagonalization of Eigen-matrices (JADE) algorithm as a case study. The results of several experiments, PSNR, SDR and SSIM index tests compared with standard mixing matrix showed that the proposed image encryption system provided effective and safe way for image encryption.

© 2015 Production and hosting by Elsevier B.V. on behalf of Faculty of Computers and Information,

KEYWORDS

Arnold’s Cat Map; Image encryption; Independent Component Analysis;

JADE

Cairo University. This is an open access article under the CC BY-NC-ND license ([http://creativecommons.](http://creativecommons/)

org/licenses/by-nc-nd/4.0/).

1. Introduction

Over the years, there has been an important development in the field of information security. Yun-Peng et al. [[1]](#_bookmark15) presented the encryption scheme that realizes the digital image encryp- tion through the chaos and improving DES. First, encryption scheme uses the logistic chaos sequencer to make the

E-mail address: [drnidaa\_muhsin@ieee.org](mailto:drnidaa_muhsin@ieee.org)

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

**Production and hosting by Elsevier**

<http://dx.doi.org/10.1016/j.eij.2015.10.001>

pseudo-random sequence, carries on the RGB with this sequence to the image chaotically, makes double time encryptions with improvement DES, and displays the respec- tive merit. Lin et al. [[2]](#_bookmark16) proposed a way to encrypt the image using a linear mixed model of blind source separation (BSS). The encrypted simultaneously multiple images with the same size by mixing it with the same number of key images are statistically independent, the size of which is equal to that of images to be encrypted. Since these multiple images cover mutually through mixing among them while the key images cover them, there are no restrictions on the main space. The proposed method has a high level of security, and the computer simulation results showed its validity.

Ravishankar and Venkateshmurthy [[3]](#_bookmark21) proposed several schemes for image encryption. These schemes are produced

1110-8665 © 2015 Production and hosting by Elsevier B.V. on behalf of Faculty of Computers and Information, Cairo University. This is an open access article under the CC BY-NC-ND license ([http://creativecommons.org/licenses/by-nc-nd/4.0/).](http://creativecommons.org/licenses/by-nc-nd/4.0/))

140 N.AbdulMohsin Abbas

in the form of random so that the content not appears. Encryption and decryption consume large amount of time. Therefore, there is a need for effective algorithm. They pro- posed a region based selective image encryption technique which provides facilities of selective encryption and selective images of reconstruction. Gao et al. [[4]](#_bookmark22) proposed a nonlinear chaotic algorithm (NCA), which uses the power function and the tangent function instead of the linear function.

Yu et al. [[5]](#_bookmark23) suggested that the efficiency of image encryp- tion algorithm depends on the reconstruction of the image using some neighboring pixel characteristics. In accordance with the characteristics of different images of various bilateral level slightly, encryption system proposed reconstructs of the bit-level. Since the permutation of sub-images composing high 4-bits of the original image has a relatively high computational complexity, in this scheme the permutation of sub-images is performed with low 4-bits instead, which therefore has a lower computational complexity.

Kamali et al. [[6]](#_bookmark24) proposed encryption system that modifies the AES algorithm on the basis of each Shift Row Transforma- tions. If the value in the first row and first column is even, the first and fourth rows are unchanged, and each byte in second and third rows is shifted periodically over different numbers. Last rows’ first and third values are unchanged and are period- ically turned to leave each byte in the rows. The second and fourth quarters of the state to a different number of bytes. Experimental result showed that MAES gave better results in terms of encryption for security against attacks and increased the statistical performance. Paul et al. [[7]](#_bookmark10) proposed encoder to convert bitmaps tricks encryption. Replacement and dissemi- nation processes, based on the matrix, to facilitate fast convert plain text into cipher text, and images encryption. The results of the simulation compared with the results obtained from the Advanced Encryption Standard (AES), showed that the pro- posed image encryption algorithm was eight times faster than AES. Gautam et al. [[8]](#_bookmark11) discussed the use of a block based transformation algorithm, in which image is divided into num- ber of blocks. These blocks are transformed before going through an encryption process. At the receiver side these

sequences for a two-way diffusion of gray values. Liu and Tian

[[11]](#_bookmark14) proposed algorithm to encrypt images using color map and spatial chaos at the bit level flipping (SBLP). First, the algorithm used the logistic chaos sequence to shuffle the posi- tions of image pixels and then to convert them into a binary matrix component including red, green and blue at one time, rather than the order of the matrix as well as at the level prior to appointment of scrambling bit that has been created by SBLP. Second, the logistics rearranged the chaotic sequence for the position of the current image pixel else. Results of the experiment and security analysis algorithm achieved good results and the complexity of encryption is low, and in addition to that, the key space is large enough to resist against a com- mon attack.

In this paper, a new efficient image encryption technique is presented. It is based on modifying the mixing matrix in Inde- pendent Component Analysis (ICA) using the chaotic Arnold’s Cat Map (ACM) for encryption. First, the mixing matrix is generated from the ACM by inserting square image of any dimension. Second, the mixing process is implemented using the mixing matrix and the image sources. The result is the encrypted images that depend on the number of sources. Third, images are decrypted using ICA algorithms. The Joint Approximate Diagonalization of Eigen-matrices (JADE) algo- rithm was tested as a case study. The results of several exper- iments, PSNR, SDR and SSIM index tests compared with standard mixing matrix showed that the resulted encrypted images from the proposed system provided effective and safe way for image encryption.

1. Arnold’s Cat Map (ACM)

According to Arnold’s transformation, an image is hit with the transformation that apparently randomizes the original orga- nization of its pixels. However, if iterated enough times, even- tually the original image reappears. The number of considered iterations is known as the Arnold’s period. The period depends on the image size; i.e., for different size images, Arnold’s per- iod will be different [[12]](#_bookmark17).

*A*

*n*

blocks were retransformed into their original position and

*xn*+1

*xn*

1 *p*

*xn*

decryption process is performed. The advantage of such

approach is used mainly on reproducing the original image without loss of information for the encryption and decryption

*yn*+1

= *yn*

(mod *N*)=

*q pq* + 1

*y* (mod *N*)

(1)

process (based on a blowfish algorithm). Fei and Xiao-cong [[9]](#_bookmark12) presented an image encryption algorithm based on two- dimensional (2D) map and complex logistics system Chua’s system. It used two successive chaos generated by the MAP logistics 2D (to change the features of color image). Then it used the chaos resulting from the successive models to maxi- mize the benefits of the Chua system on the production of new pixel values. Simulation results showed that the algorithm has good properties of confusion and diffusion, and the big key space.

Ye and Zhao [[10]](#_bookmark13) proposed chaos-based image encryption scheme using affine modular maps, which are extensions of lin- ear congruential generators, acting on the unit interval. A per- mutation process utilized two affine modular maps to get two index order sequences for the shuffling of image pixel posi- tions, while a diffusion process employed another two affine modular maps to produce two pseudo-random gray value

where *N* is the size of the image, *p* and *q* are positive integer and *det*(*A*) = 1. (*xn*, *yn*) is the position of samples in the *N* × *N* data such as image, so that

(*xn*; *yn*)∈ {0; 1; 2; ... ; *N* — 1}

And (*xn*+1, *yn*+1) is the transformed position after cat map, Cat map has two typical factors, which bring chaotic move- ment: tension (multiply matrix in order to enlarge *x*, *y*) and fold (taking mod in order to bring *x*, *y* in unit matrix).

Eq. [(1)](#_bookmark0) is used to transform each and every pixel coordi- nates of the image. When all the coordinates are transformed, the image resulted is a scrambled image. At a certain step of iterations, if the resulted image reaches our anticipated target (i.e. up to secret key), we have achieved the requested scrambled image. The decryption of image relies on the transformation periods (i.e. the number of iterations to be followed = Arnold’s period — secret key) [[13]](#_bookmark18).

Image encryption based on Independent Component Analysis and Arnold’s Cat Map 141

1. Independent Component Analysis (ICA)

ICA defines a generative model for observed multivariate data, which usually is given as a large database of samples. In this model, data variable are assumed to be linear or nonlinear mixtures of some unknown latent variables, and mixing system is also unknown. And it is assumed that the underlying vari- ables of non-Gaussian are independent of each other and are called independent components (IC) of the observed data. These independent components are also called sources or fac- tors that can be found by ICA [[14,15]](#_bookmark19).

The basic linear model relates the unobservable source image and the observed mixtures:

*x*(*t*)= *As*(*t*) (2)

where *s*(*t*)= [*s* (*t*), ... , *s* (*t*)]*T* is a *m* × 1 column vector

1

*m*

Sometimes this approach is referred to as ‘‘decorrelation and rotation”, and it depends on the measurement of non- Gaussian signals. For Gaussian signals, the higher order statis- tics are zero already and so no meaningful separation can be achieved by ICA methods. For non-Gaussian random signals the implication is that not only should the signals be uncorre- lated, but also the higher order cross-statistics (e.g., moments or cumulants) are zero [[18]](#_bookmark26). The JADE algorithm can be sum- marized as:

1. *Initialization.* Estimate a whitening matrix *W* and set

b

*Z* = *W X* .

b

1. *Form statistics.* Estimate a maximal set {*Qi* } of cumulant matrices.

*Z*

b

1. *Optimize an orthogonal contrast.* Find the rotation matrix *V*b

such that the cumulant matrices are as diagonal as possible,

collecting the source images, similarly vector *x*(*t*) collects the

that is, solve (arg min P *Off* (*V* + *Q*b *ZV* )).

*n* observed signals, *A* is a *n m* matrix of unknown mixing

×

coefficients, *n* P *m*, and *t* is the time index. This model is instantaneous (or memoryless) because the mixing matrix con- tains fixed elements, and also noise-free.

In order to recover the original source images from the observed mixtures, we use a simple linear separating system [[16]](#_bookmark20): *y*(*t*)= *Bx*(*t*) (3)

where *y*(*t*)= [*y* (*t*), .. . , *y* (*t*)] is an estimate *s*(*t*), and *B* is a

1

*m*

*T*

*i* *i*

1. *Separate.* Estimate *A* as

*A*b = *V*b*W*c—1. (4)

And/or estimate the components as *S*b = *A*b—1*X* = *V*b +*Z*.

4. Proposed system

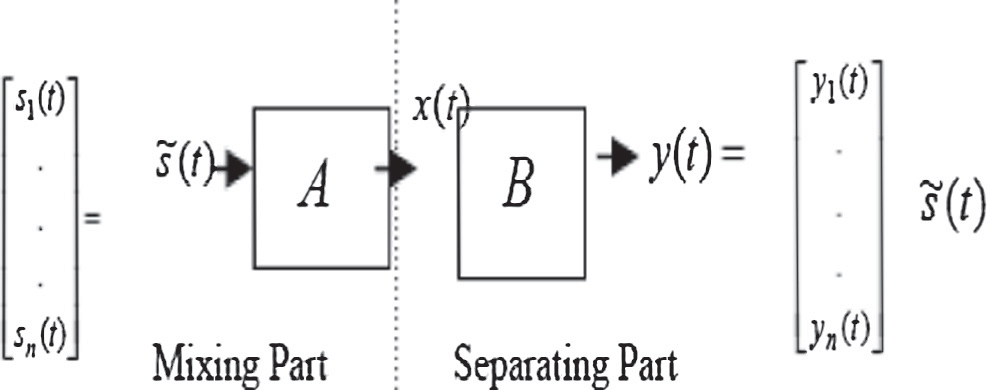
*n n* (assume *n m*) separating matrix, as shown in [Fig. 1](#_bookmark3).

× =

There are essentially two distinct, at the expense of the ICA, off-line (batch) processing and on-line algorithms. This paper focuses on batch algorithm using JADE algorithm, and on a common approach for batch ICA algorithms by the following two stages of procedure [[17]](#_bookmark25):

1. Decorrelation or whitening. This stage seeks to diago- nalize the covariance matrix of the input signals. This is done through computing the sample covariance matrix, giving the second order statistics of the observed output. From this, a matrix is computed by eigen decomposition which whitens the observed data.
2. Rotation. This stage reduces a measure of the higher order statistics which will ensure that the non- Gaussian output signals are as statistically independent as possible. It is clear that this stage can be carried out by a unitary rotation matrix, to provide the higher order independence. And it is performed by finding a rotation matrix which jointly diagonalize eigenmatrices formed from the fourth order cumulants of the whitened data. The outputs from this stage are the independent components.

The proposed system has two stages, first we used Arnold’s Cat Map (ACM) algorithm, second we used JADE algorithm to recover the original images. [Fig. 2](#_bookmark4), represents the proposed system.



***x(t) = As(t)***

***y(t) = Bx(t)***

**Sources Estimated Sources**

Steps of the proposed system

1. Arnold’s Cat Map (ACM) algorithm
   1. Input any arbitrary image
   2. Use num as variable which is represented the No. of Iterations
   3. Determine the No. of rows and columns. Which are represented by the variables row and col respectively.
   4. for inc = 1 to num for row1 = 1 to row

for col1 = 1 to col nrowp = row1 ncolp = col1

for ite = 1 to inc

Shuﬄe the positions of the pixels of the image using Eq. [(1)](#_bookmark0) end

Result the new encryption image end

end end

1. Encryption algorithm

The steps are:

* 1. Input Two images
  2. Convert the images to vectors and assign to S
  3. Mixing matrix A which is the result from ACM algorithm
  4. Apply Eq. [(2)](#_bookmark1) to get the image encryption

C. Decryption algorithm and evaluation process

1. Apply JADE in Eq. [(4)](#_bookmark2) to get the decrypted image
2. Evaluation Process

Figure 1 Mixing and separating. Unobserved signals; observa- tions *x*(*t*), estimated source images *y*(*t*).

142 N.AbdulMohsin Abbas

1. Measurements criteria
   1. *Signal to distortion ratio (SDR)*
      * r*x* the variance of *x*;
      * r*y* the variance of *y*;

2

2

* + - r*xy* the covariance of *x* and *y*;

2 2

●

To evaluate the quality of the separated signals by calculating the signal-to-distortion ratio (SDR) between the separated signal *s*~ *t* and the original source image *s t* before mixing, a higher value of SDR is good because of the superiority of the signal to that of the distortion. The SDR in dB (decibel) is calculated as follows [[19]](#_bookmark27):

( ) ( )

P *s*(*t*)2

*c*1 = (*k*1*L*) , *c*2 = (*k*2*L*) , two variables to stabilize the

division with weak denominator;

* + - *L* the dynamic range of the pixel-values (typically this is 2#bits per pixel — 1);
    - *k*1 = 0.01 and *k*2 = 0.03.

*5.3. Peak signal to noise ratio (PSNR)*

SDR = 10log10 P

*t*

(*s*(*t*)— *s*~(*t*))2

*t*

(dB) (5)

A higher value of PSNR is good because of the superiority of the signal to that of the noise. The larger the PSNR the better

* 1. *The Structural SIMilarity (SSIM) index*

the image separation result is.

255

*N*

The structural similarity (SSIM) index is a method for measur- ing the similarity between two images. Structural information

PSNR = 10log10

*M*

*MN y*=1 *x*=1

,ﬃ*M*ﬃﬃﬃﬃ*S*ﬃﬃﬃ*E*ﬃﬃﬃ

(dB) (7)

is the idea that the pixels have strong inter-dependencies espe- cially when they are spatially close. These dependencies carry important information about the structure of the objects in the visual scene. The resultant SSIM index is a decimal value between 1 and 1, and value 1 is only reachable in the case of two identical sets of data.

—

The SSIM metric is calculated on various windows of an image. The measure between two windows s and *y* of common size *N* × *N* is [[20]](#_bookmark28):

MSE = 1 XX[*I*(*x*, *y*)— *I*'(*x*, *y*)]2

where *I*(*x*, *y*) is the original image, *I*'(*x*, *y*) is the approxi- mated version and (*M*, *N*) are the dimensions of the images. A lower value for Mean Square Error (MSE) means less error, and as seen from the inverse relation between the MSE and PSNR, this translates into a high value of PSNR. Here, the signal is the original image, and the noise is the error in reconstruction.

SSIM *x*, *y*  (2l*x*l*y* + *c*1)(2r*xy* + *c*2)

(l2 + l2 + *c*1)(r2 + r2 + *c*2)

( )=

(6)

With

*x y x y*

1. Results and discussions

* l*x* the average of *x*;
* l*y* the average of *y*;



***A* \***

Encryption Process

*X= AS*

Convert Images to vectors and Assign to ***S***

Input two Images

*X*

**(a)**

***A***

as mixing matrix

Arnold’s Cat Map (ACM)

Input arbitrary Image

Reorder of Y

JADE

Algorithm

Decryption Images

Evaluation the results



Y

Decryption Process

**(b)**

Figure 2 The proposed system, (a) produce the mixing matrix,

(b) image encryption and decryption.

The proposed system was done under Dell Laptop, with O.S. Window system, Processor Core 2 Duo and RAM 2.00 GB, which is implemented using MATLAB. The experimental results are shown in [Table 1](#_bookmark5) which shows the comparison between standard mixing matrix (random matrix) and Arnold Cat Map matrix using the three parameters. This comparison was carried out with different images and different dimensions. In order to provide quantitative measures on the per- formance of the objective quality assessment models, we use the performance evaluation criteria (SDR, SSIM and

PSNR).

We observed the SDR from [Figs. 3–5](#_bookmark6) using 7 images with (120 120), (128 128) and (512 512) dimensions. The results are irregular, and sometimes the result is likely to favor random matrix than the Arnold Cat Map matrix and vice versa.

× × ×

For using the SSIM as comparison criterion, the result is shown in [Figs. 6–8](#_bookmark8) also we used 7 images with (120 120),

×

(128 128) and (512 512) dimensions. The results of Arnold Cat Map matrix are better than random matrix.

× ×

The PSNR results from [Figs. 9–11](#_bookmark7) shown with those of Arnold Cat Map matrix are better than random matrix.

Beside of the objective test, we clarify the subjective test as shown in [Table 2](#_bookmark9); we chose samples of images to show the dif- ference between the Arnold Cat Map matrix and random matrix.

Table 1 Comparison between random matrix and Arnold Cat Map matrix using PSNR, SDR and SSIM index.

Image encryption based on Independent Component Analysis and Arnold’s Cat Map

143

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Image dimension | Image no. | Image name | | PSNR | | SDR | | | | SSIM index | | | |
| 1 | | | 2 | Random | Arnold | 1 | | 2 | | 1 | | 2 | |
|  | | |  | matrix | matrix |  | |  | |  | |  | |
|  |  |  |  |  |  | Random | Arnold | Random | Arnold | Random | Arnold | Random | Arnold |
|  |  |  |  |  |  | matrix | matrix | matrix | matrix | matrix | matrix | matrix | matrix |
| 120 × 120 | 1.  2. | Avatar1 Avatar1 | Avatar2 Cabpic | 5.7039  6.3340 | 10.8314  13.9242 | —1.6357  7.9761 | 6.0227  7.9761 | 5.9344  8.4852 | 5.9344  8.4852 | —0.1950  —0.0693 | 0.323  0.6904 | 0.6165  0.1169 | 0.616  0.7218 |
|  | 3.  4. | Cus4  Avatar2 | Xxx  Cus2 | 4.7103  5.3303 | 10.8878  9.7250 | 2.2885  4.6796 | 2.2885  4.6796 | 2.1789  4.5871 | 2.1789  4.5871 | —0.0226  —0.0583 | 0.4933  0.5151 | —0.0226  0.3420 | 0.6597  0.2924 |
|  | 5.  6. | debbie  18 | barbara  debbie | 5.4368  5.8150 | 9.8059  10.1908 | —2.2127  2.7486 | 6.9680  2.7486 | 1.9642  6.6115 | 1.9642  6.6115 | —0.0427  —0.1099 | 0.2465  0.6179 | 0.6116  0.2280 | 0.6116  0.2289 |
|  | 7. | Cus4 | barbara | 5.4777 | 10.0865 | —4.4679 | 4.7917 | 2.3372 | 2.3372 | —0.1114 | 0.3412 | 0.5844 | 0.5844 |
| 128 × 128 | 1.  2. | 1  3 | 2  4 | 4.5697  5.3127 | 10.8155  9.0138 | 14.4711  1.4780 | 14.471  1.4780 | 2.3848  3.2239 | 2.3848  3.2239 | —0.1343  —0.1734 | 0.8642  0.4850 | 0.1419  0.2737 | 0.2147  0.3493 |
|  | 3.  4.  5. | 5  7  lenna | 6  baboon na2 | 5.4490  4.9310  6.1625 | 7.8741  11.4455  9.1758 | —0.0898  5.4544  0.7354 | 3.9366  5.4544  0.7354 | 2.5312  4.7586  4.4537 | 2.5312  4.7586  4.4537 | —0.1646  —0.0711  —0.1408 | 0.2454  0.6080  0.5312 | 0.4780  —0.0875  0.2294 | 0.4780  0.6984  0.2647 |
|  | 6. | mandel | 1 | 6.1551 | 11.2806 | —1.0602 | 4.8670 | 12.335 | 12.335 | —0.3731 | 0.4757 | 0.6630 | 0.6630 |
|  | 7. | lenna | 2 | 6.0286 | 9.0229 | —2.3487 | 3.7098 | 1.7356 | 1.7356 | —0.2001 | 0.3148 | 0.5241 | 0.5241 |
| 512 × 512 | 1.  2. | 1  14 | 2  15 | 5.1543  5.8254 | 9.2045  9.2619 | 2.6092  3.4320 | 2.6092  3.4320 | —0.818  3.6300 | —0.818  3.6300 | —0.0916  —0.0559 | 0.6356  0.6108 | 0.0735  0.2668 | 0.2372  0.2536 |
|  | 3. | 16 | debbie | 5.4594 | 10.5912 | 3.9158 | 3.9158 | 7.3022 | 7.3022 | —0.0208 | 0.6907 | 0.3866 | 0.2143 |
|  | 4. | barbara | 18 | 5.9035 | 8.3079 | 1.2493 | 3.3956 | 3.4543 | 1.6724 | —0.1004 | 0.2165 | 0.4498 | 0.4498 |
|  | 5.  6.  7. | barbara  12  17 | house  11  4 | 6.5413  5.9476  5.7275 | 10.5930  7.9630  8.6466 | —1.5690  1.1416  4.4850 | 4.1637  1.1416  4.0636 | 7.5353  1.8317  3.8439 | 7.5353  1.8317  3.2631 | —0.1110  —0.0372  0.1140 | 0.2356  0.6949  0.1722 | 0.7005  0.2711  0.6822 | 0.7005  0.1576  0.6822 |

144 N.AbdulMohsin Abbas

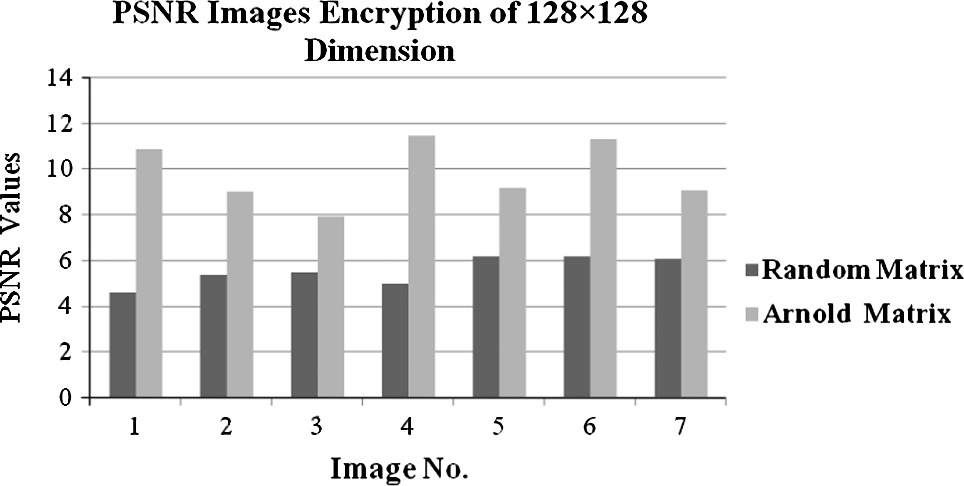
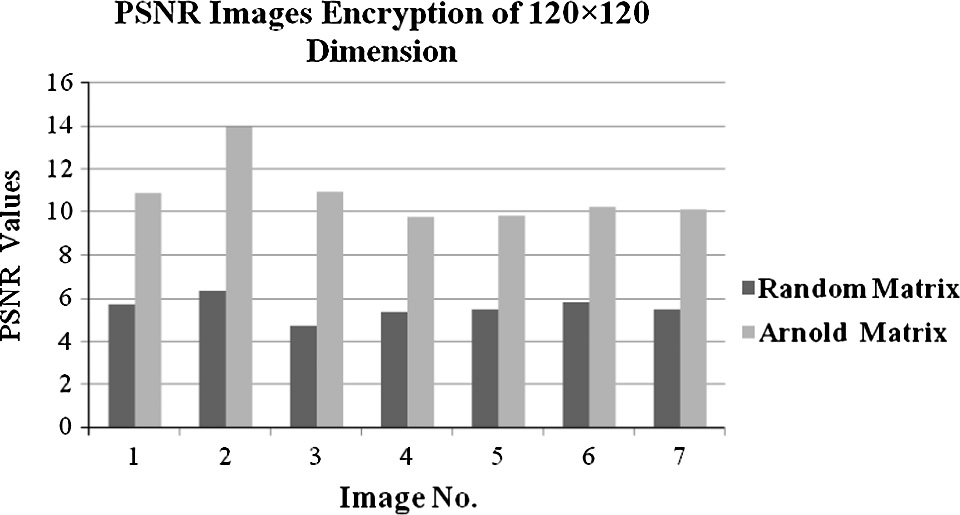
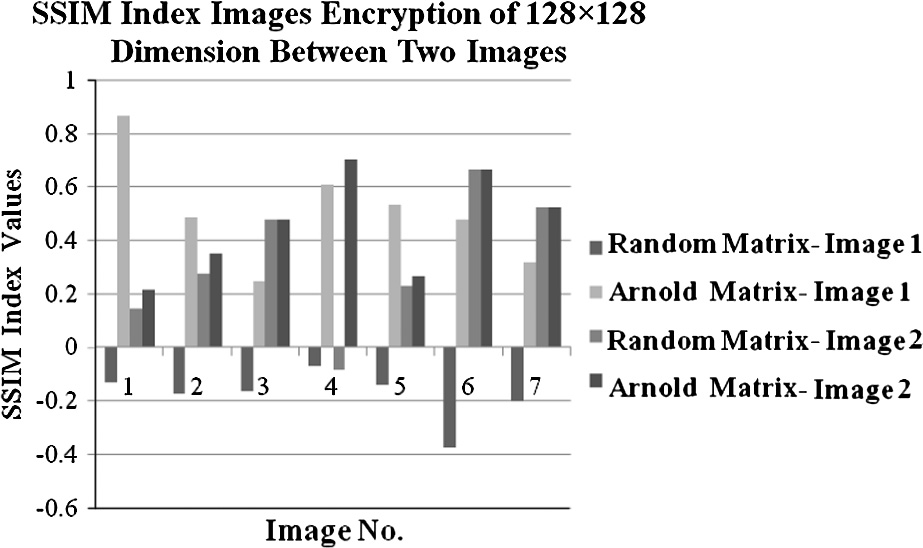
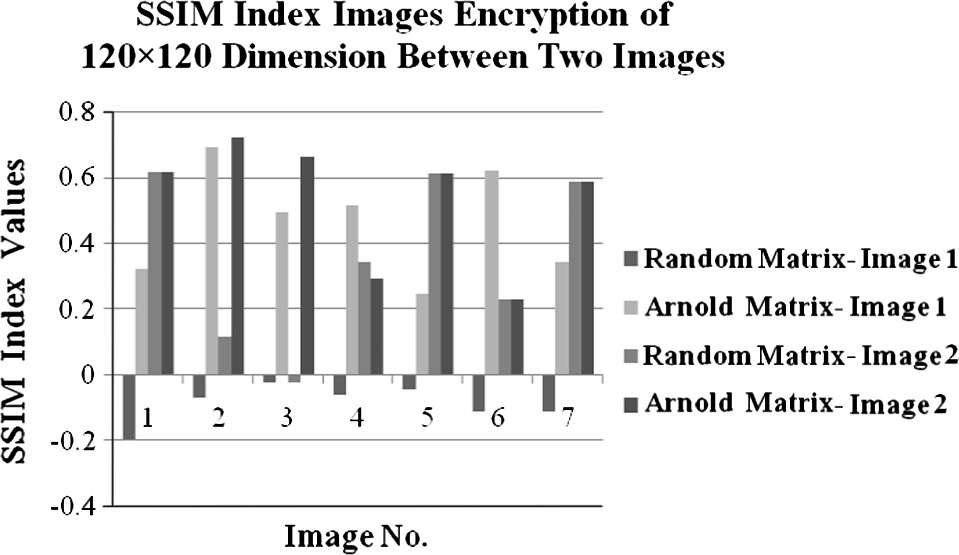
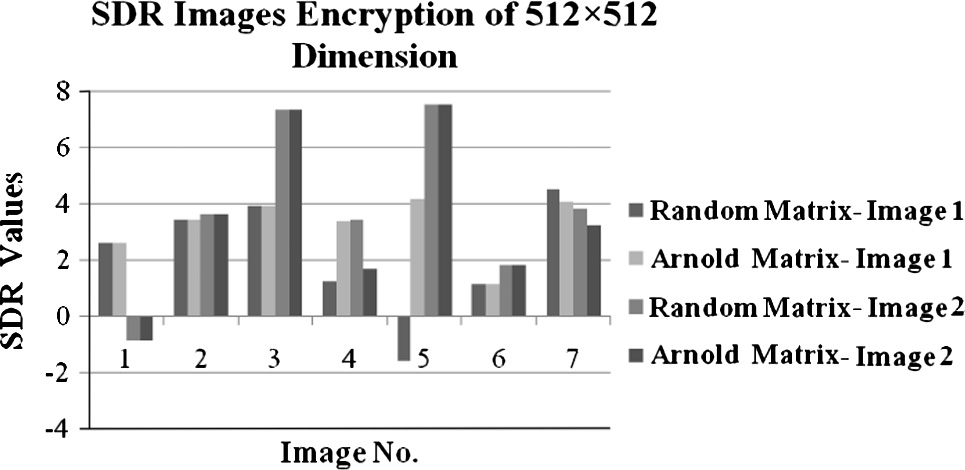
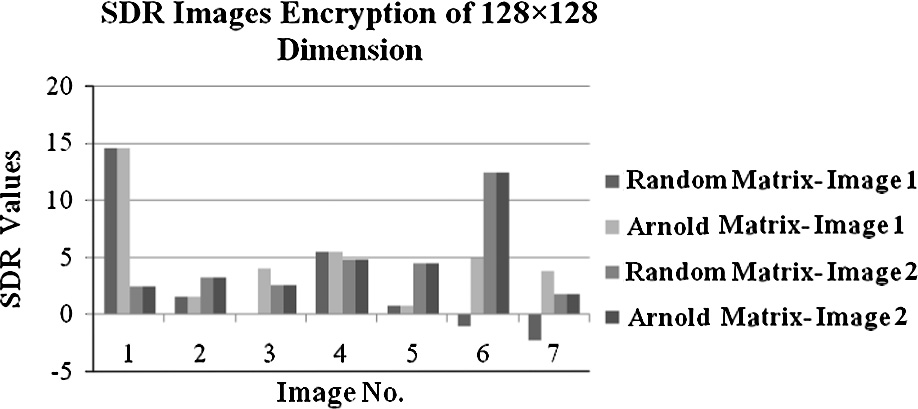
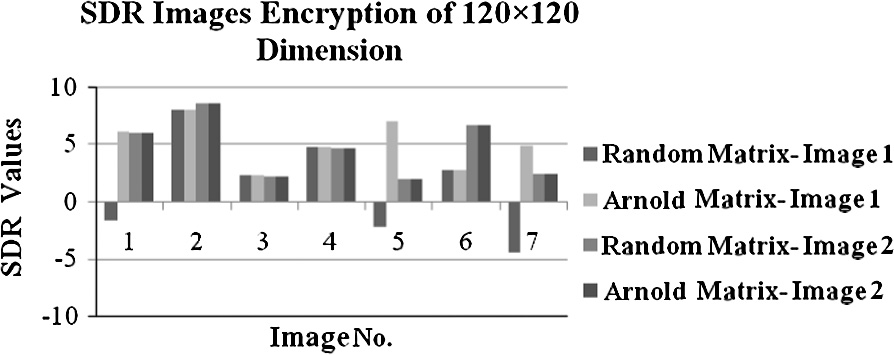


Figure 3 SDR images encryption of 120 × 120 dimension.

Figure 7 SSIM images encryption of 128 × 128 dimension.

Figure 4 SDR images encryption of 128 × 128 dimension.

Figure 8 SSIM images encryption of 512 × 512 dimension.

Figure 5 SDR images encryption of 512 × 512 dimension.

Figure 9 PSNR images encryption of 120 × 120 dimension.

Figure 6 SSIM images encryption of 120 × 120 dimension. Figure 10 PSNR images encryption of 128 × 128 dimension.

Image encryption based on Independent Component Analysis and Arnold’s Cat Map 145

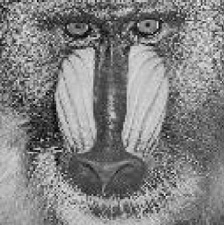
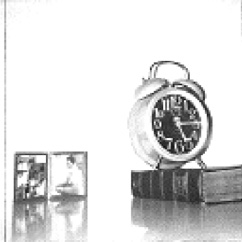
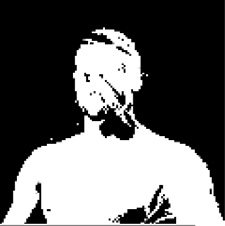
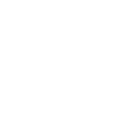
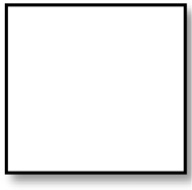
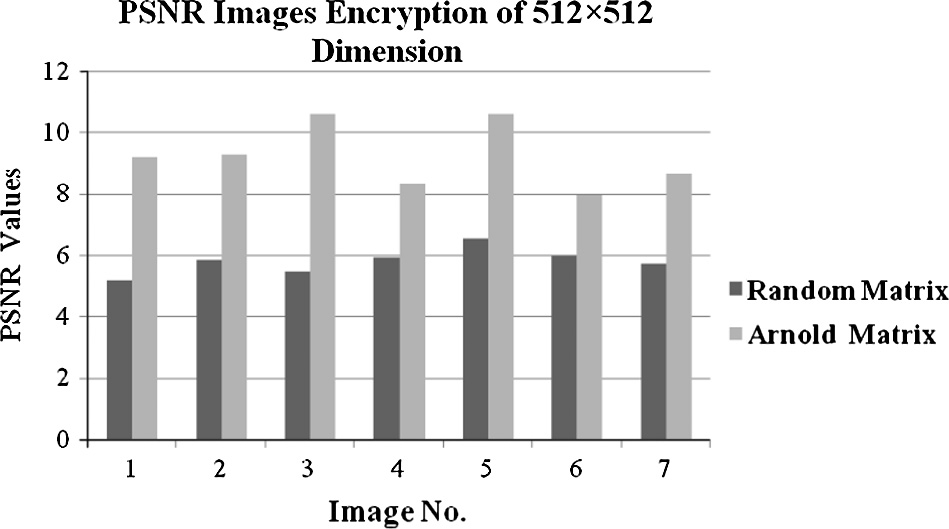


Table 2 Samples of subjective test of random matrix and Arnold Cat Map matrix.

Dimension Mixed images Original image Arnold Cat Map matrix Random matrix

Encrypted Decrypted Encrypted Decrypted

120 120 Two original images mixed

×

1 and 2

Two original images mixed 1 and 2

128 128 Two original images mixed

×

1 and 2

Two original images mixed 1 and 2

512 512 Two original images mixed

×

1 and 2

(*continued on next page*)

146 N.AbdulMohsin Abbas



Table 2 (*continued*)

Dimension Mixed images

Original image Arnold Cat Map matrix

Encrypted Decrypted

Random matrix

Encrypted

Decrypted

Two original images mixed

1 and 2

1. Conclusions

In this paper, we proposed a new Encryption method consists of a combination of Independent Component Analysis and Arnold Cat Map matrix. The experimental results showed that the proposed approach yields a better encryption performance compared to random matrix using JADE algorithm. The results have shown the unintelligibility of the tested images using Arnold Cat Map matrix in comparison with random matrix. Also it can be estimated that the cryptanalytic efforts that need to analyze this proposed system will be very high in comparison with the efforts paid to the system based on ICA alone.

For future works we can study in detail the strength of the ACM generator matrix and check its effort on the final results (in encryption and decryption).

References

1. Yun-Peng Zhang, Wei Liu, Shui-ping Cao, Zheng-jun Zhai, Xuan Nie, Wei-di Dai. Digital image encryption algorithm based on chaos and improved DES. In: IEEE international conference on systems, man, and cybernetics, San Antonio, TX, USA; October 2000.
2. Lin Qiu-Hua, Yin Fu-Liang, Zheng Yong-Rui. Secure image communication using blind source separation. In: Emerging technologies: frontiers of mobile and wireless communication conference, vol. 1; 2004. p. 261–4.
3. Ravishankar KC, Venkateshmurthy MG. Region based selective image encryption. In: International conference on computing & informatics, ICOCI ’06; 2006.
4. [Gao Haojiang, Zhang Yisheng, Liang Shuyun, Li Dequn. A new](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0020) [chaotic image encryption algorithm. Chaos Solit Fract](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0020) [2006;29:393–9](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0020).
5. Yu Hai, Zhu Zhiliang, Chen Guanrong. An efficient encryption algorithm based on image reconstruction. In: International workshop on chaos fractals theories and applications; 2009.
6. Kamali SH, Shakerian R, Hedayati M, Rahmani M. A new modified version of advanced encryption standard based algorithm for image encryption. In: 2010 International conference on electronics and information engineering (ICEIE 2010).
7. Paul AJ, Mythili P, Paulose Jacob K. Matrix based crypto- graphic procedure for efficient image encryption. In: Recent advances in intelligent computational systems conference (RAICS); 2011.
8. [Gautam A, Panwar M, Gupta PR. A new image encryption](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0040) [approach using block based transformation algorithm. IJAEST](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0040) [2011;8(1):90–6](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0040).
9. Fei Xiang, Xiao-cong Guo. An image encryption algorithm based on scrambling and substitution using hybrid chaotic systems. In: Seventh international conference on computational intelligence and security; 2011. p. 882–5.
10. [Ye Ruisong, Zhao Haiying. An efficient chaos-based image](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0050) [encryption scheme using affine modular maps. Int J Comput](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0050) [Network Inform Security (IJCNIS) 2012;4(7):41–50](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0050).
11. [Liu Rui, Tian Xiaoping. New algorithm for color image encryp-](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0055) [tion using chaotic map and spatial bit level permutation. J Theor](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0055) [Appl Inform Technol 2012;43(1):89–93](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0055).
12. [Pradhan Chittaranjan, Saxena Vilakshan, Bisoi Ajay Kumar.](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0060) [Imperceptible watermarking technique using Arnold’s transform](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0060) [and cross chaos map in DCT domain. Int J Comput Appl 2012;](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0060) [55(15)](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0060).
13. [Ashtiyani M, Moradi Birgani P, Karimi Madahi SS. Speech signal](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0065) [encryption using chaotic symmetric cryptography. J Basic Appl](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0065) [Sci Res 2012;2(2):1678–84](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0065).
14. [Hyvarinen A, Oja E. Independent component analysis: algorithms](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0070) [and applications. Neural Networks 2000;13:411–30](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0070).
15. [Comon P, Jutten C. Handbook of blind source separation](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0075) [independent component analysis and applications. Academic](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0075) [Press is an imprint of Elsevier; 2010](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0075).
16. [Cardoso JF. Blind signal separation: statistical principles. Proc](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0080) [IEEE 1998;86(10):2009–25](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0080).
17. [Cardoso JF, Souloumiac A. Blind beamforming for non Gaussian](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0085) [signals. IEEE Proc F 1993;140(6):362–70](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0085).
18. [Dong Tianbao, Lei Yingke, Yang Jingshu. An algorithm for](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0090) [underdetermined mixing matrix estimation. Neurocomputing](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0090) [2012:1–9 (Elsevier)](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0090).
19. [Virtanen Tuomas, Gemmeke Jort F, Raj Bhiksha. Active-set](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0095) [newton algorithm for overcomplete non-negative representations](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0095) [of audio. IEEE Trans Audio Speech Lang Process 2013;21(11):](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0095) [2277–89](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0095).
20. [Wang Zhou, Bovik Alan C, Sheikh Hamid R, Simoncelli Eero P.](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0100) [Image quality assessment: from error visibility to structural](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0100) [similarity. IEEE Trans Image Process 2004;13(4)](http://refhub.elsevier.com/S1110-8665(15)00049-3/h0100).