

Efficient Arnold and Singular Value Decomposition based Chaotic Image Encryption

Ashraf Afifi

Department of Computer Engineering
Computers and Information Technology college
Taif University, Al-Hawiyah 21974, Kingdom of Saudi Arabia

Abstract—This paper proposes an efficient image encryption that is based on Arnold transform (AT) and the Singular value decomposition (SVD). The proposed method employs AT on a plain image to transpose all image pixels in the positions, then a diffusion process is applied to the resulted encrypted image via SVD decomposing into three segments. The decryption process aims to derive the plain image from the cipher image. Matlab simulation experiments are done to examine the suggested method. The achieved results show the superiority of the suggested approach with respect to encryption quality.

Keywords—Encryption arnold transform; singular value decomposition; chaotic image encryption

I. INTRODUCTION

Nowadays, the internet and multimedia networks have captured attention in information security researches. Encryption is employed to achieve security. Image encryption is used increasingly in military, communication networks, medical image applications [1-6].

The security of multimedia data which have a high relationship among neighboring pixels has drawn a great attention, recently. The conventional data encryption techniques like AES, IDEA, Triple-DES, and other symmetric ciphering techniques are well known but they may be unsuitable for efficient image ciphering [7].

The main characteristics of chaotic techniques are their high sensibility to control parameters and initial conditions, thus their features can be exploited for achieving the required cryptographic characteristics. In 1998, Fridrich suggested the primary public framework for chaos-based image ciphering. This framework is made up of diffusion and confusion mechanisms [8]. Firstly, the pixels of image are shuffled by employing a 2D chaotic map such as cat, baker, and standard maps. After that, the values of pixels are sequentially altered utilizing a specific discretized 1D chaotic map through the diffusion mechanism. The Fridrich's framework has been considered the most common architectures in different proposed chaos-based image ciphering techniques [9-11].

This paper is mainly focusing on the communications applications with high security levels using AT based SVD security schemes. This scheme is worked by transposing the plain image. Then, the original image will be independently AT then decomposed into three matrices via SVD.

The remainder of the paper has been organized as follows: Section 2 covers the methodology and the main tools employed

in the proposed method, namely the AT and SVD. Section 3 is devoted to detail the enciphering and deciphering phases of the suggested AT SVD image cipher. Section 4 explores the AT SVD of the image cipher detailed security study. Finally, Section 5 presents the conclusions.

II. METHODOLOGY

This section presents a literature survey on the AT and SVD which were used for image encryption method.

A. The AT

The AT is defined as the Cat's mapping [19]. It aims to shift the pixels' positions instead of changing their estimates. Recently, it was employed for image ciphering and watermarking [12-15]. The AT of a pixel (a, b) of an image $f(a, b)$ of size $N \times N$ pixels is defined by $f(a', b')$ and can be expressed mathematically:

$$\begin{bmatrix} a' \\ b' \end{bmatrix} = AT((a, b), N) = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} \pmod{N} \quad (1)$$

Where $\begin{bmatrix} a \\ b \end{bmatrix}$ and $\begin{bmatrix} a' \\ b' \end{bmatrix}$ represent the initial and the position of pixel of shifted image, respectively. 'Mod' defines the modular arithmetic operation. The parameter N is the target image size, which is used to determine the period of AT. The AT period is determined by [16]:

$$\text{Period} = \min[p : [AT(f(a, b), N)]^p = f(a, b)] \quad (2)$$

Where "min" defines the minimum value and p defines the number of iterations. The number of times AT is represented fixed at different values along with different N for improving the image ciphering security [20].

B. The SVD

The SVD is one of the best fit and reliable techniques for matrix decomposition employed in linear algebra. This analogous to the Hermite matrix or symmetry matrix employing a background of eigenvectors. Such method is not only efficient but also stable in decomposing the image into a collection of linearly independent segments, each of which has its energy contribution [17]. Regarding $m \times n$ matrix, orthogonal matrices U and V exist, each with $m \times n$ elements, respectively.

The SVD of X is defined as:

$$X = U * S * V^T \quad (3)$$

Where $S = \text{diag}(\sigma_1, \sigma_2, \dots, \sigma_\Gamma)$, where $\sigma_i, (i = 1, \dots, \Gamma)$ are the singular values of the matrix X with $\Gamma = \min(m, n)$ and satisfying $\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_\Gamma$.

The right singular vectors are the first columns of V and the left singular vectors are the first columns of U . The SVD technique can be applied in digital image cipher and watermarking. The image can be split into three segments then secure them in a variety of ways so that only at the time all the three image segments come together and are multiplied with the right order the information could be retrieved [18-20].

III. THE SUGGESTED AT-SVD CIPHERING METHOD

In this section, the suggested AT- SVD image cryptosystem will be defined in terms of two basic processes namely the encryption and decryption.

A. Encryption Process

This process can be listed in the following steps:

- The clear image is independently shuffled employing the AT.
- The scrambled plain image is decomposed into three encrypted segments with SVD into USV as illustrated in Fig. 1(a).

B. Decryption Process

This process can be listed in the following steps:

- The three encrypted images are firstly multiplied by applying the SVD.
- The inverse AT is implemented to the resulted ciphered image to retrieve the decrypted image as illustrated in Fig. 1(b).

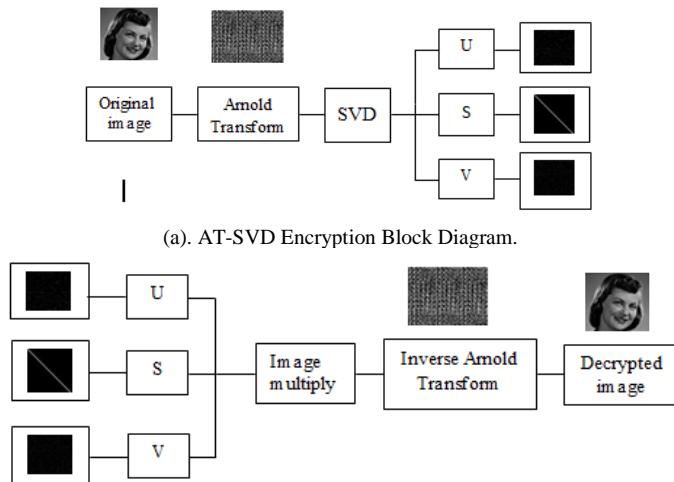


Fig. 1. AT-SVD Decryption Block Diagram.

IV. SIMULATION RESULTS AND PERFORMANCE ANALYSIS

Several measuring tests are carried out to examine the proposed AT- SVD image cryptosystem. Also, its performance is compared with the AT. Tests are performed using 512x512-sized Girl, Peppers and Baboon images as illustrated in Fig. 2.

The ciphering outcomes after employing the proposed AT- SVD image cryptosystem and conventional AT are shown in Fig. 3 Girl, Peppers and Baboon images respectively. It is shown that encrypting with the suggested AT- SVD image cipher succeeded in all images concealment in details.

A. Information Entropy

The information entropy determines the expected entropy value included for the ciphered image. The information entropy is defined as [21-23]:

$$H(K) = - \sum_{i=1}^{2^N-1} P(K_i) \log P(K_i) \quad (4)$$

where $P(K_i)$ represents the probability of symbol. It is shown that the image is good if it has a high estimation of entropy. The entropy information estimations for the cipher images uses the suggested AT- SVD image cipher and AT as depicted in Table I. The information entropy results, illustrate the efficiency of the suggested AT- SVD image cipher when compared to AT cipher. Finally, the entropy outcomes of ciphered image channels resulted by the proposed AT-SVD image cipher is the same with their comparing values in AT plain images.

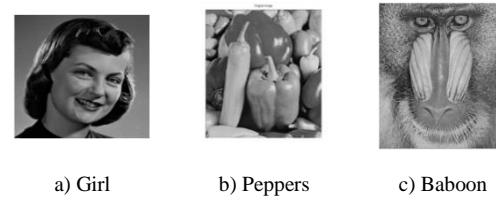


Fig. 2. Test Images - Girl, Peppers and Baboon.

Encryption Scheme

Arnold SVD

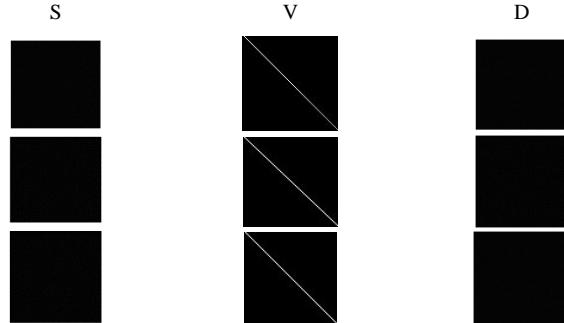


Fig. 3. Ciphered Results of Girl, Peppers and Baboon Images Employing Arnold and the Proposed Arnold SVD Image Cryptosystem.

TABLE I. ENTROPY OUTCOMES OF CIPHERED GIRL, PEPPERS AND BABOON IMAGES EMPLOYING ARNOLD AND THE PROPOSED ARNOLD SVD IMAGE CRYPTOSYSTEM

Image	Encrypted image with Arnold and Arnold SVD			
	Arnold	Arnold SVD		
		S	V	D
Girl	7.0818	4.5749	0.0329	3.1633
Peppers	7.5937	4.5775	0.0332	3.1732
Baboon	7.3583	4.5758	0.0296	3.1706

B. Histogram Test

The histogram test is performed to ensure that the suggested AT- SVD image cipher. For better encryption, the ciphered image's histograms should be completely different from the plain image's histograms. Fig. 4 illustrates the histograms of Girl, Peppers and Baboon images and the histogram of their ciphered versions. The histograms of ciphered Girl, Peppers and Baboon plain images are completely distinguishable from the Girl, Peppers and Baboon plain images histograms.

C. Encryption Quality Results

The correlation coefficient (C_c), the histogram deviation (D_H) and irregular deviation (D_I) and, are calculated for comparing the quality of different ciphered images. The correlation coefficient $r(I_{mg}, E_{nt})$ is estimated between the original and ciphered image that arranged like 1-D sequences as [21-23]:

$$r(I_{mg}, E_{nt}) = \frac{\text{cov}(I_{mg}, E_{nt})}{\sqrt{D(I_{mg})} \sqrt{D(E_{nt})}}, \quad (5)$$

$$\text{cov}(I_{mg}, E_{nt}) = \frac{1}{L} \sum_{l=1}^L (I_{mg}(l) - \text{Mean}(I)) (E_{nt}(l) - \text{Mean}(E_{nt})), \quad (6)$$

$$D(I_{mg}) = \frac{1}{L} \sum_{l=1}^L (I_{mg}(l) - \text{Mean}(I_{mg}))^2, \quad (7)$$

$$D(E_{nt}) = \frac{1}{L} \sum_{l=1}^L (E_{nt}(l) - \text{Mean}(E_{nt}))^2, \quad (8)$$

where L is the pixel numbers within the source image. The aim is to get small C_c estimations between the original image $I_{mg}(x_i, y_j)$ and cipher $E_{nt}(x_i, y_j)$ image. Table II shows the C_c estimates among the source image and encrypted image for AT and the suggested AT- SVD image cipher. The outcomes proof that the suggested AT-SVD image cipher achieve C_c values that are close to ones achieved by AT in Girl, Peppers and Baboon image. This archives the success of the proposed AT- SVD image cipher with respect to C_c experiment.

The D_H calculates the encryption quality between the source and the cipher images. The D_H can be computed as [21-23]:

$$D_H(I, E) = \frac{\left| \sum_{i=0}^{255} d(i) \right|}{M \times N}, \quad (9)$$

where $d(i)$ is the absolute difference amplitude value among the enciphered and the source image histograms of at level i . The estimates M and N resemble the *plain* image dimensions. The main object is to verify higher D_H value confirming the encrypted images are deviated from their corresponding image. Table III illustrates the D_H experiment calculations for the original and ciphered image using AT and the proposed AT- SVD image cipher. The results of the proposed AT- SVD image cipher give larger D_H values compared with Arnold.

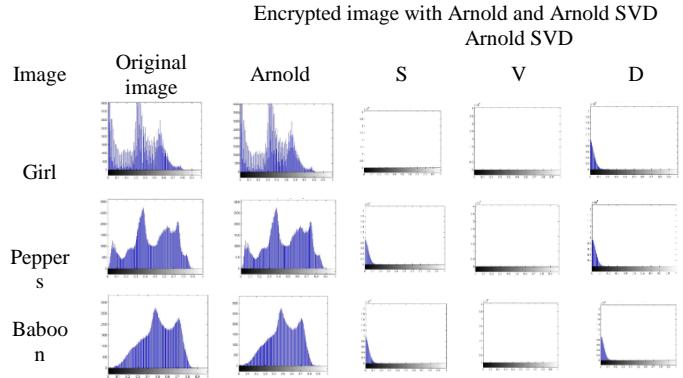


Fig. 4. Histogram Results of the Original Images and Encrypted using Proposed Arnold and Arnold SVD.

TABLE II. CC BETWEEN PLAIN AND ENCRYPTED IMAGES EMPLOYING SUGGESTED ARNOLD AND ARNOLD SVD

Image	Encrypted image with Arnold and Arnold SVD			
	Arnold	Arnold SVD		
		S	V	D
Girl	-0.0022	0.003167	-0.0015	-0.0013
Peppers	-0.0031	0.0015	-0.0025	0.0056
Baboon	-0.0093	0.0018	0.000829	-0.00538

TABLE III. HISTOGRAM DEVIATION BETWEEN SOURCE AND CIPHER IMAGES USING PROPOSED ARNOLD AND ARNOLD SVD

Image	Encrypted image with Arnold and Arnold SVD			
	Arnold	Arnold SVD		
		S	V	D
Girl	0	1.5209	1.4610	1.3033
Peppers	0	1.8117	1.4978	1.5864
Baboon	0	1.9499	1.4985	1.7166

The D_I characterizes the encryption quality in terms of deviation outcomes [22-24]. The irregular deviation can be estimated as [22-24]:

$$D_I = \frac{\left| \sum_{l=0}^{255} h_d(l) \right|}{M \times N}, \quad (10)$$

$$h_d(i) = |h(i) - M|, \quad (11)$$

where the histogram of ciphered image at level i is $h(i)$, and M is the calculated average value for ciphered image an ideal consistent histogram. The main aim is to achieve lower D_I values that show a good quality of ciphered. Table IV show D_I estimates for AT and the suggested AT- SVD image cipher. The suggested AT- SVD image cipher has tiny Im_d values against AT which conforms their achieved encrypted quality.

D. Differential Result

The differential test measures how the cipher images with AT and our AT- SVD image cipher are affected by one-pixel modification. Two common measurements are used; unified average changing Intensity (UACI) and number-of pixels changing rate (NPCR). Assume two cipher images E_1 and E_2 having their source images with only one-pixel difference. In E_1 and E_2 , the pixel estimates at index (a_i, b_j) are $E_1(a_i, b_j)$ and $E_2(a_i, b_j)$, respectively. In bipolar array $D(a_i, b_j)$ with equal ciphered image sizes, the coefficients $D(a_i, b_j)$ are calculated with $E_1(a_i, b_j)$ and $E_2(a_i, b_j)$ values. If $E_1(a_i, b_j) = E_2(a_i, b_j)$, then $D(a_i, b_j) = 1$; otherwise $D(a_i, b_j) = 0$. The NPCR can be calculated as [24-25]:

$$NPCR(E_1, E_2) = \frac{\sum_{i,j} D(a_i, b_j)}{W \times H} \times 100\%, \quad (12)$$

Where, W and H correspond to the width and the height of the ciphered image. The UACI can be calculated as [22-24]:

$$UACI(E_1, E_2) = \frac{1}{M \times N} \left[\sum_{x_i y_j} \frac{|E_1(a_i, b_j) - E_2(a_i, b_j)|}{255} \right] \times 100\%, \quad (13)$$

TABLE IV. IRREGULAR DEVIATION BETWEEN SOURCE AND ENCRYPTED IMAGES USING IMAGES USING PROPOSED ARNOLD AND ARNOLD SVD

Image	Encrypted image with Arnold and Arnold SVD			
	Arnold	Arnold SVD		
		S	V	D
Girl	1.9844	1.9844	1.9839	1.9844
Peppers	1.9844	1.9844	1.9839	1.9844
Baboon	1.9844	1.9844	1.9833	1.9844

The UACI computes the mean intensity of difference among the two ciphered images. The outcomes of the NCPR and the UACI values are shown in Table V. The outcomes ensure that the proposed AT-SVD image cipher is too sensitive to little modifications, but the AT ciphering is less sensitive to small modifications in image.

E. Noise Immunity Measure

The robustness of the proposed AT-SVD image cipher in the AWGN existence is measured in the process of deciphering.

- The PSNR

The PSNR estimates the encryption image components. The PSNR is expressed as [24-25]:

$$PSNR(I, D) = 10 \log \frac{(255)^2}{\sum_{i=0}^{W-1} \sum_{j=0}^{H-1} [I(x_i, y_j) - D(x_i, y_j)]^2} \quad (14)$$

where, $I(x_i, y_j)$ and $D(x_i, y_j)$ are the gray level of the intensity value at location (x_i, y_j) of the original and decipher image, respectively. High PSNR estimates show good resistance to noise. The noise resistance values are given in Tables VI and VII. The outcomes prove that the suggested AT-SVD image cipher has good resistance to noise thus it can be a best choice for ideal telecommunication applications.

- The SSIM

The SSIM can be computed as [25]:

$$SSIM(x, y|w) = \frac{(2\bar{w}_x \bar{w}_y + V_1)(2\sigma_{w_x w_y} + V_2)}{(\bar{w}_x^2 + \bar{w}_y^2 + V_1)(\sigma_{w_x}^2 + \sigma_{w_y}^2 + V_2)} \quad (15)$$

TABLE V. ESTIMATIONS OF NPCR AND UACI FOR TWO ENCRYPTION IMAGES FOR TESTED IMAGES USING SUGGESTED ARNOLD AND ARNOLD SVD

Image	Encrypted image with Arnold and Arnold SVD			
	Arnold	Arnold SVD		
		S	V	D
Girl	NCPR	98.1594	100	24.5590
	UACI	0	0	0
Peppers	NCPR	99.9992	100	47.5876
	UACI	0	0	0
Baboon	NCPR	99.9935	100	52.7199
	UACI	0	0	0

TABLE VI. PSNR ESTIMATES OF IMAGES IN THE EXISTENCE OF AWGN WITH DIFFERENT SNR (SNR IN DB) USING ARNOLD SVD

Image	PSNR			
	AWGN			
	10 dB	20 dB	30 dB	40 dB
Girl	-11.3978	3.3322	7.6368	8.3292
Peppers	-18.9071	-1.8042	4.6188	5.6515
Baboon	-19.4560	-2.2318	4.3681	5.4727

TABLE VII. PSNR IMAGES ESTIMATES IN THE EXISTENCE OF AWGN WITH DIFFERENT SNR (SNR IN DB) USING ARNOLD SVD

Image	PSNR				
	AWGN				
	10 dB	20 dB	30 dB	40 dB	
Girl					
Peppers					
Baboon					

where, V_1 , V_2 are minor constants, \bar{w}_x and \bar{w}_y are the mean of w_x and w_y regions, respectively. $\Sigma_{w_x}^2$ is the variance of w_x region and $\sigma_{w_x w_y}$ is covariance among two regions w_x and w_y . The SSIM outcomes are given in Table VIII. The values prove that the suggested AT- SVD image cryptosystem has better resistance to noise.

- The FSIM

The FSIM permits to evaluate the deciphered image and can be defined as [25]:

$$\text{FSIM} = \frac{\sum_{x \in \Omega} B_L(x).PV_m(x)}{\sum_{x \in \Omega} PC_m(x)} \quad (16)$$

where Ω is the special domain of image, $B_L(x)$ corresponds the overall equivalence between $PV_m(x)$ and two images is phase congruency value. Large FSIM values make the noise immunity better. The FSIM measures outcomes are given in Table IX. The results prove that the AT- SVD image cryptosystem is noise resistant.

TABLE VIII. SSIM ESTIMATES IN THE EXISTENCE OF AWGN WITH DIFFERENT SNR (SNR IN DB) USING ARNOLD SVD

Image	Structure Similarity Index (SSIM)			
	AWGN			
	10 dB	20 dB	30 dB	40 dB
Girl	9.085*10 ⁻⁶	3.662*10 ⁻⁴	0.0048	0.0337
Peppers	1.058*10 ⁻⁶	9.065*10 ⁻⁵	4.74*10 ⁻⁴	0.0022
Baboon	9.77*10 ⁻⁷	9.659*10 ⁻⁵	2.769*10 ⁻⁴	0.0010

TABLE IX. FSIM ESTIMATES IN THE EXISTENCE OF AWGN WITH DIFFERENT SNR (SNR IN DB) USING ARNOLD SVD

Image	Structure Similarity Index (FSIM)			
	AWGN			
	10 dB	20 dB	30 dB	40 dB
Girl	0.0029	3.66*10 ⁻⁴	0.1645	0.5218
Peppers	8.76*10 ⁻⁴	0.0167	0.0845	0.2653
Baboon	8.858*10 ⁻⁴	0.0183	0.0783	0.1992

V. CONCLUSION

An efficient chaotic encryption of images based on AT and SVD is the main finding of this paper. In the proposed technique, the plain image is submitted to AT confusion and SVD diffusion. For the decryption phase, the cipher image segments are composed by the SVD diffuser and then inversely transformed by AT in order to derive the original image. A set of experiments have been performed in order to test the AT-SVD image cryptosystem. The obtained outcomes prove the efficiency of the suggested AT- SVD image cipher.

REFERENCES

- [1] R. Tao, J. Lang, Y. Wang, "Optical image encryption based on the multiple parameter fractional Fourier transform," Opt. Lett. 33, pp. 581–583, 2008.
- [2] H.M. Ozaktas, A. Koc, I. Sari, M.A. Kutay, "Efficient computation of quadratic phase integrals in optics," Opt. Lett. 31, pp. 35–37, 2006.
- [3] Z. Liu, S. Liu, "Randomization of the Fourier transform," Opt. Lett. 32, pp. 478–480, 2007.
- [4] Z. Liu, S. Liu, "Double image encryption based on iterative fractional Fourier transform," Opt. Commun. vol. 275, pp. 324–329, 2007.
- [5] Chengqing L, Shujun L, Asim M, Nunez J, Alvarez G, "On the security defects of an image encryption scheme", Image Vis comp.; 2781371-81, 2009.
- [6] Chengqing L, Lo K., "Optimal quantitative encryptanalysis of permutation-only multimedia ciphers against plaintext attacks", Signal Process, 91:949-54, 2011.
- [7] Li, S., Chen, G., Zheng, X.: Chaos-based encryption for digital images and videos. In: Furht, B., Kirovski, D. (eds.) Multimedia Security Handbook. CRC Press, Florida (2004).
- [8] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," International Journal of Bifurcation and Chaos in Applied Sciences and Engineering, vol. 8, no. 6, pp. 1259–1284, 1998.
- [9] R. Ye, H. Huang, Application of the Chaotic Ergodicity of Standard Map in Image Encryption and Watermarking, I. J. Image, Graphics and Signal Processing, 19–29, 2010.
- [10] H. Liu, X. Wang, Color image encryption using spatial bit-level permutation and high-dimension chaotic system, Optics Communications, 284, 3895–3903, 2011.
- [11] R. Ye, A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism, Optics Communications, 284, 5290–5298, 2011.
- [12] ZJ. Liu, I. Xu, T. Liu, H. Chen, P.F. Li, C. Lin, S.T., Liu. Optics Communications 284,123, 2011.
- [13] W, Chen, C, Quan, C.J, Tay, Optics Communications , pp. 282-3680, 2009.
- [14] X.P.Deng, D.M, Zhao, Optics Communications, pp. 284-5623, 2011.
- [15] Z.J. Liu,M, Gong Y.K. Dou, F. Liu , S, Lin, M.A. Ahmed, J.M. Dai, S.T. S.T. Liu, Optics and Lasers in Engineering, pp. 50-248, 2012.
- [16] Vilardy JM, Torres CO, Jumenez, C "Double image encryption method using the Arnold transform in the fractional Hartley domain" Proc SIE 8785, [87851R-87851/SR], 2013.
- [17] Bhatnagar G, Wu QMJ, Raman B, "SVD –based robust watermarking using fractional cosine transform, DPIE, 7708, 1-11, 2010.
- [18] Gaurav B, Bhatnagar, Q.M, Jonathan WU, "Selective image encryption based on pixels of interest and singular value decomposition" DSP journal, vol. 22,648-663, 2012.
- [19] Linfei Chen, Daomu Zhao, Fan Ge, "Image encryption based on singular value decomposition and Arnold transform in fraction domain" Optics communication journal, vol. 291, 98-103, 2013.
- [20] Phool Singh, A.K.. Yadav, Kehar Singh, "Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition" Optics and Laser in Engineering journal, vol. 91, 187-195, 2017.

- [21] Andrew B. Watson, "Image Compression Using the Discrete Cosine Transform", Technical Report, NASA Ames Research Center, Mathematica Journal, 4(1), 1994, p. 81-88, 1994.
- [22] J. Fridrich, "Symmetric Ciphers Based on Two-dimensional Chaotic Maps," International Journal of Bifurcation and Chaos, vol. 8(6), pp. 1259-1284, 1998.
- [23] Osama S. Faragallah, "Digital Image Encryption Based on the RC5 Block Cipher Algorithm," Sensing and Imaging: An International Journal, vol. 12(3), pp. 73-94, Springer, 2011.
- [24] Osama S. Faragallah, "An Enhanced Chaotic Key-Based RC5 Block Cipher Adapted to Image Encryption," International Journal of Electronics, vol. 99(7), pp. 925-943, Taylor & Francis, 2012.
- [25] Ensheerah A. Naeem, Mustafa M. Abd Elnaby, Hala S. El-sayed, Fathi E.Abd El-Samie, and Osama S. Faragallah, "Wavelet Fusion for Encrypting Images with Few Details", Computers and Electrical Engineering, vol. 60, pp. 450-470, 2016

AUTHOR'S PROFILE



Ashraf Afifi received the B.Sc.(Hons.), M.Sc., and Ph.D. degrees in Electronic and Communication Engineering from Zagazig University, Egypt, in 1987, 1995, and 2002, respectively. He is currently Associate Professor with the Department of Computer Engineering, Faculty of Computers and Information Technology, Taif University, Saudi Arabia. He is a coauthor of about 35 papers in international journals and conference proceedings. His research interests cover communication security, image processing, and image encryption.