Hindawi
Security and Communication Networks
Volume 2017, Article ID 5790189, 9 pages
https://doi.org/10.1155/2017/5790189

Research Article

A Novel Fuzzy Encryption Technique Based on Multiple Right Translated AES Gray S-Boxes and Phase Embedding

Naveed Ahmed Azam

Faculty of Engineering Sciences, GIK Institute of Engineering Sciences and Technology, Topi, Pakistan

Correspondence should be addressed to Naveed Ahmed Azam; naveedzm961@gmail.com

Received 15 July 2016; Revised 6 October 2016; Accepted 17 October 2016; Published 11 January 2017

Academic Editor: Pascal Lorenz

This paper presents a novel image encryption technique based on multiple right translated AES Gray S-boxes (RTSs) and phase embedding technique. First of all, a secret image is diffused with a fuzzily selected RTS. The fuzzy selection of RTS is variable and depends upon pixels of the secret image. Then two random masks are used to enhance confusion in the spatial and frequency domains of the diffused secret image. These random masks are generated by applying two different RTSs on a host image. The decryption process of the proposed cryptosystem needs the host image for generation of masks. It is therefore, necessary, to secure the host image from unauthorized users. This task is achieved by diffusing the host image with another RTS and embedding the diffused secret image into the phase terms of the diffused host image. The cryptographic strength of the proposed security system is measured by implementing it on several images and applying rigorous analyses. Performance comparison of the proposed security technique with some of the state-of-the-art security systems, including S-box cryptosystem and steganocryptosystems, is also performed. Results and comparison show that the newly developed cryptosystem is more secure.

1. Introduction

The demand of security of digital images is increased due to extensive transmission of different image files through internet [1, 2]. Therefore, it is essential to develop some algorithms to secure secret images. Different types of image security techniques are proposed by the researchers. Cryptography and steganography are two different widely used techniques for securing the content of secret images. The basic principle of cryptography is to transform secret image (plain image) into diffused image (cipher image) by creating confusion in its information. In many cryptosystems, substitution box (S-box) is solely responsible for creation of diffusion in image [3]. Daemen and Rijmen proposed a block cipher which is used by National Institute of Standard and Technology as Advanced Encryption Standard (AES) [4]. At present, AES is commonly used cryptosystem. Due to the fundamental role of S-box in AES, many cryptographers have paid their attention to study the AES S-box. An algebraic expression for Rijndael block cipher is presented in [5]. In [6], a new simple mathematical description of the AES S-box is given. A permutation polynomial representation of the AES S-box is presented in [7]. It is observed that the polynomial of the AES S-box has only nine nonzero terms which reveals that the security of AES is suspected against computational attacks [6, 7]. In order to remove this weakness of AES, many researchers have proposed new S-boxes (e.g., refer to [8–13]). In [8], an improved S-box is proposed. The drawback of their work is that their S-box cannot be implemented by using the existing framework of AES. The reason behind low complexity of the AES S-box is identified in [9]. Moreover, a new version of S-box is also presented in [9]. In [10], another S-box is developed based on affine mapping having 253 nonzero terms in its polynomial and reuses the existing implementation of AES. The algebraic complexity of the AES S-box is further enhanced by introducing a new S-box based on Gray codes in [11]. The improved S-box has 255 nonzero terms and reuses the whole existing framework of AES. A generalization of Gray S-box is presented in [12]. Right translation and regular representation of Galois field GF(2^8) are used to generate 256 different RTSs all with high algebraic complexity and satisfying other security tests including nonlinearity, bit independence, strict avalanche, linear approximation, differential approximation, algebraic complexity, correlation, and histogram. Similar to Gray S-box, RTSs are also compatible with the existing implementation of AES S-box. Furthermore, it is claimed in [12] that the latest computational attacks, such as linear, differential, and algebraic attacks [14, 15], can be effectively encountered with a cryptosystem based on multiple S-boxes as compared to a security system relaying on single S-box.

In steganography, secret image is embedded into another image called host image. The embedding is done in such a way that unauthorized users cannot detect the presence of the secret image in the resulting image [16–19]. Recently, many scientists have developed new image security algorithms based on combination of cryptography and steganography. In [20], a steganocryptosystem is proposed by using optical encryption, phase embedding, and fixed data hiding technique for Gray scale images. In [21], an improved version of steganocryptosystem with adaptive data hiding technique is presented. Chaotic S-boxes are used to improve the security of secret image after embedding it into a host image in [22]. In [23], secret image is first encrypted by AES and then embedded into host image by using least significant bit (LSB) embedding technique. Similarly, many other researchers proposed steganocryptosystems (e.g., refer to [24–27]).

In this paper, we propose a novel image security system based on variable multiple RTSs and steganography. The proposed technique uses four different RTSs and phase embedding technique. Fuzzy approach is used for the selection of RTSs which depends upon pixels of the secret image. The proposed algorithm also utilizes spatial and frequency domains of the secret image for confusion purpose. The aim of this technique is to develop a security system which can efficiently resist the computational attacks as compared to single S-box security techniques and steganocryptosystems. Several tests are applied on the proposed cryptosystem to evaluate its security strength. The experimental results show that the proposed security technique has high resistance against computational attacks as compared to some of the well-known existing security algorithms. Rest of the paper is organized as follows: Section 2 consists of preliminaries. Novel encryption technique is presented in Section 3. Section 4 consists of analyses and comparisons. Finally, conclusion and future directions are given in Section 5.

2. Preliminaries

2.1. Fuzzy Set. A fuzzy set is a pair (f, X), where X is a set and f is a function from set X to the interval $[0, 1]$. The function f is called membership function and it indicates the grade of membership of elements of X in (f, X). Nowadays, fuzzy theory is widely used in many cryptosystems (e.g., refer to [28–30]).

2.2. Right Translated AES Gray S-Boxes (RTSs). A technique for the generation of multiple S-boxes is introduced in [12]. This technique uses the regular representation of Galois field $GF(2^8)$ and Gray codes [31]. The main advantage of this technique is that it generates an algebraically complex S-box corresponding to each element of $GF(2^8)$. Since there are 256 elements in $GF(2^8)$, therefore there are 256 different RTSs. The mathematical expression for the generation of RTSs is given below:

$$\xi(g) = S_{\mathrm{AES}} \circ \rho_g \circ G, \tag{1}$$

where g is an element of $GF(2^8)$, S_{AES} is the AES S-box, ρ_g is a permutation representation of g, G is the Gray code mapping, and $\xi(g)$ is the resultant RTS corresponding to g.

3. The Proposed Security System

In this section, we presented a new security system based on RTSs and steganography. Let I be a secret image and J a host image. Both I and J are Gray scale images of same dimensions $M \times N$. The main steps of the proposed encryption and decryption algorithms are given below.

3.1. The Encryption Algorithm

Step 1. Fuzzy selection criterion for RTS:

(a) Define a fuzzy set $(f, GF(2^8))$ by

$$f(g) = \frac{\#(g)}{M \times N}, \tag{2}$$

where $\#(g)$ is the frequency of g in I. This fuzzy set gives the grade of membership of each element of Galois field $GF(2^8)$ in the secret image.

(b) Suppose l is the supremum of the range of f; that is, $l = \sup\{f(g)\}$.

(c) Now, calculate preimages $g_1, g_2, g_3, \ldots, g_n$ of l. The infimum g of the preimages is the minimum element of $GF(2^8)$ which has maximum grade of membership in the secret image I.

(d) Diffuse I with $\xi(g)$, RTS corresponding to g, to get I_g.

Step 2. Generation of random masks and confusion in spatial and frequency domains:

(a) Fix an element c of $GF(2^8)$ and select three RTSs $\xi(S_1)$, $\xi(S_2)$, and $\xi(S_3)$ by using (1) and following three equations:

$$\begin{aligned} S_1 &= g + c, \quad (\mathrm{mod}\ 256), \\ S_2 &= S_1 + c, \quad (\mathrm{mod}\ 256), \\ S_3 &= S_2 + c, \quad (\mathrm{mod}\ 256). \end{aligned} \tag{3}$$

(b) Apply $\xi(S_1)$ and $\xi(S_2)$ on the host image J to get its two different diffused versions J_1 and J_2.

(c) Now generate two random masks R_1 and R_2 for creation of confusion in spatial and frequency domains of the diffused secret image I_g. The mathematical expressions of these masks are given below:

$$R_1 = \exp\left(\frac{i\pi J_1}{128}\right),$$
$$R_2 = \exp\left(\frac{i\pi J_2}{128}\right). \quad (4)$$

The random noise is then generated in the content of I_g by using

$$I_R = F^{-1}\left[F\left(I_g \times R_1\right) \times R_2\right], \quad (5)$$

where F is the Fourier transformation and F^{-1} is the inverse Fourier transformation.

Step 3. Securing the host image and embedding process:

The process of decryption cannot be completed until R_1 and R_2 are known. Traditionally, R_1 and R_2 can be retrieved by embedding them in I_R. But, this process increases the size of encrypted image and affects the quality of decrypted image [20–22]. Despite this, we embed I_R in the host image because R_1 and R_2 can be regenerated by J. The host image is secured from third party by diffusing J with RTS corresponding to S_3, that is, $\xi(S_3)$. Finally, I_R and g are embedded in the phase terms of the diffused host image J_3. The following is the mathematical equation of embedding process:

$$I_S = J_3 \exp\left(i\frac{\pi}{2}I_R\right). \quad (6)$$

The proposed encryption process is elaborated in Figure 1(a).

3.2. The Decryption Algorithm

Step 1. In the decryption process, first of all J_3, I_R, and g are extracted by calculating complex modulus and argument of I_S:

$$J_3 = \left|I_S\right|,$$
$$I_R = \frac{2}{\pi}\arg\left(I_S\right). \quad (7)$$

Step 2. Apply inverse of $\xi(S_3)$ on J_3 to generate random masks R_1 and R_2 by using Step 2 of the proposed encryption technique. Now, calculate their complex conjugates $\overline{R_1}$ and $\overline{R_2}$ because they can cancel the effect of random masks as shown below:

$$\begin{aligned} R_1 \times \overline{R_1} &= \exp\left(\frac{i\pi J_1}{128}\right) \times \exp\left(-\frac{i\pi J_1}{128}\right) \\ &= \exp\left(\frac{i\pi J_1}{128} - \frac{i\pi J_1}{128}\right) = \exp(0) = 1. \end{aligned} \quad (8)$$

Step 3. Next, random masks are removed by using the following equation:

$$I_g = F^{-1}\left[F\left(I_R\right) \times \overline{R_2}\right] \times R_1. \quad (9)$$

Step 4. Finally, inverse of RTS corresponding to g is applied on I_g to restore the secret image I.

The flowchart of the proposed decryption process is shown in Figure 1(b).

4. Security Analyses and Comparison

We implemented the proposed technique and other security systems, presented in [10–12, 23, 24, 32–34], with the help of Matlab on 31 Gray scale images of dimensions 225×225. These test images were taken from [35]. We used image of Lena as host image for our experiments. The aim of this section is to investigate and compare the strength of the proposed security algorithm with some of the existing cryptosystems based on single S-box and combination of S-box and steganography.

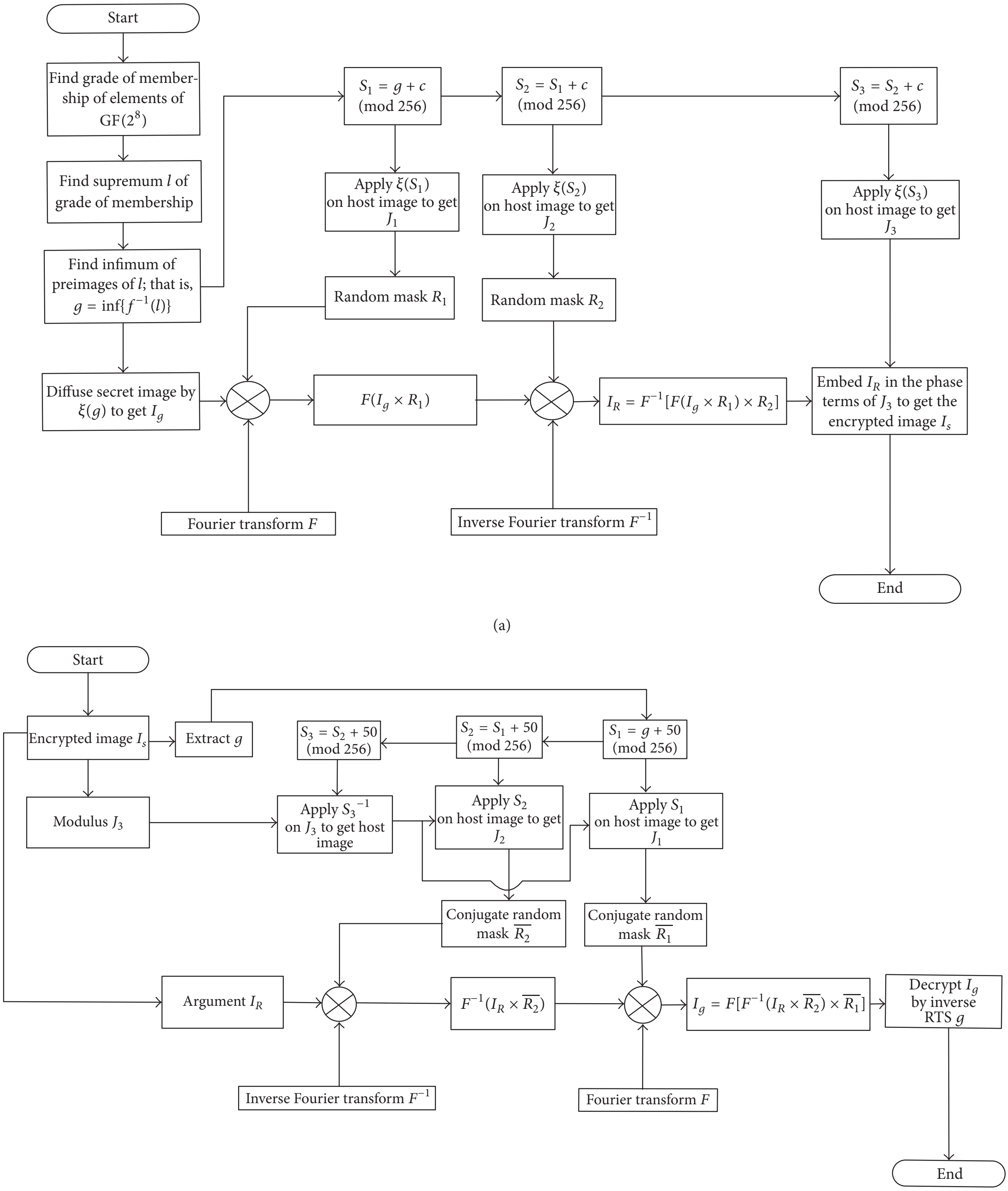
4.1. Objective Fidelity Criteria. The purpose of this experiment is to measure the amount of error in the reconstructed image and original image. A cryptosystem is good if the value of error is high and if the value of error is small then the security of cryptosystem is suspicious. Root mean square error (RMSE) and peak signal to noise ratio (PSNR) are the two commonly used parameters to measure the level of fidelity [36–38]. RMSE and PSNR are given by the equations:

$$\text{RMSE} = \sqrt{\frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\left(I(x,y) - I'(x,y)\right)^2}{M \times N}},$$
$$\text{PSNR} = 10\log_{10}\left[\frac{(255)^2}{\sum_{x=1}^{M}\sum_{y=1}^{N}\left(I(x,y) - I'(x,y)\right)^2} \times M \times N\right], \quad (10)$$

where I denotes plain image and I' denotes cipher image.

We applied fidelity analysis on the proposed technique and other security systems. A comparison of the experimental results is given in Figures 2(a) and 2(b). It is clear from Figures 2(a) and 2(b) that the proposed cryptosystem is creating maximum value of RMSE and minimum value of PSNR as compared to other security techniques. Hence, the proposed technique is satisfying objective fidelity criterion efficiently more than that of other cryptosystems.

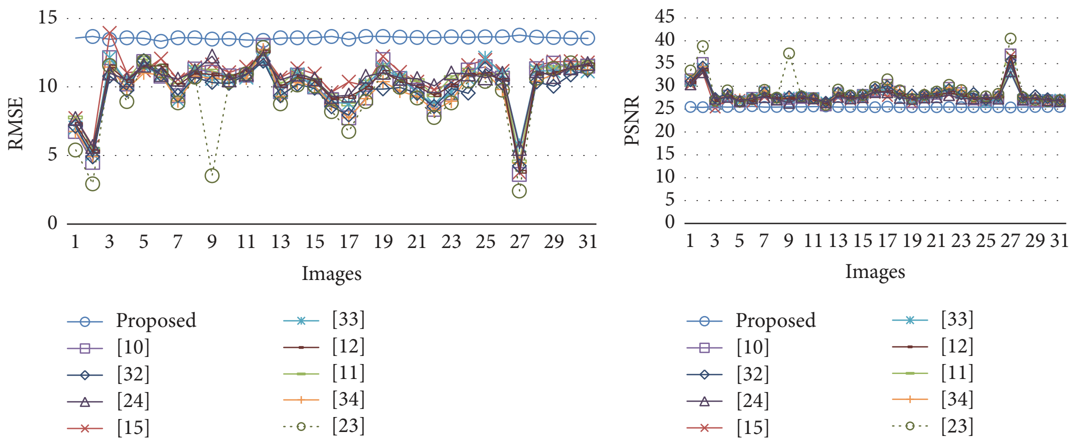
4.2. Sensitivity Analysis. Generally, a cryptanalyst uses differential attack to steal the information from the ciphered image. In this attack a slight change is produced in the pixels of the image to analyze the extent of change in the resultant image. Unified average changing intensity (UACI) is used to measure the level of security of a cryptosystem against differential


Start
Find grade of membership of elements of GF(2^8)
Find supremum l of grade of membership
Find infimum of preimages of l; that is, $g = \inf\{f^{-1}(l)\}$
Diffuse secret image by $\xi(g)$ to get I_g
$S_1 = g + c$ (mod 256)
$S_2 = S_1 + c$ (mod 256)
$S_3 = S_2 + c$ (mod 256)
Apply $\xi(S_1)$ on host image to get J_1
Apply $\xi(S_2)$ on host image to get J_2
Apply $\xi(S_3)$ on host image to get J_3
Random mask R_1
Random mask R_2
$F(I_g \times R_1)$
$I_R = F^{-1}[F(I_g \times R_1) \times R_2]$
Embed I_R in the phase terms of J_3 to get the encrypted image I_s
Fourier transform F
Inverse Fourier transform F^{-1}
End
Start
Encrypted image I_s
Extract g
$S_3 = S_2 + 50$ (mod 256)
$S_2 = S_1 + 50$ (mod 256)
$S_1 = g + 50$ (mod 256)
Modulus J_3
Apply $S_3{}^{-1}$ on J_3 to get host image
Apply S_2 on host image to get J_2
Apply S_1 on host image to get J_1
Conjugate random mask $\overline{R_2}$
Conjugate random mask $\overline{R_1}$
Argument I_R
$F^{-1}(I_R \times \overline{R_2})$
$I_g = F[F^{-1}(I_R \times \overline{R_2}) \times \overline{R_1}]$
Decrypt I_g by inverse RTS g
Inverse Fourier transform F^{-1}
Fourier transform F
End

(a)

(b)

Figure 1: (a) Flowchart of encryption algorithm. (b) Flowchart of decryption algorithm.



(a) (b)

Figure 2: (a) Results and comparison of RMSE. (b) Results and comparison of PSNR.

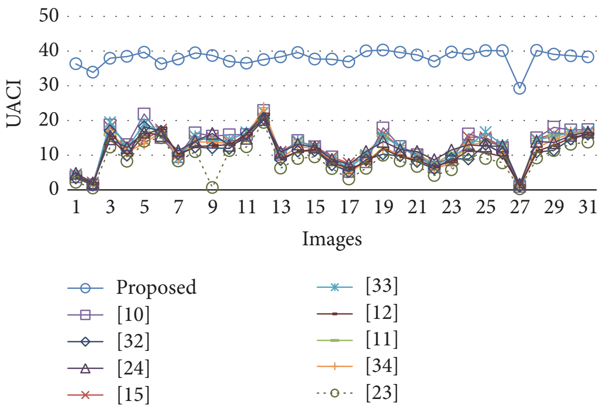


Figure 3: Results and comparison of UACI.

attack [32, 39]. The mathematical expression for calculation of UACI is given below:

$$\mathrm{UACI} = \frac{1}{M \times N}\left[\frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\left|I(x,y) - I'(x,y)\right|}{255}\right] \times 100. \tag{11}$$

The results of this experiment are shown in Figure 3. It is evident from Figure 3 that the proposed technique generates maximum value of UACI. Hence it resists differential attack efficiently as compared to other techniques.

4.3. Correlation and Contrast Analysis. The pixels of plain image are highly correlated in horizontal, vertical, and diagonal directions. A cryptosystem is secure if it can reduce correlation and increase contrast between pixels significantly. The correlation coefficient r_{xy} is calculated by the following expression:

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{H(x)}\sqrt{H(y)}}, \tag{12}$$

where

$$\operatorname{cov}(x,y) = \frac{1}{M}\sum_{i=1}^{M}\left(x_i - E(x)\right)\left(y_i - E(y)\right),$$
$$H(x) = \frac{1}{M}\sum_{i=1}^{M}\left(x_i - E(x)\right)^2, \tag{13}$$
$$E(x) = \frac{1}{M}\sum_{i=1}^{M}x_i.$$

We calculated the correlation of pixels in vertical, horizontal, and diagonal directions and their results are plotted in

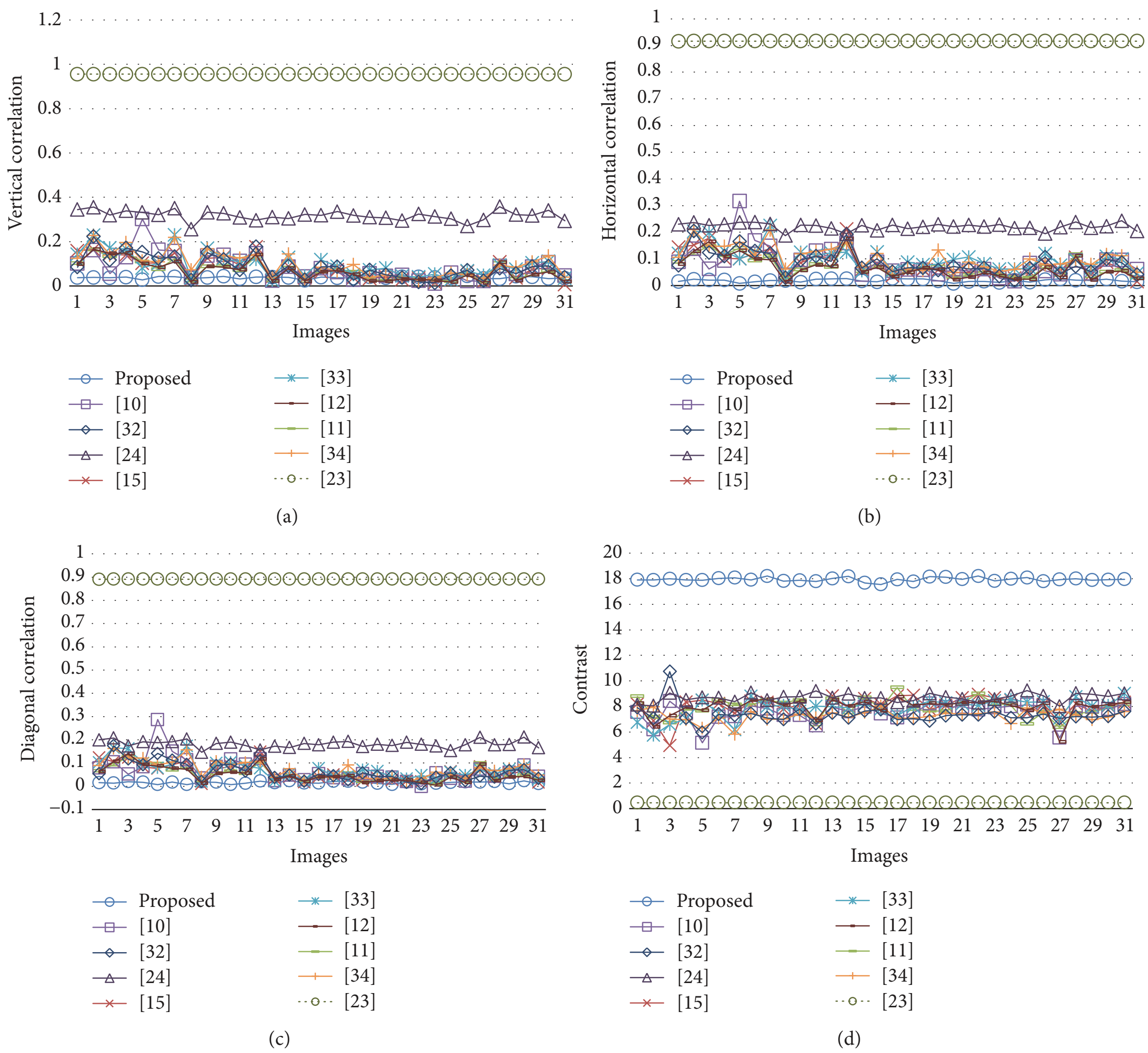


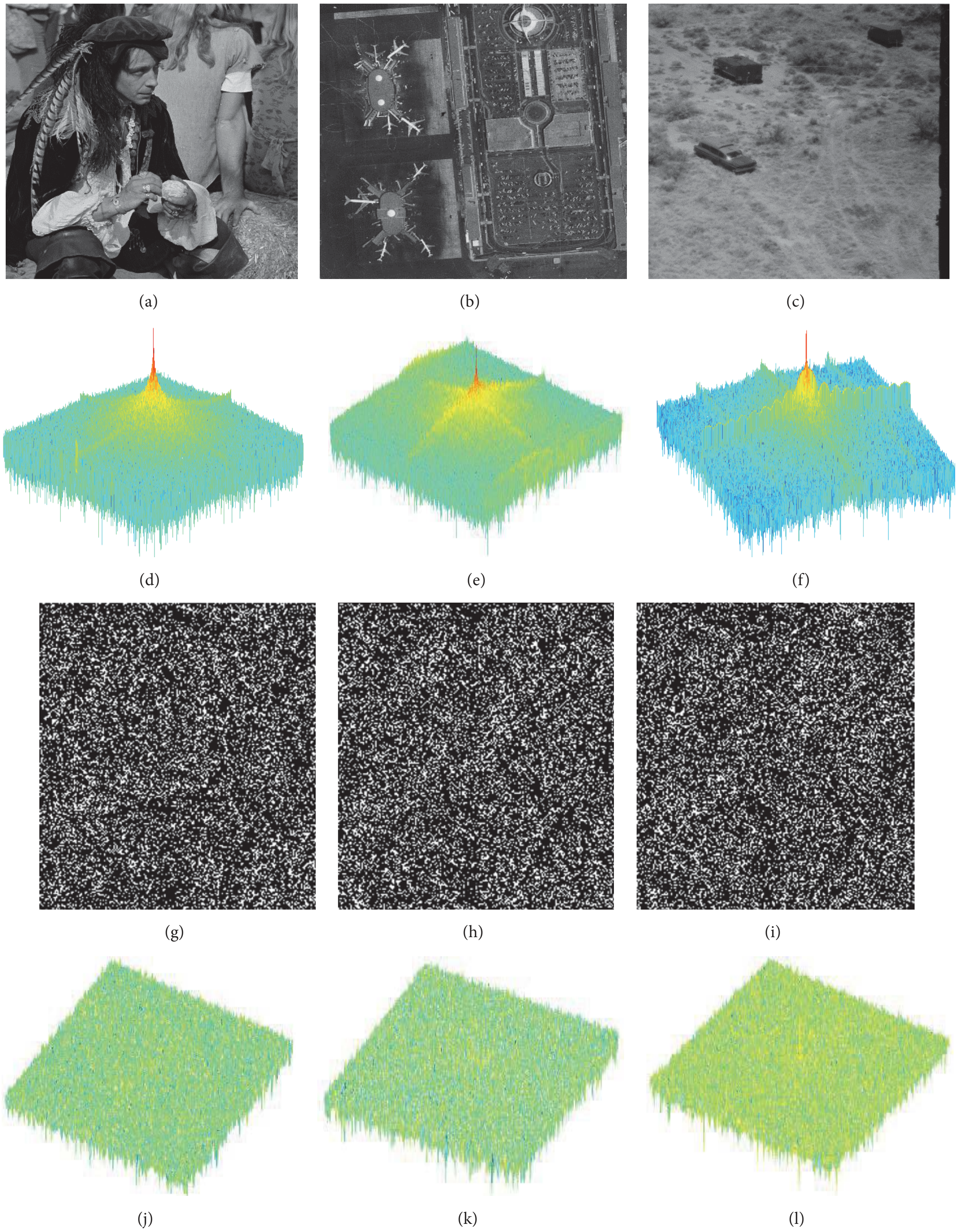
Figure 4: (a) Results and comparison of vertical correlation. (b) Results and comparison of horizontal correlation. (c) Results and comparison of vertical correlation. (d) Results and comparison of contrast analysis.

Figures 4(a)–4(c). The results of contrast analysis are shown in Figure 4(d). These figures indicate that the proposed security technique produces minimum correlation and maximum contrast.

4.4. Spectrum Magnitude Analysis. In an image, the frequency spectrum is not uniformly distributed. A cryptosystem is said to be good if it distributes frequency uniformly and creates significant difference between the spectrums of plain image and cipher image. We have applied this test on all 31 images. Three encrypted images and their frequency spectrums are shown in Figures 5(g)–5(i) and Figures 5(j)–5(l), respectively. Figures 5(d)–5(f) show frequency spectrums of the secret images. Note that the frequency distribution in Figures 5(d)–5(f) is concentrated in a small region located in the middle of each image. Usually, this small region suffers from security attacks. It is evident from Figures 5(j)-5(i) that the frequency is distributed uniformly in the encrypted images. Hence, encrypted images by the proposed scheme are secure against statistical attacks.

5. Conclusion

In this study, we proposed a Gray scale image encryption technique based on RTSs and steganography. The proposed cryptosystem uses multiple RTSs and phase embedding technique for the generation of confusion in spatial and frequency domains of secret image. Fuzzy approach is used for the selection of RTSs. Analyses and comparison showed that the proposed security system is more secure as compared to some of the well-known cryptosystems based on single S-box and combination of S-box and steganography. In future, the newly developed algorithm can be used for the encryption of color image and data hiding purpose with some modifications.



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

(j) (k) (l)

Figure 5: (a) Secret image. (b) Secret image. (c) Secret image. (d) Frequency spectrum of (a). (e) Frequency spectrum of (b). (f) Frequency spectrum of (c). (g) Encryption of (a). (h) Encryption of (b). (i) Encryption of (c). (j) Frequency spectrum of (g). (k) Frequency spectrum of (h). (l) Frequency spectrum of (i).

Competing Interests

There is no conflict of interests regarding publication of this article.

Acknowledgments

The author thanks Shahid Ahmad for proofreading this paper.

References

[1] A. Philip, "A generalized pseudo-Knight's tour algorithm for encryption of an image," *IEEE Potentials*, vol. 32, no. 6, pp. 10–16, 2013.

[2] J. Liu, H. Jin, L. Ma, Y. Li, and W. Jin, "Optical color image encryption based on computer generated hologram and chaotic theory," *Optics Communications*, vol. 307, pp. 76–79, 2013.

[3] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[4] J. Daemen and V. Rijmen, *The Design of RIJNDAEL: AES—The Advanced Encryption Standard*, Springer, Berlin, Germany, 2002.

[5] N. Ferguson, R. Schroeppel, and D. Whiting, "A simple algebraic representation of Rijndael," in *Selected Areas in Cryptography SAC '01*, vol. 2259 of *Lecture Notes in Computer Science*, pp. 103–111, Springer, 2001.

[6] S. Murphy and M. J. Robshaw, "Essential algebraic structure within the AES," in *Advances in Cryptology—CRYPTO 2002: 22nd Annual International Cryptology Conference Santa Barbara, California, USA, August 18–22, 2002 Proceedings*, vol. 2442 of *Lecture Notes in Computer Science*, pp. 1–16, Springer, Berlin, Germany, 2002.

[7] J. Rosenthal, "A polynomial description of the Rijndael advanced encryption standard," *Journal of Algebra and Its Applications*, vol. 2, no. 2, pp. 223–236, 2003.

[8] J. Liu, B. Wei, X. Cheng, and X. Wang, "An AES S-box to increase complexity and cryptographic analysis," in *Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA '05)*, pp. 724–728, Taipei, Taiwan, March 2005.

[9] L. Jingmei, W. Baodian, and W. Xinmei, "One AES S-box to increase complexity and its cryptanalysis," *Journal of Systems Engineering and Electronics*, vol. 18, no. 2, pp. 427–433, 2007.

[10] L. Cui and Y. Cao, "A new S-box structure named affine-power-affine," *International Journal of Innovative Computing, Information and Control*, vol. 3, no. 3, pp. 751–759, 2007.

[11] M.-T. Tran, D.-K. Bui, and A.-D. Duong, "Gray S-box for advanced encryption standard," in *Proceedings of the International Conference on Computational Intelligence and Security (CIS '08)*, pp. 253–258, December 2008.

[12] M. Khan and N. A. Azam, "Right translated AES gray S-boxes," *Security and Communication Networks*, vol. 8, no. 9, pp. 1627–1635, 2015.

[13] M. Khan and N. A. Azam, "S-boxes based on affine mapping and orbit of power function," *3D Research*, vol. 6, article 12, 2015.

[14] T. Jakobsen and L. R. Knudsen, "The interpolation attack on block ciphers," in *Fast Software Encryption: 4th International Workshop, FSE'97 Haifa, Israel, January 20–22 1997 Proceedings*, Lecture Notes in Computer Science, pp. 28–40, Springer, Berlin, Germany, 1997.

[15] N. T. Courtois and J. Pieprzyk, "Cryptanalysis of block ciphers with overdefined systems of equations," in *Advances in Cryptology—ASIACRYPT 2002: 8th International Conference on the Theory and Application of Cryptology and Information Security Queenstown, New Zealand, December 1–5, 2002 Proceedings*, vol. 2501 of *Lecture Notes in Computer Science*, pp. 267–287, Springer, Berlin, Germany, 2002.

[16] T.-S. Chen, C.-C. Chang, and M.-S. Hwang, "A virtual image cryptosystem based upon vector quantization," *IEEE Transactions on Image Processing*, vol. 7, no. 10, pp. 1485–1488, 1998.

[17] Y.-C. Hu, "High-capacity image hiding scheme based on vector quantization," *Pattern Recognition*, vol. 39, no. 9, pp. 1715–1724, 2006.

[18] C.-C. Chang, C.-Y. Lin, and Y.-Z. Wang, "New image steganographic methods using run-length approach," *Information Sciences*, vol. 176, no. 22, pp. 3393–3408, 2006.

[19] W.-Y. Chen, "Color image steganography scheme using set partitioning in hierarchical trees coding, digital Fourier transform and adaptive phase modulation," *Applied Mathematics and Computation*, vol. 185, no. 1, pp. 432–448, 2007.

[20] G.-S. Lin, H. T. Chang, W.-N. Lie, and C.-H. Chuang, "Public-key-based optical image cryptosystem based on data embedding techniques," *Optical Engineering*, vol. 42, no. 8, pp. 2331–2339, 2003.

[21] C.-H. Chuang and G.-S. Lin, "Optical image cryptosystem based on adaptive steganography," *Optical Engineering*, vol. 47, no. 4, Article ID 047002, 2008.

[22] I. Hussain, N. A. Azam, and T. Shah, "Stego optical encryption based on chaotic S-box transformation," *Optics & Laser Technology*, vol. 61, pp. 50–56, 2014.

[23] R. Manoj, N. Hemrajani, and A. K. Saxena, "Secured steganography approach using AES," *International Journal of Computer Science Engineering and Information Technology Research*, vol. 3, no. 3, pp. 185–192, 2013.

[24] H. Sharma, "Secure image hiding algorithm using cryptography and steganography," *IOSR Journal of Computer Engineering*, vol. 13, no. 5, pp. 1–6, 2013.

[25] H. Al-Assam, R. Rashid, and S. Jassim, "Combining steganography and biometric cryptosystems for secure mutual authentication and key exchange," in *Proceedings of the 2013 8th International Conference for Internet Technology and Secured Transactions (ICITST '13)*, pp. 369–374, IEEE, London, UK, March 2013.

[26] D. Bloisi and L. Iocchi, "Image based steganography and cryptography," in *Proceedings of the 2nd International Conference on Computer Vision Theory and Applications (VISAPP '07)*, pp. 127–134, Barcelona, Spain, March 2007.

[27] K. Challita and H. Farhat, "Combining steganography and cryptography: new directions," *International Journal of New Computer Architectures and their Applications*, vol. 1, no. 1, pp. 199–208, 2011.

[28] P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption with fuzzy keyword search: a provably secure scheme under keyword guessing attack," *IEEE Transactions on Computers*, vol. 62, no. 11, pp. 2266–2277, 2013.

[29] C. Kuo, S. Wang, J. Lin, C. Wang, and J. Yan, "Image encryption based on fuzzy synchronization of chaos systems," in *Proceedings of the IEEE 37th Annual Computer Software and Applications Conference (COMPSAC '13)*, Kyoto, Japan, July 2013.

[30] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in *Advances in Cryptology—EUROCRYPT 2005*, vol. 3494 of *Lecture Notes in Computer Science*, pp. 457–473, 2005.

[31] M. Gardner, “The binary Gray code,” in *Knotted Doughnuts and Other Mathematical Entertainments*, chapter 2, W. H. Freeman, New York, NY, USA, 1986.

[32] X.-Y. Wang, S.-X. Gu, and Y.-Q. Zhang, “Novel image encryption algorithm based on cycle shift and chaotic system,” *Optics and Lasers in Engineering*, vol. 68, pp. 126–134, 2015.

[33] I. Hussain, T. Shah, M. A. Gondal, W. A. Khan, and H. Mahmood, “A group theoretic approach to construct cryptographically strong substitution boxes,” *Neural Computing and Applications*, vol. 23, no. 1, pp. 97–104, 2013.

[34] J. Kim and R. C.-W. Phan, “Advanced differential-style cryptanalysis of the NSA’s Skipjack block Cipher,” *Cryptologia*, vol. 33, no. 3, pp. 246–270, 2009.

[35] http://sipi.usc.edu/database/database.php.

[36] H. Bahjat and M. A. Salih, “Speed image encryption scheme using dynamic Galois field GF(P) matrices,” *International Journal of Computer Applications*, vol. 89, no. 7, pp. 7–12, 2014.

[37] C. H. Chuang and G. S. Lin, “Data steganography for optical color image cryptosystems,” *International Journal of Image Processing*, vol. 3, no. 6, pp. 318–327, 2010.

[38] O. M. Olaniyi, O. T. Arulogun, E. O. Omidiora, and O. O. Okediran, “Enhanced stegano-cryptographic model for secure electronic voting,” *Journal of Information Engineering and Applications*, vol. 5, no. 4, 2015.

[39] S. Som and S. Sen, “A non-adaptive partial encryption of grayscale images based on chaos,” *Procedia Technology*, vol. 10, pp. 663–671, 2013.

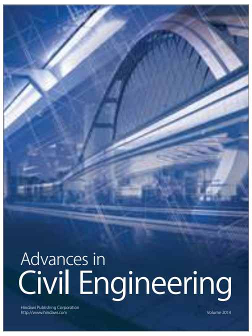
Journal of
Engineering

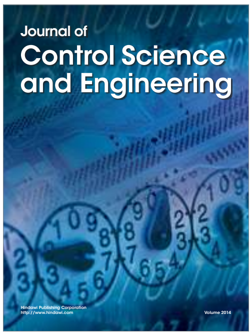
The Scientific
World Journal

International Journal of
Rotating
Machinery

Journal of
Sensors

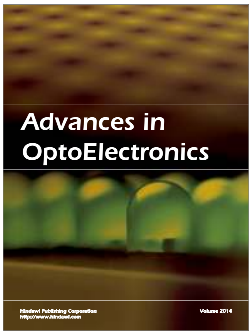
International Journal of
Distributed
Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science
and Engineering

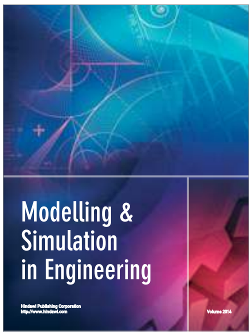
Journal of
Robotics

Journal of
Electrical and Computer
Engineering

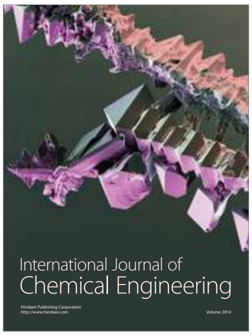

Advances in
OptoElectronics

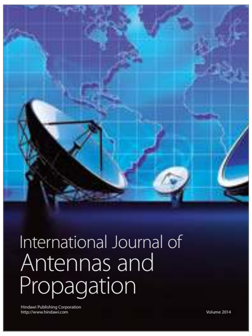
VLSI Design

International Journal of
Navigation and
Observation

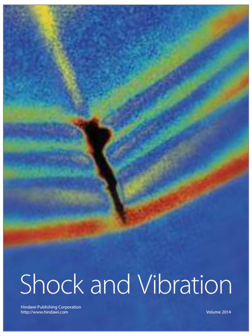

Modelling &
Simulation
in Engineering

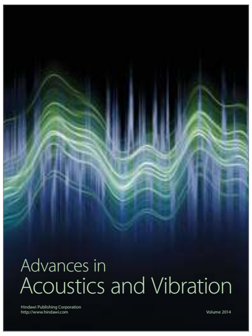
International Journal of
Aerospace
Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration