EFFICIENT SCRAMBLING-SUBSTITUTION IMAGE SECURITY SCHEME USING CHAOTIC ARNOLD-LOGISTIC MAPS IN THE DISCRETE COSINE TRANSFORM

Mohammed A. AlZain

Department of Information Technology, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia

ABSTRACT

This paper introduces an efficient scrambling-substitution image security scheme using chaotic Arnold and Logistic (Arnold-Logistic) maps in the discrete cosine transform (DCT). The Arnold map is employed as a scrambling stage while the Logistic map is employed as a substitution stage. The hybrid Arnold-Logistic mapping is performed in the DCT. The encipherment phase of the introduced DCT-based Arnold-Logistic security scheme begins by applying the DCT to the plainimage and the resulted DCT coefficient of the plainimage are scrambled for m iterations using the Arnold transformation. Then, the Arnold-based transformed DCT coefficients are substituted for n iterations using the Logistic map and the inverse of DCT (IDCT) is employed to produce the cipherimage. The decipherment phase of the introduced DCT-based Arnold-Logistic security scheme is the inverse of the encryption stage and begins by applying the DCT to the cipherimage. The resulted DCT coefficient of the cipherimage is inversely substituted for n iterations using the inverse Logistic map. Then, the inverse Logistic-based transformed DCT coefficients are inversely scrambled for m iterations using the inverse Arnold map and the IDCT is employed to produce the decrypted image. A series of test experiments are applied to investigate the introduced DCT-based Arnold-Logistic security scheme. The outcome results demonstrated the superiority of the introduced DCT-based Arnold-Logistic security scheme from the security point of view.

KEYWORDS

Arnold map, Logistic map & DCT.

1. INTRODUCTION

Now, we are currently living in an era in which information represents the currency of the global market. The top companies in the world such as Twitter, Google, and Facebook are all part of the information multi-billion dollar industry. Google, for example, is making most of its revenue by collecting information about your search queries and advertising for products or services that you are looking for. In addition, these companies possess some of our valuable information, from important emails to other various types of information stored on cloud storage services such as Google Drive and One Drive from Microsoft.

All this sensitive information is stored in servers which are acceptable over the internet. Due to the huge advancement in communications networks in the last decade, a hacker from anywhere in the world can attack these servers and have unauthorized access to your information. The effect of information theft can be devastating to our lives. For instance, if someone attacks a banking server, the savings may be lost. For all these reasons, the information must be stored in a way that

it can be read-only by authorized personnel. Information security becomes a hot topic and it is urgent to secure the information from different types of attacks. This can be achieved using encryption [1-10]. Encryption may be considered an effective solution for securing information.

Encryption is the art of coding information in a way that makes it unreadable to an adversary [11-16]. The sender encrypts the information before sending it using an encryption key. Upon receiving the encrypted information, the receiver decrypts the information with the decryption key. Without a decryption key, the attacker cannot retrieve the information. That is why the decryption key must be kept secret.

Encryption methods may be categorized in several ways; they may be classified as symmetric and asymmetric encryption algorithms [17-20]. Symmetric encryption algorithms use a unique key for enciphering/deciphering and asymmetric encryption employs different keys for enciphering/deciphering [21-24]. Examples of symmetric encryption are RC6 [25, 26, 27, 28] and the Advanced Encryption Standard (AES). Examples of asymmetric encryption are Elgamal encryption and RSA, named after Rivest, Shamir and Adleman [29, 30]. Symmetric Encryption is more efficient and secure compared to its asymmetric counterparts, but they present the challenge of securely sharing the key with the receiver [31, 32].

Encryption algorithms can also be classified as substitution algorithms and permutation algorithms [33, 34]. Substitution algorithms change the values of the information bits with other pseudorandom values [35, 36]. On the other hand, the permutation algorithms are only scrambling the information bits without changing their values [37, 38]. Examples of substitution algorithms are RSA and AES. Examples of permutation algorithms may include the baker and cat maps [39, 40]. By and large, the substitution algorithms are more secure than the permutation algorithms but on the other hand, the permutation algorithms are much faster than the substitution algorithms [41, 42]. Substitution algorithms are more suitable for offline applications such as downloading information from the internet. Permutation algorithms are more suitable for online applications such as online gaming and video streaming.

The main aim of this paper is to introduce an efficient DCT-based Arnold-Logistic image security scheme. The proposed DCT-based Arnold-Logistic image security system employs Arnold and Logistic maps in the DCT. The proposed DCT-based Arnold-Logistic image security scheme is composed of scrambling and substation layers. The Arnold map is utilized in the scrambling layer and iterated for m iterations. The Logistic map is utilized in the substitution layer and iterated for n iterations. The hybrid Arnold-Logistic transformations are employed in the DCT.

The rest of this paper is arranged as follows. Section 2 provides the fundamental knowledge for the DCT, Arnold, and Logistic maps. Section 3 introduces the DCT-based Arnold-Logistic image security scheme. Section 4 gives and provides the outcomes of the introduced DCT-based Arnold-Logistic security scheme. Finally, the paper conclusion is presented in Section 5.

2. FUNDAMENTAL KNOWLEDGE

This section reviews the three essential key mechanisms used to realize the proposed confusion-diffusion image Security Scheme using chaotic Arnold-Logistic maps in the DCT; the chaotic logistic map, the chaotic Arnold map, and the DCT.

2.1. Discrete Cosine Transform (DCT)

The DCT is considered a strategy for transforming the digital signal into its frequency elementary components. Figure 1 shows the DCT transform of the 8x8 segment.

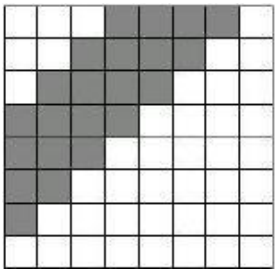


Figure 1. DCT transform of 8x8 segments

With the DCT, the image can be represented as a sinusoid sum of varying frequencies and magnitudes. With the image $f(x,y)$, the 2-D DCT and the IDCT are defined as [43-45]:

$$C(u,v)=\frac{2}{N}\alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}f(x,y)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad (1)$$

$$f(x,y)=\frac{2}{N}\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}\alpha(u)\alpha(v)C(u,v)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad (2)$$

where $f(x,y)$ denotes the pixel intensity at location (x,y), and $C(u,v)$ denotes the DCT coefficient at the transform location (u,v) [43-45].

$$\alpha(u)=\ \alpha(v)\ =\begin{cases}1/\sqrt{2} & u=v=0\\ 1 & \text{otherwise}\end{cases} \quad (3)$$

2.2. Arnold Map

The Arnold map was proposed by Vladimir Arnold in 1960 [46]. The generalized form Arnold map can be mathematically expressed as [46-47]:

$$\begin{pmatrix}x'\\ y'\end{pmatrix}=\begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}(\text{mod } N) \quad (4)$$

where N denotes the image size. The transformation Arnold map in Eq. 4 can be modulated for providing a series of Arnold transformations as follows [47]:

$$\begin{pmatrix}x'\\ y'\end{pmatrix}=\begin{pmatrix}i & i+1\\ 1 & 1\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}(\text{mod } N) \quad (5)$$

OR

$$\begin{pmatrix}x'\\ y'\end{pmatrix}=\begin{pmatrix}i+1 & i\\ 1 & 1\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix}(\text{mod } N) \quad (6)$$

where i €{1,2,3...}.

2.3. 2-D Chaotic Logistic Map

The basic dependency of a logistic map on different control parameters makes it widely used in chaos based applications, which exhibit high sensitivity to the parameters initial conditions.
The 1D logistic map represents one of the simplest models that present chaotic behaviour which can be mathematically described by Eq. 7 as [48]:

$$X_{n+1} = rX_n(1 - X_n) \tag{7}$$

where X_n values belong to the interval [0, 1], and parameter r values belong to the interval [0, 4].

The 2-D logistic map offers a more complex, chaotic behaviour than the 1D logistic map which is sufficient enough to make the secret information encrypted by this map more difficult to be extracted [49]. The 2-D chaotic logistic map can be mathematically expressed as [49]:

$$\text{2D Logistic map}: \begin{cases} x_{i+1} = r(3y_i + 1)x_i(1 - x_i) \\ y_{i+1} = r(3x_i + 1)y_i(1 - y_i) \end{cases} \tag{8}$$

3. THE INTRODUCED DCT-BASED ARNOLD-LOGISTIC SECURITY SYSTEM

In this section, the introduced DCT-based Arnold-Logistic security scheme is explored. The encryption/decryption stages of the DCT-based Arnold-Logistic security system are shown in the next subsections.

3.1. Encipherment

The encipherment stage of the DCT-based Arnold-Logistic image security scheme begins by applying the DCT to the plainimage and the resulted DCT coefficients of the plainimage are scrambled for m iterations using the Arnold transformation. Then, the Arnold-based transformed DCT coefficients are substituted using the Logistic map for n iterations and the inverse DCT is employed to produce the final cipherimage.

The encipherment steps of the DCT-based Arnold-Logistic image security scheme may be listed as follows:

1. The DCT is applied to the plainimage $PI(x_i, y_j)$
   $$E_1(x_i, y_j) = DCT[PI(x_i, y_j)] \tag{9}$$
2. The Arnold map is applied to scramble the DCT coefficient of the plainimage.
   $$E_2(x_i, y_j) = Arnold[E_1(x_i, y_j)] = Arnold[DCT[PI(x_i, y_j)]] \tag{10}$$
3. The Arnold-based transformed DCT coefficients are substituted using the Logistic map.
   $$E_3(x_i, y_j) = Logistic[E_2(x_i, y_j)] = Logistic[Arnold[DCT[PI(x_i, y_j)]]] \tag{11}$$
4. The final cipherimage $E(x_i, y_j)$ is obtained by applying the inverse DCT (IDCT) to $E_3(x_i, y_j)$.
   $$E(x_i, y_j) = IDCT(E_3(x_i, y_j)) = DCT(Logistic[Arnold[DCT[PI(x_i, y_j)]]]) \tag{12}$$

3.2. Decipherment

The decipherment stage of the DCT-based Arnold-Logistic security scheme represents the inverse of the encipherment stage and starts by applying the DCT to the cipherimage. The resulted DCT coefficient of the cipherimage is inversely substituted for n iterations using the inverse Logistic map. Then, the inverse Logistic-based transformed DCT coefficients are scrambled for m iterations using the inverse Arnold map and the IDCT is employed to produce the decrypted image.

The decipherment steps of the DCT-based Arnold-Logistic image security scheme may be listed as follows:

1. The DCT is applied to the cipherimage $CI(x_i, y_j)$

$$D_1(x_i, y_j) = DCT[CI(x_i, y_j)] \quad (13)$$

2. The inverse Logistic (InvLogistic) map is applied to the DCT coefficient of the cipherimage.

$$D_2(x_i, y_j) = InvLogistic[D_1(x_i, y_j)] = InvLogistic[DCT[CI(x_i, y_j)]] \quad (14)$$

3. The inverse Arnold (InvArnold) map is applied to the inverse Logistic-based transformed DCT coefficients.

$$D_3(x_i, y_j) = InvArnold[D_2(x_i, y_j)] = InvArnold[InvLogistic[DCT[CI(x_i, y_j)]]] \quad (15)$$

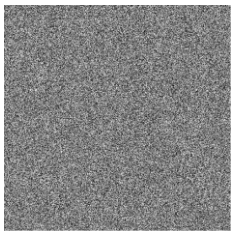
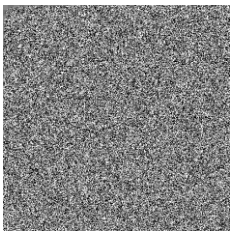
4. The deciphered image $D(x_i, y_j)$ is produced by applying the IDCT to $D_3(x_i, y_j)$.

$$D(x_i, y_j) = IDCT(D_3(x_i, y_j)) = IDCT(InvArnold[InvLogistic[DCT[CI(x_i, y_j)]]]) \quad (16)$$

4. EXPERIMENTAL RESULTS AND DISCUSSION

In this section, various tests are performed to examine the Arnold-Logistic and the introduced DCT-based Arnold-Logistic image security systems. The experimental tests are carried out on a set of grayscale test images that include Boat, Cameraman, Lena, and Peppers images. Each image has a size of 512 x 512 pixels.

Figure 2 shows the visual encryption results of different samples for Arnold-Logistic and the proposed DCT-based Arnold-Logistic image security systems. It can be seen that both of Arnold-Logistic and the introduced DCT-based Arnold-Logistic security systems can effectively encrypt images that have a random noise shape and are completely different from their corresponding plainimages.

Image name	Plainimage	Arnold-Logistic image cipher	DCT-based Arnold-Logistic image cipher
boat			

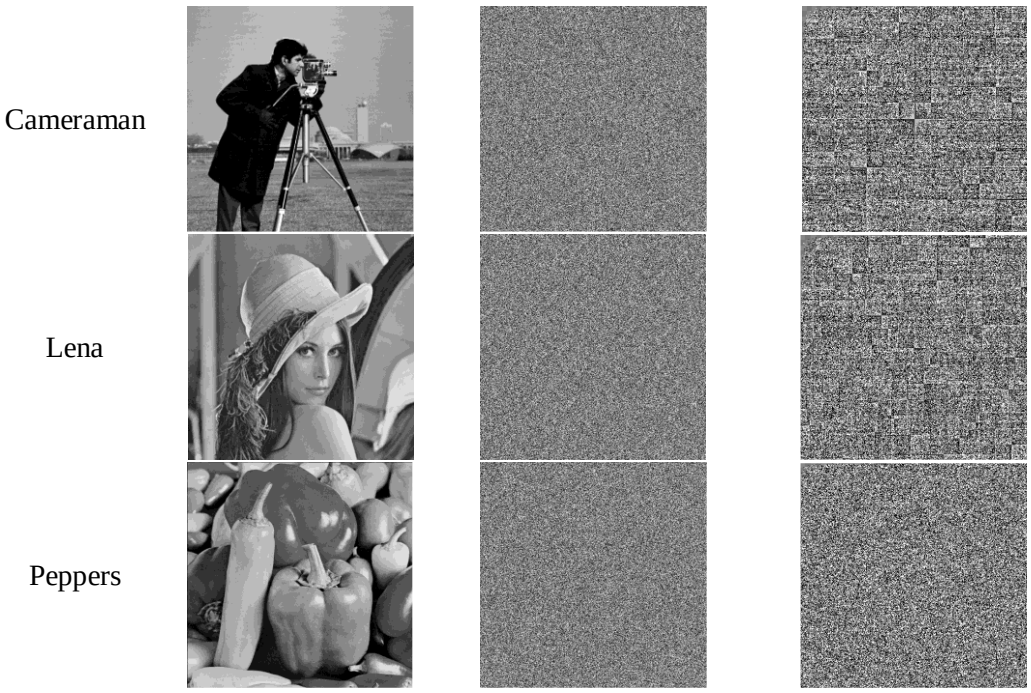
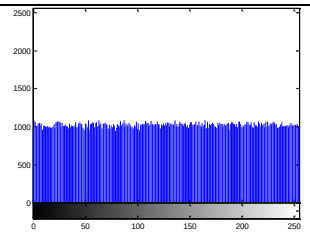
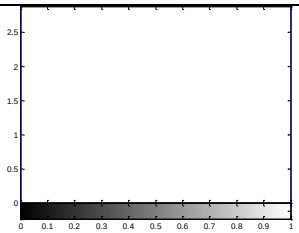
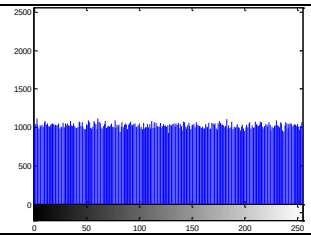
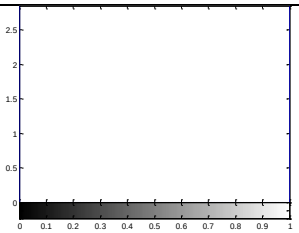


Figure 2. Encryption results of different samples for Arnold-Logistic and the introduced DCT-based Arnold-Logistic security systems

Figure 3 shows the histogram distributions of encryption results of different samples for Arnold-Logistic and the introduced DCT-based Arnold-Logistic security systems. A good encrypted image must show a uniform histogram distribution. It is noted that both of Arnold-Logistic and the proposed DCT-based Arnold-Logistic image security systems can produce cipherimages of a uniformly distributed histogram that are completely different from histograms of their respected plainimages.

Image name	Arnold-Logistic image cipher	DCT-based Arnold-Logistic image cipher
boat		
Cameraman		

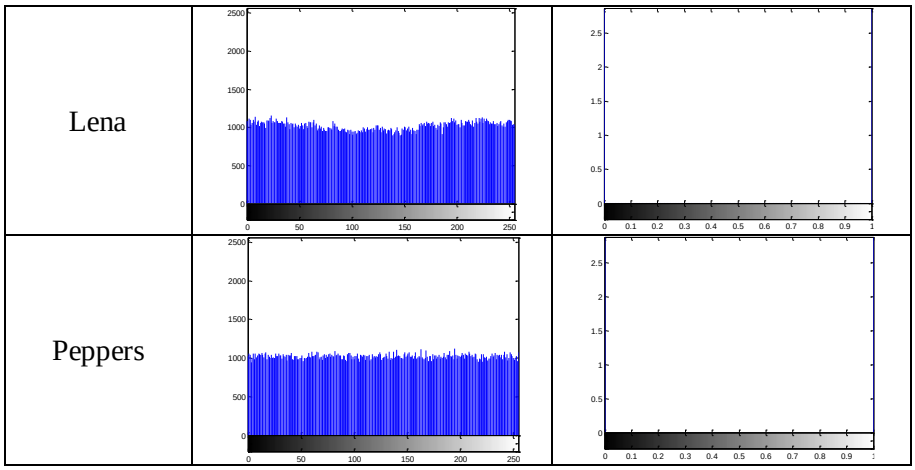


Figure 3. Histogram results of different samples for Arnold-Logistic and the introduced DCT-based Arnold-Logistic security systems.

Table 1. Entropy results of different samples for Arnold-Logistic and the introduced DCT-based Arnold-Logistic security systems.

Image name	Plainimage	Encryption Scheme	
		Arnold-Logistic image cipher	DCT-based Arnold-Logistic image cipher
Boat	7.124	7.9995	7.821
Cameraman	7.009	7.9993	7.279
Lena	7.446	7.9993	7.854
Peppers	7.594	7.9993	7.880

Table 1 demonstrates the entropy results of different samples for Arnold-Logistic and the introduced DCT-based Arnold-Logistic security systems. A good encrypted image must show an entropy value that is closed to the optimal value of 8 to overcome the entropy attack [50]. It can be noted that both of Arnold-Logistic and the proposed DCT-based Arnold-Logistic image security systems can produce cipherimages of entropy values that are close to the ideal value of 8. This again illustrates the efficiency of both Arnold-Logistic and the proposed DCT-based Arnold-Logistic image security systems against the entropy attack.

Table 2. CC results of different samples for Arnold-Logistic and the introduced DCT-based Arnold-Logistic security systems.

Image name	Encryption Scheme	
	Arnold-Logistic image cipher	DCT-based Arnold-Logistic image cipher
Boat	0.0009	-0.0015
Cameraman	0.0027	0.0018
Lena	0.0001	0.0004
Peppers	0.0035	-0.0020

Table 2 illustrates the correlation coefficients (CC) results of different samples for Arnold-Logistic and the introduced DCT-based Arnold-Logistic security systems. A good encrypted

image must have a CC that is closed to the optimal value of zero to overcome the statistical attack [51]. It can be noted that both of Arnold-Logistic and the proposed DCT-based Arnold-Logistic image security systems can produce cipherimages of CC values that are close to the ideal value of zero. This again illustrates the superiority of both Arnold-Logistic and the proposed DCT-based Arnold-Logistic image security systems against statistical attacks.

Table 3. ID results of different samples for Arnold-Logistic and the introduced DCT-based Arnold-Logistic security systems.

Image name	Encryption Scheme	
	Arnold-Logistic image cipher	DCT-based Arnold-Logistic image cipher
Boat	0.637	0.247
Cameraman	0.601	0.522
Lena	0.687	0.230
Peppers	0.638	0.217

Table 3 shows the irregular deviation (ID) results of different samples for Arnold-Logistic and the proposed DCT-based Arnold-Logistic image security system. A good encryption algorithm should have ID that is closed to its ideal value of zero [52]. It is noted from Table 3 that the introduced DCT-based Arnold-Logistic security system has good ID values compared with the Arnold-Logistic image security systems because it has ID values that are close to their ideal value of zero. This again illustrates the success of the introduced DCT-based Arnold-Logistic security system in comparison with the Arnold-Logistic image security system.

Table 4. HD results of different samples for Arnold-Logistic and the introduced DCT-based Arnold-Logistic security systems.

Image name	Encryption Scheme	
	Arnold-Logistic image cipher	DCT-based Arnold-Logistic image cipher
Boat	0	1.2457
Cameraman	0	1.2330
Lena	0	1.2477
Peppers	0	1.2451

Table 4 shows the histogram deviation (HD) results of different samples for Arnold-Logistic and the introduced DCT-based Arnold-Logistic security systems. An efficient cipher should maximize the deviation between the cipherimage and its corresponding plainimage [53]. So, A good encryption algorithm must have high ID values. It is seen from Table 4 that the introduced DCT-based Arnold-Logistic image security system has good ID values compared with the Arnold-Logistic image security systems. This again illustrates the effectiveness of the proposed DCT-based Arnold-Logistic image security system in comparison with the Arnold-Logistic image security system.

The number of pixels change rate (NPCR) estimates the percentage of the number of pixels change rate and the ideal value of NPCR for an efficient image cipher is 99.6 [54-55]. Table 5 lists the NPCR results of different samples for Arnold-Logistic and the introduced DCT-based Arnold-Logistic image security systems. A good encryption algorithm should have high NPCR values. It can be noticed from Table 5 that the proposed DCT-based Arnold-Logistic image

security system has good NPCR values compared with the Arnold-Logistic image security system. This again illustrates the effectiveness of the proposed DCT-based Arnold-Logistic image security system in comparison with the Arnold-Logistic image security system.

Table 5. NPCR results of different samples for Arnold-Logistic and the introduced DCT-based Arnold-Logistic security systems.

Image name	Encryption Scheme	
	Arnold-Logistic image cipher	DCT-based Arnold-Logistic image cipher
Boat	99.6208	100
Cameraman	99.6025	100
Lena	99.5967	100
Peppers	99.5891	100

Table 6. UACI results of different samples for Arnold-Logistic and the introduced DCT-based Arnold-Logistic security systems.

Image name	Encryption Scheme	
	Arnold-Logistic image cipher	DCT-based Arnold-Logistic image cipher
Boat	12.7363	25.5926
Cameraman	12.7712	25.6873
Lena	12.7692	25.6338
Peppers	12.7569	25.5928

The unified average change intensity (UACI) estimates the percentage of intensity difference between the cipherimage and its corresponding plainimage and the ideal value of UACI for an efficient image cipher is 33.33. Table 6 lists the UACI results of different samples for Arnold-Logistic and the introduced DCT-based Arnold-Logistic security systems. A good encryption algorithm should have high UACI values. It is noticed from Table 6 that the introduced DCT-based Arnold-Logistic image security system has good UACI values compared with the Arnold-Logistic image security system. This again proves the success of the introduced DCT-based Arnold-Logistic security system in comparison with the Arnold-Logistic image security system.

5. CONCLUSIONS

An efficient DCT-based Arnold-Logistic image security scheme is introduced. The introduced DCT-based Arnold-Logistic image security system employs Arnold and Logistic maps in the DCT. The proposed DCT-based Arnold-Logistic image security scheme is composed of scrambling and substation layers. The Arnold map is utilized in the scrambling layer and iterated for m iterations. The Logistic map is utilized in the substitution layer and iterated form iterations. The hybrid Arnold-Logistic transformations are employed in the DCT. The proposed DCT-based Arnold-Logistic image security scheme is tested with respect to several security measures. The results of the security investigation ensured and confirmed that the proposed DCT-based Arnold-Logistic image security scheme is secure and immune against different types of security attacks.

ACKNOWLEDGEMENTS

This study was funded by the Deanship of Scientific Research, Taif University Researchers Supporting Project number (TURSP-2020/98), Taif University, Taif, Saudi Arabia.

CONFLICT OF INTEREST

The author declares no conflicts of interest.

REFERENCES

[1] F. An and J. Liu, "Image encryption algorithm based on adaptive wavelet chaos," Journal of Sensors, vol. 2019, 2768121, pp. 1-12, 2019.
[2] B. Stoyanov&G. Nedzhibov, “Symmetric key encryption based on rotation-translation equation,” Symmetry, vol. 12, no. 1, 73, pp. 1-12, 2020.
[3] S. Aljawarneh&M. B. Yassein, “A multithreaded programming approach for multimedia big data: encryption system, Multimedia Tools and Applications,” vol. 77, no. 9, pp. 10997-11016, 2018.
[4] A. Arab, M. J. Rostami and B. Ghavami, “An image encryption method based on chaos system and AES algorithm,” The Journal of Supercomputing, vol. 75, no. 10, pp. 6663–6682, 2019.
[5] A. Al-Haj, “Providing integrity, authenticity, and confidentiality for header and pixel data of DICOM images,” Journal of digital imaging, vol. 28, no. 2, pp. 179-187, 2015.
[6] O. Faragallah, H. El-sayed, A. Afifi and W. El-Shafai, "Efficient and secure opto-cryptosystem for color images using 2D logistic-based fractional Fourier transform," Optics and Lasers in Engineering, vol. 137, 106333, 2021.
[7] A. Gutub, N. Al-JuaidandF.Khan, “Counting-based secret sharing technique for multimedia applications,” Multimedia Tools and Applications, vol. 78, no. 5, pp. 5591-5619, 2019.
[8] M. Al-Ghamdi, M. Al-Ghamdi and A. Gutub, “Security enhancement of shares generation process for multimedia counting-based secret-sharing technique” Multimedia Tools and Applications, pp. 1-28, 2016.
[9] O. S. Faragallah, W. El-Shafai, A. I. Sallam, I. Elashry, E. M. EL-Rabaie, A. Afifi, M. A. AlZain, J. F. Al-Amri, F. E. Abd El-Samie, and H. S. El-sayed, "Cybersecurity framework of hybrid watermarking and selective encryption for secure HEVC communication," Journal of Ambient Intelligence and Humanized Computing, vol. 13, pp. 1215-1239, 2022.
[10] O. S. Faragallah, M. A. AlZain, H. S. El-sayed, J. F. Al-Amri, W. El-Shafai, A. Afifi, E. A. Naeem, and B. Soh, "Secure color image cryptosystem based on chaotic logistic in the FrFT domain," Multimedia Tools and Applications, vol. 79, pp. 2495-2519, 2020.
[11] Xu, L., Gou, X., Li, Z., & Li, J. (2017). A novel chaotic image encryption algorithm using block scrambling and dynamic index-based diffusion. Optics and Lasers in Engineering, 91, 41-52.
[12] Chai, X., Chen, Y., &Broyde, L. (2017). A novel chaos-based image encryption algorithm using DNA sequence operations. Optics and Lasers in engineering, 88, 197-213.
[13] O. S. Faragallah, A. Afifi, W. El-Shafai, H. S. El-sayed, M. A. AlZain, J. F. Al-Amri, and F. E. Abd El-Samie, "Efficiently encrypting color images with few details based on RC6 and different operation modes for cybersecurity applications," IEEE Access, vol. 8, pp. 103200-103218, 2020.
[14] Alanazi, Norah &Alanizy, Alanood&Baghoza, Noura& Al Ghamdi, Manal&Gutub, Adnan. (2018). 3-Layer PC Text Security via Combining Compression, AES Cryptography 2LSB Image Steganography.
[15] Yavuz, E., Yazıcı, R., Kasapbaşı, M. C., &Yamaç, E. (2016). A chaos-based image encryption algorithm with simple logical functions. Computers & Electrical Engineering, 54, 471-483.
[16] Ye, G., & Huang, X. (2016). A secure image encryption algorithm based on chaotic maps and SHA-3. Security and Communication Networks, 9(13), 2015-2023.
[17] Guesmi, R., Farah, M. A. B., Kachouri, A., &Samet, M. (2016). Hash key-based image encryption using crossover operator and chaos. Multimedia tools and applications, 75(8), 4753-4769.

[18] S. Rajesh, V. Paul, V. G. Menon and M. R. Khosravi, "A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices," Symmetry, vol. 11, no. 2, 393, 2019.
[19] R. Roman, J. Lopez and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," Future Generation Computer Systems, vol. 78, pp. 680-698, 2018.
[20] M A. M. El-Bendry and A. E. A. Azzm, "Complexity considerations: efficient image transmission over mobile communications channels," Multimedia Tools and Applications, vol. 78, pp. 16633-16664, 2019.
[21] T. N. P. Madhuri, M. S. Rao, P. S. Santosh, P. Tejaswi and S. Devendra, "Data Communication Protocol using Elliptic Curve Cryptography for Wireless Body Area Network," 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), pp. 133-139, 2022.
[22] B. Yao, H. Sun, H. Wang and J. Su, "Maximal Planar Graphs As Topological Authentications For Asymmetric Encryption," 2021 IEEE 2nd International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA), pp. 133-138, 2021.
[23] M. E. Kahla, M. Beggas, A. Laouid, M. Kara and M. AlShaikh, "Asymmetric Image Encryption Based on Twin Message Fusion," 2021 International Conference on Artificial Intelligence for Cyber Security Systems and Privacy (AI-CSP), pp. 1-5, 2021.
[24] Q. Zhang, "An Overview and Analysis of Hybrid Encryption: The Combination of Symmetric Encryption and Asymmetric Encryption," 2021 2nd International Conference on Computing and Data Science (CDS), 2021, pp. 616-622, 2021.
[25] A. M. Ashraf and W. Elmedany, "Securing IoT data at physical layer by using RC6 encryption technique," 4th Smart Cities Symposium (SCS 2021), pp. 537-544, 2021.
[26] O. S. Faragallah, A. Afifi, W. El-Shafai, H. S. El-sayed, M. A. AlZain, J. F. Al-Amri, and F. E. Abd El-Samie, "Efficiently encrypting color images with few details based on RC6 and different operation modes for cybersecurity applications," IEEE Access, vol. 8, pp. 103200-103218, 2020.
[27] O. S. Faragallah, H. S. El-sayed, A. Afifi, and S. F. El-Zoghdy, "Small details gray scale image encryption using RC6 block cipher," wireless Personal Communications, vol. 118, no. 2, pp. 1559-1589, 2021.
[28] A. Sallam, E. EL-Rabaie, and O. S. Faragallah,, "HEVC selective encryption using RC6 block cipher technique," IEEE Transactions on Multimedia, vol. 20, no. 7, pp. 1636-1644, 2018.
[29] S. Roy, A. Stavrou, B. L. Mark, K. Zeng, S. M. P D and K. N. Khasawneh, "Characterization of AES Implementations on Microprocessor-based IoT Devices," 2022 IEEE Wireless Communications and Networking Conference (WCNC), pp. 55-60, 2022.
[30] A. S., G. K., P. J. and N. V., "Medical Color Image Encryption Using Chaotic Framework and AES Through Poisson Regression Model," 2022 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET), 2022, pp. 316-321
[31] A. Abukari, E. Bankas, and M. Iddrisu, "A secured video conferencing system architecture using a hybrid of two homomorphic encryption schemes: a case of zoom," International Journal of Engineering Research & Technology (IJERT), vol. 9, pp. 237-240, 2020.
[32] O. S. Faragallah, W. El-Shafai, A. Afifi, I. Elashry, M. A. AlZain, J. F. Al-Amri, B. Soh, H. M. El-Hoseny, H. S. El-Sayed, and F. E.Abd El-Samie, "Efficient three-dimensional video cybersecurity framework based on double random phase encoding," Intelligent Automation & Soft Computing, vol. 28, pp. 353-367, 2021.
[33] M. Lewandowski and S. Katkoori, "Enhancing PRESENT-80 and Substitution-Permutation Network Cipher Security with Dynamic "Keyed" Permutation Networks," 2021 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), pp. 350-355, 2021.
[34] M. Lewandowski and S. Katkoori, "Enhancing PRESENT-80 and Substitution-Permutation Network Cipher Security with Dynamic "Keyed" Permutation Networks," 2021 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), pp. 350-355, 2021.
[35] A. Arı and F. Özkaynak, "Generation of Substitution Box Structures Based on Blum BlumShub Random Number Outputs," 2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), pp. 677-682, 2022.
[36] E. Jintcharadze, T. Sarajishvili, A. Surmanidze and D. Khojava, "Implementation and Comparative Analysis of Symmetric Encryption Model Based on Substitution Cipher Techniques," 2021 IEEE East-West Design & Test Symposium (EWDTS), pp. 1-6, 2021.

[37] H. Wang, Q. Wang, L. Yu and J. Zhao, "Image Encryption Algorithm Based on Double Scrambling," 2019 IEEE International Conference on Mechatronics and Automation (ICMA), pp. 2201-2205, 2019.
[38] S. Sun, "A Novel Hyperchaotic Image Encryption Scheme Based on DNA Encoding, Pixel-Level Scrambling and Bit-Level Scrambling," in IEEE Photonics Journal, vol. 10, no. 2, pp. 1-14, 2018.
[39] O. S. Faragallah, A. Afifi, I. F. Elashry, E. A. Naeem H. M. El-Hoseny, H. S. El-sayed, and A. M. Abbas, "Efficient optical double image cryptosystem using chaotic mapping-based Fresnel transform," Optical and Quantum Electronics, vol. 53, pp. 1-26, 2021.
[40] Y. Luo, J. Yu, W. Lai, and L. Liu, "A novel chaotic image encryption algorithm based on improved baker map and logistic map," Multimed.Tools Appl., vol. 78, pp. 22023-22043, 2019.
[41] I. F. Elashry, W. El-Shafai, E. S. Hasan, S. El-Rabaie, A. M. Abbas, F. E. Abd El-Samie, H. S. El-sayed, and O. S. Faragallah, "Efficient chaotic-based image cryptosystem with different modes of operation," Multimedia Tools and Applications, vol. 79, pp. 20665-20687, 2020.
[42] G. Hu, D. Xiao, Y. Zhang, and T. Xiang, "An efficient chaotic image cipher with dynamic lookup table driven bit-level permutation strategy," Nonlinear Dynamics, vol. 87, no. 2, pp. 1359-1375, 2017.
[43] Syed Ali Khayam, "The Discrete Cosine Transform (DCT): Theory and Application" Michigan State University, March 2003.
[44] L. Meng-En, C. Chien-Feng, L. Tsung-Nan and C. Chun-Nan, "The application of discrete cosine transform (DCT) combined with the nonlinear regression routine on optical auto-focusing", Digest of Technical Papers International Conference on Consumer Electronics ICCE 2009, pp. 1 – 2, 2009.
[45] L. Z. Cheng, "On computing the two-dimensional (2-D) type IV discrete cosine transform (2-D DCT-IV)," IEEE Signal Processing Letters, Vol. 8, Issue. 8, pp. 239 – 241, August 2001.
[46] A. A. Mohammed, M. A. M. Abdullah and E. Elbasi, "A Hybrid Watermarking Scheme Based on Arnold Cat Map Against Lossy JPEG Compression," 2021 International Conference on Information Security and Cryptology (ISCTURKEY), pp. 93-98, 2021.
[47] P. Adhikary, A. Phadikar, H. Mandal and P. K. Singh, "Digital Image Watermarking Technique Using Arnold Transform and Lifting," 2021 5th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech), pp. 1-5, 2021.
[48] Chai Wah Wu, Nikolai F. Rulkov, "Studying Chaos via 1-D Maps", IEEE Transactions on Circuits and Systems: Fundamental Theory and Applications, Vol.40, No.10, 1993.
[49] Yue Wu, Gelan Yang, Huixia Jin, and Joseph P. Noonan, "Image Encryption using the Two-dimensional Logistic Chaotic Map", Journal of Electronic Imaging, vol. 21, no. 1, 013014, 2012.
[50] Zou, L., Sun, J., Gao, M., Wan, W., & Gupta, B. B. (2019). A novel coverless information hiding method based on the average pixel value of the sub-images. Multimedia Tools and Applications, 78(7), 7965-7980.
[51] O. S. Faragallah, A. Afifi, H. S. El-sayed, M. A. AlZain, J. F. Al-Amri, F. E. Abd El-Samie, and W. El-Shafai, "Efficient HEVC integrity verification scheme for multimedia cybersecurity applications," IEEE Access, vol. 8, pp. 154112-154135, 2020.
[52] Li, Y., Wang, C., & Chen, H. (2017). A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation. Optics and Lasers in Engineering, 90, 238-246.
[53] O. S. Faragallah, A. Afifi, W. El-Shafai, H. S. El-sayed, E. A. Naeem, M. A. AlZain, J. F. Al-Amri, B. Soh, and F. E. Abd El-Samie, "Investigation of chaotic image encryption in spatial and FrFT domains for cybersecurity applications," IEEE Access, vol. 8, pp. 42491-42503, 2020.
[54] Xu, L., Gou, X., Li, Z., & Li, J. (2017). A novel chaotic image encryption algorithm using block scrambling and dynamic index-based diffusion. Optics and Lasers in Engineering, 91, 41-52.
[55] A. M. Hemdan, O. S. Faragallah, O. Elshakankiry, and A. Elmhalaway, "A fast hybrid image cryptosystem based on random generator and modified logistic map," Multimedia Tools and Applications, vol. 78, no. 12, pp. 16177-16193, 2019.

AUTHOR

Mohammed A. AlZain has achieved his PhD degree from the Department of Computer Science and Computer Engineering at La Trobe University, Melbourne, Australia in Sept 2014. Dr.AlZain's PhD research is in Cloud Computing Security. His thesis title was: Data security, Data management, Performance evaluation for a multi-cloud computing model. He has received his Bachelor degree in Computer Science from King Abdulaziz University, Saudi Arabia in 2004, and then achieved his Master's degree in Information Technology from La Trobe University in 2010.Currently, Dr.AlZain is an Associate Professor in the College of Computers and Information Technology at Taif University in Saudi Arabia. His area of interest: Cloud Computing Security, multimedia security. Email: m.alzain@tu.edu.sa.