IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Mathematical Modelling of Engineering Problems
Vol. 9, No. 2, April, 2022, pp. 539-544
Journal homepage: http://iieta.org/journals/mmep

IMGTXT: Image to Text Encryption Based on Encoding Pixel Contrasts

Seerwan Waleed Jirjees*, Farah Flayyeh Alkhalid

Control and Systems Engineering Department, University of Technology, Baghdad 10066, Iraq

Corresponding Author Email: seerwan.w.jirjees@uotechnology.edu.iq

https://doi.org/10.18280/mmep.090233

Received: 1 November 2021
Accepted: 18 February 2022

Keywords:
encryption image, image to text, image security, histogram, entropy, decryption image, cryptography, brute force

ABSTRACT

Nowadays, when data is exchanged over the internet, the security of data is critical in every element of life. Unauthorized network access is possible due to information transmission. As image usage increased in most communications, image privacy became an issue. Image encryption is one of the methods used to protect images online. In this paper, we proposed a new approach called IMGTXT that converts the image to text by coding the pixel values depending on locations then encrypts them by any trust encryption text algorithm, so that this method provides resistance to a variety of attacks such as histogram attacks and brute force attack. The state of the art of this research is the image is represented as a text and there is no relationship between the cipher-image and the plain image. Although this results in a large data volume. The proposed technique builds and testes on various images with different sizes, the recorded results demonstrate the technique's efficacy and robustness to resist the brute force attack and statistical cryptanalysis of original and encrypted images.

1. INTRODUCTION

Since early years, humans realized there is information should not be declared to all, and they saved messages against falling into the wrong hand, Myriad approaches of protection are depended ranging from a simple verification password to the most complex Cryptography, Cryptography is the approach of encoding the information, which is the state of the art to hold secure communication at the time of increasing unauthorized users, The main idea is to convert clear message to ambiguous message, however, Cryptography can be applied on different transferring files styles i.e. (images, texts, videos, sounds …) [1].

Confidentiality, Data Integrity, Authentication, and Non-Repudiation are the four fundamental principles of cryptography [2]. Images can be encrypted using a variety of different methods to ensure that they are only accessible to authorized users. Image encryption solutions are regularly investigated to meet the requirements for real-time data security when data is transported over the internet. Traditional algorithms have a number of limitations, including low-level efficiency when dealing with massive amounts of multimedia [3, 4]. Encryption consists mostly of two techniques: pixel permutation and pixel diffusion. Pixel permutation modifies the pixel's position, but pixel diffusion modifies the pixel's intensity values, which spread throughout the image [5-7].

In this research, a multilevel encryption method has developed an approach for image encryption by transferring image to text and then encrypting the text, so called image to text encryption (IMGTXT) as it provides excellent performance, acceptable computation, and a high level of security. The contribution of this research is a new algorithm proposed to coding image pixels to text through re-arrange the contrast of each pixel and its location for the three patterns (RGB), this arrangement is done in a complex fashion which is unexpected to estimate.

The rest of this paper is organized as follows. Section 2 is a review of prior works' literature. The suggested IMGTXT method is described in Section 3. Section 4 contains an analysis and evaluation of performance. Finally, in Section 5, the conclusions are presented.

2. LITERATURE REVIEW

Many previous studies were conducted to secure the data by combining cryptography and steganography. Others studied encryption of texts or encryption of images.

Akhshani et al. [8] proposed the implementation of image encryption scheme based on the quantum logistic map using logistic map, with very satisfying results, it differed the work that ours encrypts image after change it to a matrix of pixels with contrast and its location. The Elliptic-curve cryptography (ECC) method is proposed by Singh, L.D., Singh, K.M. [9]; ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Next, a random decimal (either 1 or 2) is appended to each pixel's value using this manner. As before, some pixel values are combined to find a large number, and then those numbers are paired together to make pairs of new pixels (this is performed to improve the efficiency of the algorithm). The ECC algorithm receives a large number as input. After that, a random number K is multiplied by the receiver's public key, and the resulting number is added to the previously generated pair of numbers. In Ref. [10], the 3D DNA matrix is utilized in the encryption process to permute and diffuse image pixels. A chaotic sequence is constructed to permute DNA pixels. Then the sub-blocks are XORed with the key DNA matrix to get the final encrypted image. Zhang et al. [11] proposed an image encryption algorithm based on the H-fractal and dynamic self-invertible matrix, like previous studies the image

stays image. Hamad and Farhan [12] also used Shuffling scheme for encryption, they used two phases in the first one used S-Box and in the second depended on shifting and rotation to create a secret key for chaotic map, The method used in the proposed is the traditional method, which converts a plain image to another, but in an encrypted way.

One such exclusive technique for data security and safety is image encryption. Gladwin and Gowthami [13] studied a new approach of ciphertext and coefficients of an image, embedded into the base image based on LSB watermarking, this study demonstrated strong cipher text embedded in the image, but as the previous study, the final form is the image with ciphered text. Farah et al. [14] also used chaotic and Jaya optimization algorithms based Lyapunov exponents and entropy measure, to get nonlinear output, Masood et al. [15] also used chaotic and Julia set. Another encryption algorithm. It's proposed in Ref. [16] that the undersized 4-bit matrix suggested addicted to an enhanced logistic category and for location scrambling plus the XOR arrangement of the extreme 4-bit matrix and the basic used then two matrices are joined into image matrix which is of 8-bit. This algorithm is used a static method to encrypt the image as the previous algorithms unlike our algorithm, it is possible to change the encryption. Hua et al. [17] used chaotic encryption for image, they presented a new 2D chaotic map based on standard logistics and tent, they called 2D-LTMM, authors showed this method can effectually fight security attacks, Abd Aljabar et al. [18] suggested Encryption VoIP based on Generated Biometric Key for RC4 Algorithm to encrypt the voice data before transmitting it over the network, by creating encryption key using face biometric recognition, the waveform of transmitted voice different from the original one.

In light of these previous techniques, we propose a new image encryption method that makes it more difficult for attackers to discover the true index of image data by converting it to ciphertext. The proposed algorithm is dynamic. It is possible to change the way the image values are encoded and converted into text. Also, the type of algorithm used to encode the text can be changed according to the system designer, this makes it resistant to many attacks, including brute force, and this makes it difficult to penetrate.

3. IMGTXT PROPOSED APPROACH

The suggested work introduces a novel cryptographic system capable of resolving difficulties with traditional cryptographic methods in histogram and entropy that used disrupting pixel positions or changing pixel values.

IMGTXT proposed converts RGB pixels for image encryption to encrypt text that illustrated in Figure 1. This technique involves, firstly create a matrix of each Numerical pixel value (0-255) from the input color image and then represent a value by indexing its (row and Colum) to get the coding value, finally after encoding all together, it will be encrypted to create ciphertext. This work has three phases.

- Encoding pixels for the encryption process.
- Decoding pixels for the decryption process.
- Conventional cryptographic method for a text that used a key for both encryption and decryption.

3.1 Encryption algorithm

For image encryption, two techniques are used. The first one converts the image to text. The second one encrypts text using a suitable encryption algorithm shown in Figure 2.

The proposed system is started with reading an input image *I* which *[R, C]* size, as known, the color image consists from three patterns (P) for primary colors Red, Green and Blue, so there are three layers for this image each *[R, C]* size, then numerates each pattern with different value, after that, the software program reads all pixels in each pattern individually, each pixel has contrast value (X) from *0 to 255*, in other words, the system reads *RXCX×3,* then refers to each pixel with four parameters [Pattern code, Pixel value, Row, Column] as denoted in Eq. (1) and Figure 3, these final parameters will convert to file text then will encrypt by any type of encryption method.

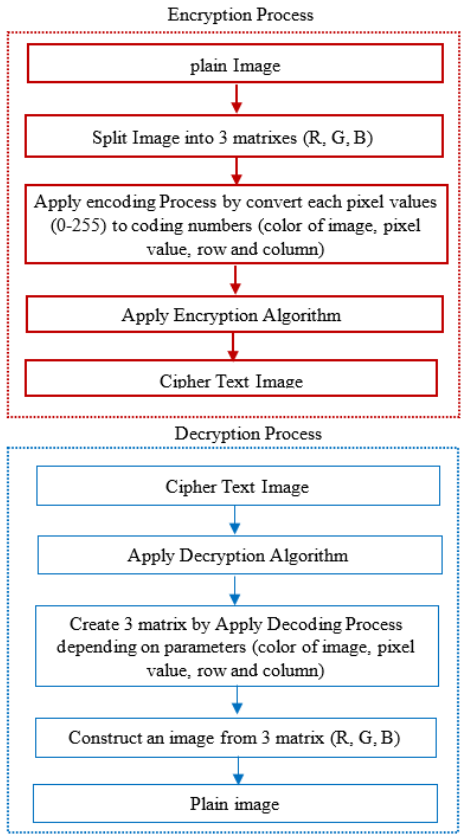


Figure 1. IMGTXT proposed for encryption and decryption process

The last phase for the proposed system is the cryptographic algorithm that was used to encrypt encoding data in the Previous step. The encryption algorithm used is of a symmetric type with a single key to encrypt and decrypt the data. as it is possible to use any method. Any method can be used with any different size of the key that depends on the designer of the system, but it must be taken into account that the strength of the encryption and the size of the key give a good ciphertext, an AES cipher with a key size of 128 bits was used and it presented very satisfactory results.

$$\text{Encoding character= P \& X \& R\& C} \tag{1}$$

$$\text{where, } P = \begin{cases} 1 \text{ if image selection is Red} \\ 2 \text{ if image selection is Green} \\ 3 \text{ if image selection is Blue} \end{cases} \tag{2}$$

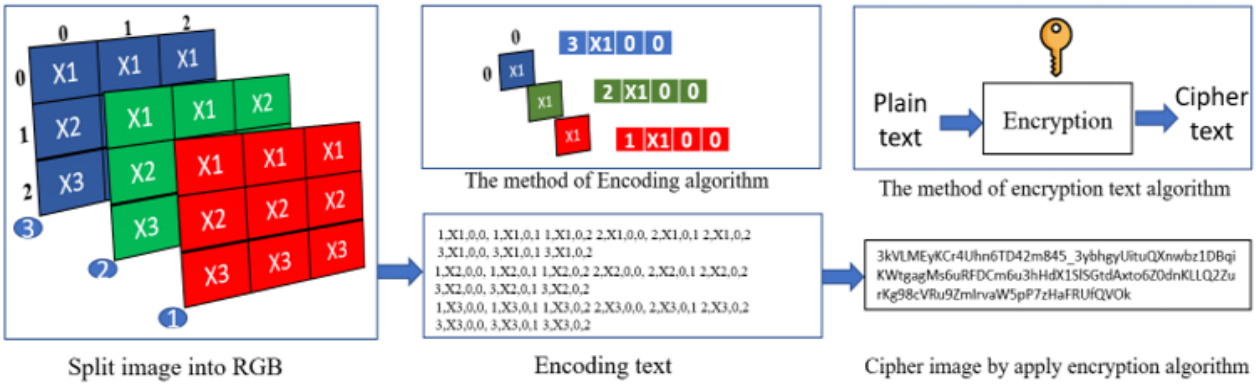


Figure 2. The proposed encryption algorithm

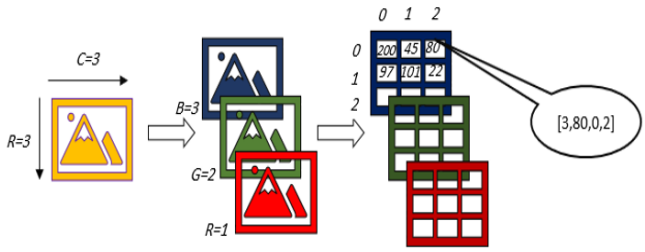


Figure 3. Referring each pixel to a set of parameters

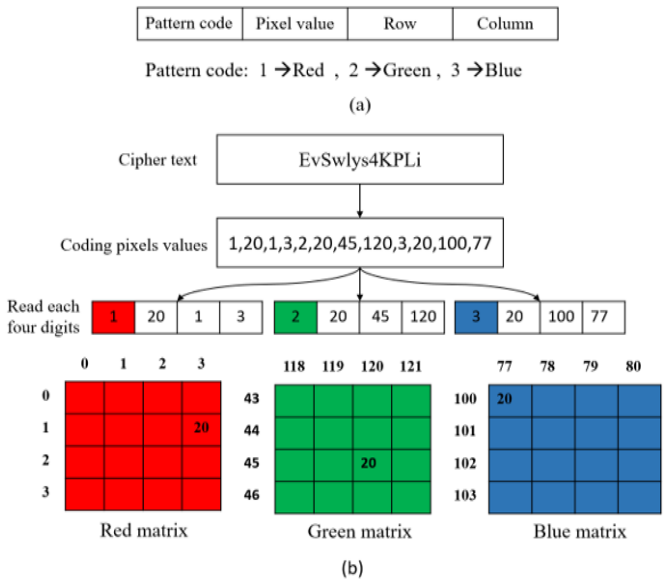


Figure 4. Decoding pixels value. (a)decoding pixel value, (b) the proposed decryption algorithm

3.2 Decryption algorithm

The first stage of the decryption process begins with converting the ciphertext into plain text, which represents the pixel contrast encoding of the image, and it is done with the same algorithm used for the encryption and with the same key.

Second, the plain text will represent the image data, where it will be decoded and converted into three matrixes that represent the RGB colors that make up the image. Figure 4 shows the method used to decode the data, where the process of reading each four numbers will be done independently, through which the type of matrix used will be determined by Through Pattern Number, then put the value of the pixel value in the specified place depending on the values of the row and column.

Algorithm 1: Encryption Process

Input :
M(r,c) //Input color image, where r,c Row and colum
K //key of encryption algorithm
Output:
E // text encryption
1: split the input color image M into three color(r,g,b)
2: define rgb //rgb =1 for r image, rgb =2 for g image, rgb =3 for b image,
3: for i=1 to 255 //where i is the value of pixel
4: create a matrix for all locations of i (r,c) in red image
5: E&=i & rgb & r & c // append four parameter to create coding value
6: end for
7: repeat step 2 to 6 to green and blue images
8: change E to byte
9: encrypted E // encryption algorithm for text

Algorithm 2: Decryption Process

Input :
E // Ciphertext
K //key of the decryption algorithm
Output:
M // plain image
1: create three matrices for (red, green, blue) images.
1: for i=1 to l // where l length of the ciphertext
2: for j=i to i+4 //read 4 digits
3: decoding digits //
7: end for j
7: end for i
8: combine three matrixes to create a plain image

4. RESULTS AND ANALYSIS

The implementation is done on python environment by using HP 15-dw2000, with Intel(R) Core (TM) i7-1065G7 CPU @ 1.50 GHz and 16.0 GB RAM. The encryption method used in the results is the AES algorithm, with a key size of 128 bits [19].

Measurement of the time required to encrypt an image is another important factor in evaluating the efficiency of algorithms. the time taken is the sum of the coding image process and the process of encryption algorithm of text. Table 1 shows the time taken for coding pixels plus the time for the ciphertext for three different sizes of images by using the AES encryption algorithm with 128 bits key size.

4.1 Histogram analysis

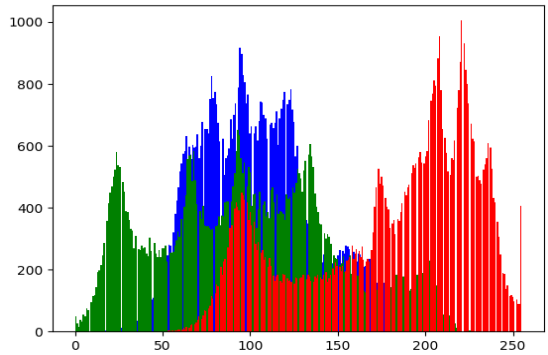
The histogram of an image shows how the pixels in the image are distributed at different levels of colors.in traditional image encryption, The histogram of the encrypted image must be fairly regular and differ significantly from the histograms of the original image that means that the numbers (0 - 255) are their number almost equal, and thus provides no evidence for the use of any statistical attack [20-23].

The histogram of cipher image in our proposed method has no effect because the image will transform into ciphertext, in Figure 3 the results show that the ciphertext is very different from the original image.

The image histogram shows that the distribution of pixels in the original image at different levels of colors does not affect the ciphertext and thus does not provide evidence of the use of any statistical attack on the proposed image encoder because the data that will be encrypted is the locations of pixel values so that the results of our final pattern file are text and not image and the attacker will not be able to analyses the histogram of text., this is one of the strong points of our research. as shown in Figure 5.

Plain image “Lena”

Histogram of Plain images

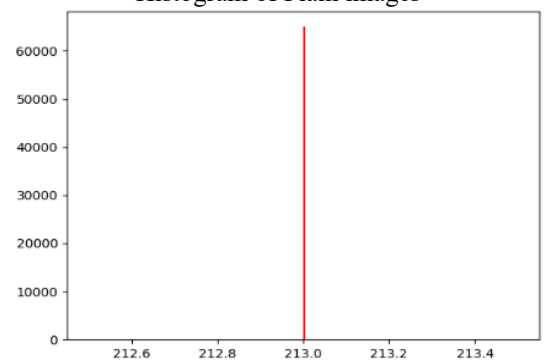


Ciphertext for encrypted image “Lena”

b'gABhW_dUYl_vBwV9FqnaaMtiwUQRnBympWrIFNdp_IA_AHq53kyuZNphUjMCAAKErvs7tDhZIXIIKAQOf5Z2Rvohq
1R98dAMoE8x8NfuvkKKPLi3iHXcuac8Y90cQcY0Dj9Y0MgNa5RDLOLAtAAodDoyBfR_rE_kLlkNK10BfueMiOv8srixu
DwJ3prOoLaFd1dmrSvssafo_6UGeNI7f9UGjJjOsavinOm2qALGRt0DyXHgU12yxYCw01PmC0GskwvJn5nWdZuS_zb6Sh
XWbwakQRUNc3f16AzRpCCPKIiXAWfwGxEvSwlys44ZKaIW9_Hs_ygmUibL1OOKwKCYSLOF6CQGZ3qk2aX15va6D
FvZshkCIuknGOuK8LxCKEMH0PGeHWvEinDtNSuQvGgLfupSmGhzEdBPCAfj1lSVspIlJCFprGqtzr4S0okjmQzhKpcrwS
BTSDPczm4JmBliZmgEIHfbSNfgdNPGe2egGqhi

Plain image “gray”

Histogram of Plain images



Ciphertext for encrypted image “gray”

b'eALaFtvfqEV8uJo1PgvSu38NKihnQwvWaH3tPAHtSgiasQfJ0SDAfNaCB8_0Ydcfr1uXcnagy_1nrAwy53RUTe1QRCZkaa
bIAIwfADmB_lTxb796KIVz8AEznRsUhT0lvDHyRNoTPkzO7io0tyc9XsY0oLi_DVGnoMIPOA374AIBRxdR8mTxIWPK57
hKJisTlsKPOmwhyWiJHDyx3gwQ7uKB4QzeUn1wkGHcifLhW1oEbZL5MtVnQ3RxTs2RjDq4ZHHjSTMTh8gpIbQLS8fJy
vAETHlopQkTDIk3d9pSwFDwgkwnnc9mj0mpdTdzhonuPBZxV82KWtTyCuVm0qXzsuu5qemU3ebYBcDqh8PeDXjoI1Qo
RIeoaVdXIKFUS1igBxPGwBkrk8fdMwTbiCNBi8ocJ6g74I6Oj260UWz2MPv0iUbc18V6tvtukhTVMEg6YOmaLhygEDA56
sX71sF7AFzWxFRP997Cqq48OnbbLjxBXiSw3

Figure 5. Experiment results for histogram analysis

Table 1. Time taken for encryption / decryption

Process	Image size					
	255*255		512*512		1024*1024	
	Coding time (sec)	Total time (sec)	Coding time (sec)	Total time (sec)	Coding time (sec)	Total time (sec)
Encryption	0.521	0.582	0.983	1.112	3.263	3.403
Decryption	0.093	0.124	0.511	0.594	1.0882	1.116

Table 2. Comparison analysis

Result Analysis	Image to Image Encryption Approach	Image to Text Encryption Approach (Proposed System)
Histogram Analysis	The values of pixels have approximately equal values	Not effected
Entropy	Must near to 8	Not effected
Password Space	less than probability	More than probability
Key Size	Static size (depending on the type of encryption algorithm)	Dynamic size (depending on which type of encryption algorithm can be used for encryption text)
Output Cipher Size	Same of plain image	Increase in size by the number of pixels that used for encoded

4.2 Brute force analysis

A good encryption system counters brute force attacks with a design that has a key area large enough to make brute force attacks infeasible [24, 25]. In our encryption algorithm, pixel value encoding is used as a chaotic scheme for composing the text before the encoding process begins. The content of the image information will be changed to values based on their locations. The encoding size of the encoded text will be relatively large compared to the image size, and this makes it difficult for the hacker to parse the large size of the ciphertext.

The strengths of our proposal to resist brute force attacks are the following points.

A) Several methods can be used to encode image pixels and below we explain three different scenarios for encoding pixel values.

Serial numbers: coding the values (0-255), By creating a default table for each value and then searching for it in all images by selecting the line and column and encoding it, and then moving to the other value as described in algorithm 1.

- Row by row: coding all values row by row in RGB images Independently.
- Column by column: coding all values column by column in RGB images Independently.

B) Use any symmetric text encryption algorithm with any key size to encrypt coding text.

It is worth noting the concept of this type of attack is password space, Each pixel is encoded with 4 numbers, the image in size r*c will be r*c*4 after converting it to text. The total number of key lengths (L) is 2^L and Each pixel is encoded with 4 numbers, the image in size r*c will be r*c*4 after converting it to text. Therefore, the password space of the proposed scheme denoted by (Ps) can e calculated in the following expression.

$$Ps=\mathbf{2^L} \times (\frac{r \times c \times 4}{L}) \quad (3)$$

4.3 Entropy

The entropy of a cipher picture is used to determine the level of uncertainty present in it [26]. The result of the encryption will be text, so the entropy of the image has no effect.

In Table 2, it shows a comparison of the proposed algorithm, which uses the image-to-text conversion method, with other encryption methods, which use the image-to-image conversion method.

5. CONCLUSION

This paper proposes a novel implementation of the Image Encryption Method that used an image to text technique that is capable of resolving the issues associated with established conventional cryptographic methods, with ideal processing time for encryption and decryption as demonstrated in results (Table 1). Although the proposed encryption technique is not superior to the popular encryption algorithms in terms of size. For this technique there is no need to displace the pixel and change the bit values, pixel values are coded and rearranged Then they are encrypted to obtain the cipher image but in text method. Multiple ways to encode pixel values for the image into text, as well as multiple choice of algorithm to encode the text, makes it impossible for attackers to crack the IMGTXT algorithm and detect the plain image from the ciphertext.

REFERENCES

[1] Denning, D.E.R., Robling, E. (1982). Cryptography and Data Security. Vol. 112. Reading: Addison-Wesley.

[2] Pawar, H.R., Harkut, D.G. (2018). Classical and quantum cryptography for image encryption & decryption. In 2018 International Conference on Research in Intelligent and Computing in Engineering (RICE), San Salvador, El Salvador, pp. 1-4. http://doi.org/10.1109/RICE.2018.8509035

[3] Rao, K.S., Sridhar, M. (2021). A novel image encryption using parity based visual cryptography. Ingénierie des Systèmes d'Information, 26(1): 135-142. https://doi.org/10.18280/isi.260115

[4] Kumar, T., Chauhan, S. (2018). Image cryptography with matrix array symmetric key using chaos based approach. International Journal of Computer Network and Information Security, 10(3): 60-66. https://doi.org/10.5815/ijcnis.2018.03.07

[5] Elhoseny, M., Shankar, K., Lakshmanaprabu, S.K., Maseleno, A., Arunkumar, N. (2020). Hybrid optimization with cryptography encryption for medical image security in the Internet of Things. Neural Computing and Applications, 32(15): 10979-10993. https://doi.org/10.1007/s00521-018-3801-x

[6] Herbadji, D., Derouiche, N., Belmeguenai, A., Herbadji, A., Boumerdassi, S. (2019). A tweakable image encryption algorithm using an improved logistic chaotic map. Traitement du Signal, 36(5): 407-417. https://doi.org/10.18280/ts.360505

[7] Li, M., Lu, D., Xiang, Y., Zhang, Y., Ren, H. (2019). Cryptanalysis and improvement in a chaotic image cipher using two-round permutation and diffusion. Nonlinear Dynamics, 96(1): 31-47. https://doi.org/10.1007/s11071-019-04771-7

[8] Akhshani, A., Akhavan, A., Lim, S.C., Hassan, Z. (2012). An image encryption scheme based on quantum logistic map. Communications in Nonlinear Science and

Numerical Simulation, 17(12): 4653-4661. https://doi.org/10.1016/j.cnsns.2012.05.033
[9] Singh, L.D., Singh, K.M. (2015). Image encryption using elliptic curve cryptography. Procedia Computer Science, 54: 472-481. https://doi.org/doi:10.1016/j.procs.2015.06.054.
[10] Chai, X., Gan, Z., Lu, Y., Chen, Y., Han, D. (2017). A novel image encryption algorithm based on the chaotic system and DNA computing. International Journal of Modern Physics C, 28(05): 1750069. https://doi.org/10.1142/S0129183117500693
[11] Zhang, X., Wang, L., Niu, Y., Cui, G., Geng, S. (2019). Image encryption algorithm based on the h-fractal and dynamic self-invertible matrix. Computational Intelligence and Neuroscience, 2019: 9524080. https://doi.org/10.1155/2019/9524080
[12] Hamad, A.S., Farhan, A.K. (2020). Image encryption algorithm based on substitution principle and shuffling scheme. Engineering and Technology Journal, 38(3): 98-103. https://doi.org/10.30684/etj.v38i3b.433
[13] Gladwin, S.J., Gowthami, P.L. (2020). Combined cryptography and steganography for enhanced security in suboptimal images. In 2020 International Conference on Artificial Intelligence and Signal Processing (AISP), Amaravati, India, pp. 1-5. https://doi.org/10.1109/AISP48273.2020.9073306
[14] Farah, M. A., Farah, A., Farah, T. (2020). An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. Nonlinear Dynamics, 99(4): 3041-3064. https://doi.org/10.1007/s11071-019-05413-8
[15] Masood, F., Ahmad, J., Shah, S.A., Jamal, S.S., Hussain, I. (2020). A novel hybrid secure image encryption based on Julia set of fractals and 3D Lorenz chaotic map. Entropy, 22(3): 274. https://doi.org/10.3390/e22030274
[16] Jabirulah, M., Srinivas, A., Kavitha, P. (2020). A digital image encryption algorithm based on bit-planes and an improved logistic map. In Recent Trends and Advances in Artificial Intelligence and Internet of Things, pp. 109-118. https://doi.org/10.1007/978-3-030-32644-9_12
[17] Hua, Z., Zhu, Z., Yi, S., Zhang, Z., Huang, H. (2021). Cross-plane colour image encryption using a two-dimensional logistic tent modular map. Information Sciences, 546: 1063-1083. http://doi.org/10.1016/j.ins.2020.09.032
[18] Abd Aljabar, R.W., Hassan, N.F. (2021). Encryption VoIP based on generated biometric key for RC4 algorithm. Engineering and Technology Journal, 39(1B): 209-221. http://doi.org/ 10.30684/etj.v39i1b.1755
[19] Mewada, S., Sharma, P., Gautam, S.S. (2016). Exploration of efficient symmetric AES algorithm. In 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Indore, India, pp. 1-5. https://doi.org/10.1109/CDAN.2016.7570921
[20] Rao, G.S., Srikrishna, A. (2021). Image pixel contrast enhancement using enhanced multi histogram equalization method. Ingénierie des Systèmes d'Information, 26(1): 95-101. https://doi.org/10.18280/isi.260110
[21] Chen, Y.Y., Hua, K.L., Tsai, Y.C., Wu, J.H. (2021). Photographic reproduction and enhancement using HVS-based modified histogram equalization. Sensors, 21(12): 4136. https://doi.org/10.3390/s21124136
[22] Alkhalid, F.F., Hasan, A.M., Alhamady, A.A. (2021). Improving radiographic image contrast using multi layers of histogram equalization technique. IAES International Journal of Artificial Intelligence, 10(1): 151-156. https://doi.org/10.11591/ijai.v10.i1.pp151-156
[23] Mahdi, S.A. (2021). An improved method for combine (LSB and MSB) based on color image RGB. Engineering and Technology Journal, 39(1B): 231-242. http://dx.doi.org/10.30684/etj.v39i1B.1574
[24] Tirado, E., Turpin, B., Beltz, C., Roshon, P., Judge, R., Gagneja, K. (2018). A new distributed brute-force password cracking technique. In International Conference on Future Network Systems and Security, Paris, France, pp. 117-127. https://doi.org/10.1007/978-3-319-94421-0_9
[25] Agarwal, A.K., Rani, L., Tiwari, R.G., Sharma, T., Sarangi, P.K. (2021). Honey encryption: Fortification beyond the brute-force impediment. In Advances in Mechanical Engineering, pp. 673-681. https://doi.org/10.1007/978-981-16-0942-8_64
[26] Ye, G., Pan, C., Huang, X., Zhao, Z., He, J. (2018). A chaotic image encryption algorithm based on information entropy. International Journal of Bifurcation and Chaos, 28(1): 1850010. https://doi.org/10.1142/S0218127418500104