Academic Journal of Nawroz University (AJNU), Vol.11, No.3, 2022

https://doi.org/10.25007/ajnu.v11n3a1301

Review of Image Encryption using Different Techniques

Rozin M. Abdullah[1], Araz Rajab Abrahim[2]
[1] Department of Information Technology Technical Collage of Informatics - Akre Duhok Polytechnic University, Duhok Polytechnic University, Kurdistan Region –Iraq
[2] Technical College of Administrative, Duhok polytechnic University, Kurdistan Region –Iraq

ABSTRACT
Encryption is one of the measures that ensure the security of images used in various fields such as military understanding, secure clinical imaging offices, Internet and intranet media, electronic banking, and individual association images such as Facebook, WhatsApp, Twitter, etc. On this huge number of images that are sent in a free and open link either during selection or messaging; Then their security ends up being a central need in individual insurance organizations and the arrangement. This article audits and summarizes various image encryption systems to further develop advanced image encryption strategies that operate with expanded flexibility and security.

KEYWORDS: Image Encryption Techniques, encryption key, Security Parameters

1. Introduction

In the past years, the main concern was the security and integrity of data, with the rapid development of computer networks, information leakage occurs in the process of transmitting and storing data across computer networks that are vulnerable to various types of attacks. To make the data secure from various attacks and for the integrity of data we must encrypt the data before it is transmitted or stored. [1, 2] Accordingly, network security and data encryption issues are considered as a significant subject. Currently, images are considered as the most important source of information. The applications of image encryption can be used in various fields like wireless communication, multimedia systems, medical imaging, telemedicine, and military communication.[3].

With the quick improvement of the internet of Things (IoT) and Data and Correspondence Innovation (ICT), the human culture is progressively situated towards interchanges utilizing the Web [4, 5]. As text, images and recordings are significant transporters of data, the security in the transmission cycle is a key examination issue. In the beyond 10 years, with the advances of innovation, the extent of shading image data in interactive media became famous [6]. Uniquely in contrast to message data, images have the qualities of containing information limit and solid connection between pixels [7]. In any case, conventional encryption techniques are not reasonable for image encryption and, in this way, different image situated calculations have been progressed. We find in the writing image encryption plans dependent on compressive detecting, DNA processing and turmoil, with the calculations fulfilling disarray and dissemination prerequisites [8, 9].

Digital images are posted online to be exchanged between different clients. These could be dark military images, singles images, medical images, and that's just the beginning. Clients will benefit from such offices that do not pay much attention to the risk of vulnerability. Accordingly, ensuring that there is no unauthorized access is vital. [7].

Image Chaotic encrypting in previous works relied on image chaos or the posting process. A fuzzy image is created by switching the places of the pixels. Chaos abilities are basically the standard guide. Scattering is the most common way to change the reflections of faint pixels in an image. The primary deployment capabilities are Chen's Guide, Calculated Guide, and Henon Map. [10]

2. IMAGE SECURITY PARAMETERS

The presentation of the image encryption system is evaluated by measurements such as connectivity between pixels, histogram, main space, and data entropy relative to the normal image and code image. The perfect image encryption calculation increases the distinction in pixel estimates between the normal image and the encrypted image. The scrambled image is made from the discretionary example that does not edit any part of the normal image and key. Thus, the encrypted image appears independent of the normal image. The accompanying clip is accurate to these display measurements. [11].

2.1 Histogram Analysis

Histograms define the measurable qualities of the images, revealing the dispersion of pixels at the top of the image. [12] The singular image histogram should be very surprising than the scrambled image graph. Normal image histograms are inherently non-uniform. While histograms of encrypted images must be uniform in nature. This means that all the pixels are similarly spread out in space.[13] the histogram of the cipher text image is significantly different from those of the original images. [14].

2.2 Correlation Coefficient (CC)

The first image has a high correlation between the nearby pixels in the representation, the scene, and the angle bearings [15]. The encrypted image must have a low relationship between nearby pixels in three ways. A decent image encryption strategy is one that minimizes this relationship in the encrypted image. [16].

2.3 Entropy Analysis

Shannon's entropy computes the required data within the image. It estimates the normal data for each bit in the image. It contains the data that can be visualized accessed in the given image. Each pixel has a distinct value. Thus, the entropy of the encrypted image means that each pixel has an equivalent probability with uniform assignment [17].

It can be computed as:

$$H(S)= -\sum_{s} \quad (p(s_i) \times p(s_i)) \qquad (1)$$

where H(S) represents the entropy of message source (S). P (s_i) denotes the probability of occurrence of si. The value of $IE \in [0, 8]$ It should be close to 8 for 8-bit image. [1, 3].

In this way, the proposed multi-image quantum encryption and compression computation can oppose the entropy assault of the data. [18].

2.4 Key Sensitivity

Image encryption calculations must be very sensitive to the key. Any modification to the prerequisites that creates the first ambiguity key will present an alternate fuzzy image.[19].

2.5 Unified Average Changing Intensity (UACI)

These measurements test the effect of a single pixel shift on the entire image that is mixed by a specific encrypt calculation. [20].

UACI measures the mean power to distinguish between normal image C1 and encrypted image C2 by. UACI can be defined as follows:

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \quad \frac{C_1(i,j)-C_2(i,j)}{255}\right] \times 100\% \qquad (2)$$

To obtain more security, the output of such encrypted image outperforms symbols with UACI near to 33%.

2.6 The Number Changing Pixel Rate (NPCR) Measure

It is characterized by the level of different pixel numbers between two blurry images, whose normal images have only one-pixel discrimination. Assuming any procedure provides a high benefit to NPCR, then, at this point, the computation is better against differential attacks. [21]

The NPCR asses the percentage of dissimilar pixels number to the entire pixels number among the two encrypted images E1 (xi, yj) and E2 (xi ,yj). When a single pixel changes.

$$NPCR(E1, E2) = \frac{\sum_{i,j} D(X_i, Y_j)}{W \times H} \text{x}100\% \qquad (3)$$

Achieving more prominent NPCR estimation, the calculation is more secure. [10]

3. IMAGE ENCRYPTION TECHNIQUES

A successful image encryption technique is the treatment of a computerized image as a piece stream and afterward encrypt this piece stream utilizing conventional information encryption plans, for example, the triple information encryption standard, progressed encryption standard, and worldwide information encryption calculation [22-23]. Be that as it may, contrasted and a piece stream, a computerized image has particular inborn properties, including information redundancies and huge pixel connections [24]. By regarding a computerized image as a piece stream to be scrambled by means of existing information encryption calculations [25]. Thusly, these systems experience the ill effects of various inadequacies, for example, low encryption efficiencies [26]. Accordingly, improvement of new image encryption calculations that enough consider the properties of computerized images can fundamentally upgrade the proficiency of image assurance [27].

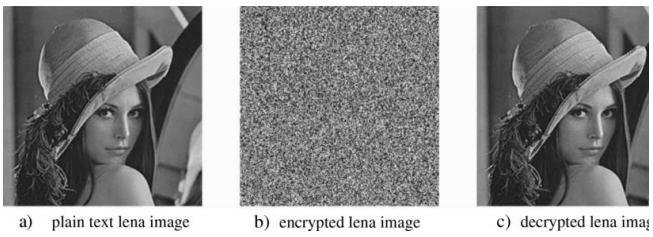

Figure. 1 Lena image encryption and decryption

3.1 Image encryption with a digital signature

A primary image encryption approach includes a system wherein a primary image graph is encrypted with random section mask. One mask is placed in the enter aircraft and the alternative one within the spatial frequency plane. These outcomes inside the formation of a desk bound white noise. In the decryption system, the encrypted or the encrypted image is Fourier converted, then multiplied by the complicated conjugate of the random section mask, and subsequently inverse Fourier transformed [28]. This is known as the double random segment encryption machine. Optical implementations of the double random segment encryption device have additionally been suggested. The encrypted image graph is recorded as a hologram by means of the use of a reference beam and the decryption of the image is finished by way of using the segment conjugate of the random segment masks [29].

Li, T., Du, B. and Liang, X., [30] The traditional chaotic model is utilized in the encryption calculation to produce two arrangements of chaotic groupings to encrypt the image, The two-layered model is utilized to create turbulent groupings to encode and scramble the image. Through the security examination, it very well may be presumed that the image encryption calculation proposed is delicate to the mystery key and has an enormous mystery key space. It can oppose thorough assaults to a serious level and can oppose clamor obstruction. The calculation has solid security and heartiness and is reasonable for image encryption with high security level.

Asl, A.M., Broumandnia, A. and Mirabedini, S.J [31] scale invariant tone image encryption technique in three-dimensional space is introduced. From the start, the two-dimensional shading image is changed over into three-dimensional space, for this situation, the red, green, and blue shading range are separated into a bunch of dark level square sub images. Then, at that point, to have disarray and dispersion properties, the 3D replacement and 3D stage activity are performed on the sub images.

Vaseghi, B., Hashemi, S.S., Mobayen, S. and Fekih, A. [32] Chaotic secure correspondence method is proposed for the encryption and secure transmission of satellite images through a station with obscure time postpone engendering. In such manner, a hearty regulator is intended to synchronize the altered Chua oscillators at the transmitter and receiver with the time delay and parametric vulnerabilities in the limited time. A blend of chaotic keys and encryption strategy

as multi-shift figure encryption and chaotic concealing of QAM images has been executed to expand the security of the remote OFDM.

Rathore, V. and A.K. Pal [33] introduced an image cryptosystem in light of confusion diffusion schematic design which points on performing stage utilizing chaotic succession produced by 2d chaotic Henon map and edge planes acquired utilizing different edge location administrators to accomplish better confusion.

3.2 Image encryption using chaotic logistic map

Of late, owing to visit stream of cutting-edge images across the world over the transmission media, it has become fundamental for secure them from spillages. Various applications like military image informational indexes, secret video conferencing, clinical imaging system, computerized TV, online individual image graph assortment, etc. require reliable, speedy and amazing security structure to store and send progressed images. The necessities to fulfill the security needs of electronic images have incited the headway of good encryption systems. During the last decade, different encryption estimations have been proposed in the composing subject to different norms [34]. Among them, conflict-based encryption techniques are seen as valuable for beneficial use as these methodologies provide a good combination of speed, high security, complexity, reasonable computational expense and computational power, etc. Modern images have obvious characteristics, for example, an abundance of data, a strong relationship between neighboring pixels, Being less sensitive when distinguishing it from text data, for example, a slight change in the attribute of any pixel of the image does not degrade the idea of the image, the collective limitations of the data, etc., so traditional codes such as IDEA, AES, DES and RSA are not considered etc. are suitable for continuous image encryption because these codes require huge computational time and high identification power. For continuous image encryption only, these codes are the best that require some guesswork and all the time without compromising security [35]. Encryption plans that are rolled out incrementally, and may even contain a greater degree of luxury features, will be of little use in continuous cycles.

Liu, X., Xiao, D. and Xiang, Y [36] Consolidating logistic map with increasingly in digit stage activities. Encryption calculation uses both increasingly in piece stage to scramble pixels. Besides, chaotic diffusion is additionally performed to additional protected images. The sensitive boundaries of strategic guide make the key space adequately enormous enough to oppose beast power assault. The quantum circuits are given and mathematical reproduction results show that the proposed conspire is secure to oppose different assaults. The computational intricacy of the proposed plot is lower than traditional image encryption.

Sirichotedumrong, W. and Kiya, H., [37] The proposed conspire has preferable execution over the regular one as far as the pressure execution. Test results showed that images scrambled by utilizing the proposed plot had a higher-pressure execution than those encoded by the traditional grayscale plan. Also, the proposed plot was affirmed to have practically a similar strength against ciphertext-just assaults as the regular grayscale-based encryption.

Wang, X., X. Zhu, and Y. Zhang [38] introduced an image encryption procedure utilizing a two-dimensional, Henon map, at first it carried out the disarray conspire utilizing chaotic grouping got by a few emphases utilizing turbulent guide approach.

Abdullah, H.N. and H.A. Abdullah [39] The proposed scheming comprises of three phases confusion rearranging and diffusion. In disarray the first image is befuddled by utilizing Arnold feline turbulent guide. the pixels of the befuddled picture are rearranged to add more irregularity and unconventionality. the rearranged picture is diffused

by a key picture created by consolidating arrangements produced from Henon and Strategic chaotic maps.

3.3 Image encryption with machine learning

Image encryption is one of the measures to maintain security. Image encryption changes a unique image to the encrypted image that people cannot perceive in the first image [40]. Image encryption accounts are primarily developed for sending images securely through a public organization [41]. If people and the machine also need to perceive the material in the encrypted image, the image must be decoded from scratch. However, when the image is decoded, anyone can perceive the essence. This implies that image decryption is reasonable to abuse protection [42].

Kamal, S.T., Hosny, K.M., Elgindy, T.M., Darwish, M.M. and Fouda, M.M. [43] Another calculation for encoding medical images in view of image squares and disorder. calculation image encryption execution tried utilizing entropy, histogram, correlation coefficient, differential assault, key space, and key awareness. Results showed that the proposed calculation is productive in scrambling both dim and shading medical images. Our calculation contrasted with other ongoing encryption calculations, and the outcomes affirm that the proposed calculation has great attributes in encoding both dark and shading medical images.

4. CRYPTOGRAPHY

Encryption strategies incorporate cryptography, which includes applying a strategy considered a calculation to plain text to transform it into something that would seem gibberish to any individual who doesn't have a key to unscramble it [44]. PC based encryption strategies use keys to scramble and unscramble information [45].

Cryptography is extensively grouped into two classifications: Symmetric key Cryptography and Asymmetric key Cryptography prevalently known as open key cryptography [46].

As of now, symmetric key cipher is also regulated as classic cipher and modern cipher [47]. Further entering to the bottom, the classic cipher is divided into conversion ciphers and substitution ciphers. Of course, modern cipher is separated into Stream Cipher and Block Cipher [48].

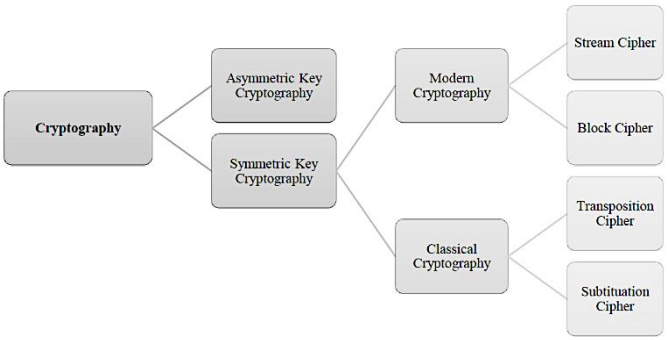

Figure.2 image Encryption Types of Cryptographies

4.1 Symmetric Key Cryptography

Symmetric key encryption in any case called symmetric encryption is where a secret key is used for both the encryption and decryption limits [49]. This method is opposite to asymmetric encryption where one key is used for obfuscation and another key is used for decryption [50].

An encryption framework in which the sender and recipient of a message share a single, plain key that is used to merge and decrypt the message. The most popular symmetric key framework is the Data Encryption Standard (DES) [51].

In cryptography, form exegesis is a encryption system in which the positions occupied by units of plaintext (which are generally characters or social affairs of characters) are conveyed by a modular structure, such that the ciphertext creates a phase of the plaintext.

An encryption method by which explicit text units are replaced by shape text, according to a nice syntax; The "units" may be single characters (the most widely recognized), groups of characters, triple groups of characters, a combination of the above, etc. [52].

Stream Cipher symmetric or secret key cipher obfuscate one piece at a time. With Stream Encryption, the number of the plaintext or comparable byte will scramble into an alternate bit or byte each time it is

encrypted [53].

Block Cipher A cipher methodology that applies deterministic computation near a symmetric key to encrypt a box of text, rather than obfuscate a small smidgen [54].

4.2 Asymmetric Key Cryptography

Asymmetric encryption in any case is called public key cryptography, is a cycle of some related keys that use one public key and one private key to encrypt and decrypt a message and protect it from unauthorized access or use [55].

An encryption cycle where certain keys are used to scramble and decode information. The keys are private anyway they are mathematically related, so much so that restoring the plaintext by decrypting the ciphertext is possible [56].

Table 1 Comparison of Image Encryption Technique

S.N	Authors	Technique Used	Key Space	Key Sensitivity	Entropy		Histogram	Correlation		NPCR %
					Original	*Cipher*		*Original*	*Cipher*	
[30]	Li, T., Du, B. and Liang	Two-dimensional Lorenz and Logistic.	10^{112}	High	7.9028	7.9895	Good	0.8817	0.0711	99.58
[36]	Liu, X., Xiao, D. and Xiang	the inter-intra bit-level permutation strategy.	2^{112}	low	6.2492	7.9969	Good	0.9477	0.0260	99.21
[37]	Sirichotedumrong, W. and Kiya	New grayscale-based block scrambling image encryption (the security of EtC systems)	2^{6912}	High	7.4434	7.4434	Same original	0.1814	0.0341	99.65
[31]	Asl, A.M., Broumandnia, A. and Mirabedini	a 3D modular chaotic map	10^{801}	Very high	7.7554	7.9998	Excellent	0.7635	0.9219	99.60
[32]	Vaseghi, B., Hashemi, S.S., Mobayen, S. and Fekih, A	Chaotic secure communication technique	2^{419}	High	7.0951	7.9986	Good	0.8452	0.9283	99.61
[43]	Kamal, S.T., Hosny, K.M., Elgindy, T.M., Darwish, M.M. and Fouda, M.M.	New Image Encryption Algorithm for Grey and Color Medical Images	10^{140}	Medium	7.8862	7.9993	Good	0.2431	0.9849	99.59
[38]	Wang, X., X. Zhu, and Y. Zhang	Josephus Traversing and Mixed Chaotic Map	2^{168}	High	7.5755	7.9971	Good	0.9721	-0.0029	99.59
[39]	Abdullah, H.N. and H.A. Abdullah	Hybrid Chaotic Map	2^{118}	high	7.5906	7.9765	Good	0.0947	-0.0051	99.60
[33]	Rathore, V. and A.K. Pal	Henon map	10^{210}	low	7.9843	7.9991	Good	0.9850	0.0082	99.51

5. CONCLUSION

In this Review, all important encryption strategies are introduced and investigated for familiarizing yourself with the crypto-privileged accounts used to encrypt the image sent through the enterprise. The results of the recreation show that each calculation has both advantages and disadvantages that depend on the methods applied to the images. This work has a survey of distinct image encryption algorithms, and concludes that the chaotic approach exhibits extreme uncertainty and provides incredible safety. Moreover, study unveils that NPCR doesn't rely upon the key sensitivity; thus, to accomplish agreeable NPCR in the square based encryption techniques, the upsides of an encoded square ought to be subject to the next cipher blocks. Moreover, results show that scrambling alone isn't adequate to offer the astounding security; there ought to be a replacement alongside rearranging. Subsequently, this audit deduces that a superior image encoding technique has the accompanying attributes to give exceptional assurance; (1) Give huge key space, (2) Profoundly key sensitive, (3) Produce a uniform histogram, (4) Fulfill to Shannon's disarray and dissemination property, (5) Diminish connection adequately between two neighboring pixels, (6) Give vulnerability in the framework, (7) High NPCR esteem (close to 100 percent) and reasonable UACI rate (close to 33 %). In addition, other than these given ascribes, an encryption technique should be quick to the point of enciphering an image. Finally, a conclusion is that all inspected encryption algorithms in this paper, are powerful and have their own benefits and bad marks in regard of speed and security compromise.

6. REFERENCES

1. Liu, Y., et al., *Chosen-plaintext attack of an image encryption scheme based on modified permutation–diffusion structure.* Nonlinear dynamics, 2016. **84**(4): p. 2241-2250.
2. Padate, R. and A. Patel, *Image encryption and decryption using AES algorithm.* International Journal of Electronics and Communication Engineering & Technology, 2015: p. 23-29.
3. Mohammad, O.F., et al., *A survey and analysis of the image encryption methods.* International Journal of Applied Engineering Research, 2017. **12**(23): p. 13265-13280.
4. Chen, X.-D., et al., *Asymmetric encryption of multi-image based on compressed sensing and feature fusion with high quality image reconstruction*. Optics & Laser Technology, 2018. **107**: p. 302-312.
5. Chen, T., et al., *Image encryption and compression based on kronecker compressed sensing and elementary cellular automata scrambling*. Optics & Laser Technology, 2016. **84**: p. 118-133.
6. Enayatifar, R., F.G. Guimarães, and P. Siarry, *Index-based permutation-diffusion in multiple-image encryption using DNA sequence.* Optics and Lasers in Engineering, 2019. **115**: p. 131-140.

7. Chai, X., et al., *A color image cryptosystem based on dynamic DNA encryption and chaos.* Signal Processing, 2019. **155**: p. 44-62.
8. Wu, J., X. Liao, and B. Yang, *Image encryption using 2D Hénon-Sine map and DNA approach.* Signal Processing, 2018. **153**: p. 11-23.
9. Wu, G.-C., et al., *New variable-order fractional chaotic systems for fast image encryption.* Chaos: An Interdisciplinary Journal of Nonlinear Science, 2019. **29**(8): p. 083103.
10. Afifi, A., *A chaotic confusion-diffusion image encryption based on Henon map.* International Journal of Network Security & Applications (IJNSA) Vol, 2019. **11**.
11. Geetha, S., et al., A literature review on image encryption techniques. International Journal of Information Security and Privacy (IJISP), 2018. 12(3): p. 42-83.
12. Yousif, S.F. Grayscale image confusion and diffusion based on multiple chaotic maps. in 2018 1st International scientific conference of engineering sciences-3rd scientific conference of engineering science (ISCES). 2018. IEEE.
13. Kaur, M. and V. Kumar, A comprehensive review on image encryption techniques. Archives of Computational Methods in Engineering, 2020. 27(1): p. 15-43.
14. Li, X.-Z., W.-W. Chen, and Y.-Q. Wang, Quantum image compression-encryption scheme based on quantum discrete cosine transform. International Journal of Theoretical Physics, 2018. 57(9): p. 2904-2919.
15. Dhall, S., S.K. Pal, and K. Sharma, A chaos-based probabilistic block cipher for image encryption. Journal of King Saud University-Computer and Information Sciences, 2018.
16. Shahna, K. and A. Mohamed, A novel image encryption scheme using both pixel level and bit level permutation with chaotic map. Applied Soft Computing, 2020. 90: p. 106162.
17. Chai, X., et al., An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations. Signal Processing: Image Communication, 2017. 52: p. 6-19.
18. Kamal, S.T., M.M. Darwish, and K.M. Hosny, Chaotic Maps for Image Encryption: An Assessment Study. Multimedia Security Using Chaotic Maps: Principles and Methodologies, 2020. 884: p. 27.
19. Geetha, S., et al., A literature review on image encryption techniques. International Journal of Information Security and Privacy (IJISP), 2018. 12(3): p. 42-83.
20. Zhao, Y. and L. Liu, A Bit Shift Image Encryption Algorithm Based on Double Chaotic Systems. Entropy, 2021. 23(9): p. 1127.
21. Mani, P., et al., Adaptive control for fractional order induced chaotic fuzzy cellular neural networks and its application to image encryption. Information Sciences, 2019. 491: p. 74-89.
22. Chen, L., et al., Double color image encryption based on fractional order discrete improved Henon map and Rubik's cube transform. Signal Processing: Image Communication, 2021. 97: p. 116363.
23. Deng, S., et al., Analysis and improvement of a hash-based image encryption algorithm. Communications in Nonlinear Science and Numerical Simulation, 2011. 16(8): p. 3269-3278.
24. Zhu, Z.-l., et al., A chaos-based symmetric image encryption scheme using a bit-level permutation. Information Sciences, 2011. 181(6): p. 1171-1186.
25. Seyedzadeh, S.M. and S. Mirzakuchaki, A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map. Signal processing, 2012. 92(5): p. 1202-1215.
26. Khan, M. and T. Shah, A literature review on image encryption techniques. 3D Research, 2014. 5(4): p. 1-25.
27. Sun, S., A novel hyperchaotic image encryption scheme based on DNA enencryption, pixel-level scrambling and bit-level scrambling. IEEE Imagenics Journal, 2018. 10(2): p. 1-14.
28. Zhang, X. and X. Wang, Multiple-image encryption algorithm based on DNA enencryption and chaotic system. Multimedia Tools and Applications, 2019. 78(6): p. 7841-7869.
29. Wang, X., L. Feng, and H. Zhao, Fast image encryption algorithm based on parallel computing system. Information Sciences, 2019. 486: p. 340-358.
30. Li, T., Du, B. and Liang, X., 2020. Image encryption algorithm based on logistic and two-dimensional Lorenz. IEEE Access, 8, pp.13792-13805.
31. Asl, A.M., Broumandnia, A. and Mirabedini, S.J., 2021. Scale invariant digital color image encryption using a 3D modular chaotic map. IEEE Access, 9, pp.102433-102449.
32. Vaseghi, B., Hashemi, S.S., Mobayen, S. and Fekih, A., 2021. Finite time chaos synchronization in time-delay channel and its application to satellite image encryption in OFDM communication systems. IEEE Access, 9, pp.21332-21344.
33. Rathore, V. and A.K. Pal, An image encryption scheme in bit plane content using Henon map based generated edge map. Multimedia Tools and Applications, 2021. 80(14): p. 22275-22300.
34. Xiong, Z., et al., Color image chaos encryption algorithm combining CRC and nine palace map. Multimedia Tools and Applications, 2019. 78(22): p. 31035-31055.
35. Strogatz, S.H., Nonlinear dynamics and chaos with student solutions manual: With applications to physics, biology, chemistry, and engineering. 2018: CRC press.
36. Liu, X., Xiao, D. and Xiang, Y., 2018. Quantum image encryption using intra and inter bit permutation based on logistic map. IEEE Access, 7, pp.6937-6946.
37. Sirichotedumrong, W. and Kiya, H., 2019. Grayscale-based block scrambling image encryption using ycbcr color space for encryption-then-compression systems. APSIPA Transactions on Signal and Information Processing, 8.
38. Wang, X., X. Zhu, and Y. Zhang, An image encryption algorithm based on Josephus traversing and mixed chaotic map. IEEE Access, 2018. 6: p. 23733-23746.
39. Abdullah, H.N. and H.A. Abdullah. Image encryption using hybrid chaotic map. in 2017 International

Conference on Current Research in Computer Science and Information Technology (ICCIT). 2017. IEEE.

40. Niyat, A.Y., M.H. Moattar, and M.N. Torshiz, Color image encryption based on hybrid hyper-chaotic system and cellular automata. Optics and Lasers in Engineering, 2017. 90: p. 225-237.
41. Yamada, Y., M. Iwamura, and K. Kise, Deep pyramidal residual networks with separated stochastic depth. arXiv preprint arXiv:1612.01230, 2016.
42. Chai, X., Y. Chen, and L. Broyde, A novel chaos-based image encryption algorithm using DNA sequence operations. Optics and Lasers in engineering, 2017. 88: p. 197-213.
43. Kamal, S.T., Hosny, K.M., Elgindy, T.M., Darwish, M.M. and Fouda, M.M., 2021. A New Image Encryption Algorithm for Grey and Color Medical Images. IEEE Access, 9, pp.37855-37865.
44. Lu, Q., C. Zhu, and X. Deng, An efficient image encryption scheme based on the LSS chaotic map and single S-box. IEEE Access, 2020. 8: p. 25664-25678.
45. Akkasaligar, P.T. and S. Biradar, Selective medical image encryption using DNA cryptography. Information Security Journal: A Global Perspective, 2020. 29(2): p. 91-101.
46. Liu, Y., et al., Optical image encryption algorithm based on hyper-chaos and public-key cryptography. Optics & Laser Technology, 2020. 127: p. 106171.
47. Pawar, H.R. and D.G. Harkut. Classical and quantum cryptography for image encryption & decryption. in 2018 International Conference on Research in Intelligent and Computing in Engineering (RICE). 2018. IEEE.
48. Ilayaraja, M., K. Shankar, and G. Devika, A modified symmetric key cryptography method for secure data transmission. International Journal of Pure and Applied Mathematics, 2017. 116(10): p. 301-308.
49. Shepherd-Barron, N.I., Some effectivity questions for plane Cremona transformations in the context of symmetric key cryptography. Proceedings of the Edinburgh Mathematical Society, 2021. 64(1): p. 1-28.
50. Sakurai, K., T. Nishide, and A. Syalim. Improved proxy re-encryption scheme for symmetric key cryptography. in 2017 International Workshop on Big Data and Information Security (IWBIS). 2017. IEEE.
51. Sen, A., A. Ghosh, and A. Nath. Bit level symmetric key cryptography using genetic algorithm. in 2017 7th International Conference on Communication Systems and Network Technologies (CSNT). 2017. IEEE.
52. Khan, S.A., H. Fakhruddin, and H.H. Rizvi, Security Enhancing by using ASCII Values and Substitution Technique for Symmetric Key Cryptography. Indian Journal of Science and Technology, 2017. 10(36).
53. Dijesh, P., S. Babu, and Y. Vijayalakshmi, Enhancement of e-commerce security through asymmetric key algorithm. Computer Communications, 2020. 153: p. 125-134.
54. Kaur, A., A Review on Symmetric Key Cryptography Algorithms. International Journal of Advanced Research in Computer Science, 2017. 8(4).
55. Zhang, J., et al. Tweaking the asymmetry of asymmetric-key cryptography on lattices: KEMs and signatures of smaller sizes. in IACR International Conference on Public-Key Cryptography. 2020. Springer.
56. Nirala, R.K. and M.D. Ansari. Performance evaluation of loss packet percentage for asymmetric key cryptography in VANET. in 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC). 2018. IEEE.