UDC 621
DOI: 10.15587/1729-4061.2022.265862

EVALUATING IMAGE ENCRYPTION ALGORITHMS FOR THE HYPERCHAOTIC SYSTEM AND FIBONACCI Q-MATRIX, SECURE INTERNET OF THINGS, AND ADVANCED ENCRYPTION STANDARD

Sabreen Ali Hussein
Master of Computer Science
Department of Mathematics and Computer
College of Basic Education*
Aseel Hamoud Hamza
Master of Computer Science
College of Law*
Suhad Al-Shoukry
Corresponding author
Lecturer
Department of Computer system Techniques
AL-Najaf Technical Institute
AL- Furat Al-Awsat Technical University
Najaf, AL-Najaf, Iraq, 54003
E-mail: inj.suhadaalzhra2010@atu.edu.iq
Musaddak Maher Abdul Zahra
PhD student
Department of Computer Techniques Engineering
Al-Mustaqbal University College
Al Hillah, Babylon, Iraq, 51002
Ali Saleem Abu Nouwar
MSc Electrical and Electronics Engineering
College of Engineering Technology
Mesallata, Libya, 61160
Sarah Ali Abdulkareem
Master in Computer Science
Department of Computer Science
Al-Turath University College
Al Mansour str., Baghdad, Iraq, 8996+87X
Mohammed Hasan Ali
Master in Computer Science
Department of Computer Techniques Engineering
Imam Ja'afar Al-Sadiq University
Najaf, Iraq, 10023
Mustafa Musa Jaber
Computer Techniques Engineering Department
Dijlah University College
Al Masafi str., Baghdad, Iraq, 00964
*University of Babylon
Al Najaf's str., Al Hillah, Babylon, Iraq, 51002

In the era of information technology, users had to send millions of images back and forth daily. It's crucial to secure these photos. It is important to secure image content using digital image encryption. Using secret keys, digital images are transformed into noisy images in image encryption techniques, and the same keys are needed to restore the images to their original form. The majority of image encryption methods rely on two processes: confusion and diffusion. However, previous studies didn't compare recent techniques in the image encryption field.This research presents an evaluation of three types of image encryption algorithms includinga Fibonacci Q-matrix in hyperchaotic, Secure Internet of Things (SIT), and AES techniques. The Fibonacci Q-matrix in the hyperchaotic technique makes use of a six-dimension hyperchaotic system's randomly generated numbers and confuses the original image to dilute the permuted image. The objectives here areto analyze the image encryption process for the Fibonacci Q-matrix in hyperchaotic, Secure Internet of Things (SIT), and Advanced Encryption Standard (AES), and compare their encryption robustness. The discussed image encryption techniques were examined through histograms, entropy, Unified Average Changing Intensity (UACI), Number of Pixels Change Rate (NPCR), and correlation coefficients. Since the values of the Chi-squared test were less than (293) for the Hyperchaotic System & Fibonacci Q-matrix method, this indicates that this technique has a uniform distribution and is more efficient. The obtained results provide important confirmation that the image encryption using Fibonacci Q-matrix in hyperchaotic algorithm performed better than both the AES and SIT based on the image values of UACI and NPCR

Keywords: Fibonacci Q-matrix in hyperchaotic, secure internet of things, AES

Received date 05.08.2022
Accepted date 06.10.2022
Published date 30.10.2022

***How to Cite**: Hussein, S. A., Hamza, A. H., Al-Shoukry, S., Abdul Zahra, M. M., Abu Nouwar, A. S., Abdulkareem, S. A., Ali, M. H., Jaber, M. M. (2022). Evaluating image encryption algorithms for the hyperchaotic system and Fibonacci Q-matrix, secure internet of things, and advanced encryption standard. Eastern-European Journal of Enterprise Technologies, 5 (2 (119)), 21–30. doi: https://doi.org/10.15587/1729-4061.2022.265862*

1. Introduction

The importance of digital images in multimedia technologies raises the stakes for user privacy protection. Image encryption is necessary to defend against unwanted user access in order to give the user this level of security and privacy. Internet communication, multimedia systems, medical imaging, telemedicine, and military communication are just a few of the

sectors where image encryption is used.Among the methods for hiding information, encryption is one of the best. Researchers have developed numerous methods for image encryption in recent years. To boost security, they employ several picture encryption concepts.The process of picture encryption involves changing the original image into one that is more complex. No one is able to view the material without the decryption key. Image encryption is used in the business world, the medical industry, military activities, and multimedia systems. The Internet of Things (IoT), a promising technology for the future, is expected to connect billions of gadgets. Increased connectivity is expected to generate mountains of data, and the security of that data may be at risk. In essence, the architecture makes use of more compact, lower-powered technology. Due to their complexity and need for numerous rounds to encrypt, conventional encryption methods are typically computationally expensive, thereby wasting the devices' limited energy. However, a simpler approach can jeopardize the intended fidelity [1–4].

In a variety of image-processing applications, the fractional-order functions outperform their similar integer-order functions. A method for encrypting color images using fractional-order chaotic systems is suggested by [5–7]. The Fibonacci Q-matrix coupled with the fractional-order 4D hyperchaotic Chen system ensures the effectiveness of the encryption method and its defense against attacks [6]. Real-time image encryption using a chaotic key generator is an illustration of an integrated encryption system as shown in Fig. 1.

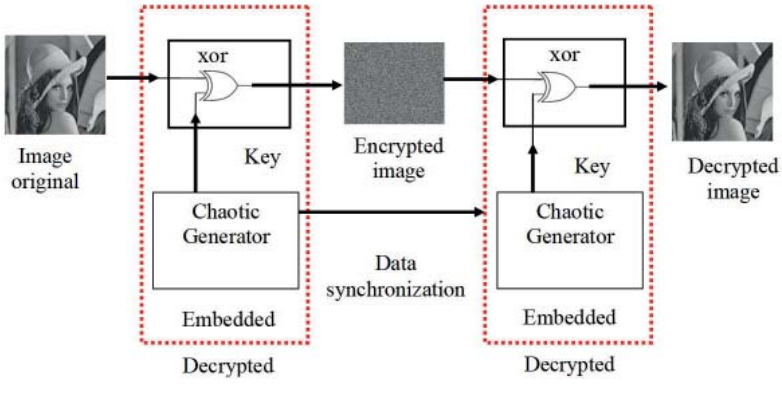


Fig. 1. Real-time image encryption using a chaotic key generator [8]

Numerous cryptographic methods have been suggested to secure the data; out of all the algorithms, one of the most used algorithms for data decryption and encryption is named the Advanced Encryption Standard (AES) [9–14]. Many academics have worked hard to create a new cryptographic algorithm prototype and have attempted to integrate it into an FPGA system. AES is a network of all conceivable data scrambling scenarios, where each output bit is dependent on each input bit, and mathematical operations are carried out. Due to the expanding use of images in a variety of fields, it is crucial to safeguard sensitive picture data from unwanted access. Such encryption algorithms also can contribute to adding secure monitoring of industrial processing such that in [15]. There are always unresolved issues regarding the analysis on image encryption processes especially for recent encryption techniques such as the Fibonacci Q-matrix in hyperchaotic to be evaluated and compared according to merit criteria on image encryption.

Therefore, research on evaluating the number of image encryption algorithms is relevant to decide which one performs better than the other among the existing recent techniques according to some image evaluation factors like UACI and NPCR.

2. Literature review and problem statements

Daily life requires the transfer of millions of images among clients. It's crucial to secure these images. Therefore, digital images are encrypted which is a familiar method used to secure image contents. On the basis of several ideas, including optical, compressive sensing, and chaotic maps image encryption, the existing image encryption methods are divided into numerous categories. The methods currently used to access the various security settings are compared [16]. A hyperchaotic system-based image encryption technique and a variable-step Josephus problem were also mentioned in the study [17]. The experimental findings demonstrated the plaintext sensitivity and resilience of the image encryption technique suggested in this paper. However, this study did not address the hyperchaotic system, so it did not produce the desired results. A unique use of fractional-order chaotic systems in color picture encryption was presented in the study [6]. They merged the Fibonacci Q-matrix with the 4D hyperchaotic Chen system of fractionalorder. They did not, however, demonstrate the ability to assess picture encryption techniques for the Secure Internet of Things (SIT) and AES. The research [5] presented an image encryption algorithm by means of a Fibonacci Q-matrix in hyperchaotic. This method confuses the original image, using numbers arbitrarily created by the six-dimensional hyperchaotic system. Although the study presented this algorithm, it did not address any of the Secure Internet of Things (SIT) and AES. In contrast, the work [18] presents a satellite picture encryption scheme based on the Josephus issue, Linear Feedback Register Shifting originator, hyperchaotic systems, and the SHA 512 hash function. However, they are unable to demonstrate the feasibility and efficacy of their strategy. Because quantum computers can defeat mathematically based encryption methods, the article [19] suggested a technique to encode quantum pictures based on a hyperchaotic system and a quantum rotating gate. Although the experimental findings of the performance study provided some security for the algorithm, this proposal did not cover all of the subtleties, such as the Fibonacci Q-matrix, the Secure Internet of Things (SIT), and AES. In terms of the AES algorithm, the Study [20] attempted to enhance security approaches by proposing chaotic image encryption to safeguard data and pictures during transmission between earth stations and satellites, but it did not address the usage of the Fibonacci Q-matrix system.

A self-adaptive double-color image encryption method was put forth by [21]. This uses 2D compressive sensing to initially compress and encrypt each RGB color component of the two input images. To create the final scrambled image, a complex image is re-encrypted using self-adaptive random phase encoding and discrete fractional random transform. By combining the benefits of a one-dimensional chaotic system with compressive sensing and the Fibonacci-Lucas transform. Research [22] developed hybrid picture compression and encryption techniques. Block compressive sensing was used by [23] to create an image encryption strategy. The

paper [24] introduced the 7D hyperchaotic system based on the 7D hyperchaotic image coding system by proposing an image coding algorithm based on the 7D similarity system and simultaneous swapping between rows and columns. But the problem was with the limitations not to mention Fibonacci Q-matrix, Secure Internet of Things (SIT), and AES.

Therefore, all this allows to argue that it is appropriate to protect images as users in the information technology era have to exchange millions of images every day. Digital image encryption is crucial for protecting image content. In image encryption techniques, digital images are converted into noisy images using secret keys. It is essential to compare and evaluate the existing image encryption algorithms such as Hyperchaotic, Fibonacci Q-matrix, Secure Internet of Things (SIT), and AES to select theappropriate one.

3. The aim and objectives of the study

The aim of the study is to evaluate image encryption algorithms for the Fibonacci Q-matrix in hyperchaotic, SIT, and AES. This will make it possible to secure image content using digital image encryption in the era of information technology, where users had to send millions of images back and forth daily.

To achieve this aim, the following objectivesare accomplished:

– to analyzethe image encryption of Hyperchaotic System and Fibonacci Q-matrix algorithm;

– to analyze the image encryption of Advanced Encryption Standard (AES);

– to analyze the image encryption of the Secure Internet of Things (SIT);

– to verify the experimental results obtainedby comparing the encryption robustness for the three techniques using the average NPCR and UACI.

4. Materials and methods

4. 1. Fibonacci Q-matrix in hyperchaotic

The security level is raised and encryption performance is enhanced by the 6D hyperchaotic system's complicated, high-dynamic characteristics. Fibonacci Q-matrix may disperse the jumbled image and is very quick and easy to use [5]. Fig. 2 depicts the encryption-decryption algorithm's flowchart.

Confusion and diffusion are the two phases that makeup encryption. Both the arrangements and values of the pixels are altered during these processes. The 6D hyperchaotic system is the foundation of the confusion step. The system's initial condition, which is based on the plain image, is first calculated. The hyperchaotic system is then iterated to produce a new vector, after which let's choose three sequences (x_1, x_3, and x_5). The order of the sorted numbers in this vector is employed to mislead the unsorted image. The diffusion process is carried out to obtain the encrypted image after confounding the plain image. The Fibonacci Q-matrix serves as the foundation for the diffusion in our algorithm. The apiece block of the scrambled image is diluted using the Fibonacci Q-matrix after being partitioned into blocks of size 2×2 each. To obtain the encrypted image, two rounds of confusion and diffusion procedures are carried out. In contrast, the steps for decryption are the opposite of those for encryption.

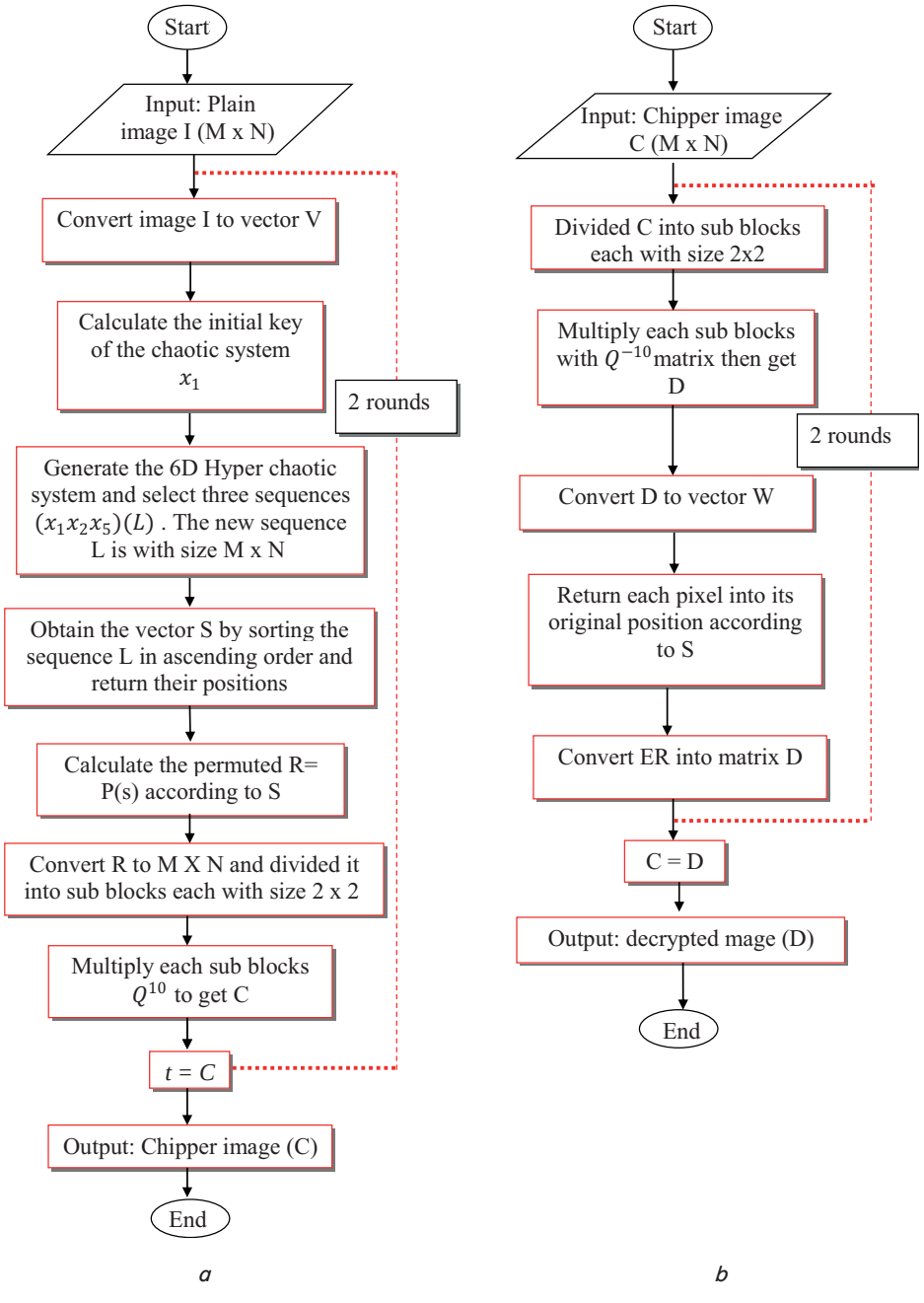


Fig. 2. Algorithm's flowchart: *a* – encryption; *b* – decryption

4. 2. Secure Internet of Things (SIT) image encryption

The SIT block cipher uses a 64-bit key and plain text to encrypt data. Each encryption round in a symmetric key scheme is based on a different set of mathematical operations designed to confuse and spread information. Better security is ensured by more rounds, but this eventually leads to more restricted energy being consumed [25]. The cryptographic methods are typically made to run between 10 and 20 times on average in order to maintain the encryption process secure enough to meet system requirements. To further increase energy efficiency, each encryption round comprises mathematical processes that work on 4 bits of data, however, in this case, only 5 rounds are taken into account.The approach makes use of the Feistel network of substitution diffusion functions to generate enough confusion and data diffusion to fend off attacks. The approach makes use of the Feistel network of substitution diffusion functions to generate enough confusion and data diffusion to fend off attacks.

For each of the five rounds, SIT uses five different 16-bit keys. With the aid of subkeys for each round, it transforms the unencrypted plain image into a protected encrypted image. At the beginning of the clock cycle, when the reset signal is high, the key data from the key memory block is put in a 64-bit register. The following two 2x1 multiplexers handle the key data in order to generate all five keys. According to the algorithm, these multiplexers are used to choose the preliminary key data from 4-bit fragments. The F-function, which is composed of two T and Sreplacement boxes performing non-linear and linear transformations as shown in Fig. 3, processes every four fragments of 16-bit data key for every clock cycle.

In four consecutive clock cycles, a multiplexer is used to pick the appropriate 16-bit matrix converted data for the four encircling key rates K4, K3, K2, and K1, but the final K5 round key is produced by a bitwise XOR operation.

4. 3. Advanced Encryption Standard image encryption

The Advanced Encryption Standard (AES) technique uses three alternative cipher key sizes with lengths of 128, 192, or 256 bits to process images with blocks of 128 bits. The algorithm goes through 10, 12, or 14 execution rounds, depending on the key dimension length that was utilized. The block size in the proposed system is 256 bits, and the key size is 128 bits. The method is used for both decrypting and encrypting images. It will require 14 cycles because the key size is 256 bits.

Image encryption is the process of converting a plain, original image into a cipher, encrypted form. The round includes the stages for image encryption shown in Fig. 1, as follows:

1) SubstituteBytes;
2) ShiftRow;
3) MixColumns;
4) AddRoundKey.

Decryption is the opposite of encryption. It refers to the transformation of a cipher image into a plain image. The round includes the next stage for picture decryption, which is depicted in Fig. 4.

The decryption image includes the stages:

1. AddRoundKey.
2. InverseShiftRow.
3. InverseSubstituteByte.
4. InverseMixColumns.

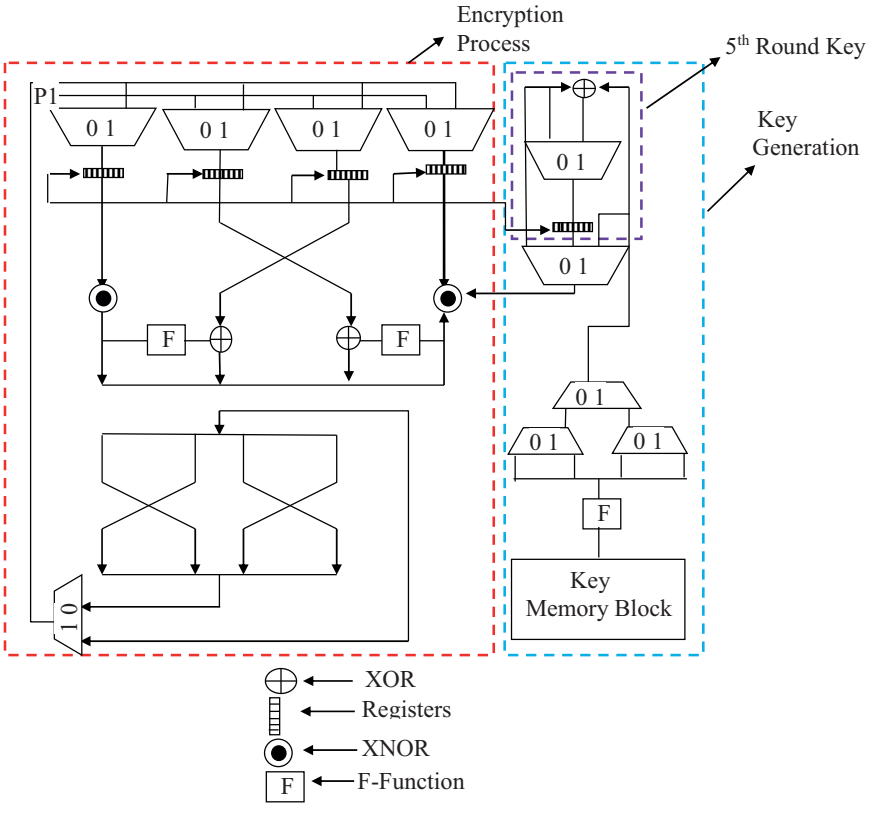


Fig. 3. Secure Internet of Things architecture

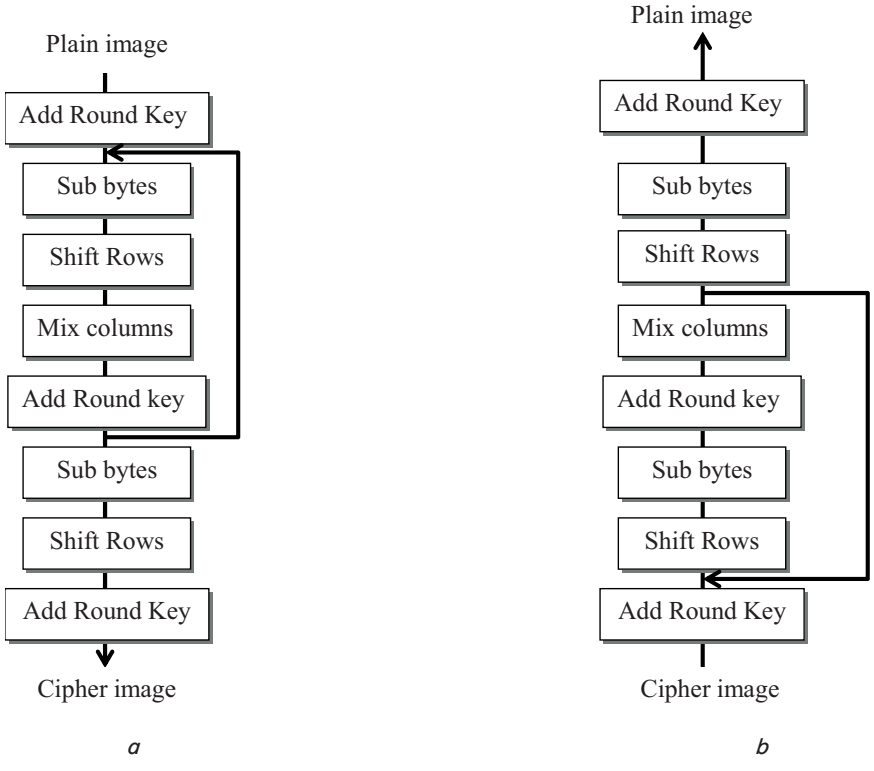


Fig. 4. Image Advanced Encryption Standard: *a* – encryption; *b* – decryption

4. 4. Evaluation parameters

The above methods are evaluated by using histograms, entropy, Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), and correlation coefficients. The efficiency of the three algorithms was evaluated using photographs of various sizes, in both color and grayscale types. The methods under consideration are also contrasted in terms of picture encryption. All experiments were carried out using MATLAB (USA-R2021a) using a laptop with a Core i5 1.6GHz CPU and 8 GB of RAM. Utilizing histograms, entropy, Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), and correlation coefficients, six tests were run to assess the presented encryption algorithm. Entropy's definition in terms of incidence probability $P(m_i)$ of the entropy $H(m)$ of an image is:

$$H(m) = \sum_{i=1}^{2^w-1} P(m_i)\log_2 \frac{1}{P(m_i)},$$

where the number 2^w denotes the total number of m_i, where the whole number of image pixels correspondsto the letter w. A perfectrate of entropy for a gray image is 8.

By figuring out the relationship between the encrypted and original photos, the attacker attempts to decrypt the encrypted images without needing the key. Small modifications in the original image's pixels have a big impact on the encrypted version, making it more challenging for hackers to decrypt the encrypted version. This assault must be thwarted by effective picture encryption methods.The robustness of this attack is based on UACI and NPCR:

$$UACI = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|C_2(i,j)-|C_1(i,j)}{255}*100\,\%,$$

$$NPCR = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N} CIF(i,j)*100\,\%,$$

$$CIF(i,j) = \begin{cases} 0, C_2(i,j) = C_1(i,j), \\ 1, C_2(i,j) \neq C_1(i,j), \end{cases}$$

where C_1 and C_2 denote the plane image and one pixel replaced the original image encrypted chipper image, respectively.

Another method to evaluate the algorithms of image encryption is to visualize the distribution of image pixels by Image Histogram. When the bar levels in the histogram approach equality, the algorithm succeeded in encrypting the image. The chi-square, which is denoted by (x^2) is a statistical hypothesis examination is calculated using the following equation to guarantee the histogram's uniform distribution:

$$x^2 = \sum_{i=1}^{Dnorm}\frac{(O_i - E_i)^2}{E_i},$$

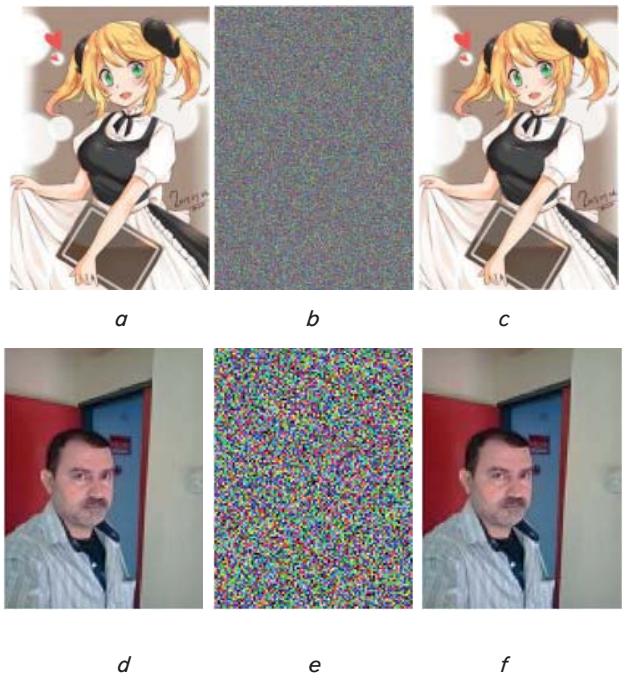
where the *Dnorm* represents thenormalized dimension of the original image,O_i denotes the grey value recurrence rate, and E_k is the estimated grey image frequency. If the value of x^2 is less than 293 the histogram of the encrypted image is regarded as uniform.

5. Results of the three image Encryption algorithms

5. 1. Fibonacci Q-matrix in hyperchaotic

The original input image, encrypted, and decrypted images for two different images in their sizes are shown in Fig. 5.

The histogram of the original and the encrypted images for the Fibonacci Q-matrix in hyperchaotic algorithm is shown in Fig. 6.



a *b* *c*

d *e* *f*

Fig. 5. Fibonacci Q-matrix in hyperchaotic algorithm: *a* – 1st original; *b* – 1st encrypted; *c* – 1st decrypted; *d* – 2nd original; *e* – 2nd encrypted; *f* – 2nd decrypted images for two different images in their sizes

The histograms of the original and the encrypted images are different and the encrypted image is of a consistent distribution, which indicates the successfulness of the applied technique.

5. 2. Advanced Encryption Standard (AES)

The original input image, encrypted, and decrypted images for two different images in their sizes are shown in Fig. 7.

a *b* *c*

d *e* *f*

Fig. 7. Advanced Encryption Standard algorithm: *a* – 1st original; *b* – 1st encrypted; *c* – 1st decrypted; *d* – 2nd original; *e* – 2nd encrypted; *f* – 2nd decrypted images for two different images in their sizes

The histogram of the original and the encrypted images for the AES algorithm is shown in Fig. 8.

The histograms of the original and the encrypted images are totally different and the encrypted image is of a consistent distribution, which indicates the successfulness of the applied technique.

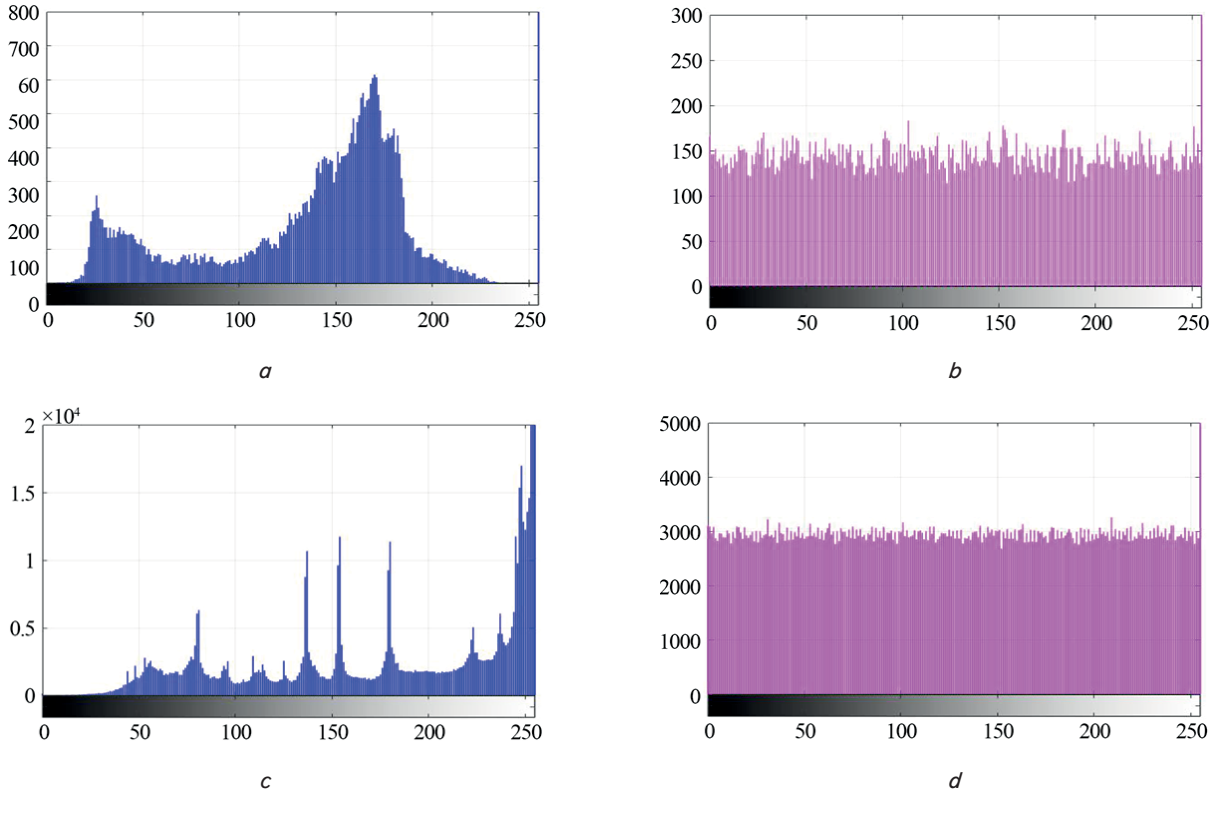


Fig. 6. The histogram for Fibonacci Q-matrix in hyperchaotic algorithm: *a* – 1st original; *b* – 1st encrypted; *c* – 2nd original; *d* – 2nd encrypted images

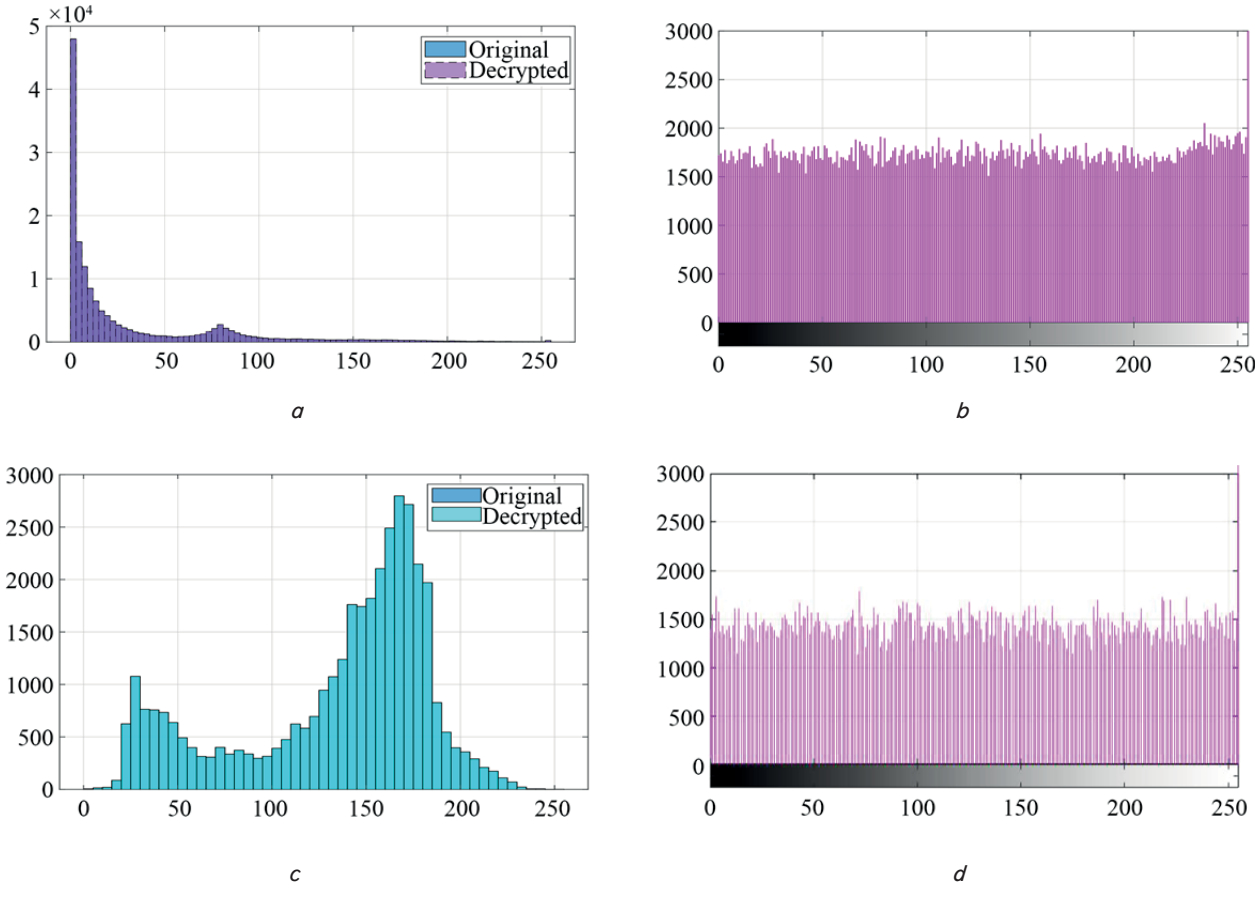


Fig. 8. The histogram for Advanced Encryption Standard algorithm: *a* – 1st original; *b* – 1st encrypted; *c* – 2nd original; *d* – 2nd encrypted images

5. 3. Secure Internet of Things (SIT)

The original input image, encrypted, and decrypted images for two different images in their sizes are shown in Fig. 9.

The histogram of the original and the encrypted images for the Secure Internet of Things algorithm is shown in Fig. 10.

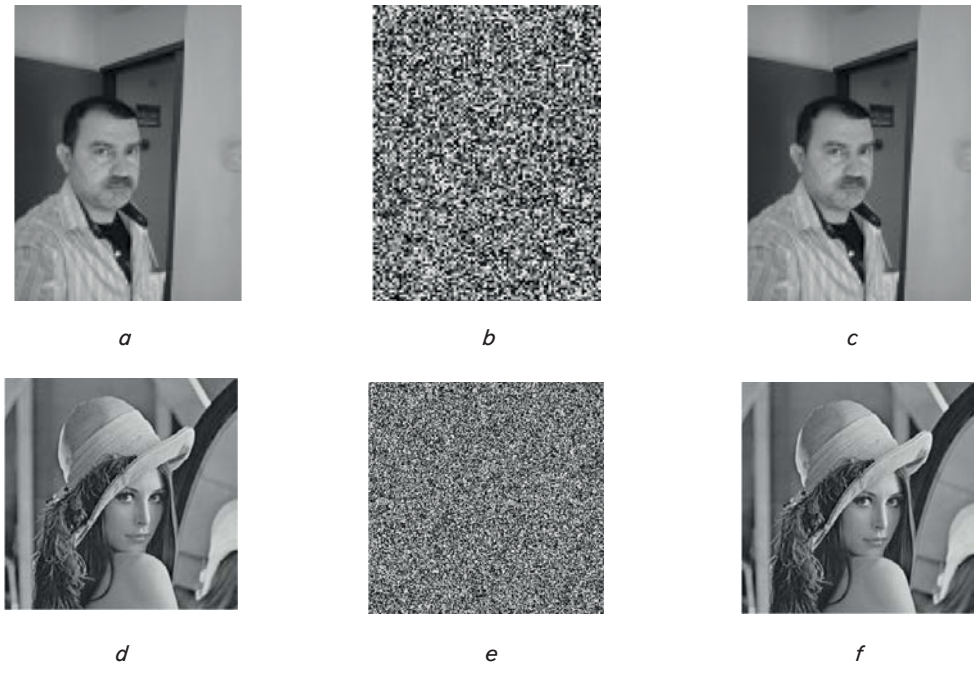


Fig. 9. Secure Internet of Things algorithm: *a* – 1st original; *b* – 1st encrypted; *c* – 1st decrypted; *d* – 2nd original; *e* – 2nd encrypted; *f* – 2nd decrypted images for two different images in their sizes

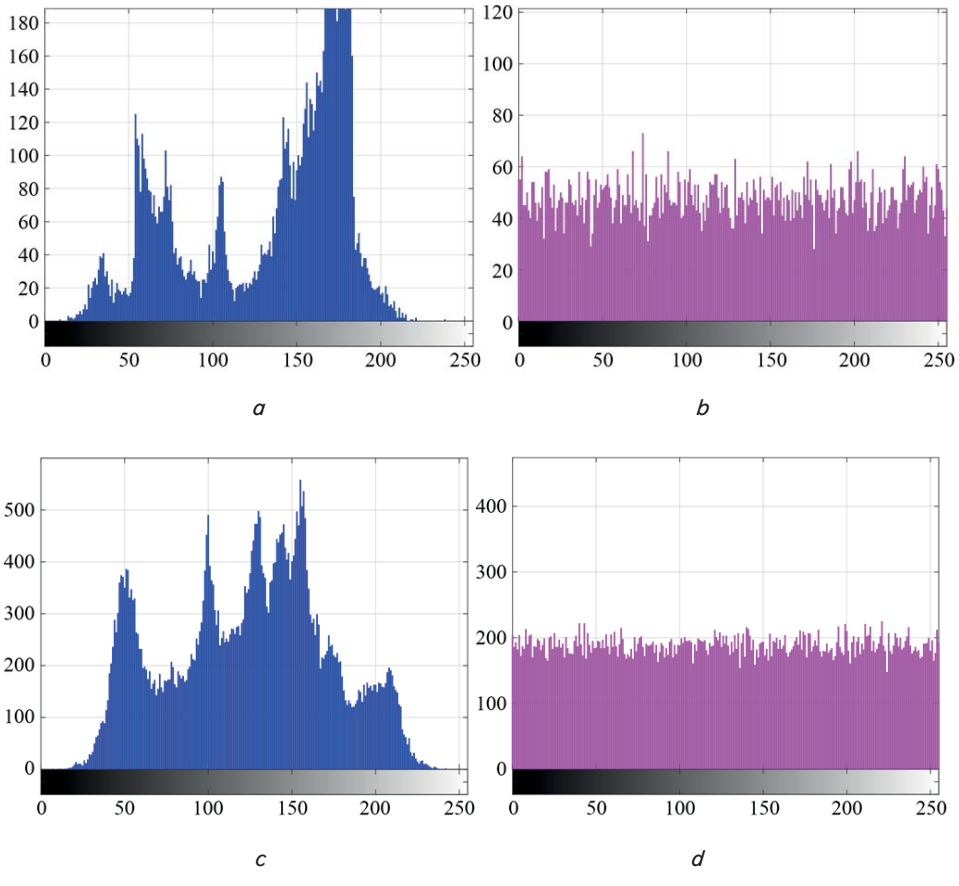


Fig. 10. The histogram for Secure Internet of Things algorithm: *a* – 1st original; *b* – 1st encrypted; *c* – 2nd original; *d* – 2nd encrypted images

The histograms of the original and the encrypted images are totally different and the encrypted image is of a consistent distribution, which indicates the successfulness of the applied technique.

5. 4. Comparison of the techniques

The evaluation factors for the three considered algorithms applied to two different images each are listed in Table 1.

The image values of UACI and NPCR confirm that the image encryption using Fibonacci Q-matrix in hyperchaotic algorithm performed better as compared with both the AES and SIT.

6. Discussion of the results of Evaluating the three image Encryption algorithms

The original input image, encrypted, and decrypted images for two different images in their sizes for the Fibonacci Q-matrix in hyperchaotic, Secure Internet of Things (SIT), and AES were shown in Fig. 5, 7, 9 respectively. In contrast, the corresponding histograms were shown in Fig. 6, 8, 10 respectively.

All the histograms of the original and the encrypted images are totally different and the encrypted image is of a consistent distribution, which ensures the effectiveness of these algorithms. Since the number in the last row of Table 1 is less than (293) for the Fibonacci Q-matrix in hyperchaotic method, this indicates that the histograms of the encrypted images produced by this technique have a uniform distribution and is the more efficient. This was also approved in the UACI and NPCR values.

Therefore, this work successfully compared and evaluated the existing image encryption algorithms including Hyperchaotic and Fibonacci Q-matrix, Secure Internet of Things (SIT), and AES to select the appropriate one for image protection.

Although Fibonacci Q-matrix in hyperchaotic algorithm was able to perform image encryption with high-security levels, the limitation of this method is that it was implemented only on gray images. Therefore, the effectiveness of applying this algorithm to encrypt color images is suggested for future work.

Table 1

Evaluation factors for the three considered methods

Description	Hyperchaotic System & Fibonacci Q-matrix		AES		SIT	
	1st image	2nd image	1st image	2nd image	1st image	2nd image
Re	7.0728 7.9830	7.4618 7.9963	4.1528 4.6630	4.2318 4.6399	2.0087 2.1316	4.5624 5.6388
NPCR	99.6826	99.6343	33.6826	33.6343	6.0457	19.4253
UACI	13.1459	15.0485	3.1459	5.0485	0.6595	0.9719
Total encryption time:	7.239820	30.254315	9.99820	34.4315	17.69820	52.72515
the correlation coefficient of the original image	[1.0; 0.9632, 0.9632; 1.0]	[1.0; 0.9611, 0.9611; 1.0]	[1.0; 0.9770, 0.9770; 1.0]	[1.0; 0.9763, 0.9763; 1.0]	[1.0; 0.9880, 0.98; 1.0]	[1.0; 0.9653, 0.963; 1.0]
the correlation coefficient of the encrypted image	[1.0; –0.0013, –0.0013; 1.0]	[1.0; 0.0021, 0.0021; 1.0]	[1.0; –0.0023, –0.0023; 1.0]	[1.0; 0.0032, 0.0032; 1.0]	[1.0; 0.7044, 0.7044; 1.0]	[1.0; 0.5503, 0.5503; 1.0]
chi-square	274.667	245.237	298.224	321.874	321.654	402.993

7. Conclusions

1. This work analyzed the image encryption of the Fibonacci Q-matrix in hyperchaotic algorithm. The encrypted image is of a consistent distribution, which indicates the successfulness of the applied technique.

2. The work analyzed the image encryption of Advanced Encryption Standard (AES). The histogram of the original and the encrypted images for the AES algorithm also succeeded but with lower performance than Fibonacci Q-matrix in hyperchaotic algorithm.

3. The application of image encryption for the Secure Internet of Things (SIT) was performed with all the evaluation parameters. The histogram of the original and the encrypted images for the SIT indicates the successfulness of the applied technique, but with lower performance than Fibonacci Q-matrix in hyperchaotic algorithm.

4. The comparison of the encryption robustness for the three techniques that were evaluated indicates that the histograms of the encrypted images produced by this technique have a uniform distribution and is the more efficient.

Conflict of interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Acknowledgments

The authors acknowledge the AL- Furat Al-Awsat Technical University, Iraq for their support and assistance.

References

1. Saddam, M. J., Ibrahim, A. A., Mohammed, A. H. (2020). A Lightweight Image Encryption And Blowfish Decryption For The Secure Internet Of Things. 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT). doi: https://doi.org/10.1109/ismsit50672.2020.9254366
2. Mishra, Z., Acharya, B. (2020). High throughput and low area architectures of secure IoT algorithm for medical image encryption. Journal of Information Security and Applications, 53, 102533. doi: https://doi.org/10.1016/j.jisa.2020.102533
3. Rabab, U. e, Ahmed, I., Aslam, M. I., Usman, M. (2018). FPGA Implementation of Secure Internet of Things (SIT) Algorithm for High Throughput Area Ratio. International Journal of Future Generation Communication and Networking, 11 (5), 63–72. doi: https://doi.org/10.14257/ijfgcn.2018.11.5.06
4. Usman, M., Ahmed, I., Imran, M., Khan, S., Ali, U. (2017). SIT: A Lightweight Encryption Algorithm for Secure Internet of Things. International Journal of Advanced Computer Science and Applications, 8 (1). doi: https://doi.org/10.14569/ijacsa.2017.080151
5. Hosny, K. M., Kamal, S. T., Darwish, M. M., Papakostas, G. A. (2021). New Image Encryption Algorithm Using Hyperchaotic System and Fibonacci Q-Matrix. Electronics, 10 (9), 1066. doi: https://doi.org/10.3390/electronics10091066
6. Hosny, K. M., Kamal, S. T., Darwish, M. M. (2022). Novel encryption for color images using fractional-order hyperchaotic system. Journal of Ambient Intelligence and Humanized Computing, 13 (2), 973–988. doi: https://doi.org/10.1007/s12652-021-03675-y
7. Padole, M. (2013). Distributed computing for structured storage, retrieval and processing of DNA sequencing data. International Journal ofInternet and Web Technology, 38, 1113–1118.
8. Tanougast, C., Dandache, A., Salah, M., Sadoudi, S. (2012). Hardware Design of Embedded Systems for Security Applications. Embedded Systems – High Performance Systems, Applications and Projects. doi: https://doi.org/10.5772/38649
9. Gamido, H. V., Sison, A. M., Medina, R. P. (2018). Implementation of Modified AES as Image Encryption Scheme. Indonesian Journal of Electrical Engineering and Informatics (IJEEI), 6 (3). doi: https://doi.org/10.11591/ijeei.v6i3.490
10. Zhang, Y. (2018). Test and Verification of AES Used for Image Encryption. 3D Research, 9 (1). doi: https://doi.org/10.1007/s13319-017-0154-7
11. Shariatzadeh, M., Rostami, M. J., Eftekhari, M. (2021). Proposing a novel Dynamic AES for image encryption using a chaotic map key management approach. Optik, 246, 167779. doi: https://doi.org/10.1016/j.ijleo.2021.167779
12. Gaur, P. (2021). AES Image Encryption (Advanced Encryption Standard). International Journal for Research in Applied Science and Engineering Technology, 9 (12), 1357–1363. doi: https://doi.org/10.22214/ijraset.2021.39542
13. Vijayakumar, P., Chittoju, C. K., Bharadwaja, A. V., Tayade, P. P., Tamilselvi, M., Rajashree, R., Gao, X. Z. (2019). FPGA implementation of AES for image encryption and decryption. International Journal of Innovative Technology and Exploring Engineering, 8 (7), 807–812.
14. Gamido, H. V., Sison, A. M., Medina, R. P. (2018). Modified AES for Text and Image Encryption. Indonesian Journal of Electrical Engineering and Computer Science, 11 (3), 942. doi: https://doi.org/10.11591/ijeecs.v11.i3.pp942-948
15. Mohammed, A. B., Al-Mafrji, A. A. M., Yassen, M. S., Sabry, A. H. (2022). Developing plastic recycling classifier by deep learning and directed acyclic graph residual network. Eastern-European Journal of Enterprise Technologies, 2 (10 (116)), 42–49. doi: https://doi.org/10.15587/1729-4061.2022.254285
16. Kaur, M., Singh, S., Kaur, M. (2021). Computational Image Encryption Techniques: A Comprehensive Review. Mathematical Problems in Engineering, 2021, 1–17. doi: https://doi.org/10.1155/2021/5012496
17. Zhang, X., Wang, L., Wang, Y., Niu, Y., Li, Y. (2020). An Image Encryption Algorithm Based on Hyperchaotic System and Variable-Step Josephus Problem. International Journal of Optics, 2020, 1–15. doi: https://doi.org/10.1155/2020/6102824

18. Naim, M., Ali Pacha, A., Serief, C. (2021). A novel satellite image encryption algorithm based on hyperchaotic systems and Josephus problem. Advances in Space Research, 67 (7), 2077–2103. doi: https://doi.org/10.1016/j.asr.2021.01.018
19. Wang, X., Su, Y., Luo, C., Nian, F., Teng, L. (2022). Color image encryption algorithm based on hyperchaotic system and improved quantum revolving gate. Multimedia Tools and Applications, 81 (10), 13845–13865. doi: https://doi.org/10.1007/s11042-022-12220-8
20. Naim, M., Ali Pacha, A. (2021). New chaotic satellite image encryption by using some or all the rounds of the AES algorithm. Information Security Journal: A Global Perspective, 1–25. doi: https://doi.org/10.1080/19393555.2021.1982082
21. Han, F., Liao, X., Yang, B., Zhang, Y. (2017). A hybrid scheme for self-adaptive double color-image encryption. Multimedia Tools and Applications, 77 (11), 14285–14304. doi: https://doi.org/10.1007/s11042-017-5029-7
22. Zhang, T., Li, S., Ge, R., Yuan, M., Ma, Y. (2016). A Novel 1D Hybrid Chaotic Map-Based Image Compression and Encryption Using Compressed Sensing and Fibonacci-Lucas Transform. Mathematical Problems in Engineering, 2016, 1–15. doi: https://doi.org/10.1155/2016/7683687
23. Pan, C., Ye, G., Huang, X., Zhou, J. (2019). Novel Meaningful Image Encryption Based on Block Compressive Sensing. Security and Communication Networks, 2019, 1–12. doi: https://doi.org/10.1155/2019/6572105
24. Sun, S., Guo, Y., Wu, R. (2019). A Novel Image Encryption Scheme Based on 7D Hyperchaotic System and Row-column Simultaneous Swapping. IEEE Access, 7, 28539–28547. doi: https://doi.org/10.1109/access.2019.2901870
25. Chandramouli, R., Bapatla, S., Subbalakshmi, K. P., Uma, R. N. (2006). Battery power-aware encryption. ACM Transactions on Information and System Security, 9 (2), 162–180. doi: https://doi.org/10.1145/1151414.1151417