Iraqi Journal of Intelligent Computing and Informatics (IJICI)
Vol. 2, 1, December 2024, pp. 22~29
ISSN: 2791-2868, DOI: 10.52940/ijici.v3i1.88

A Study on Secure Image Encryption Based on Blockchain

Batool Arif Salim[*1,2,5], Hameed Abdulkareem Younis[1,3,6], Maalim A. Aljabery[1,4,7]
[1]Department of Computer Science, Basra University, Basra, Iraq
[2]https://orcid.org/0009-0004-9037-9110, [3]https://orcid.org/0000-0003-4580-9287, [4]https://orcid.org/0000-0002-6133-494X
[5]batool98almayahi@gmail.com,[6]hameed.younis@uobasrah.edu.iq,[7]maalim.aljabery@uobasrah.edu.iq q

Article Info

Article history:

Received October, 2, 2024
Revised December, 27, 2024
Accepted December, 31, 2024

Keywords:

Blockchain Technology
Entropy
Hash Function
Histogram
Image Encryption

ABSTRACT

Over recent decades, image data violations have created great difficulties, and image encryption has been an appealing field of research. Most people acknowledge this as a practical method of safe transmission. However, many studies have been conducted in various ways, and new and helpful algorithms have been proposed to improve the encryption systems of safe images. To increase this security, blockchain technology used by this technology eliminates or reduces the role of the third party by enabling two parties to transact with each other means that the Blockchain system can function in a peer-to-peer manner without a reliable third party required to ensure trust. This technology was first adopted to create digital cryptocurrencies, like Bitcoin and Ethereum. This technology has a range of characteristics, including transparency, anonymity, decentralization, immutability, and minting. With the advancement of Internet and communications, the exchange of sensitive data across multiple parties has become very easy. However, the problems associated with such communications are lack of integrity, confidentiality, and authenticity etc, caused by insecure channels. This paper aims to review recent key studies on secure image encryption based on blockchain in addition, explore how these two technologies can be combined to solve the problem of transport between unsafe channels where the blockchain network ensures that any tampering in the image will lead to the detection as any transaction in the blockchain tampers the associated hash. In addition, we comprehensively examine the key concepts and the most important metrics used to evaluate the model's performance and discussion of future work.

Corresponding Author:

Batool Arif Salim
Department of Computer Science, Basra University, Basra, Iraq
Email: batool98almayahi@gmail.com

1. INTRODUCTION

Image encryption has become a popular field of study in recent years. It is widely acknowledged as a practical, secure transmission method. Creating a high-quality noisy image is the goal of every image encryption algorithm to keep information secret [1]. Two types of encryption techniques exist generally: symmetric and asymmetric [2]. Symmetric key encryption encrypts and decrypts data using the same key for both the sender and the recipient [3]. Two types of symmetric encryption algorithms exist streaming and block codes. In the streaming code, every encrypted bit is encrypted independently by supplementing a bit of the stream key with a plain text bit, such as the RC4. However, using the same keys, a block of bits is simultaneously encrypted, which stands for block codes. Certain block codes, such as Data Encryption Standard (DES), utilize the Feistel network, whereas others, such as the Advanced Encryption System (AES), do not use [4]. Different keys are used in asymmetric key encryption, also called public key encryption, where the decryption method utilizes the private key, and the encryption method utilizes the public key. The private key is only accessible to approved individuals, whereas the public key is accessible to everyone as its name suggests, such as the Rivest–Shamir–Adleman (RSA) [3]. As shown in Figure 1, blockchain technology is used to enhance security, authentication, and data integrity by encrypting images.

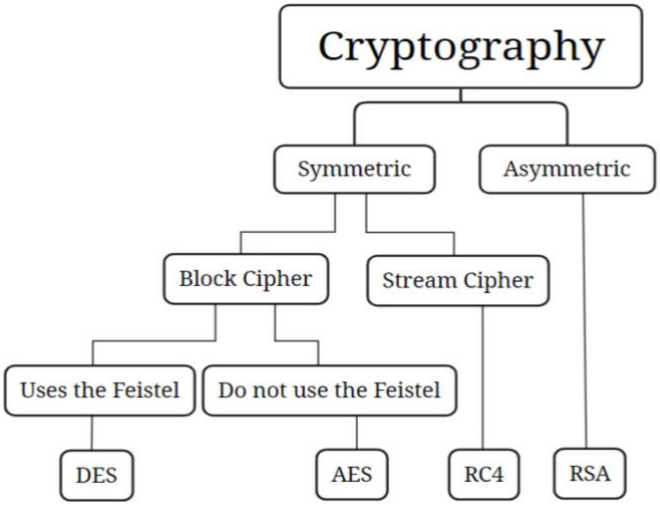

Figure 1. Cryptography types

1.1. Overview of blockchain technology

The first description of blockchain technology dates back to 1991, and it uses hash functions to verify the authenticity of digital documents [5]. With its various practical applications, such as Bitcoin, IoT security, food safety, healthcare, and many more, Blockchain has become a revolutionary technology since the groundbreaking work of S. Nakamoto in 2008 [6]. Figure 2 shows a simplified structure of blockchain [7].

Blockchain is a dispensed open ledger that registers transactions between parties efficiently in a permanent manner and verifiable [8]. The data is stored, and once saved, the information is unchangeable and kept in the form of an incrementally growing chain. To guarantee data integrity and stop data manipulation, using a cryptographic hash function, every block of data is linked to the before one [9]. Because every block is created with timestamp and hashing, this link continues all the way modified. Each block owns a distinct hash value, and each block is copy for all of the users connected to the network [10]. Although it is a one-way code generated from the sender's side and cannot secure the file or the data within it, the hash value is an essential component of the blockchain. The hash code produced by the hash function is not utilized for encryption or security reasons; it is solely used for authentication [11]. By converting the input of numbers and letters into an encrypted output of a fixed length using a mathematical function or algorithm, a hash is produced [12]. Blockchain technology in general is categorized into three primary types according to their usage and feature characteristics:

- **Public Blockchains:** Blocks containing all transaction details are stored in an open distributed ledger called a public blockchain. The data included within each block is accessible to the public and is not readily removed or altered e.g., Bitcoin and Ethereum [13]. In a permissionless or public blockchain, system users do not need permission to participate within a network. Complicated consensus processes like stacking one's own or puzzle-solving coinage are used to verify these blocks [14].
- **Private Blockchains:** Only authorized users can access a private blockchain, which access is limited given "by invitation only" [5], which are created especially for certain companies. The administrator can configure both endorser and non-endorser peers in this system network. In contrast to public blockchains, where consensus-building takes time, only a small number of nodes are authorized in this instance [2]. Some well-known private blockchains are Corda, Hyperledger Projects, Multichain, etc. [15].
- **Consortium Blockchains:** Also known as hybrid blockchains, are a combination of public and private blockchains. Semiprivate and semi-decentralized structures characterize this blockchain. The hybrid network supports features found in both private and public blockchains. Although it operates across various organizations, it has a restricted user group [16]. These networks, often called semiprivate networks, contain both a public and a private portion of the blockchain. While the public portion is accessible to everyone, the private portion is managed by a select group of people [17]. R3, Energy Web Foundation, and others are a few instances of this kind of blockchain [15]. The types of blockchains are shown in Figure 3.

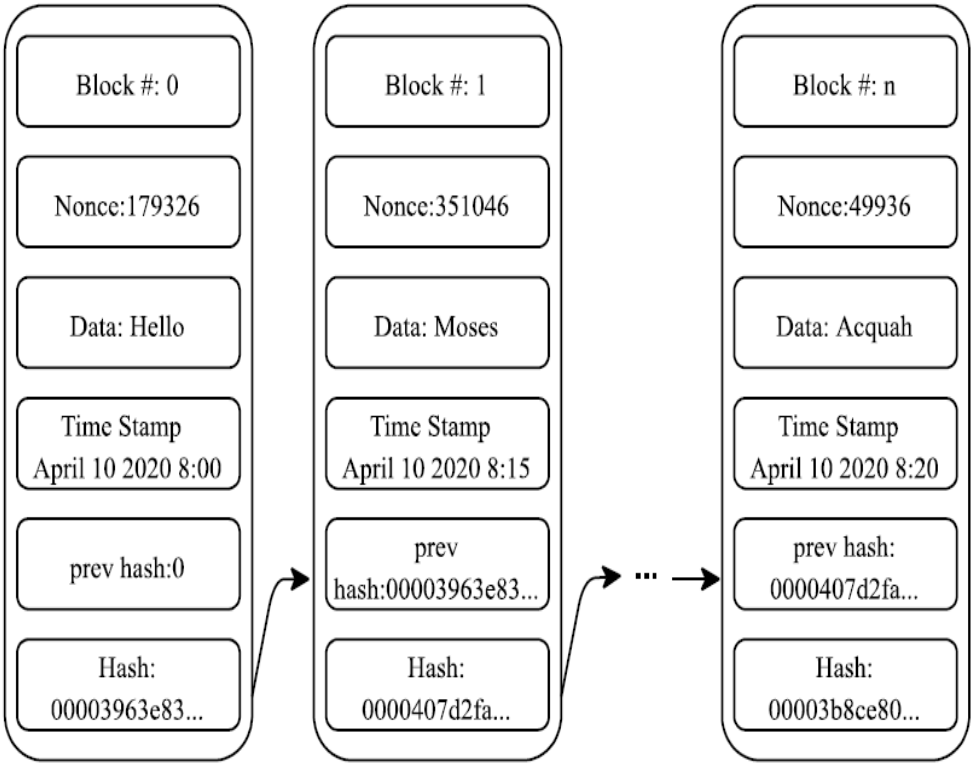

Figure 2. Simplified structure of blockchain

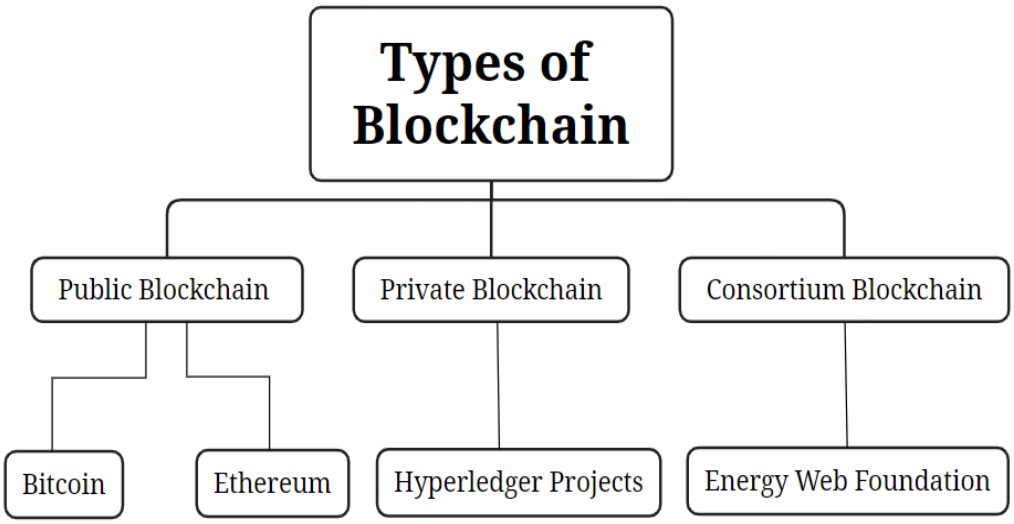

Figure 3. Types of blockchain

2. RELATED WORKS

P. W. Khan and Y. Byun [2]. They suggest a permission private blockchain-based method for protecting the image while encrypting it in the context of the IIoT. The cryptographic pixel values of an image are kept on the blockchain in this approach. This keeps the image data private and safe. Based on the results obtained, the unified averaged changed intensity (UACI) is 33.4187%, the entropy value is 7.9978 bits, and 99.6023% is the number of pixels change rate (NPCR). The encrypted results demonstrate that the proposed method is highly effective in securing data and preventing leaks.

A. S. Jamil and A. M. S. Rahma [4]. It is suggested that blockchain technology be used in conjunction with the Data Encryption Standard (DES) algorithm to increase the level of authentication between sender and recipient and to enhance the security of sent images by improving the key during the encryption process. Based on the outcomes of using the suggested model to encode images, it was discovered that the entropy value was 7.988 bits, it is the highest value if compared to the previous values produced using the conventional technique and has a high degree of accuracy.

E. Borandag [10]. To lessen the carbon imprint, recyclables must be sorted and collected properly. Recycle Chain, a blockchain-based platform, had been created within this context to track recyclables. A new dataset of 4000 images was constructed and named Recycle Chain DS to identify recycling objects. This dataset was used to train the artificial intelligence software developed using deep learning. A proper object recognition success rate of 98.2% was attained in the laboratory trials.

M. Y. Jabarulla and H. N. Lee [13]. They offer a unique dispensed patient-centric image management (PCIM) system to maintain patient privacy and safety without relying on a centralized infrastructure. They used the Inter-Planetary File System (IPFS), a technology for distributed file systems, with the newly developed Ethereum blockchain in this system. The evaluation's findings proved that the suggested plan is workable and effective.

R. Bhaskaran et al [18]. Presents a new safe blockchain-enabled optimal lightweight cryptography-based image encryption (BC-LWCIE) strategy in the context of Industry 4.0. Constructing an ideal LWC-based hash value with optimal key generation using the chicken swarm optimization (CSO) algorithm is another aspect of the BC-LWCIE technique. To maintain confidentiality in the Industrial Internet of Things (IIoT) context, the BC-LWCIE approach retains the encrypted image's cryptology pixel values in Blockchain Technology (BCT). NPCR is 99.570% based on the results collected.

B. Li et al [19]. Rather than having miners calculate pointless hash values, they suggest a system that takes advantage of the computation blockchain miners' power for segmenting images in biomedicine. This enables miners to segment the images as part of the Proof-of-Useful-Work (PoUW) mechanism, addressing several shortcomings of other related approaches, this study sets itself apart from other PoUW.

X. Xiao et al [20]. Creates, utilizing Hyperledger Fabric, a blockchain-based reliable image copyright protection system called (BB-RICP). Adopting Fabric, for example, lessens the efficiency, economics, and availability constraints of existing blockchain platforms, as embodied by Ethereum. BB-RICP has achieved integrated copyright lifecycle management, which is another achievement. Finally, Kubernetes helps simulate BB-RICP to confirm such users can function dependably within a blockchain network.

B. Liu et al [21]. Suggests a blockchain-based secure exchange and distributing system of X-ray medical image data, which may be processed for additional scientific research. The standard cloud-based image data management solution is compromised by security issues that are resolved by the scheme presented in this research. The results show that the mean classical 46.7 dB is peak signal-to-noise ratio (PSNR).

S. Inam et al [22]. Because cloud storage solutions are open, they can be subject to various security risks. Consequently, this study proposes the Blockchain-based Chaotic Arnold's cat map Encryption scheme (BCAES). Using Arnold's cat map encryption algorithm, BCAES first encrypts the image. It then transfers the encrypted image to a cloud server and saves the endorsed plain image document in a blockchain. Numerous analytical methods have been employed to scrutinize the suggested plan.

J. H. Horng et al [23]. They proposed a reversible data hiding in encrypted images (RDHEI) approach to embed private information into the medical images. In this approach, the stream cipher was used to create additional space for data embedding. A hash value generated from the RDHEI output is stored in the blockchain. In this innovative blockchain-based RDHEI system, ciphered steganographic medical images (CSMIs) can be securely shared by users with other participants in the blockchain network.

M. Acharya and R. S. Sharma [24]. This paper suggests an image encryption method based on Feedback Carry Shift Register (FCSR) and blockchain technology. In the proposed solution the image is encrypted, and its values are kept on the blockchain. The FCSR ensures image information security, and blockchain ensures privacy and security in transit because it uses symmetric and asymmetric encryption, enhancing the overall security of the data.

A summary of the previously studied related works is provided in Table 1. Considering the related works, we observed that private blockchains are the most commonly used type, specifically designed for certain organizations, along with Ethereum, which is one application of public blockchain. Blockchain is used to store the image-encrypted pixel values as in [2], [18], and [24]. It can also be used to store the signed document for the original image as in [22]. For the hash function, SHA-256 was the most commonly used hash where it was used in [2], [19], [20], [22], and [24]. It should be noted that SHA-3 also gained interest and adoption in some blockchain projects as an alternative to enhancing security. Where it is directed to be used in [10] and [23].

For the type of images used in this research. The benchmark images were used in [18], and [23]. Also, the medical images are used in [4], [13], [22], and [23]. And about the type of consensus mechanism used Proof-of-Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and others.

Table 1: A summary of related works

Ref.	Year	Algorithm	Type or Application of Blockchain	Hash Function	Type of Image	Consensus Mechanism
[19]	2019	×	×	SHA 256	Biomedical image	Proof-of-Useful-Work (PoUW)
[2]	2020	×	Private blockchain	SHA 256	Grayscale images	×
[21]	2020	Hash algorithm	×	×	X-Ray medical image	×
[13]	2021	OpenPGP (Pretty Good Privacy) protocol	Ethereum	×	Medical images	Proof-of-Concept (POC)
[23]	2021	Symmetric key algorithm, stream ciphering	Consortium blockchain	SHA-2 and SHA-3	Benchmark images, Medical gray images	Practical Byzantine Fault Tolerance (PBZT)
[24]	2021	Feedback Carry Shift Register (FCSR)	Permissioned blockchain	SHA 256	Grayscale images	Proof-of-Work (PoW)
[18]	2022	LWC-hash function	Private blockchain	×	Benchmark images	×
[4]	2023	Data Encryption Standard (DES)	Circular blockchain technology	×	Medical images	×
[10]	2023	Deep learning Convolutional Neural Network (CNN)	Ethereum	SHA-3	Camera image	Proof-of-Stake (PoS)
[20]	2023	GM algorithms, specifically SM2, SM3, and SM4	Hyperledger Fabric	SHA 256	Watermarked images	Practical Byzantine Fault Tolerance (PBFT)
[22]	2024	Henon map, Arnold's cat map, and orthogonal matrices	Ethereum	SHA 256	Medical images	×

Table 2 (A, B) shows the results. For the research [2] four grey images were used and entropy, NPCR, UACI, and correlation coefficient metrics were used to evaluate their encryption strength. In [4] three grey samples were used and entropy, MSE, and PSNR were used for evaluation [18]. Color and grey images were used with NPCR, MSE, and PSNR for an evaluation. In [22] five color images were used and entropy, NPCR, UACI, MSE, PSNR, and correlation coefficient were used to evaluate their encryption. Finally, in the research [24] four grey images were used and entropy, NPCR, UACI, and correlation coefficient metrics were used to evaluate their encryption strength.

Table 2-A: A summary result of related works

Ref.	Color of image	Images	Entropy (bits)	NPCR (%)	UACI (%)	MSE (dB)	PSNR (dB)
[2]	gray	Cameraman Lena Man Truck	7.9972 7.9978	99.6023	33.4187		
[4]	gray	Sample a Sample b Sample c	7.933 7.965 7.988			104.345 103.987 103.675	27.880 27.870 27.890
[18]	color gray	Airplane Baboon Barbara Cameraman House Lena		99.340 99.230 97.260 99.470 96.890 99.570		0.053 1.475 0.256 0.019 0.126 0.027	60.89 46.44 54.05 65.34 57.13 63.82
[22]	color	Image (1) Image (2) Image (3) Image (4) Image (5)	7.9992 7.9991 7.9992 7.9992 7.9992	99.63	33.21	14051.56	6.65
[24]	gray	Lena Cameraman Peppers Baboon	7.9986	99.69	33.45		

Table 2-B: A summary result of related works

Ref.	Image	Correlation Coefficient				
		Type of Image	Color of image	Horizontal	Vertical	Diagonal
[2]	Cameraman	Original image		0.944198	0.961276	0.899276
		Encrypted image		-0.042225	0.036725	-0.058265
[22]		Original image	Blue Green Red	0.9776 0.9668 0.9597	0.9759 0.9688 0.9711	0.9568 0.9402 0.9365
		Encrypted image	Blue Green Red	0.00007 0.0036 0.0009	0.0044 -0.0006 0.0064	-0.0019 -0.0030 -0.0027
[24]	Lena	Encrypted image		0.0033	0.0025	-0.0041

3. PERFORMANCE EVALUATION METRICS

A strong encryption algorithm in the context of image encryption must possess these characteristics: after encryption, the ciphertext image's histogram is more average, has good information entropy, low ciphertext correlation, can withstand differentiating attacks [25]. Researchers who evaluated the effectiveness of encryption used different metrics. Here are the details of each metric:

3.1. Histogram analysis

The image histogram holds significant importance in image analysis. The frequency distribution of a perfect cipher image should be uniform. If histograms of an encrypted image are uniform and random-like, it can be inferred that the recommended method lacks any useful statistical information about an encrypted image [26].

3.2. Entropy analysis

Entropy determines the image uniformity by quantifying image randomness [27]. It is an important test for examining information randomness. Equation (1) can be applied to compute entropy, a degree of doubt in communication systems. p (I_n) represents the probability of (I_n), and I denotes for the image [2].

$$E(I) = \sum_{n=1}^{256} p(I_n)\, log_2\, p(I_n) \qquad (1)$$

3.3. Differential attack

To find out if the suggested encryption method can protect against differential attacks. The number of pixels changing rate (NPCR) and the unified average changing intensity (UACI) are two important evaluation factors for differential attack analysis [28].

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \qquad (2)$$

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \qquad (3)$$

where M and N are the height and width of the image, respectively. $D(i.\ j)$ = 0 when it is the same value in C_1 and C_2, while it is 1 when it is different. $C_1(i, j)$ and $C_2(i, j)$ represent Original and encrypted images.

3.4. Correlation coefficient analysis

The original image owns many redundant pixel values and strongly correlates with neighboring pixels. Yet, the correlation between neighboring pixels should drastically drop once the image has been encrypted. Consequently, when the correlation value approaches 0, the redundancy decreases. If the correlation value remains high or is extremely near 1, it indicates that the encryption operation was unsuccessful [29].

3.5. Pixel difference analysis

One way to compare encrypted and unencrypted image data is with pixel difference analysis. The difference between the pixels of plain and encrypted images is measured using two parameters. First is the Mean Square Error (MSE), and the second is the Peak Signal Noise Ratio (PSNR) [30]. MSE is expressed by the following equation [31]. PSNR is expressed by the following equation [32].

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[P_{mg}(i,j) - C_{mg}(i,j)]^2 \quad (4)$$

Here, P_{mg} shows the input image. C_{mg} shows the encrypted image. (i, j) denotes pixel coordinates. m and n show the size of the input image.

$$PSNR = 10.log_{10}\frac{(peakval)^2}{MSE} \quad (5)$$

Here, the peakval (Peak Value) is the maximum in the image data. If it is an 8-bit unsigned integer data type, the peakval is 255.

4. FUTURE WORKS

For future work that aims to provide a secure and tamper-proof way to protect images, we plan to accomplish this by using the combination of image encryption algorithms and Blockchain technology. For hash function and blockchain technology, we will use SHA-256 which is commonly used in blockchain technology in addition to SHA-3 because it is rare and hopefully gives us better results. So, we will use the private blockchain for blockchain. In existing solutions, the main trend is to encrypt the image, divide it into parts, and store these parts in the blockchain. Confidentiality is maintained by encrypting AES, while authenticity is ensured by storing each encrypted block in the blockchain with an associated hash.

5. CONCLUSION

In this paper, we highlighted recent studies related to the integration of image encryption and blockchain technology. Blockchain technology can achieve authentication between sender and receiver using the hash function. Every new block's hash value is relied on the prior block. To modify a single record in the blockchain, it is necessary to recompute all subsequent blocks, which is nearly impossible. This technology creates a chain of immutable blocks, a fundamental aspect of blockchain that ensures data remains permanent and unchangeable, thereby protecting it from corruption. Private blockchains emerged as the most commonly used type specifically designed for certain organizations. Fast transaction speeds characterize this type, as only a limited number of nodes have permission to validate transactions, ensuring that the data remains private and protects users' privacy. In a permissionless or public blockchain, system users do not need permission to participate within a network. The hybrid blockchain supports features found in both private and public blockchains. Although it operates across various organizations, it has a restricted user group. From this research, we also deduced the types of metrics most used to measure the cryptographic power of the image including NPCR and UACI used to examine whether the suggested encryption algorithm can resist differential attacks, and entropy analysis is considered an important test for analysis randomness of information. In addition, it provides insights into possible future works to enhance security and efficiency.

REFERENCES

[1] Y. Pourasad, R. Ranjbarzadeh, and A. Mardani, "A New Algorithm for Digital Image Encryption based on Chaos Theory," *Entropy*, vol. 23, no. 3, pp. 1–16, 2021, doi: 10.3390/e23030341.

[2] P. W. Khan and Y. Byun, "A Blockchain-based Secure Image Encryption Scheme for the Industrial Internet of Things," *Entropy*, vol. 22, no. 2, pp. 1–26, 2020, doi: 10.3390/e22020175.

[3] A. K. Bermani, T. A. K. Murshedi, and Z. A. Abod, "A hybrid cryptography technique for data storage on cloud computing," *J. Discret. Math. Sci. Cryptogr.*, vol. 24, no. 6, pp. 1613–1624, 2021, doi: 10.1080/09720529.2020.1859799.

[4] A. S. Jamil and A. M. S. Rahma, "Cyber Security for Medical Image Encryption Using Circular Blockchain

Technology based on Modify DES Algorithm," *Int. J. online Biomed. Eng.*, vol. 19, no. 3, pp. 99–112, 2022, doi: 10.3991/ijoe.v19i03.37569.
[5] E. Kotter, L. Marti-Bonmati, A. P. Brady, and N. M. Desouza, "ESR white paper: blockchain and medical imaging," *Insights Imaging*, vol. 12, no. 1, 2021, doi: 10.1186/s13244-021-01029-y.
[6] S. Sahoo, A. M. Fajge, R. Halder, and A. Cortesi, "A hierarchical and abstraction-based blockchain model," *Appl. Sci.*, vol. 9, no. 11, 2019, doi: 10.3390/app9112343.
[7] M. A. Acquah, N. Chen, J. S. Pan, H. M. Yang, and B. Yan, "Securing Fingerprint Template Using Blockchain and Distributed Storage System," *Symmetry (Basel).*, vol. 12, no. 6, pp. 1–15, 2020, doi: 10.3390/SYM12060951.
[8] S. Makridakis, "Blockchain : Current Challenges and Future Prospects / Applications," pp. 1–16, 2019.
[9] K. Koptyra and M. R. Ogiela, "Imagechain—application of blockchain technology for images," *Sensors (Switzerland)*, vol. 21, no. 1, pp. 1–12, 2021, doi: 10.3390/s21010082.
[10] E. Borandag, "A Blockchain-Based Recycling Platform Using Image Processing, QR Codes, and IoT System," *Sustain.*, vol. 15, no. 7, 2023, doi: 10.3390/su15076116.
[11] P. Nivethini, S. Meena, V. Krithikan, and G. Prethija, "Data Security using Blockchain Technology," *Int. J. Adv. Appl.*, no. October, pp. 279–282, 2019.
[12] A. Roshanzamir, V. Weerakkody, N. Rana, M. Rahmati, and M. Shajari, "Blockchain and Image Processing to Reinforce Provenance in the Narrative of a Handwoven Carpet," *Int. J. Adv. Internet Technol.*, vol. 12, no. 3, pp. 61–75, 2019, [Online]. Available: http://www.iariajournals.org/internet_technology/
[13] M. Y. Jabarulla and H. N. Lee, "Blockchain-based distributed patient-centric image management system," *Appl. Sci.*, vol. 11, no. 1, pp. 1–20, 2021, doi: 10.3390/app11010196.
[14] M. N. M. Bhutta *et al.*, "A Survey on Blockchain Technology: Evolution, Architecture and Security," *IEEE Access*, vol. 9, pp. 61048–61073, 2021, doi: 10.1109/ACCESS.2021.3072849.
[15] P. K. Paul, "Blockchain Technology and its Types—A Short Review," *Int. J. Appl. Sci. Eng.*, vol. 9, no. 2, 2021, doi: 10.30954/2322-0465.2.2021.7.
[16] V. Nehra, A. K. Sharma, and R. K. Tripathi, *Blockchain Implementation for Internet of Things Applications*, no. March. 2020. doi: 10.1016/B978-0-12-819816-2.00005-8.
[17] J. Z. L. Covarrubias and I. N. L. Covarrubias, "Different types of government and governance in the blockchain," *J. Gov. Regul.*, vol. 10, no. 1, pp. 8–21, 2021, doi: 10.22495/jgrv10i1art1.
[18] R. Bhaskaran, R. Karuppathal, M. Karthick, J. Vijayalakshmi, S. Kadry, and Y. Nam, "Blockchain Enabled Optimal Lightweight Cryptography Based Image Encryption Technique for IIoT," *Intell. Autom. Soft Comput.*, vol. 33, no. 3, pp. 1593–1606, 2022, doi: 10.32604/iasc.2022.024902.
[19] B. Li, C. Chenli, X. Xu, T. Jung, and Y. Shi, "Exploiting computation power of blockchain for biomedical image segmentation," *IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Work.*, vol. 2019-June, pp. 2802–2811, 2019, doi: 10.1109/CVPRW.2019.00339.
[20] X. Xiao, X. He, Y. Zhang, X. Dong, L. Yang, and Y. Xiang, "Blockchain-based reliable image copyright protection," *IET Blockchain*, vol. 3, no. 4, pp. 222–237, 2023, doi: 10.1049/blc2.12027.
[21] B. Liu, M. Liu, X. Jiang, F. Zhao, and R. Wang, "A Blockchain-Based Scheme for Secure Sharing of X-Ray Medical Images," *Adv. Intell. Syst. Comput.*, vol. 895, no. 6, pp. 29–42, 2020, doi: 10.1007/978-3-030-16946-6_3.
[22] S. Inam, S. Kanwal, R. Firdous, and F. Hajjej, "Blockchain based medical image encryption using Arnold's cat map in a cloud environment," *Sci. Rep.*, vol. 14, no. 1, pp. 1–22, 2024, doi: 10.1038/s41598-024-56364-z.
[23] J. H. Horng, C. C. Chang, G. L. Li, W. K. Lee, and S. O. Hwang, "Blockchain-Based Reversible Data Hiding for Securing Medical Images," *J. Healthc. Eng.*, vol. 2021, 2021, doi: 10.1155/2021/9943402.
[24] M. Acharya and R. S. Sharma, "A novel image encryption based on feedback carry shift register and blockchain for secure communication," *Int. J. Appl. Eng. Res.*, vol. 16, no. 6, pp. 466–477, 2021.
[25] T. Li, B. Du, and X. Liang, "Image Encryption Algorithm Based on Logistic and Two-Dimensional Lorenz," *IEEE Access*, vol. 8, pp. 13792–13805, 2020, doi: 10.1109/ACCESS.2020.2966264.
[26] G. K. Shraida and H. A. Younis, "An Efficient Diffusion Approach for Chaos-Based Image Encryption and DNA Sequences," *Iraqi J. Electr. Electron. Eng.*, vol. 18, no. 2, pp. 69–74, 2022, doi: 10.37917/ijeee.18.2.9.
[27] B. A. Salim, M. A. Aljabery, and H. A. Younis, "AES-Based Steganography Using Blockchain: A Novel Approach for Secure Text Hiding in Encrypted Images," *Inform.*, vol. 48, no. 21, pp. 67–78, 2024, doi: 10.31449/inf.v48i21.6689.
[28] H. Zhang and H. Hu, "An Image Segmentation Encryption Algorithm based on Hybrid Chaotic System," *IEEE Access*, vol. 7, pp. 103047–103058, 2019, doi: 10.1016/j.dsp.2023.104367.
[29] P. N. Andono and D. R. I. M. Setiadi, "Improved Pixel and Bit Confusion-Diffusion based on Mixed Chaos and Hash Operation for Image Encryption," *IEEE Access*, vol. 10, no. October, pp. 115143–115156, 2022, doi: 10.1109/ACCESS.2022.3218886.
[30] M. Khan, S. S. Jamal, M. M. Hazzazi, K. M. Ali, I. Hussain, and M. Asif, "An Efficient Image Encryption Scheme based on Double Affine Substitution Box and Chaotic System," *Integration*, vol. 81, no. November 2020, pp. 108–122, 2021, doi: 10.1016/j.vlsi.2021.05.007.
[31] J. Jain and A. Jain, "Securing E-Healthcare Images Using an Efficient Image Encryption Model," *Sci. Program.*, vol. 2022, pp. 1–11, 2022, doi: 10.1155/2022/6438331.
[32] U. Sara, M. Akter, and M. S. Uddin, "Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study," *J. Comput. Commun.*, vol. 07, no. 03, pp. 8–18, 2019, doi: 10.4236/jcc.2019.73002.