

Bolstering image encryption techniques with blockchain technology - a systematic review

Narmadha Annadurai, Agusthiyar Ramu

Department of Computer Applications, SRM Institute of Science and Technology, Chennai, India

Article Info

Article history:

Received Jul 4, 2024

Revised Nov 19, 2024

Accepted Dec 15, 2024

Keywords:

Blockchain technology

Hybrid algorithms

IIoT

Image encryption

IoT

ABSTRACT

Multimedia data plays a momentous role in present world. With the advancements in various fields of research like internet of things (IoT), industrial IoT (IIoT), cloud computing, medical image processing, and many more technologies, the digital images have already encroached the multimedia eon. The major challenge lies in providing a tamper proof image with higher level of security and confidentiality while being transmitted through a public network. Image encryption techniques are considered to be the predominant method to anticipate security from any unauthorized user access. This has indeed provoked the researchers to create new diverse and hybrid algorithms for encrypting the images. At present blockchain has been the most prevalently discussed method for security and the next level of security can be foreseen using the blockchain encryption techniques. This paper identifies the literature which mainly focuses on assorted image encryption techniques with blockchain technology applied on digital images from heterogeneous sources. An overview has been proposed to discuss on these techniques.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Narmadha Annadurai

Department of Computer Applications, SRM Institute of Science and Technology

Ramapuram, Chennai, India

Email: na0968@srmist.edu.in

1. INTRODUCTION

In this rapid growing era of internet and technologies, digital images are considered to be one of the most important sources of information. In fact, digital images are now omnipresent, impinging on various sectors across the globe. From social media platforms to medical diagnostics, digital images serve as crucial data for different applications. Every day, billions of devices generate immense volumes of image data, contributing to a visual-dominated ecosystem. These images, whether two-dimensional or three-dimensional, have a profound impact on the human brain, as visual data is processed more rapidly than any other form of information. This is why images have become the ideal medium for communication and information exchange in today's integrated and interconnected world [1]-[6]. However, with the growing reliance on image data comes an increase in security concerns. The sheer volume of digital images being transmitted over the internet opens up multiple avenues for potential cyber threats. These threats can range from unauthorized access and data breaches to image manipulation and theft of sensitive information. In particular, the transmission of image data over networks presents several challenges, as malicious actors may intercept, alter, or misuse the data during the transfer process. As such, ensuring the confidentiality, integrity, and security of digital images has become a significant priority for both individuals and organizations [7]-[10]. Blockchain technology has gained significant attention as a potential solution for enhancing the security of

image data. Originally developed as the underlying technology for Bitcoin, blockchain was created to address the issue of double-spending in digital currency transactions. Its decentralized nature, where transactions are verified by a network of nodes, ensures that data is immutable and tamper-resistant. Over the years, the applications of blockchain technology have expanded beyond cryptocurrencies, with its potential being explored in various domains such as supply chain management, healthcare, and even digital image security [11]-[14]. When integrated with encryption techniques, blockchain technology can significantly enhance the security of image data. Encryption plays a key role in protecting image data by converting it into an unreadable format that can only be deciphered by authorized parties with the correct decryption key. This ensures that even if an image is intercepted during transmission, it remains secure and inaccessible to unauthorized users. By combining encryption with blockchain, the security framework becomes even more robust, providing additional layers of protection [15]-[18]. One of the key features of blockchain technology is its decentralized structure. Traditional centralized systems store data in a single location, making them vulnerable to attacks. If a hacker manages to breach the centralized system, they can potentially gain access to all the stored data. In contrast, blockchain operates on a distributed ledger, where data is stored across multiple nodes. Each node in the network has a copy of the entire blockchain, ensuring that no single point of failure exists. This decentralized structure makes it significantly more challenging for attackers to compromise the system, as they would need to simultaneously breach multiple nodes to alter the data. Despite the numerous advantages that blockchain technology offers for image data security, it is important to recognize that the technology is not without its challenges. One of the primary concerns with blockchain is its scalability. As the number of transactions on a blockchain network increases, the size of the blockchain also grows, leading to slower transaction processing times [19]-[22]. For applications that generate large volumes of image data, such as social media platforms or security surveillance systems, this scalability issue can hinder the efficiency of the blockchain system. Moreover, the decentralized nature of blockchain requires significant computational power and energy consumption, particularly for networks that rely on consensus algorithms like proof of work (PoW). The researches [23]-[25] provides a systematic review by systematically exploring the integration of blockchain with image encryption techniques, identifying the gaps in current research, and offering new insights into potential areas for future work. Unlike existing reviews that focus solely on individual domains, this paper bridges the two fields, analyzing their synergies and the unique security challenges that arise in real-time systems like internet of things (IoT) and healthcare. Moreover, we introduce a new classification framework that categorizes the existing methods based on their applicability to specific use cases such as medical imaging, industrial IoT (IIoT), and large-scale decentralized systems.

2. UTILIZATION OF IMAGE ENCRYPTION

Image data are utilized in diverse aspects on multiple domains of advanced technologies like medical imaging, artificial intelligence, and computer vision, image data consists of very sensitive and confidential information which is prone to various kinds of attacks when transferred through the unsecured channel. Security of these images are considered to be essential which can be obtained through image encryption techniques. Figure 1 shows the recent applications of image encryption.

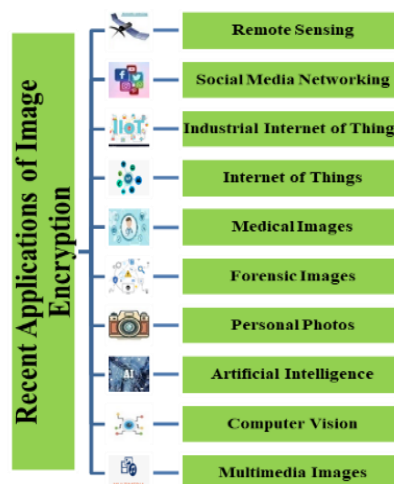


Figure 1. Recent applications of images encryption

3. IMAGE DATA OVERVIEW

An image data is defined as group of pixels. Image is represented by its height and width (Dimensions). If the dimension of the image is 255×255 , then the number of pixels present in the image is 65,025 pixels. A pixel is a point on the image which takes a red, green, and blue (RGB) color. Each pixel is capable of storing three binary codes of red, green, and blue (RGB) which takes 8 bit and this will be multiplied by number of pixels present in an image. This is shown in the Figure 2. displays an image which represents the pixels of the given image and Figure 3. displays the RGB value taken by each pixel in the image. These representations are carried out using MATLAB.

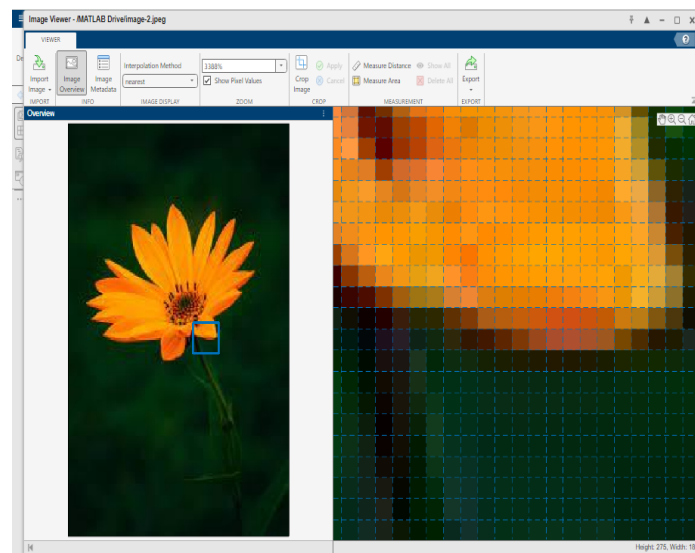


Figure 2. Pixel representation of the image

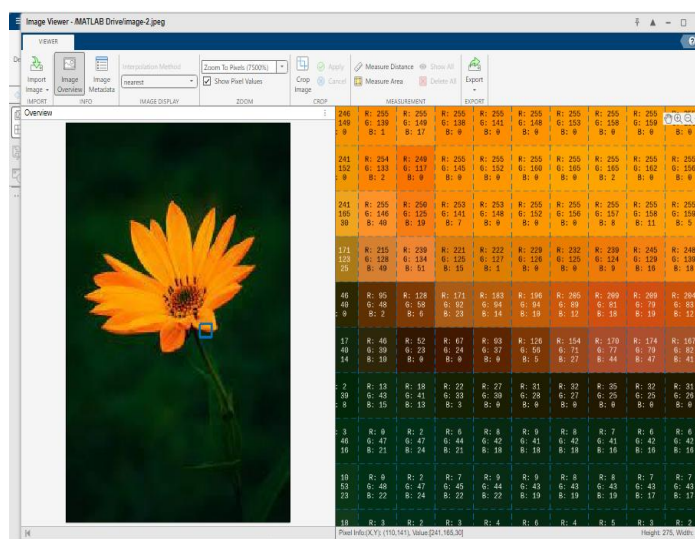


Figure 3. RGB value of each pixel in the image

4. IMAGE CRYPTOGRAPHY

Image cryptography applies the process of encryption and decryption to the given image data. Encryption of image is a pivotal component of information security and image cryptography that focus explicitly on strong holding the integrity and confidentiality of digital image. It is a process which converts an original image into an encrypted image using secret key. Obtaining the original image back using secret key is called as decryption. Figure 4 shows the overview of image encryption.



Figure 4. Image encryption overview

Mathematical algorithms and functions are using some key values are applied on the image data to encrypt and decrypt it. The processes are represented by,

$$E_{ek}(PI) = CI \quad (1)$$

$$D_{dk}(CI) = PI \quad (2)$$

where E and D represents encryption and decryption, ek and dk represents encryption key and decryption key and PI and CI represent plain image and cipher image respectively. $E_{ek}(PI) = CI$ denotes the encryption method applied on the plain original image (PI) and obtained the cipher converted image (CI). $D_{dk}(CI) = PI$ represents the decryption method applied on the cipher image CI to regain the original plain image.

5. NEED FOR ENCRYPTING IMAGE

Image encipherment focuses on converting an image data into indecipherable and enigmatic structure, making it abstruse to illegitimate individuals. Encryption of digital images are carried out for three important reasons the first is to store the images securely, second is to attain image data confidentiality which allows only the authorized person to gain access over the image data while being transmitted over network and the third reason is to establish integrity that helps to easily detect unauthorized alterations and modifications to the image data. Though the illegitimate user gains control over the image data, it would be difficult to decrypt it without knowing the encryption key.

6. IMAGE ENCRYPTION PERFORMANCE MEASURES

6.1. Key space analysis

This analysis is considered as a predominant security measure for any encryption technique. This is because a better image encryption technique takes a key space of at least 2^{100} [14]. A good encryption algorithm makes use of large key space which makes it more secure from brute force attack.

6.2. Histogram analysis

Tonal dissemination of pixels of any image is defined as histogram. Chi-square test is carried out check the histogram. It is evaluated as (3).

$$\chi^2 = \sum_{i=0}^{255} \frac{(f_i - s)^2}{s} \quad (3)$$

Where, f_i =frequency of the pixel value i. S=dimension of image, here it is 255.

6.3. Entropy analysis

It is the measure of how the pixel values of the image is randomly distributed.

$$H = - \sum_{k=0}^{G-1} P(k) \log_2 (P(k)) \quad (4)$$

Here, H=entropy. G=gray value of the image given as input. P(k)=probability of symbol k occurred.

6.4. Correlation coefficient

Correlation coefficient (r) is defined as the statistical measures or the relationships between the adjacent pixel values of an image.

$$r = \frac{\sum_{i=1}^N (x_i - x_m)(y_i - y_m)}{\sum_{i=1}^N (x_i - x_m)^2 \sum_{i=1}^N (y_i - y_m)^2} \quad (5)$$

Where, x_i and y_i are pixel intensity in images. x_m and y_m are mean intensity of the images.

6.5. Mean squared error (MSE)

Calculates the difference between enciphered and deciphered images. It is used to find the correctness of the decryption algorithm and the image obtained on the receiver's end has been retrieved without distortion.

$$MSE = \frac{\sum_{m,n} [I_1(i,j) - I_2(i,j)]^2}{(m*n)} \quad (6)$$

Where, I_1 and I_2 are the given plain and cipher image respectively. m and n are image dimensions.

6.6. Peak signal to noise ratio (PSNR)

It is an expression of signal power to noise power in ratio.

$$PSNR = 10 \log_{10} (R^2 / (MSE)) \quad (7)$$

Where, R = power of signal. MSE = power of noise. Expressed as db.

6.7. Differential attacks

Cryptosystems are exposed to differential attack which infers to find out the secret key or the original image. NPCR and UACI are the measures used to strength of the cryptosystem against this attack.

6.8. Number of pixel change (NPCR)

Helps to identify the number of value and position changes in pixels of image data.

$$NPCR = \frac{\sum_{i=1}^M \sum_{j=1}^N D(i,j)}{M * N} * 100\% \quad (8)$$

Where,

$$D(i,j) = \begin{cases} 1, & \text{if } C1 \neq C2 \\ 0, & \text{if } C1 = C2 \end{cases}$$

$C1$ and $C2$ are cipher images. M and N are height and width of the images.

6.9. Unified average changing intensity (UACI)

Identifies the changes in the pixel intensities in the images.

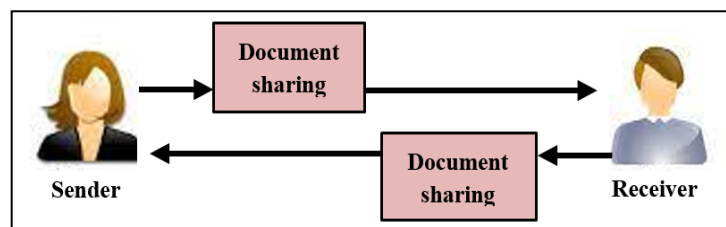
$$UACI = \frac{\sum_{i=1}^N \sum_{j=1}^M |C1(i,j) - C2(i,j)|}{255 * M * N} * 100\% \quad (9)$$

M and N are height and width of the 8-bit image.

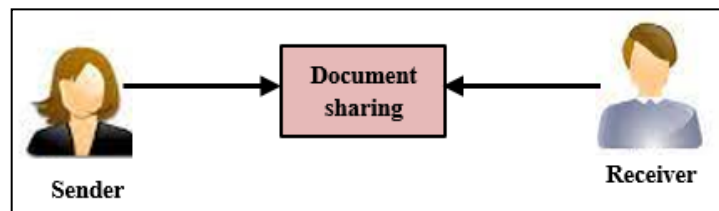
7. BLOCKCHAIN TECHNOLOGY

Basically, blockchain is a decentralized computation and information sharing platform. This platform enables individuals from heterogeneous domains to make coherent decisions. This technology was introduced to overcome the problems in traditional and centralized information sharing methods. Figure 5 depicts the block diagram of different document and other data sharing models in data management. In traditional method (Figure 5(a)) of information sharing if the sender wants to share a document, ideally the sender will write the content in his/her own document and shares it with the receiver. The receiver will

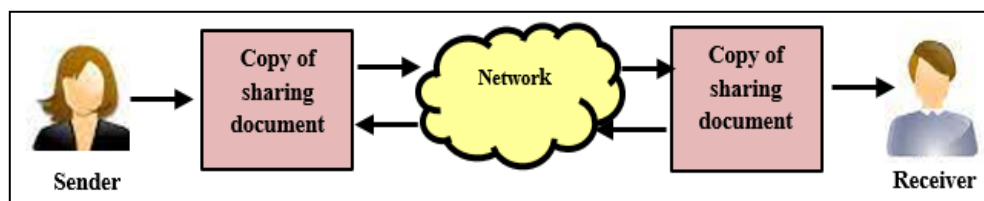
update the document with his own content and shares back the document to the sender. The major disadvantage in this method is that the sender and the receiver cannot simultaneously edit the document. To overcome this problem, centralized platform (Figure 5(b)) was developed where the sender and the receiver can edit and work on the same document simultaneously. The disadvantage here is that it acts as a single point of failure where the person can't work using insufficient bandwidth or manage the data loss that occurs due system failure. These are the issues which makes researchers to move from a centralized system to a decentralized and distributed system. In decentralized system (Figure 5(c)) multiple points of coordination will be there. In distributed system environment everyone collectively executes a job.



(a)



(b)



(c)

Figure 5. Sharing models in data management: (a) traditional document, (b) centralized document, and (c) decentralized and distributed document

Advantages of block chain over image data: blockchain technology offers many advantages for image data. Image encryption is an area with which blockchain connects itself to guarantee increased reliability. In general, an image is viewed in two or three dimensions which contains very sensitive and useful information. Since most of the conventional mechanisms are central, blockchain can be relied to solve the security problems. Immense level of security can be achieved for high magnitude images. Moreover, morphing of images stored in a blockchain is impossible. Increased possibility in accessing the remote images because the blockchain does not have a central server. When it comes to accessibility, the authorized person is given access to monitor the data. Figure 6 explains the general framework on how blockchain based image encryption strategies are interspersed for images. Images taken from different domains like images from IoT, IIoT devices, medical images, and images from social media, are considered. First the taken image is subjected to any one or combination of different types of permutation or substitution techniques adopted by the researcher. This method produces a distorted shuffled image. The shuffled image obtained is encrypted using any of the encryption or hashing algorithm, the result will be an encrypted image. The cryptographic pixel values of the obtained encrypted image are stored in blockchain. This results in a tamper proof secured images.

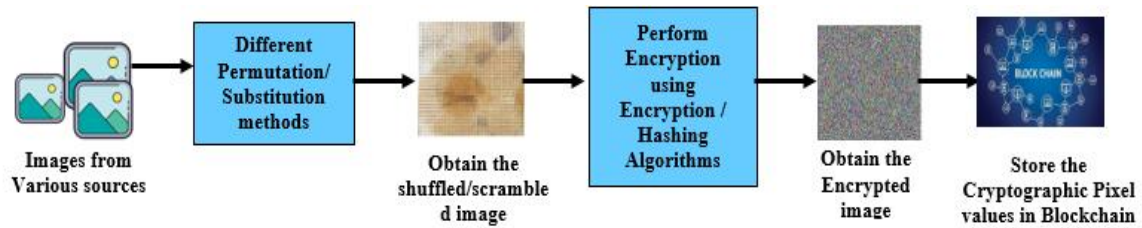


Figure 6. Block diagram of blockchain based image encryption framework

8. OVERVIEW OF VARIOUS BLOCKCHAIN BASED ENCRYPTION TECHNIQUES

Previous studies have extensively explored both image encryption and blockchain technology as individual domains. Traditional encryption methods, such as advanced encryption standard (AES), data encryption standard (DES), and Rivest-Shamir-Adleman (RSA), are commonly used for securing digital data, including images. However, their application in large-scale systems, such as IoT, IIoT, and medical imaging, is often limited by the computational overhead and real-time processing requirements. Similarly, blockchain technology has been employed in various sectors to secure digital transactions, maintain decentralized records, and ensure data integrity.

The combination of image encryption with blockchain is relatively new and underexplored. Some studies have proposed encrypting digital images and storing the encrypted data on a blockchain. For example, Li *et al.* [16] proposed a blockchain-based secure image storage system for IoT environments. However, these studies often rely on classical encryption techniques and lack focus on domain-specific requirements like those in healthcare or industrial settings.

While several review papers have been published on either image encryption or blockchain technology, few focus on the integration of these two fields. Most existing reviews tend to limit their scope to individual advancements in image encryption algorithms or blockchain implementations in decentralized systems. For instance, surveys by Zhang *et al.* [23] and Kumar *et al.* [6] have discussed traditional encryption techniques, such as AES and RSA, as well as their applications to secure image transmission. Similarly, blockchain- focused reviews, like those by Gupta *et al.* [20], highlight the use of decentralized ledger systems in applications such as cryptocurrencies and secure data storage. However, none of these reviews explore the potential for integrating image encryption with blockchain in domains like IoT, medical imaging, and industrial systems.

- Our contribution: this review fills a critical gap in the literature by providing a comprehensive survey of the methods that integrate image encryption with blockchain technology. We critically examine the existing techniques, categorize them based on their security protocols and efficiency in real-time systems, and propose a novel classification framework that focuses on:
- Use-case applicability: medical imaging, IIoT, and large-scale secure data transmission.
- Security performance metrics: measuring the trade-offs between encryption strength, blockchain transaction speed, and scalability.
- Synergistic innovations: identifying promising approaches where the synergy between encryption techniques and blockchain can improve security and efficiency.

This paper also highlights the gaps and challenges in the current body of literature, particularly with respect to the performance trade-offs between encryption complexity and blockchain scalability, and suggests avenues for future research in this emerging field. Table 1 provides the summary of various image encryption techniques proposed by different authors on the images obtained from heterogeneous sources. All these encryption techniques integrate blockchain technology after encrypting the image data. The results and observations are summarized along with the limitations and the future enhancements discussed by the authors.

9. SECURITY AND COMPLEXITY ANALYSIS OF BLOCKCHAIN AND IMAGE ENCRYPTION TECHNOLOGIES

In any cryptographic system or secure communication framework, both security proofs and complexity assessments are crucial for evaluating the robustness and feasibility of the proposed techniques. This review synthesizes the current state of the art by analyzing the security proofs and computational complexities for both blockchain-based systems and image encryption technologies. In the literature on blockchain and image encryption, security proofs are crucial for demonstrating that methods meet core security requirements such as confidentiality, integrity, and authenticity. Provable security models are commonly used for image encryption techniques, showcasing their resistance to known attacks like brute force or differential cryptanalysis. For example, encryption algorithms like RSA, DES, and AES provide

well-established proofs of security based on computational hardness, such as the difficulty of factoring large primes (RSA) or solving specific problems (AES). In blockchain security, protocols often rely on byzantine fault tolerance (BFT) and zero-knowledge proofs (ZKPs) to secure the network, especially in scenarios integrating image encryption, such as in healthcare and IoT. Research by Zhang *et al.* [23] highlights the use of ZKPs to protect medical image privacy while using blockchain for secure transmission, though many systems still lack formal proofs against issues like double-spending or Sybil attacks, especially in resource-constrained IoT environments. Additionally, the integration of homomorphic encryption with blockchain has emerged as a solution for secure image transmission, where security proofs ensure that encrypted images can be processed without revealing their content, a vital feature in privacy-sensitive fields like healthcare.

Complexity assessment is essential in determining the feasibility of deploying encryption and blockchain solutions, particularly in real-time and resource-constrained environments like IoT and IIoT. For image encryption, methods such as chaotic maps and elliptic curve cryptography (ECC) provide high security but are often computationally intensive, posing challenges for real-time implementation. Studies by Kumar and Mathew [17] indicate that while ECC offers stronger security per bit than RSA, its key generation and encryption processes are slower, especially with large image datasets. Chaotic encryption techniques, such as logistic maps, have lower computational complexity but may be less secure, prompting the development of hybrid methods that combine chaotic encryption with traditional algorithms to balance security and complexity. Blockchain's complexity primarily arises from its consensus mechanisms.

Table 1. Summary of the survey on various image encryption carried out with blockchain

References	Algorithms used	Applied on	Result/observation	Limitations	Proposed future enhancements
Khan and Byun [1]	Image encryption based on blockchain	IIoT	Ideal entropy value close to 8 is obtained which makes it safe from brute force attack.	Usage of sensors with low memory and transaction speed	Web and cloud services can resolve this problem of deficient sensor memory
Bhaskaran <i>et al.</i> [2]	BC-LWCIE technique light weight cryptography technique	IIoT	Accomplished higher NPCR and PSNR	Only images of 256 pixels is considered.	Attribute based encryption and digital signature approaches can be implemented for security performance
Durga <i>et al.</i> [3]	Chaotic encryption scheme (CES) blockchain mode	IoT-medical images	Secure from brute force attack	Limited computing resources and lack of memory.	For testing security implementing 5G will be efficient in future.
Khayyat <i>et al.</i> [4]	Block chain-enabled model with SSO-HCNN	IIoT	Resulted in good entropy, minimum MSE and maximum PSNR and CC	Optimization techniques is tedious	LWC with biometric schemes can be adopted to ensure security.
Brabin <i>et al.</i> [5]	RDH scheme with block or stream cipher	All digital images	Achieved high PSNR	Original images is not obtained at the decoding phase due to compression and decompression of JPEG image.	Replication of the original image without data loss has to be focused in decoding phase
Kumar <i>et al.</i> [6]	Block chain and homomorphic BGV encryption scheme	Medical images	Achieved a model which is highly resistant to data leakage	Training the model consumes more Time and cost	Aim to provide a cost effective solution
Shareef <i>et al.</i> [7]	AES technique inter planetary file system (IPFS) is used to encrypt and generate hash value		Transferred images are stored in multiple nodes, makes it difficult for the hackers to access	Image key generation is tedious	Focus to introduce new blockchain hashing.
Acharya and Sharma [8]	Blockchain and feedback carry shift register (FCSR)	All digital images	Feedback carry shift register with Arnold map is implemented.	Secure from statistical attacks	More shuffling techniques can be implemented
Ghazal <i>et al.</i> [9]	Computational intelligence approach with encryption framework using private blockchain.	IoMT	Works in three phases, training, validation and private blockchain,	Training phase and accuracy in validation is highly efficient.	Need to provide effective training methods for dataset to increase efficiency
Alohali <i>et al.</i> [10]	Image encryption process with AOA driven by block chain	All digital images	Blockchain, image encryption and optimal key generation is used	Resulted in MSE of 0.0430 and PSNR 61.80 dB	Key generation is tedious

10. DISCUSSION

Table 1 caters the literature review of the study carried out by various authors that is observed carefully to furnish the significance of image encryption techniques and blockchain technology in protecting the image data. It is observed from the above review that many authors are focusing on image encryption along with blockchain. As presented above Khan and Byun [1] has suggested a method which stores the pixel values of the image which is obtained using proposed cryptographic technique in a blockchain. Hashing is performed on the collected data and stored over the blockchain. Bhaskaran *et al.* [2] has discussed about light weight cryptography which is enabled with blockchain. Key is generated by chicken swarm optimization (CSO) algorithm. Durga *et al.* [3] has proposed a novel chaotic encryption (CES) which uses permutation technique based on blockchain system. Khayyat *et al.* [4] has introduced neural network which is implemented using chaotic maps for key generation, enabled with blockchain and optimization by applying shark smell technique. Brabin *et al.* [5] has proposed reversible data hiding technique which is stored in blockchain. The other authors have proposed homomorphic encryption technique, AES technique with inter planetary file system, feedback carry shift registers with blockchain, Arnold map with blockchain. The above study has furnished few blockchain based techniques for image encryption. In future the following can be considered. New encryption techniques can be proposed and explored by integrating with blockchain to provide better results.

- i) Deep learning key generation techniques can be implemented instead of tradition key generation for encryption.
- ii) Diverse image dataset may enhance the study. In the above study only images from IoT devices are considered.
- iii) Comparative study of various techniques can be presented to identify the most efficient techniques.
- iv) Comparison on different security measures may be carried out to analyses and understand the performance of each and every technique.
- v) Since processing image data consumes more time and space, focusing on developing a new algorithm based on these parameters to reduce complexity will be very useful.
- vi) Cost effective methods has to be identified when integrating with blockchain.
- vii) Reproducing the original image without data loss has to be concentrated in the upcoming researches. To that domain should be conducted.

11. CONCLUSION

This survey presents the existing blockchain based image encryption schemes which are applied with various permutation techniques before encryption. It has been observed that a plain image is considered as group of pixels and these pixels has a high level of correlation between each other. All the encryption techniques applied by most of the authors mainly aim to reduce this correlation that exist between the neighboring pixels. Finally, to make digital images highly secure the researchers focus on storing the encrypted pixel values of the images inside block chain. More intense research can be accomplished in the image encryption domain using blockchain technology. Applying blockchain for images is still an open area for the researchers. Image data is obtained from various sources on which encryption can be focused on every separate area in future. More focus can be stressed on directly encrypting images using block chain technology without applying any traditional, modern and novel encryption techniques. From this systematic review, it has been perceived that encryption of images are either carried out in one of the following two ways. First by applying various types of traditional and modern image encryption schemes and storing the cryptographic pixel values. The second method is by directly applying blockchain based image encryption to the images due to its decentralized storing. Both of the above-mentioned techniques have their own advantages and disadvantages. This opens up new avenues for the researchers to enhance image encryption by integrating with blockchain.

FUNDING INFORMATION

Authors state no funding involved in this manuscript.

AUTHOR CONTRIBUTIONS STATEMENT

Narmadha A: Conceptualization, methodology, literature review, data collection, manuscript drafting, Software, Data analysis, interpretation of results, manuscript editing, and critical revisions. Agusthiyar R: Technical validation, Final Analysis, Investigation and manuscript proofreading, review and editing, Supervision, project administration, and final approval of the manuscript. All authors have read and approved the final version of this manuscript and agree to be accountable for the work's accuracy and integrity. The author's contribution is given below in the form of table for reference.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Narmadha A	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Agusthiyar R		✓		✓	✓	✓				✓		✓	✓	✓

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review & Editing

Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

CONFLICT OF INTEREST STATEMENT

The author(s) declare that there are no conflicts of interest related to this research. No financial, personal, or professional relationships have influenced the work presented in this paper. All research findings and interpretations are solely based on objective analysis and scientific inquiry.

DATA AVAILABILITY

- The data that support the findings of this study are openly available in [Data Sources Images - Free Download on Freepik] at <https://www.freepik.com/free-photos-vectors/data-sources>.
- The data that support the findings of this study are also free available in [Free Stock Photos, Royalty Free Stock Images & Copyright Free Pictures · Pexels] at <https://www.pexels.com/>.
- The Formula for image security measures of this research is available in <https://onlinelibrary.wiley.com/doi/full/10.1155/2016/6714164>.
- The authors confirm that all the block diagrams are created by the author itself with the help of Miro tool at miro.com and also with the help of inserting shapes using MS word.
- The pixel value calculation of the image data is derived using online Matlab tool at <https://www.mathworks.com/products/matlab-online.html>.




REFERENCES

- [1] P. W. Khan and Y. Byun, "A blockchain-based secure image encryption scheme for the industrial internet of things," *Entropy*, vol. 22, no. 2, p. 175, Feb. 2020, doi: 10.3390/e22020175.
- [2] R. Bhaskaran, R. Karuppathal, M. Karthick, J. Vijayalakshmi, S. Kadry, and Y. Nam, "Blockchain enabled optimal lightweight cryptography based image encryption technique for IIoT," *Intelligent Automation and Soft Computing*, vol. 33, no. 3, pp. 1593–1606, 2022, doi: 10.32604/iasc.2022.024902.
- [3] R. Durga, E. Poovammal, K. Ramana, R. H. Jhaveri, S. Singh, and B. Yoon, "CES blocks—a novel chaotic encryption schemes-based blockchain system for an IoT environment," *IEEE Access*, vol. 10, pp. 11354–11371, 2022, doi: 10.1109/ACCESS.2022.3144681.
- [4] M. M. Khayyat, M. M. Khayyat, S. Abdel-Khalek, and R. F. Mansour, "Blockchain enabled optimal hopfield chaotic neural network based secure encryption technique for industrial internet of things environment," *Alexandria Engineering Journal*, vol. 61, no. 12, pp. 11377–11389, 2022, doi: 10.1016/j.aej.2022.05.002.
- [5] D. Brabin, C. Ananth, and S. Bojjagani, "Blockchain based security framework for sharing digital images using reversible data hiding and encryption," *Multimedia Tools and Applications*, vol. 81, no. 17, pp. 24721–24738, 2022, doi: 10.1007/s11042-022-12617-5.
- [6] R. Kumar *et al.*, "Blockchain and homomorphic encryption based privacy-preserving model aggregation for medical images," *Computerized Medical Imaging and Graphics*, vol. 102, 2022, doi: 10.1016/j.compmedimag.2022.102139.
- [7] A. A. Shareef, P. L. Yannawar, A. S. H. Abdul-Qawy, and M. G. Almusharref, "Share and retrieve images securely using blockchain technology," *International Journal on Technical and Physical Problems of Engineering*, vol. 14, no. 3, pp. 207–211, 2022.
- [8] M. Acharya and R. S. Sharma, "A novel image encryption based on feedback carry shift register and blockchain for secure communication," *International Journal of Applied Engineering Research*, vol. 16, no. 6, pp. 466–477, 2021.
- [9] T. M. Ghazal, M. K. Hasan, S. N. H. S. Abdullah, K. A. A. Bakar, and H. Al Hamadi, "Private blockchain-based encryption framework using computational intelligence approach," *Egyptian Informatics Journal*, vol. 23, no. 4, pp. 69–75, 2022, doi: 10.1016/j.eij.2022.06.007.
- [10] M. A. Alohal *et al.*, "Blockchain-driven image encryption process with arithmetic optimization algorithm for security in emerging virtual environments," *Sustainability (Switzerland)*, vol. 15, no. 6, 2023, doi: 10.3390/su15065133.
- [11] M. P. McBee and C. Wilcox, "Blockchain technology: principles and applications in medical imaging," *Journal of Digital Imaging*, vol. 33, no. 3, pp. 726–734, 2020, doi: 10.1007/s10278-019-00310-3.
- [12] B. Patrickson, "What do blockchain technologies imply for digital creative industries?," *Creativity and Innovation Management*, vol. 30, no. 3, pp. 585–595, 2021, doi: 10.1111/caim.12456.
- [13] M. Kaur, S. Singh, and M. Kaur, "Computational image encryption techniques: a comprehensive review," *Mathematical Problems in Engineering*, vol. 2021, 2021, doi: 10.1155/2021/5012496.
- [14] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, "A new image encryption algorithm for grey and color medical images," *IEEE Access*, vol. 9, pp. 37855–37865, 2021, doi: 10.1109/ACCESS.2021.3063237.
- [15] C. Tiken and R. Samli, "A comprehensive review about image encryption methods," *Harran Üniversitesi Mühendislik Dergisi*, vol. 7, no. 1, pp. 27–49, 2022, doi: 10.46578/humder.1066545.




- [16] Y. Li, Y. Tu, J. Lu, and Y. Wang, "A security transmission and storage solution about sensing image for blockchain in the Internet of Things," *Sensors*, vol. 20, no. 3, p. 916, 2020.
- [17] R. Kumar R and J. Mathew, "How to evaluate the security and performance of an image encryption system," *International Journal of Scientific Research in Science, Engineering and Technology*, pp. 302–311, 2020, doi: 10.32628/ijrsrset207372.
- [18] M. Singh and A. K. Singh, "A comprehensive survey on encryption techniques for digital images," *Multimedia Tools and Applications*, vol. 82, no. 8, pp. 11155–11187, Mar. 2023, doi: 10.1007/s11042-022-12791-6.
- [19] D. G. Ciric, Z. H. Peric, M. Milenkovic, and N. J. Vucic, "Evaluating similarity of spectrogram-like images of DC motor sounds by pearson correlation coefficient," *Elektronika ir Elektrotechnika*, vol. 28, no. 3, pp. 37–44, 2022, doi: 10.5755/j02.eie.31041.
- [20] M. Gupta, K. K. Gupta, and P. K. Shukla, "Session key based fast, secure and lightweight image encryption algorithm," *Multimedia Tools and Applications*, vol. 80, no. 7, pp. 10391–10416, 2021.
- [21] S. Neelakandan, J. R. Beulah, L. Prathiba, G. L. N. Murthy, E. F. I. Raj, and N. Arulkumar, "Blockchain with deep learning-enabled secure healthcare data transmission and diagnostic model," *International Journal of Modeling, Simulation, and Scientific Computing*, vol. 13, no. 4, 2022, doi: 10.1142/S1793962322410069.
- [22] R. Li, "Fingerprint-related chaotic image encryption scheme based on blockchain framework," *Multimedia Tools and Applications*, vol. 80, no. 20, pp. 30583–30603, 2021, doi: 10.1007/s11042-020-08802-z.
- [23] R. Zhang, R. Xue, and L. Liu, "Security and privacy for healthcare blockchains," *IEEE Transactions on Services Computing*, vol. 15, no. 6, pp. 3668–3686, 2021.
- [24] U. Padmavathi and N. Rajagopalan, "Blockchain enabled emperor penguin optimizer based encryption technique for secure image management system," *Wireless Personal Communications*, vol. 127, no. 3, pp. 2347–2364, 2022, doi: 10.1007/s11277-021-08800-w.
- [25] N. Sammeta and L. Parthiban, "Data ownership and secure medical data transmission using optimal multiple key-based homomorphic encryption with hyperledger blockchain," *International Journal of Image and Graphics*, vol. 23, no. 3, 2023, doi: 10.1142/S0219467822400034.

BIOGRAPHIES OF AUTHORS



Narmadha Annadurai    is working as assistant professor in the Department of Computer Applications at Shri Krishnaswamy College for Women. She is currently pursuing her Ph.D. at SRM Institute of Science and Technology, Ramapuram, Chennai, in the field of cryptography and network security. She has received her Bachelor degree and Master degree in computer science from Queen Mary's College (A) Madras University, Chennai, Tamilnadu in 2012 and 2014 respectively. She has also received her M. Phil degree from Quaid-e-Millath College for Women, Chennai, Tamilnadu. She has attended various international conferences and workshops and completed NPTEL courses related to her research domain. Her areas of interests include image encryption, block chain, and deep learning. She can be contacted at email: na0968@srmist.edu.in.



Professor Dr. Agusthiyar Ramu    is a well-known academician in the field of higher education with 23 years of teaching experience. He has received his Ph.D. from Anna University, Chennai in the field of data mining in the year 2017. He started his teaching profession from 2002 and now he is working as a professor in the Department of Computer Science and Applications, Faculty of Science and Humanities, SRMIST, Ramapuram Campus. He has received his Post Graduate MCA degree from Madurai Kamaraj University, Tamil Nadu, India in 2001, and M. Phil degree from Periyar University, Tamil Nadu, India in 2008 respectively. His research interests include data mining, artificial intelligence, and machine learning. He has published 18 research publications in indexed journals and 25 publications in international and national conferences. He is guiding 8 research scholars in SRM Institute of Science and Technology, Ramapuram. He has three patents in the field of IoT and machine learning. He has written a text book titled "Artificial intelligence- a handbook with a practical approach." He can be contacted at email: agusthir@srmist.edu.in.