DOI:

Enhancing Image Security with Introduction to Blockchain

Akil Saji
Dept of Information Technology, Amal Jyothi College of Engineering
APJ Abdul Kalam Technological University.
Kerala, India
akiltheredr@gmail.com

Sreeyuktha Ramesh
Dept of Information Technology, Amal Jyothi College of Engineering
APJ Abdul Kalam Technological University.
Kerala, India
sreeyuktharamesh@gmail.com

Aabel Jacob
Dept of Information Technology, Amal Jyothi College of Engineering
APJ Abdul Kalam Technological University.
Kerala, India
aabeljacob2001@gmail.com

Ms. Saumya Sadanandan
Dept of Information Technology, Amal Jyothi College of Engineering
APJ Abdul Kalam Technological University.
Kerala, India
saumyasadanandan@amaljyothi.ac.in

Rosmartina Shaju
Dept of Information Technology, Amal Jyothi College of Engineering
APJ Abdul Kalam Technological University.
Kerala, India
rosmartinashaju@gmail.com

Dr. S N Kumar
Dept of Electrical and Electronics, Amal Jyothi College of Engineering
APJ Abdul Kalam Technological University.
Kerala, India
snkumar@amaljyothi.ac.in

***Abstract*— This paper focuses mainly on Blockchain Based Image Encryption techniques. In addition, it also focuses on different image encryption techniques. The secrecy, integrity, and authenticity of images become a crucial concern as more and more people utilize digital means for sending and storing images. There are various techniques discovered sometimes to encrypt the images to make them more secure. This paper presents a survey of over 25 research papers over the years from 2000 till date. Furthermore, the paper briefly touches on the challenges and limitations of blockchain-based image encryption and presents potential future research directions in this field. Overall, the paper highlights the potential of blockchain-based image encryption as a promising approach to protect digital images from unauthorized access and data breaches.**

***Keywords*— blockchain, image encryption**

I. Introduction

In recent years, blockchain technology has gained significant attention due to its potential applications in various domains such as finance, healthcare, supply chain, and more. One of the promising applications of blockchain is in the field of image encryption. The use of blockchain for image encryption provides a secure and decentralized platform to store and transfer images.

II. Studies Related To Blockchain Based Image Encryption

Smart cameras and image sensors are widely used in industrial processes, but they are at risk of disclosure and privacy breach in the Industrial Internet of Things. Blockchain technology is the modern-day solution for trust issues and eliminating or minimizing the role of the third party. This paper proposes a permissioned private blockchain-based solution to secure the image while encrypting it. Based on the number of pixels change rate (NPCR), the unified average changed intensity, and information entropy analysis, authors evaluate the strength of proposed image encryption algorithm ciphers with respect to differential attacks. Encrypted results show that the proposed scheme is highly effective for data leakage prevention and security. There are still limitations in

DOI:

this technology's use, such as limited computing resources and the speed of transactions. Web services can resolve this problem, but more work will be done on this technology to make it more efficient and adaptable.[1]

A study by authors presents a blockchain-driven image encryption technique using arithmetic optimization with a fractional-order Lorenz system. The FOLS method integrates the Arnold map, tent map, and fractional Lorenz system, and an arithmetic optimization algorithm (AOA) was used to achieve the maximum PSNR value. Blockchain technology is an open, decentralized, and transparent distributed database that can be maintained by the group, and its major features are high credibility, decentralization, transparency, versatility, autonomy, traceability, anonymity, intelligence, reward mechanisms and irreversibility.[2]

This scheme proposes an encrypted image retrieval based on blockchain, which can solve the problem of malicious cloud servers returning wrong or incomplete search results by searching on the smart contract. The scheme stores the encrypted index on the blockchain, ensures the integrity and correctness of search results, outsources the corresponding encrypted images to the cloud server to reduce storage cost, and designs a double-layer index structure using bag of visual word model and sim hash in the process of image similarity index. Experiments show that the reliability, high retrieval efficiency, and precision of the scheme also have a good privacy protection effect. Future work will include trusted execution environment tree, homomorphic encryption, secure multi-party computing (SMC), and zero-knowledge proof to further reduce the cost without disclosing image privacy. Feature fusion based on convolutional neural network and principal component analysis has achieved better similarity machining effect.[3]

This is a novel fingerprint-related chaotic image encryption scheme that uses the blockchain framework to ensure that the encrypted image was sent correctly to the distributor. The proposed method has the following superiorities: security, authenticity, and traceability. The problem of distributing enormous quantity of secret keys in plaintext-related schemes is overcome, while the resistance to chosen plaintext attack is preserved. The method equips high security level and is applicable to real network environments.[4]

A color image encryption algorithm using the H'enonzigzag map and chaotic restricted Boltzmann machine is introduced in this paper. The algorithm includes the permutation phase and the diffusion phase, where two pseudorandom number sequences are used for row permutation and column permutation, respectively. CRBM is used for bitxor operation with the R, G, and B components of the scrambled image. A series of numerical experiments and analyses on encrypted images prove that the proposed algorithm is more secure than state-of-the-art algorithms, and a novel image encryption/decryption system is proposed. A color image encryption algorithm combining H'enon-zigzag-based permutation and chaotic restricted Boltzmann machine-based diffusion is introduced. It has two features: asymmetric encryption/decryption of images and authoritative verification of the integrity of encrypted images. The algorithm is robust against statistical attacks, brute force attacks, differential attacks, and data loss attacks, and uses blockchain to store and send the secret keys and 256-bit hash code of the encrypted image. It may be the first application of blockchain in the field of digital image encryption.[5]

An image encryption technique based on blockchain, and Feedback carry shift register (FCSR) is discussed in this paper. The solution encrypts the image and stores the values on the blockchain. The robustness of the proposed technique has been evaluated against differential attack based on Number of Pixels Change Rate (NPCR), Unified Averaged Changed Intensity (UACI) and information entropy analysis. The value attained was near the ideal value 8. The technique is also found to be efficacious against data loss in transit. The two FCSR sequences are then totally XOR-ed and used as the key for the image diffusion process. The final image is highly secure, and the transfer of this image takes place in the Inter Planetary File System (IPFS) network. The results of the demonstration suggest that the image is robust against adversary and blockchain network ensures that any tampering in the image will lead to detection.[6]

In [7] a blockchain based security framework for sharing digital images in a multiuser environment is put forth. It combines blockchain technology, reversible data hiding and encryption to provide different levels of security services. Reversible data hiding in combination with encryption protects the confidentiality, integrity and authentication of digital images. JPEG compression is used to enhance the hiding capacity and variable length user signatures can be embedded in the image blocks. Experimental results show that the proposed framework provides high security and the proposed reversible data hiding scheme provides high capacity and image quality.[7]

It demonstrates using a Blockchain network coupled with use of perceptual hashes and appropriate smart contract logic providing better mechanism for copyright violation detection than current systems. Perceptual hashes keep away from avalanche effect and are less susceptible to perceptual changes in images such as rotation, cropping, re-sizing, conversion to gray scale, salt and pepper noise, exposure or saturation change etc. The Blockchain transactions only contain IPFS hashes for retrieving images and permits distributed storage of images with the help of Inter Planetary File System (IPFS). After thorough evaluation, the perceptual hashes are effective and efficient copyright infringement detection tools.[8]

A blockchain-based searchable encryption scheme for Electronic Health Records (EHRs) sharing is designed to help different healthcare institutions share medical records securely. It provides convenience to patients, but also allows efficient sharing of medical information among researchers. To enable doctors and researchers to access patients' health data without disclosing their personal data, the desensitization technique should be used before the information is shared among others. This paper proposes a blockchain based searchable encryption scheme for EHRs sharing, using smart contracts such as Ethereum. The scheme utilizes the complex Boolean expression to extract the EHRs to construct the index. The smart contract used in the proposed scheme is designed to trace monetary rewards, including transaction fees, among the involved parties in the multi-user setting. It guarantees fairness among the data owners and users and guarantees that data users can receive accurate search results without additional verification. The data owner has full control over who can see their data. It proposes a blockchain based searchable encryption for EHRs sharing scheme, using a designated smart contract in blockchain to replace the centralized server. The scheme attains fairness in the sense that honest users (and not the malicious entity) will be rewarded, and security analysis and performance evaluations suggest it is feasible and effective. Future research will evaluate its utility in a real-world setting, as well as its scalability across different institutions and countries.[9]

Blockchain technology is a decentralized distributed data management technology by data encryption, data chain storage and distributed consensus mechanism. It has attracted research interest in both academic and industry domain due to its attributes of anti-tampering, integrity, and strong consistency. The basic architecture of the blockchain is shown in Figure 1. It leverages a chain structure to store user transfer records, Hash pointer to achieve logical links between data blocks, and proof-of-work (PoW) as the consensus mechanism. Bitcoin can be regarded as a special currency based on blockchain technology. The blockchain technology is a decentralized infrastructure that uses chained data structure to verify and store data and uses distributed node consensus mechanism to generate and update data. It can be divided into public, alliance, and exclusive blocks. The blockchain based digital currency or smart contract platform belongs to the public blockchain, while the alliance blockchain requires a coalition of interests to jointly maintain the operation. This paper discusses the main technique and applications of blockchain technology, including mainstream consensus mechanisms, data encryption mechanisms, and parallel blockchain.[10]

The Internet of Things (IoT) has enabled the connection of billions of physical devices, smart meters, wireless temperature sensors, and intelligent vehicle accessories, leading to the emergence of different technologies. One of these technologies is the blockchain, which is a distributed database that can fully remedy the global economic system. However, existing methods suffer from limitations such as low throughput, complexity of consensus algorithms, scalability and overload, and limited bandwidth and information processing capability. Previous methods only addressed device authentication to check if they can be trusted or not. The proposed CBcA method has been evaluated in both cases of authorization and the transmission of device blocks and the transmitted data. It solves the limitations and problems that existed in the previous methods by using an identitybased signature to secure connections between nodes in the blockchain platform. It also prevents the exchange of information between malicious nodes against the resources of each node in the network, resulting in improved scalability and reduced complexity of the hyper ledger algorithm. This paper discusses the proposed CBcA method for securing communication between IoT devices, which uses the SHA256 hashing mechanism to improve scalability and reduce the complexity of the consensus algorithm. The first step of the proposed method deals with the authentication of each device using the identity-based identity-based system. The paper also explains how IoT and blockchains can be integrated to create a fully distributed, secure, and low latency ecosystem.[11]

This suggested study presents a private blockchain based encryption framework using a computational intelligence approach, which scales effetely as datasets develop and is easier to use and more stable than other protection systems. The detection accuracy of the resulting security system is 0.93 in the training phase and 0.91 in the validation phase, which is higher than earlier printed systems. [12]

The Internet of Things (IoT) is an object used to connect various devices in a network to get data through the internet. Blockchain technology is being used for other purposes, such as healthcare, transportation, IoT, and other fields. Singh et al. conducted research about using blockchain technology to secure data on IoT. The research was conducted by making secure communication simulations of two IoT devices without and using blockchain technology. The results showed that the IoT system using blockchain technology has a higher level of security than the IoT system without, as demonstrated by testing of attack simulations and observations of avalanche effects.[13]

DOI:

This paper addresses the problem of providing identity privacy and transaction security in decentralized energy trading using a decentralized approach. It uses public key cryptography to provide a certain level of security and integrity of information, but the most important issue when dealing with public keys is ensuring their authenticity without relying on a trusted third party. This article discusses a trading system that enables peers to anonymously negotiate energy prices and securely perform trading transactions. It uses blockchain technology, multi-signatures and anonymous encrypted message propagation streams to provide certain levels of privacy and security. The system is resistant to known attacks, does not reveal identities of trading parties, and keeps financial profiles secure and private. It is a feasible and reliable direction towards decentralized energy trading with higher privacy and security compared to traditional centralized trading solutions.[14]

A study by Rakesh, Shadakshari et al [16] a novel distributed and tamper proof media transaction framework based on blockchain architecture to address the lack of self-retrievable information of transaction trails or content modification histories. It uses compressive sensing to detect tampering and retrieve original content.[15]

III. STUDIES BASED ON IMAGE ENCRYPTION

Ciphering medical images is an important issue, as the size of image data is much larger than text data. To minimize the time to encrypt and transfer images, it is important to choose a robust, rapid and easy method to implement cryptosystem. To transfer medical images without losses, crypto-compression is an interesting solution with a rate varying between 1.3 and 3.8. The quality of the encryption depends on the chosen crypto-system, as encryption increases the entropy of the image and thus the number of bits necessary by pixel.[16]

The contents in [18] propose a new image encryption technique using 2-D chaotic Henon map, Hilbert curve and cyclic shift operation to ensure both pixel level and bit level permutation. SCAN patterns are used for pixel scrambling process, while the random key stream is generated from randomized bit pattern method. The proposed method uses the previous pixel value, one element from the key stream and a secret value to achieve good confusion and diffusion properties. It can efficiently resist common security attacks such as statistical attack, entropy attack, differential attack and chosen plaintext attack.[17]

Cryptography is a technique used to protect sensitive data from hackers by encrypting the text message from readable form into unreadable form. This paper proposes a hybrid encryption technique based on the Text-to-Image Encryption Algorithm (TTIE) and the Diffie Hellman technique. The total number of permutations is approximately 3.1489941982705027534465953480025 e +212Enhancements are carried out on the TTIE encryption algorithm by adding a new level of security. The proposed technique is evaluated by decrypting the message sent by the sender and retrieving the original message.[18]

Encryption is a common technique used to protect multimedia image security in storage and transmission over the network. Vector quantization (VQ) is the main encryption technique, while a symmetric block encryption algorithm creates a chaotic map. There have been many other image encryption algorithms proposed, such as block cipher, selective encryption, and video encryption. A new uniform scrambling and block-based image shuffling is proposed to achieve a good shuffling effect. Encryption is a common technique used to protect multimedia image security in storage and transmission over the network. It has applications in various fields, such as internet communication, medical imaging and military communication. Vector quantization (VQ) is the main encryption technique, while a symmetric block encryption algorithm creates a chaotic map. Other image encryption algorithms have been proposed, such as block cipher and selective encryption. A new uniform scrambling and block-based image shuffling is proposed to achieve a good shuffling effect and the encryption of the shuffled image is performed using a chaotic map to enforce the security of the proposed encryption.[19]

Data is one of the essential assets for all enterprises and is required to be effectively protected. There are various forms of data security algorithms, each with its own scope of application, beneficial factors, and limiting factors. Information Security is the procedures and approaches used to secure sensitive, private and confidential information from illegal access, usage, misappropriation, revelation, obliteration, alteration, and availability. In open environments, there are several security problems associated with the processing and transmission of digital images, so it is necessary to affirm the integrity and confidentiality of the data. The proposed paper presents a model where deep learning-chaos map can be used to strengthen the encryption performance of digital images by balancing security demands and image quality demands. Deep neural networks are found to offer better results even in unstructured data with complete independence towards data labelling, and chaotic behavior offers extensive security. This paper discusses different techniques for detection schemes used in power transmission lines and proposes a unique mechanism of performing image security with deep neural network. It uses stacked encoder and enhanced chaotic map to overcome the iterative problem of

DOI:

feed-forward and generate better results than other machine learning approaches.[20]

An optical image encryption algorithm using hyper-chaotic systemand public key cryptography theory is used to create an asymmetric encryption system. The algorithm uses double random phase encoding in Fresnel domain to encrypt the key sequences and Fresnel diffraction parameters, and the RSA algorithm is used to asymmetrically encode the key sequence to obtain the corresponding public and private keys. The feasibility, security and robustness of the proposed algorithm are verified by numerical simulation experiments, and it can effectively resist statistical analysis attacks, differential attacks and noise attacks, and has high operational efficiency. It also solves the problem of secure transmission and distribution of keys in optical encryption systems and has high security and certain practicability.[21]

Chaotic cryptography has been extended to image and video encryption schemes, spreading out the pseudo random number base to a wide flat spread spectrum in terms of time and space. This proposed chaos-based image cipher is suitable for applications like wireless communications and will be implemented and tested in FPGA hardware.[22]

Digital information sharing is increasingly common, but it is important to keep sensitive information secure from unauthorized access. Traditional encryption algorithms are not suitable for image encryption due to bulk data capacities and high correlations among pixels. The proposed encryption system based on chaotic standard map has a satisfactory security level with a low computational complexity, making it a good candidate for real-time secure image transmission applications.[23]

Image encryption is a scientific issue that has become increasingly important in recent decades. Traditional encryption algorithms such as the Data Encryption Standard (Davies, 1981) and River–Shamir–Adlemaare are not always secure for image encryption, so new efficient techniques have been developed. One of the most used kinds of encryption schemes is based on chaotic signals, which have the characteristics of ergodicity, randomicity and regularity, and pixels hold the characteristic of discrete distribution. Chaos in fractional differential equations (FDEs) has gained much attention and some real applications have been suggested, but the main difficulty is to obtain numerical solutions. This paper discusses the use of fractional chaotic maps to develop a novel image encryption scheme. It uses the fractional chaotic time series in the scrambling technique and proposes a new encryption technique based on chaotic maps of integer order, which has the following characteristics: a parameter which can be varied from zero to one while the case of ¼ 1 shrinks to encryption schemes using classical maps.[24]

IV. Conclusion

It can be concluded that blockchain technology can provide a secure and decentralized platform for encrypting and storing digital images. The immutability and transparency features of blockchain can ensure the authenticity and integrity of the encrypted images. However, the paper also highlighted some challenges and limitations of using blockchain for image encryption, such as the high computational and storage requirements, the scalability issues of blockchain networks, and the complexity of implementing and integrating blockchain based solutions with existing systems. Overall, blockchainbased image encryption has the potential to address some of the security and privacy concerns related to digital image transmission and storage. However, further research and development are needed to improve the scalability, efficiency, and usability of blockchain-based image encryption solutions.

V. References

[1] Khan, P.W.; Byun, Y. A Blockchain-Based Secure Image Encryption Scheme for the Industrial Internet ofThings.Entropy2020,22,175.https://doi.org/10.3390/e22020175

[2] Alohali, M. A., Aljebreen, M., Al-Mutiri, F., Othman, M., Motwakel, A., Alsaid, M. I Osman, A. E. (2023). Blockchain Driven Image Encryption Process with Arithmetic Optimization Algorithm for Security in Emerging Virtual Environments. Sustainability, 15(6), 5133.

[3] Li, X., Li, J., Yu, F., Fu, X., Yang, J., Chen, Y. (2021, May). BEIR: A Blockchain-based Encrypted Image Retrieval Scheme. In 2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD) pp. 452-457). IEEE.

[4] Li, R. (2021). Fingerprint-related chaotic image encryption scheme based on blockchain framework. Multimedia Tools and Applications, 80, 30583-30603.

[5] Feixiang, Z., Mingzhe, L., Kun, W., Hong, Z. (2021). Color image encryption via Henon-zigzag ´ map and chaotic restricted Boltzmann machine over Blockchain. Optics Laser Technology, 135, 106610.

[6] Acharya, M., Sharma, R. S. (2021). A novel image encryption based on feedback carry shift register and blockchain for secure communication. International Journal of Applied Engineering Research, 16(6), 466-477.

[7] Brabin, D., Ananth, C., Bojjagani, S. (2022). Blockchain based security framework for sharing digital images using

reversible data hiding and encryption. Multimedia Tools and Applications, 81(17), 24721-24738.

[8] Mehta, R., Kapoor, N., Sourav, S., Shorey, R. (2019). Decentralised Image Sharing and Copyright Protection using Blockchain and Perceptual Hashes. 2019 11th International Conference on Communication Systems Networks(COMSNETS).doi:10.1109/comsnets.2019.871 144010.1109/COMSNETS.2019.8711440

[9] Chen, L., Lee, W.-K., Chang, C.-C., Choo, K.-K. R., Zhang, N. (2019). Blockchain based searchable encryption for electronic health record sharing. Future GenerationComputerSystems.doi:10.1016/j.future.2019.0 1.01810.1016/j.future.2019.01.018

[10] Guo, L., Xie, H., Li, Y. (2019). Data Encryption based Blockchain and Privacy Preserving Mechanisms towards Big Data. Journal of Visual Communication and Image Representation,102741.doi:10.1016/j.jvcir.2019.1027411 0.1016/j.jvcir.2019.102741

[11] Fotohi, R., Shams Aliee, F. (2021). Securing communication between things using blockchain technology based on authentication and SHA-256 to improving scalability in large-scale IoT. Computer Networks,197,108331.doi:10.1016/j.comnet.2021.108331 10.1016/j.comnet.2021.108331

[12] Ghazal, T. M., Hasan, M. K., Abdullah, S. N. H. S., Bakar, K. A. A., Al Hamadi, H. (2022). Private blockchain-based encryption framework using computational intelligence approach. Egyptian Informatics Journal, 23(4), 69-75.

[13] Fakhri, D., Mutijarsa, K. (2018). Secure IoT Communication using Blockchain Technology. 2018 International Symposium on Electronics and Smart Devices (ISESD). doi:10.1109/isesd.2018.8605485 10.1109/ISESD.2018.8605485

[14] N. Z. Aitzhan and D. Svetinovic, "Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams," in IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 5, pp.840-852, 1 Sept.-Oct. 2018, doi: 10.1109/TDSC.2016.2616861

[15] Bhowmik, D., Feng, T. (2017). The multimedia blockchain: A distributed and tamper-proof media transaction framework. 2017 22nd International Conference on Digital Signal Processing (DSP). doi:10.1109/icdsp.2017.809605110.1109/ICDSP.2017.80 96051

[16] Jean-Claude Borie, William Puech, Michel Dumas. Crypto-Compression System for Secure Transfer of Medical Images. MEDSIP: Medical Image and Signal Processing, Sep 2004, Malte, France. pp.327- 331. fflirmm00108807f

[17] K.U., S., Mohamed, A. (2020). A novel image encryption scheme using both pixel level and bit level permutation with chaotic map. Applied Soft Computing, 106162. doi:10.1016/j.asoc.2020.106162 10.1016/j.asoc.2020.106162

[18] Abusukhon, A., Anwar, M. N., Mohammad, Z., Alghannam, B. (2019). A hybrid network security algorithm based on Diffie Hellman and Text-to-Image Encryption algorithm. Journal of Discrete Mathematical Sciences and Cryptography,1–17. doi:10.1080/09720529.2019.1569821 10.1080/09720529.2019.1569821

[19] Rakesh, S., Kaller, A. A., Shadakshari, B. C., Annappa, B. (2012). Image encryption using block based uniform scrambling and chaotic logistic mapping. International Journal on Cryptography and Information Security, 2(1), 49-57.

[20] Maniyath, S. R., V, T. (2020). An efficient image encryption using deep neural network and chaotic map. Microprocessors and Microsystems, 77, 103134. doi:10.1016/j.micpro.2020.103134 10.1016/j.micpro.2020.103134

[21] Liu, Y., Jiang, Z., Xu, X., Zhang, F., Xu, J. (2020). Optical image encryption algorithm based on hyper-chaos and public key cryptography. Optics Laser Technology, 127,106171.doi:10.1016/j.optlastec.2020.10617110.1016/ j.optlastec.2020.106171

[22] Sathishkumar, G. A., Sriraam, D. N. (2011). Image encryption based on diffusion and multiple chaotic maps. ArXiv preprint arXiv:1103.3792.

[23] Avasare, M. G., Kelkar, V. V. (2015). Image encryption using chaos theory. 2015 International Conference on Communication, Information Computing Technology (ICCICT).doi:10.1109/iccict.2015.704568710.1109/iccict. 2015.7045687

[24] Wu, G.-C., Baleanu, D., Lin, Z.-X. (2015). Image encryption technique based on fractional chaotic time series. Journal of Vibration and Control, 22(8), 2092–2099. doi:10.1177/1077546315574649 10.1177/107754631557464