EasyChair Preprint

№ 9219

# A Study of Image Encryption Based on Blockchain

V Niranjani, C Chandiya, D Dhanushya and G Harithaa



November 1, 2022

# A STUDY OF IMAGE ENCRYPTION BASED ON BLOCKCHAIN

*Niranjani V[1] , Chandiya C[2] , Dhanushya D[3] , Harithaa G[4]*

*[1] Assistant Professor, [2,3,4] UG Scholar*
*Department of Computer Science and Engineering,*
*Sri Eshwar College of Engineering,*
*Coimbatore, Tamil Nadu, India.*

.

***Abstract---*** ***Nowadays, the majority of the data on the internet is multimedia. Protecting that data is our top priority. On occasion, new methods for encrypting and decrypting images to make them more secure are discovered and created. A large percentage of encryption methods require secret keys to guard against unauthorized access to the data. Many techniques and algorithms for image encryption have been proposed. As we examine many research articles on various forms of encryption for storing and sending massive amounts of data. Here we attempt to use two different algorithms for security and encryption and decryption purposes. For security, we are using Reversible Data Hiding and for encryption and decryption, we use using Rivest Shamir Adleman algorithm.***

***Keywords---Encryption; Decryption; Security; Transmission; Compression; Capacity; Image Encryption***

## I. INTRODUCTION

Image is very important in day-to-day life. It is very important to secure our Images. Image encryption is the technique of encrypting confidential images using an encryption method so that only authorized users may decipher them. For images that are stored on laptops, smartphones, or in the cloud, encryption gives us an extra layer of security. Image Encryption is very important to protect our information from Third party. Cryptography plays an important role in the security field. A complicated form to track information and communication protection is called cryptography. Many algorithms have been used to encrypt and decrypt messages. Several security problems are associated with image processing so it is important to maintain Integrity. Encryption is a very common technique that is used everywhere. It is the technology of encrypting the original data. Data security can be preserved if the encryption method has a high level of security.

Cryptography is the method of protecting information through the use of codes so that only the person who requires information can process it and read it. It is a set of calculations based on the rules called algorithms. These algorithms make use of cryptographic keys, digital signatures, browsing on the internet online, and private communications including credit card transactions and email.

The fields of cryptanalysis and cryptology are connected to cryptography. It covers methods to conceal information in storage or transit including microdots, word-image fusion, and other methods. The four main concerns of Cryptography are:

1. Confidentiality.
2. Integrity.
3. non-repudiation.
4. Authentication.

Cryptosystems are collections of many cryptographic algorithms. These algorithms are used to encrypt or decrypt messages to secure communications. A cipher suite employs two different algorithms: one for encryption and the other for key exchange and another for message authentication. Single-key or symmetric-key encryption techniques employ a block cipher and a secret key that the transmitter and receiver utilize for encryption and decryption of data, respectively. A public key linked to the sender is used to encrypt messages, and a private key is used to decrypt that information

A blockchain is defined as a chain of blocks that contains information. It is distributed ledger technology (DLT) that holds various records that are linked together using Cryptography. It is one-to-one computer network that is used for the secure transfer of data without requiring third parties. It is challenging to modify data once it has been stored on a blockchain.

It comprises databases, computers, and software applications. The initial block is called as the Genesis block. Each block is connected to the one before it. Blocks are used to record transactions across multiple computers so that particular blocks cannot be altered without the alteration of the subsequence block. The Main advantage of blockchain is Reliability, Fraud Prevention, Collaboration, and Decentralized. It is used in different sectors which include Markets, Government Sector, health, etc.

Rivest-Shamir-Adleman (RSA) encryption algorithm works with two separate keys and is called an asymmetric cryptography algorithm. It employs two keys, private key and then public key. Private key can only be used by those with authority and a public key can be used by anyone. This algorithm uses logarithmic functions to resist brute force. RSA consists of two main parts: When data needs to be recovered after being scrambled, the method of encryption and decryption must be used, key creation is what is used to produce those keys. After embedded information has been extracted Data Hiding (RDH) is used to exact restoration of the original signal. It embeds bits by altering the host signal. The reversible data hiding scheme provides lesser complexity and perceptibility.

## II. RELATED WORKS

Images are stored on the blockchain based on pixel values, preserving the safety and privacy of the pictures.. Khan, depending on the change in pixel numbers and information entropy, strength of the algorithm was evaluated by comparing it with differential attacks [ 1]. The concept of blockchain decentralization and tamper protection is used [2]. Li, Xianxian method has more reliability and high search efficiency and schema accuracy, and good privacy protection effect.

A system based on cryptography techniques named classical and quantum cryptography is used. Pawar Cryptography deals with mathematics and computational efficiency. Photon polarization and uncertainty principle are used in quantum cryptography [3] for the internet's safe data transmission.

Encryption of digital fingerprints is used to secure Images [4]. The algorithm uses a chaotic map for encoding the pixel addresses of the fingerprint and scrambling pixel values and increasing security. A bit-level permutation is used. Liu algorithm is a combination of mixing and confusing processes. For encoding, pixel addresses Chaotic map is used and to scramble pixel values and increase security bit-level permutation is used.

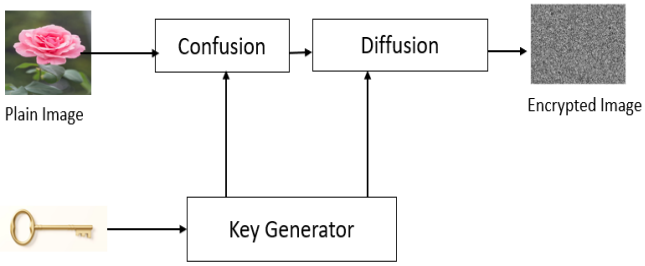


Fig. 1 Image for encryption process [4]

An approach named a secret sharing scheme is implemented [5] BWM, AS and character relocation Techniques are used for Image and text key encryption. Das attempt is made to increase safety and security. The picture key size is the restriction and it must be less than the original image. The digital encryption technique called the image-processing technique is used [6]. Pan demonstrates a spatial advantage in terms of image security and dependability.

The logistic chaotic mapping and DNA technique is used in [7]. The logistic chaotic mapping by inserting a real DNA chain into the image which is mainly used for image encryption. After that, the DNA and logistic method are collaborated by inserting a new algorithm by which we can easily encrypt the grayscale image. Zhang enlarges the key space and also reduces the attacks.

For image encryption and storage, the SMS4 commercial cipher algorithm is used in [8], which will accomplish image encryption and decryption. Lei also amplify the functions and also based on this system they provide the designing of commercial cipher products. MATLAB is very efficient in performing mathematical operations mainly for arrays and matrices and is easy to implement [9]. Qu Ding by using the histogram and key sensitivity analysis the best-encrypted image is attained and has a strong base for image encryption on software and hardware.

Edge information algorithm is used in [10]. Image salient regions always have more important information than edge information. Wen for generating sensible ciphertexts visually salient region encryption to encrypt and decrypt the visually meaningful cipher text. thus, the salient regions of the natural images were hidden.

Color image encryption which uses the AES algorithm for encryption is used [11]. The intensity values of pixels are calculated by using a hen on-chaotic map and Nayak uses two chaotic maps. Key Space is large and protects from Brute force attacks.

Based encryption technique is used where Pixel values are used in multiple locations using the affine transform technique [12] After that, each block of two pixels

from the modified image is encrypted using the XOR technique. Nag Any large-scale image can be secured by using encryption and decryption methods. A hybrid technique to image encryption that combines steganography with encryption is employed [13]. A modification to AES called Modified AES (MAES) is used. Saini, improved shift row transformation that increases AES security Multiple secret images are used by using a huge cover image.

Chaotic based FGPA implementation by Advanced Encryption Standard (AES) with pipeline techniques is used [14] Parallel memories are used to implement each round which increase the speed. Shah use Key expansion which is synchronized with a Round unit to ensure availability of a Round key in every clock.

8-bit color images are encrypted using bidirectional diffusion-based image encryption.[15] Images are compressed to make them smaller and accelerate the transmission speed, Ravi uses Bidirectional diffusion-based encryption then compression. The image is reduced into larger number of small blocks.

A method known as chaotic key sequence generation, which is produced by states of the application by using linear feedback shifting register with logistic map creation. [18]. Image encryption and images are stitched in this method. It will also be able to transfer many images at time. For higher order protection and large size image transport it is mostly used.

Image encryption involves three steps [19]. Twister PRNG and S-box is used. To estimate the scheme's performance, various measurements and studies are done. Using chaotic maps, a diffusion-based encryption technique is employed [16]. The S-box is first created using a chaotic map, and then the pixel values are changed to create a non-linearity element. Then, another random sequence with modified values is produced using the standard logistic chaotic map. The pre-encrypted images' color components are then combined to generate a set of random, uniformly dispersed images.

## III. METHODOLOGY

The approach has four steps: identification, choice, assessment, and validation. Using a multi-criteria choice process, like the Simple Multi Criteria decision Rating Technique, an acceptable Distributed Ledger platform is chosen. After the available blockchain platforms have been identified. The chosen system is then thoroughly assessed taking into account the system architecture, libraries, tools, applications that are specific to a given area, and capabilities analysis of the chosen blockchain platform. The creation of an enterprise solution based on blockchain has validated the suggested methodology. Regardless of the scale, any stakeholder might choose an appropriate blockchain platform to construct a blockchain application using the process protocol outlined.

By creating a secure and transparent environment for the exchange of digital currencies like Bitcoin, blockchain technology works. Records are protected by the hash codes that every block in the blockchain uses. This is primarily caused by the identical length of hash codes produced by hash functions. Any attempt to change a block of data would produce a fresh hash value. Undoubtedly, trust issues arise with a network that is open to all users and preserves privacy protection. Therefore, in order to establish confidence, players must go through a number of consensus methods, including Proof of Work and Stake.

Asset tracking is made easier by the distributed, immutable database known as blockchain and the recording of transactions inside a business network. A blockchain network allows for the recording and trading of almost everything of value, diminishing risk and increasing efficiency for over all users.

cryptocurrency is the first digital money to leverage blockchain technology. Peer to peer internet transactions is made possible by this digital store of value without the use of an intermediary. The blockchain network is a distributed system made up of nodes (computers) that examine and evaluate any new transactions that are undertaken Several consensus models are employed in conjunction with the mining approach to reach this combined agreement. The difficult computational issue has taken a lot of work from each node trying to add a new transaction, as demonstrated by the mining process, and is thus entitled to payment. The requirements must be verified by the network before a transaction may be accepted as legitimate.

There is enough bitcoin on the sender account to complete the intended transfer. The intended recipient has not received the intended payment in transmission. A transaction is added to the digital ledger and encrypted using cryptography after it has been verified and approved by all nodes. A public key used in cryptography is accessible to all, where as a secret private key is maintained as secret. To preserve those transactions involving that currency on the blockchain network, a digital wallet is utilized to store, send, and receive it. Each block in the blockchain has a public address that is a collection of characters. The Bitcoin cash is allocated to the wallet's public address when a transaction is made using this public address. The wallet's private key, which acts as the user's digital signature and is utilized to confirm the execution of each transaction, it is employed to demonstrate who is the owner of the public address. The user's secret key must be used before creating the decryption key. The secret key was compressed using sophisticated mathematical techniques.

**Data Embedding Procedure**: To guarantee the necessary confidentiality, the RSA algorithm is used which encrypt the image before the data concealing operation. Reversible data hiding undergoes two steps for encrypting image. To boost the overall embedding capacity, the first watermark is embedded using the bit substitution method in the first phase and the second watermark is inserted using the histogram shifting approach in the next phase. step 1: The original picture is fully encrypted by RSA encryption using a secret key matrix that is the same size as the image. Only the sender, who encrypts the data, is aware of the secret key matrix, which the receiver also needs to be aware of the order to restore the original plain image. step 2: The encrypted image is broken up into portions of the same size that don't overlap on each other in order to add the first watermark. step 3: The number of bits that can be inserted will change depending on the size of the image. Adding a second watermark will boost the encrypted image's overall embedding capacity by increasing the number of embedded bits. Using the histogram shifting technique, the watermark is included into the watermarked encrypted image and operations are performed.

## IV. CASE STUDY

Security is a key issue in todays and future networks. Blockchain will be the technology of choice for secure information exchange in future networks. Attackers using the internet mostly target on digital photos. The security framework for exchanging digital photographs in a multi user setting is based on blockchain technology. Reversible data hiding and encryption are used as part of the framework. New schemes have also been proposed for reversibly hiding large amounts of data to secure images. Reversible data hiding and encryption work together to safeguard the authenticity, confidentiality, and integrity of digital images. Some methods involve first compressing the digital image to make room for data hiding, and then adding the user's signature. The entire image is then encrypted. It uses lossy JPEG compression to create large volumes. Any stream cypher or symmetric block cypher may be used for encryption. Reversible data hiding strategy offers great capacity and image quality, while the blockchain-based framework offers excellent security.

## V. CONCLUSION

From the study of various papers, image encryption was done by many algorithms like Advanced Encrypted Standard (AES) which was highly efficient and used 128-bit format, Triple DES which is advanced of DES and uses three individual keys, Chaotic map is used for encoding the pixel, RSA which uses a pair of keys for encryption. The algorithms which are used in many places provides a less level of a security. The digital image security is very important in today's digital environment as a result of communications of digital resources via open networks occur on increasing basis. In order to make the image more secure, we are going to propose a system which uses two algorithms, Reversible data hiding for Security and RSA algorithm for encryption and Decryption. This will provide more security to our image.

## VI. REFERENCES


[1] Khan, Prince Waqas, and Yungcheol Byun. "A blockchain-based secure image encryption scheme for the industrial Internet of Things." Entropy 22, no. 2 (2020): 175.

[2] Li, Xianxian, Jie Li, Feng Yu, Xuemei Fu, JunHao Yang, and Yue Chen. "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, 2021.

[3] Pawar, Harshad R., and Dinesh G. Harkut. "Classical and quantum cryptography for image encryption & decryption." In 2018 International Conference on Research in Intelligent and Computing in Engineering (RICE), pp. 1-4. IEEE, 2018..

[4] Liu, Rui. "Chaos-based fingerprint images encryption using symmetric cryptography." In 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery, pp. 2153-2156. IEEE, 2012.

[5] Das, Ramkrishna, Sarbajit Manna, and Saurabh Dutta."Cumulative image encryption approach based on user defined operation, character repositioning, text key and image key encryption technique and secret sharing scheme." In 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), pp. 748-753. IEEE, 2017.

[6] Pan, Hailan, Yongmei Lei, and Chen Jian. "Research on digital image encryption algorithm based on double logistic chaotic map." EURASIP Journal on Image and Video Processing 2018, no. 1 (2018): 1-10.

[7] Zhang, Tian Tian, Shan Jun Yan, Cheng Yan Gu, Ran Ren, and Kai Xin Liao. "Research on image encryption based on dna sequence and chaos theory." In Journal of Physics: Conference Series, vol. 1004, no. 1, p. 012023. IOP Publishing, 2018.

[8] Lei, Zhang, Li Li, and Gao Xianwei. "Design and realization of image encryption system based on SMS4 commercial cipher algorithm." In 2011 4th International Congress on Image and Signal Processing, vol. 2, pp. 741-744. IEEE, 2011.

[9] Zhang, Qi, and Qun Ding. "Digital image encryption based on advanced encryption standard (AES)." In 2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC), pp. 1218-1221. IEEE, 2015.

[10] Wen, Wenying, Yushu Zhang, Yuming Fang, and Zhijun Fang. "A novel selective image encryption method based on saliency detection." In 2016 Visual Communications and Image Processing (VCIP), pp. 1-4. IEEE, 2016.

[11] Nayak, Pragyanshree, Sanjeet Kumar Nayak, and Satyabrata Das. "A secure and efficient color image encryption scheme based on two chaotic systems and advanced encryption standard." In 2018 International conference on advances in computing, communications and informatics (ICACCI), pp. 412-418. IEEE, 2018.

[12] Nag, Amitava, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar, and Partha Pratim Sarkar. "Image encryption using affine transform and XOR operation." In 2011 International conference on signal processing, communication, computing and networking technologies, pp. 309-312. IEEE, 2011.

[13] Saini, Jaspal Kaur, and Harsh K. Verma. "A hybrid approach for image security by combining encryption and steganography." In 2013 IEEE second international conference on image information processing (ICIIP-2013), pp. 607-611. IEEE, 2013.

[14] Shah, Syed Shahzad Hussain, and Gulistan Raja. "FPGA implementation of chaotic based AES image encryption algorithm." In 2015 IEEE International Conference on Signal and Image Processing Applications (ICSIPA), pp. 574-577. IEEE, 2015.

[15] Sreelakshmi, K., and Renjith V. Ravi. "An encryption-then-compression scheme using autoencoder based image compression for color images." In 2020 7th International Conference on Smart Structures and Systems (ICSSS), pp. 1-5. IEEE, 2020.

[16] Luo, Yuling, Minghui Du, and Dong Liu. "JPEG image encryption algorithm based on spatiotemporal chaos." In 2012 Fifth International Workshop on Chaos-fractals Theories and Applications, pp. 191-195. IEEE, 2012.

[17] Ali, Tahir Sajjad, and Rashid Ali. "A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box." Multimedia Tools and Applications (2022): 1-25.

[18] Kankonkar, Jyoti TG, and Nitesh Naik. "Image security using image encryption and image stitching." In 2017 International Conference on Computing Methodologies and Communication (ICCMC), pp. 151-154. IEEE, 2017.

[19] Gabr, Mohamed, Wassim Alexan, Kareem Moussa, Belal Maged, and AlHussain Mezar. "Multi-Stage RGB Image Encryption." In 2022 International Telecommunications Conference (ITC-Egypt), pp. 1-6. IEEE, 2022.

[20] Morales, Y., L. Díaz, and C. Torres. "Radial Hilbert transform in terms of the Fourier transform applied to image encryption." In Journal of physics: Conference series, vol. 582, no. 1, p. 012063. IOP Publishing,2015..

[21] https://www.investopedia.com/terms/b/blockchain. asp

[22] https://en.wikipedia.org/wiki/Blockchain

[23] https://scialert.net/fulltext/?doi=jai.2014.123.135

[24] M. AL-Laham Mohamad, “Encryption-decryption RGB color image using matrix multiplication”, International Journal of Computer Science & InformationTechnology (IJCSIT), Vol. 7, No 5, October 2015.

[25] Saksham Wason, Piyush Kumar and Shubham Rathi, “Text and image encryption using color image as a key”, International Journal of Innovative Research in Technology (IJIRT), 2014.