Encrypted Image Retrieval Scheme on Blockchain

[1]NiranjaniV, [2]Chandiya C, [3]Dhanushya D and [4]Harithaa G
[1,2,3,4]Department of Computer Science and Engineering, Sri Eshwar College of Engineering, Coimbatore, India.
[1]niranjani.v@sece.ac.in,[2]chandiya.c2019cse@sece.ac.in,[3]dhanushya.d2019cse@sece.ac.in,[4]harithaa.g@sece.ac.in

Article Info
A. Haldorai et al. (eds.),*2nd International Conference on Materials Science and Sustainable Manufacturing Technology,*
Advances in Computational Intelligence in Materials Science.
Doi:https://doi.org/10.53759/acims/978-9914-9946-9-8_7
©2023TheAuthors.PublishedbyAnaPubPublications.
This is an open access article under the CC BY-NC-ND license. (http://creativecommons.org/licenses/by-nc-nd/4.0/)

Abstract- Blockchainhas flourished in a variety of industries throughout a period known as the "digital economy", including finance and digital copyright. Blockchain is highlighting the storage issue more and more. In order to lessen the demand for node storage, the existing blockchain maintains block information in external storage devices. Blockchain transaction retrieval issue is brought on by the new blockchain storage approach. The issue arises when the user is required to download the decentralized blockchain ledger information from the external storage system. Since, they couldn't locate the node comprising that particular transaction, therefore which results in significant communication overhead. We take advantage of the data that is Blockchain is semi-structured for this issue and obtain the common traits of blockchain transactions like the Date and account address. Next, we create a method for retrieving blockchain transactions. Because of the absence of an effective account-specific secondary search data structure addresses, we suggest the scalable B+ tree. For encryption and decryption of Images we have used Elliptic curve Cryptography algorithm and AES algorithm. For Generating Hash value we have used ECDSA Algorithm.

Keywords–Security; Compression, Transmission,Image Encryption and Decryption, Capacity,Decentralization, Smart Contract, Ledger, Tamper-Proof, Proof of Stack.

I. INTRODUCTION

The Satoshi Nakamoto-created Bitcoin project is where the blockchain technology has its roots. The application and exploration of this cutting-edge decentralized ledger technology have yielded impressive results in a variety of industries, including finance, supply chain management, and edge computing. The rapid advancement of blockchain has also made several issues more apparent. Due to the append-only nature of blockchain data, it continuously accumulates, they put a tremendous amount of storage demand on blockchain nodes. Each blockchain node maintains an exact copy of the data in the blockchain ledger. The node's storage is under too much strain. So, Many blockchain nodesmust simultaneously store ledger information, which result in a significant unnecessary storage space. The blockchain system can become centralized, lose its decentralized nature, and become difficult to scale if there is much load on one location for storing. This can prevent preventing brand-new blockchain nodes from joining the network.. Academia have suggested Blockchain node storage strain can be reduced by Blockchain data storageexternal networks with distributed storage, such as IPFS. The fundamental concept behind these cryptocurrency storage options to place the complete block document on the internet tolessen the burden storage nodes on the blockchain.

Using blockchain nodes keeps block a list of the transaction records, and more. In order to make sure the blockchain cannot be altered. In Storage network hash and summary will be used by the blockchain node to verify the block data when accessing the block.As opposed to that, a blockchain is a collection of interconnected blocks that serves as a ledger for transactional data. A blockchain transaction today can enable the transfer of digital money, voucher records, logistical tracking, among other sorts of information recording. The smallest ledger unit is a transaction record.

When ledger data is maintained across a network of external storage, retrieving blockchain transactions becomes more difficult. The issue with retrieving blockchain transactions is caused by the fact that, when the blockchain ledger is stored in external storage networks, blockchain nodes no longer have access to all of the data in the bitcoin nodes and not anymore own local copy of the complete blockchain ledger. Consequently, it has become difficult to retrieve blockchain transactions. The target transaction occurs when users attempt to view the transactional target record, but the blockchain node is unable to locate the requested block that contains it.. In order to view the transaction, blockchain nodes must periodically download the complete from the storage, ledger using blockchain internet, which results in minimal transmission costs and a subpar user experience.

The most crucial component of the retrieving blockchain transactions is difficult to retrieve transactions across several blocks using the attributes of the transaction records. The problem of blockchain retrieval is new, and academia have done a lot of research on it. The present study primarily focus on research into query semantic retrieval function, efficiency improvement of existing blockchain systems and research into blockchain retrieval methods.

The B+ tree as well as the Merkle tree properties are combined to transform the blockchain from a conventional hash-based query to a key-based query. Furthermore, to increase the retrieval effectiveness of the blockchain, this type of research mostly takes into account the addition of other databases or the insertion of redundant data. It will not specifically improve the capacity of retrieval, but the additional cost of the system is reduced. It does not meet the demands of this case and only does optimization at the application layer. Research on blockchain retrieval technique suggests a dual combination bloom filter (DCOMB) approach, in order to increase adaptability, integrates the blockchain's timestamp with the Internet of Things' data stream.

Tu offers a number of options, such as getting account information, creating a reverse index between the block hash and the account address, and managing it utilising a B+ tree. This paper establishes an effective blockchain transaction retrieval method. This method extracts the universal characteristics of blockchain transactions, such as Date and account information, for consequently problem such as retrieving hashing algorithm transactions based on semi-structured blockchain data features. To address the absence of an effective this query structure, this study suggests a further search data structure called the B+ tree, which is scalable and flexible and can manage account addresses. It is based on B+ trees and bloom filters.

A database, on the other side, is made to hold substantially more data so that it may be rapidly and readily accessed, filtered, and changed by multiple users at once.

- Ledger: This is a continuously expanding file.
- Permanent: Once a transaction is recorded in a blockchain, it can be permanently added to the ledger.
- Secure: Blockchain stores data in a safe manner. To make sure that the information is locked inside the blockchain, it uses very sophisticated cryptography.
- Chronological: When a transaction is chronological, it follows the one before it.
- Immutable: This property indicates that as transactions are added to the blockchain, this ledger cannot ever be altered.

A chain of blocks containing information makes up a blockchain. Each block serves as a permanent database for the blockchain and records all of the most recent transactions. A new block is generated each time when the block is finished.

Blockchain, a distributed ledger system, is regarded by its proponents as one of the best methods for transaction security.

II. LITERATURE SURVEY

By storing the images on the manner of pixels the confidentiality are preserved. By comparing Khan's method to differential attacks [1] based on entropy, the method's effectiveness was evaluated. It makes use of the tamper-proof, decentralized blockchain concept [2]. More dependability, high search efficiency, correct schema, and efficient privacy protection are offered by the Li, Xian approach. It makes use of a system built on both traditional and quantum cryptography techniques. Applied cryptography is concerned with math and computing effectiveness. Quantum cryptography [3] uses the uncertainty principle and photon polarization to ensure the security of data transmission over the internet. Pictures are protected through the encryption of digital fingerprints [4].

The approach scrambles the pixel values and encodes the fingerprint's pixel addresses using a chaotic map to increase security. It uses a bit-level permutation. The Liu algorithm combines procedures for blending and perplexing information Pixel addresses are used for encoding. A chaotic map's pixel values are made unpredictable using bit-level permutation to increase security.

Pictures are protected through the encryption of digital fingerprints [4]. The approach scrambles the pixel values and encodes the fingerprint's pixel addresses using a chaotic map to increase security. It uses a bit-level permutation. The Liu algorithm combines procedures for blending and perplexing information. Pixel addresses are used for encoding. Bit-level permutation utilised to confuse values of pixels on chaotic chart and boost security.**Fig 1** shows image utilized in the encryption process.

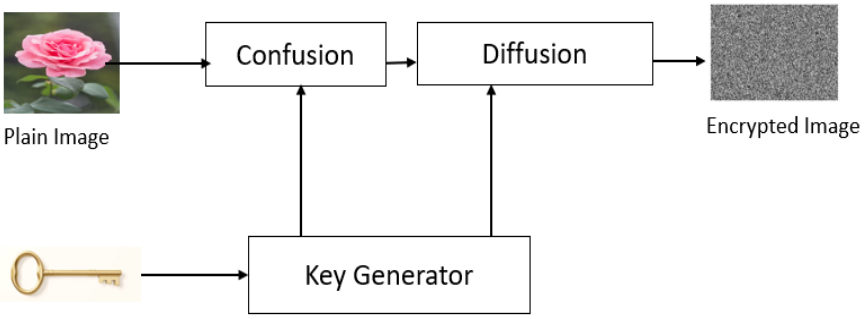

Fig1. Image utilized in the encryption process [4]

The adoption of a secret sharing plan technique [5] feature relocation techniques are employed for picture and encryption. An effort has undertaken to improve the safety. The restriction is that picture key size should be smaller than the original image. [6]. In terms of visual dependability , Pan demonstrates a geographical edge.
Chaos theory and the DNA technique are used in [7]. The erratic map, which is primarily utilised for image encryption. It involves putting a genuine DNA chain into the image. The logistic approach and DNA are then combined, and a new algorithm is inserted to make it possible to quickly encrypt grayscale images. Zhang increases the key space while decreasing attacks.

The SMS4 cypher method is used in [8] for image encryption and storage, allowing for photo encryption and decoding Lei enhances the features and offers the creation of commercial encryption products based on this technology. MATLAB is simple to use and extremely effective at executing mathematical calculations, particularly on arrays and matrices [9].

In [10] Edge information is employed. Edge information is never more essential than the prominent parts of an image. For the purpose of encrypting and decrypting the visually significant cypher text, Wen generates comprehensible ciphertexts. The key areas of the natural photos were therefore obscured. The AES technique for encryption is used to encode colour images [11]. Nayak employs two chaotic maps to calculate the intensity values of each pixel using a hierarchical chaotic map. Large and resistant to brute force strikes is the Key Space.

Using the affine transform technique, based encryption is applied when pixel values are used many times [12]. Steganography and encryption are both used in a hybrid method for image encryption [13]. The Modified AES (MAES) version of AES is employed. Improved shift row transformation with AES security through Saini Using a massive cover image allows for the usage of multiple secret images.

FGPA is implemented using pipeline techniques and the Advanced Encryption Standard (AES) on a chaotic basis [14]. Each round is implemented using parallel memories, which quickens the process. Bidirectional diffusion-based image encryption is used to encrypt images that are 8 bits in color.[15] Ravi compresses photos after bidirectional diffusion-based encryption to reduce file size and increase transmission speed. The image is divided up into several little blocks.

A process for creating chaotic key sequences that uses the application's states to generate logistic maps and linear feedback shifting registers. [18]. This technique stitches images together while encrypting them. Moreover, multiple photos can be transferred at once. It is mostly utilised for higher level protection and large size image transfer.

There are three processes to image encryption [19]. S-box and Twister PRNG are employed. Many measurements and investigations are conducted to gauge the plan's effectiveness. A diffusion method is used with chaotic maps [16]. A chaotic map is used to build the S-box first, and a non-linearity element is then added by altering the pixel values.

III. RESEARCH METHODOLOGIES

A secure picture retrieval system that is being proposed uses the B+ tree and ECDSA algorithm on a blockchain. The hash value is established using ECDSA, and image retrieval using a B+ tree. For encryption and decryption, ECC is utilized. Blockchain have a complex retrieval scenario that calls for a retrieval system with quick, reliable, and dynamic updating capabilities. A set of matching systems is necessary in order to get good retrieval results with outstanding performance.Here, we describe the manner in which the blockchain transaction retrieval system operates. The B+ tree is highly traditional retrieval scheme that supports range retrieval and has the advantage of effective retrieval speed. Addresses of the accounts and hashes of the block are handled as key and value and controlled using the B+ tree in recovery process. The id(address) of the block is fetched as the key during transaction retrieval to acquire the block hash for the full transaction, and linked block. The B+ structured tree uses the account address retrieval items directly due to account address expansion, giving in an extraordinarily big tree structure and search space that actually affect retrieval speed.

Advantages include a high level of security, no application performance issues, a quick procedure for signing and verifying the execution of the expanding application security requirements. This security technique is the most accurate since it's utilized in both software and hardware.**Fig 2** shows image retrieval process.

Steps in this process includes the following:

1. Onceblockchain's higher node module has obtained the block and verified it, the collection module obtains the block, then data is transferred to the storage module for storing the complete block. In parallel, block information is examined to draw out the retrieval-related features of data. This structure's maintenance module receives it from this module in order to create or modify the retrieval structure .Account address are sent to the next module by the block retrieval analysis once it has extracted the retrieval targets.
2. The block must be stored and obtained. The retrieval structure must be updated. A file containing a tracking between the hash and offset is where the block of data obtained from the collection module is saved. Locally and on IPFS, block files can be kept. Once the retrieval module obtains hashes of the block, in which the transaction

record is included. we can access each block through the storage module. This module also stores address of retrieval structure.

3. The mainduty to update time to time and maintain various retrieval structures, including account address followed by timestamp updates and retention of collected retrieval feature information for the proper retrieval structure.
4. The main duty is to find the block holding the transaction data using a single feature alone or a hybrid retrieval with the information from the retrieval feature.

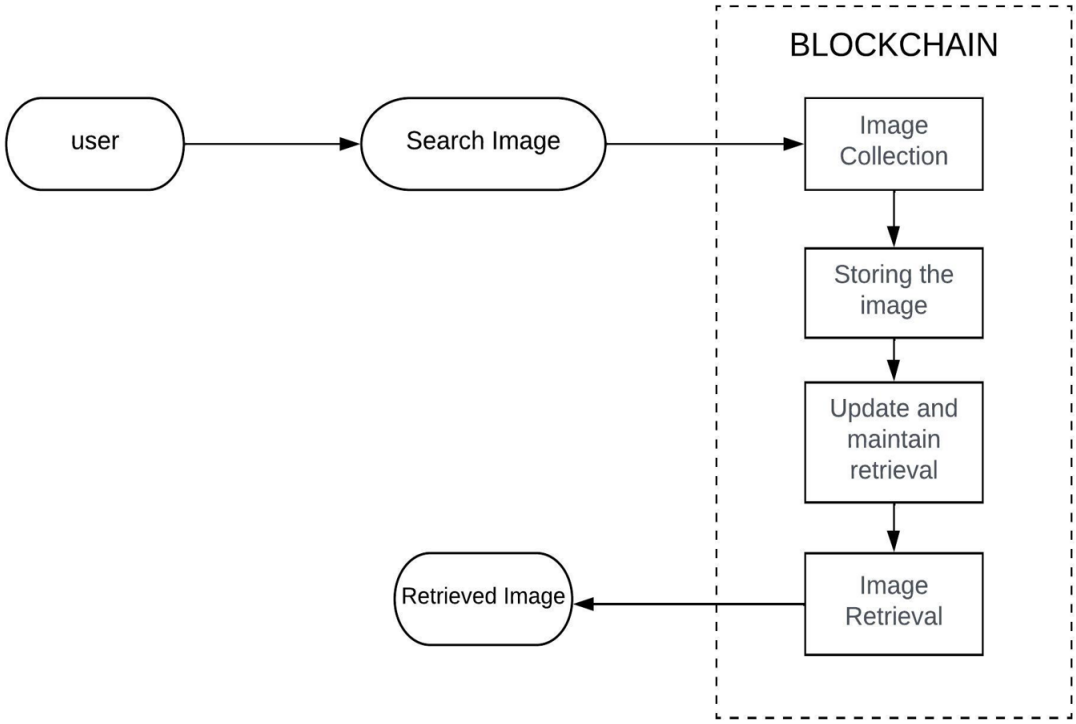

Fig 2. Image retrieval process

Encryption And Decryption Using Elliptic Curve Cryptography(ECC) Algorithm

ECC uses a key-based encryption method to protect the data. For the purposes of decrypting and encrypting online traffic, it focuses on pairs of private and public keys. Like elliptic curve factorization, there are a few integer factorization methods having applications in cryptography.

Steps

These are the ECC domain specifications over HG(r).:

T = (r, b, c, H, o, i)

- r = q or r = 2^n
- b and c ∈ HG(r)

$z^2 \equiv y^3 + by + c \pmod p$ for r = q > 3

$z^2 + yz = y^3 + by^2 + c$ for $r = 2^n \geq 1$

- a base point H = (yH, zH) on F(back)(HG(r)),
- a prime n that corresponds to H's order

(A smallest positive integer s such that sQ = P determines a point Q's order on an elliptic curve.)

i = #F/o. where #F denotes the curve order and reflects number of points on the curve.

An elliptic curve has the following equation:

$Z^2 = y^3 + by + c$

where,

F -> Elliptic Curve

Q -> Points on the curve

o -> Upper limit (That must be prime number)

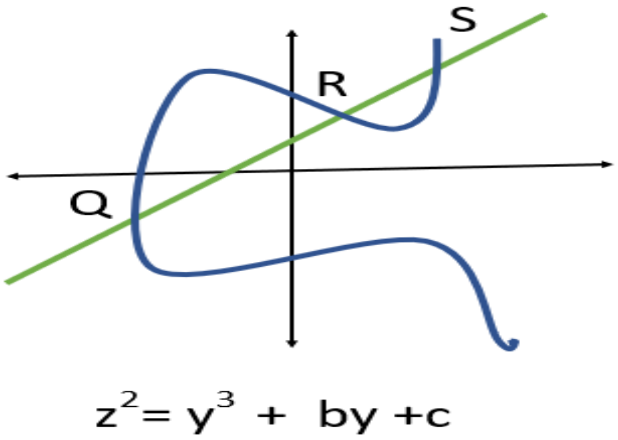

Fig 3. ECC curve

The **Fig 3** denotes the Ecc curve.

Key Generation
Throughout the procedure, both the keys are generated.
The number 'e' must now be selected from the range of 'o' numbers.

The following equation can be used to create the public key.
R = e * Q

e is the random integer we chose at random from the range of (1 to o-1). Q is the curve's pivot point.
"R" stands for public key, and "e" stands for private key.
For an entity B, a public key R = (yQ, zQ) connected to a domain parameter (r, b, c, H, o, I is created.

procedure

- Choose an integer e at random or a pseudo-random number within the range [1, o -1].
- Determine R = eH.
- B's private key is e, while A's public key is R.

ECC Key Validation
A public key is verified using the procedure described below: R = (yQ , zQ) linked to a domain parameter (r, b, c, H, o, I for an entity B:

- Verify that R 1 P.
- Verify that the yQ and zQ elements of the HG are accurately represented (r).
- Verify that R is located on the elliptic curve defined by variables b and c.
- Make sure oR = P.

Encryption
Let us stand up for the message we're trying to get out. The curve must be used to convey this idea.
Think about n having point N on the curve F.
Choose 'l' randomly from the range [1 - (o-1)].
Let D1 and D2 be the two created cypher texts.

D1= l*Q
D2 = N + l*R
D1 and D2 will be send.

Decryption

N = D2 – e * D1

The message "n" that was transmitted to us must be recovered from the "M" that was sent.

Proof
N = D2 – e * D1
'N' can be represented as 'D2 – e * D1′
D2 – e * D1 = (N + l * R) – e * (l * Q)
(D2 = N + I * R and D1 = l * Q)
= N + l * e * Q – e * l *Q (canceling out l * e * Q)
= N (Original Message)

Elliptic Curve Digital Signature Algorithm (ECDSA)
In addition to accessible key (public key) RA and the personal key eA, entity B also contains the domain parameters E = r, b, c, H, o, I and entity C also has copies of E and RA.

A sign m by performing the following:

- Choose l at random from the range [l,o-l].
- Calculate s = y1 mod o and lH = (y1,z1). Go to step 1 if s = 0.
- Determine L-1 mod o. Determine f = SHA-1 (n).
- Determine t = l-1f + eA. s mod o.

Go to step 1 if t = 0.

The message n's signature from B is (s, t).
The following actions are taken by C in order to confirm B's signature (s, t) on n: Check to see if s and t are in range [1,o-1].

Calculate f = SHA-1 (n).

- Determine x=t-1 mod o.
- Calculate the values v1 = fx mod o and v2 = sx mod o.
- Calculate (y1,z1)=v1H+v2RA.
- Determine w = y1 mod o.
- Just accept the signature if w = s.

SHA-1 refers to the hash function's 160 bits.

Elliptic Curve Authenticated Encryption Scheme (ECAES)
B performs the actions for C to encrypt the message:

- Selects an integer s at random from the range [1, o-1].
- Determine S = sH.
- Determine L = isRB = (LX, LY). Verify that L 1 P:
- Determine l1|| l2 = LEG (LX).
- Calculate d = (l1, n). Calculator u = MAC (l2, d).
- Send S, D, and U to C.

ENS using a symmetric encryption method like Triple-DES
Whereas, MAC is short for the Message Authentication Code.LEG represents a crucial derivation function.

C executes the following in order to decrypt ciphertext (S, d, and u):

- Validate S's partial key.
- Determine L = ieBR = (LX, LY).. Verify that L 1 P:
- Determine l1 || l2 = LEG (LX).
- Make sure u = MAC (l2, d).

Calculate m = ENC-1 (l1, d)

AES Algorithm

The program's basis of multiple replacements, combinations, and linear transformations carried out on 16-byte data items gives rise to the term "block cypher," which refers to the algorithm. The term "rounds" describes how frequently the processes are repeated. The encryption key is used to create a unique round key, which is then utilized in each round's calculations. When compared to traditional stream cyphers, AES has the distinguishing benefit that a single bit change affects the block. Box Cryptor also uses 256bit keys! AES cannot yet be attacked successfully. As a result, international governments, financial organizations, and high security systems continue to favor AES as their preferred encryption standard.

IV. RESULT AND DISCUSSION

Following graph indicates the Encryption time for all techniques. The quickest Encryption time is recorded by the AES-ECC method.**Fig 4** shows comparison for encryption time.

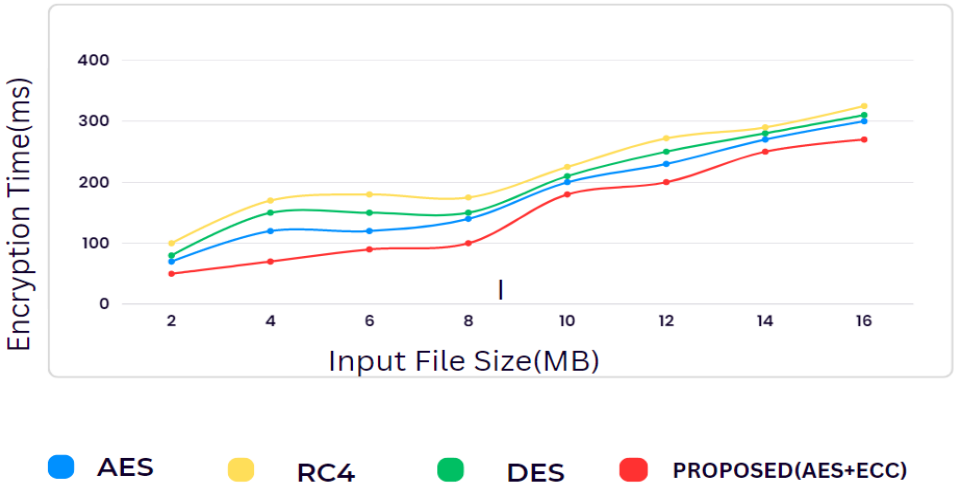

Fig 4. Comparison for Encryption Time

Following graph indicates that the Decryption time for all techniques comparing with image size and time taken to decrypt. The quickest Decryption time is also recorded by the AES-ECC method.**Fig 5** shows comparison for decryption time.

Fig 5. Comparison for Decryption Time

V. CONCLUSION

We proposed an encrypted picture retrieval framework based on blockchain that can address the issue that a rogue cloud servergives inaccurate or partial search outcomes. In addition, we create an index structure utilizing Simhash and BOVW

model toenhance the effectiveness and precision of picture recuperation, and thethis scheme's index generating mechanism is also modularizable into further searchable encryption strategies. Wemerely Wish that additional Blockchain can be used by researchers to address the issues with trust that arise during encrypted picture search, invest more time investigating methods for quicker eventually realise encrypted image retrieval on the blockchain, and more precise encrypted image retrievalWe obviously hope that additional academics will use blockchain to address the issues with trust that arise when searching for encrypted images, invest more time in researching methods for retrieving encrypted images quickly and accurately,and lastly implement encoded picture access on a ledger. As comparison to a regular cloud server,The expense of upholding our anonymityoperations using block chain technology, includingretrieving the unencrypted directory, however, has notoptimum at this time. To further we'll also strive to incorporate trustworthy execution environments safe multi-party computing (SMC), homomorphic encryption, and negligible proofcreating an index, we also investigate feature fusion based on principal component analysis and convolutional neural networks, which has improved similarity matching results.

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]. X. Li, J. Li, F. Yu, X. Fu, J. Yang, and Y. Chen, "BEIR:A Blockchain-based Encrypted Image Retrieval Scheme," 2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD), May 2021, doi: 10.1109/cscwd49262.2021.9437677.

[3]. H. R. Pawar and D. G. Harkut, "Classical and Quantum Cryptography for Image Encryption & Decryption," 2018 International Conference on Research in Intelligent and Computing in Engineering (RICE), Aug. 2018, doi: 10.1109/rice.2018.8509035.

[4]. R. Liu, "Chaos-based fingerprint images encryption using symmetric cryptography," 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery, May 2012, doi: 10.1109/fskd.2012.6234120.

[5]. R. Das, S. Manna, and S. Dutta, "Cumulative image encryption approach based on user defined operation, character repositioning, text key and image key encryption technique and secret sharing scheme," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Sep. 2017, doi: 10.1109/icpcsi.2017.8391813.

[6]. H. Pan, Y. Lei, and C. Jian, "Research on digital image encryption algorithm based on double logistic chaotic map," EURASIP Journal on Image and Video Processing, vol. 2018, no. 1, Dec. 2018, doi: 10.1186/s13640-018-0386-3.

[7]. T. T. Zhang, S. J. Yan, C. Yan Gu, R. Ren, and K. X. Liao, "Research on Image Encryption Based on DNA Sequence and Chaos Theory," Journal of Physics: Conference Series, vol. 1004, p. 012023, Apr. 2018, doi: 10.1088/1742-6596/1004/1/012023.

[8]. Z. Lei, L. Li, and G. Xianwei, "Design and realization of image encryption system based on SMS4 commercial cipher algorithm," 2011 4th International Congress on Image and Signal Processing, Oct. 2011, doi: 10.1109/cisp.2011.6100292.

[9]. Q. Zhang and Q. Ding, "Digital Image Encryption Based on Advanced Encryption Standard (AES)," 2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC), Sep. 2015, doi: 10.1109/imccc.2015.261.

[10]. W. Wen, Y. Zhang, Y. Fang, and Z. Fang, "A novel selective image encryption method based on saliency detection," 2016 Visual Communications and Image Processing (VCIP), Nov. 2016, doi: 10.1109/vcip.2016.7805456.

[11]. P. Nayak, S. K. Nayak, and S. Das, "A Secure and Efficient Color Image Encryption Scheme based on Two Chaotic Systems and Advanced Encryption Standard," 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Sep. 2018, doi: 10.1109/icacci.2018.8554728.

[12]. A. Nag et al., "Image encryption using affine transform and XOR operation," 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies, Jul. 2011, doi: 10.1109/icsccn.2011.6024565.

[13]. J. K. Saini and H. K. Verma, "A hybrid approach for image security by combining encryption and steganography," 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013), Dec. 2013, doi: 10.1109/iciip.2013.6707665.

[14]. S. S. H. Shah and G. Raja, "FPGA implementation of chaotic based AES image encryption algorithm," 2015 IEEE International Conference on Signal and Image Processing Applications (ICSIPA), Oct. 2015, doi: 10.1109/icsipa.2015.7412256.

[15]. K. Sreelakshmi and R. V. Ravi, "An Encryption-then-Compression Scheme Using Autoencoder Based Image Compression for Color Images," 2020 7th International Conference on Smart Structures and Systems (ICSSS), Jul. 2020, doi: 10.1109/icsss49621.2020.9201967.

[16]. Y. Luo, M. Du, and D. Liu, "JPEG Image Encryption Algorithm Based on Spatiotemporal Chaos," 2012 Fifth International Workshop on Chaos-fractals Theories and Applications, Oct. 2012, doi: 10.1109/iwcfta.2012.49.

[17]. T. S. Ali and R. Ali, "A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box," Multimedia Tools and Applications, vol. 81, no. 15, pp. 20585–20609, Mar. 2022, doi: 10.1007/s11042-022-12268-6.

[18]. S. Murugan and Anandakumar H., "Privacy Information Leakage Prevention in Cognitive Social Mining Applications," Cognitive Social Mining Applications in Data Analytics and Forensics, pp. 188–212, 2019, doi: 10.4018/978-1-5225-7522-1.ch010.

[19]. M. Gabr, W. Alexan, K. Moussa, B. Maged, and A. Mezar, "Multi-Stage RGB Image Encryption," 2022 International Telecommunications Conference (ITC-Egypt), Jul. 2022, doi: 10.1109/itc-egypt55520.2022.9855767.

[20]. K. B. Sarmila and S. V. Manisekaran, "A Study on Security Considerations in IoT Environment and Data Protection Methodologies for Communication in Cloud Computing," 2019 International Carnahan Conference on Security Technology (ICCST), Oct. 2019, doi: 10.1109/ccst.2019.8888414.