International Journal of Applied Engineering Research ISSN 0973-4562 Volume 16, Number 6 (2021) pp. 466-477

A Novel Image Encryption Based on Feedback Carry Shift Register and Blockchain for Secure Communication

Malika Acharya
Department of Computer Science and Engineering
Rajasthan Technical University, Rawatbhatta,
Akelgarh, 324022, Rajasthan, India

Rama Shankar Sharma
Department of Computer Science and Engineering
Rajasthan Technical University, Rawatbhatta,
Akelgarh, 324022, Rajasthan, India

Abstract

Images have emerged as a great source of information in the past decade. There role in the field of medicine, military, architecture, etc. is indispensable. Thus image information security is the need of the hour. Over the last decade blockchain has garnered much attention in context of trust issues and third party elimination. The following paper proposes an image encryption technique based on blockchain and Feedback carry shift register (FCSR). The proposed solution encrypts the image and stores the values on the blockchain. The FCSR ensures image information security and blockchain ensures the security and privacy in the transit. 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 strength against the brute force attack is demonstrated based on entropy analysis. The value attained was near the ideal value 8. The proposed technique is also found to be efficacious against data loss in transit.

Keywords: Mnemonic phrase, Arnold map, blockchain, statistical attacks, differential attacks, stream ciphers, block ciphers, confusion-diffusion, feedback carry shift register, chaos theory.

1. INTRODUCTION

In today's era, multimedia as a source of information can't be undermined, especially images. Images have their special stake in field of military, medical, architecture, astronomy, etc. Thus information exchange through images has garnered a decent concern over the past few decades. Image security has seen the researchers divided in two categories i.e. a.) Image Watermarking. b) Image Encryption. Our focus in this paper will be on image encryption.

Image encryption is different from text encryption due the large size, bulk data capacity and high correlation between the pixels. The difference between text and image encryption are enumerated further [1]. First, the large data amount present in the image might remain even on compression. Second, the decision of compression then encryption or encryption then confusion is crucial in encryption. Randomness of the encrypted image relies critically on the compression process. The images can be compressed in lossy or lossless compression. Third, the mode of operation also critically affects the encryption. ECB mode are quite insufficient to use , while the CBC mode is time consuming yet efficacious against adversary. As a result the traditional encryption algorithms that have proved their mantle in the text encryption, are not efficacious enough for the image encryption. José A.P. Artiles,et al (2019) proposed an image encryption technique based on AES and Logistic map [2]. The technique proposed AES s-box generation based on fixed number of chaotic bits i.e. 3. While in the second round the 48 bits of the S-box were cyclically shifted to right. The modified S-boxes were evaluated to be more robust. The second algorithm proposed in this work involved Randomshifts that replaced MixColumn and shiftRows steps of the AES. The technique was demonstrated to be robust against different attacks yet susceptible to inherent demerits. The naïve algorithms that convert the two dimension streams as one dimension stream and then encrypt have been propounded in past few years but they are fail to solve the issues discussed above. The required characteristics from the cryptographic algorithms include complexity issues that involves whether the entire image is encrypted in one go or bitwise [3]. If the encryption is all at one time than the algorithm would be time consuming with significant computational complexity. Second, requirement is of compliance to format information. The encryption technique should not change the format information stored in the image , else the quality of the deciphered image would reduce. Third, the encryption technique must be immune to any transmission error that might crop up due to external noise.

In the past few years' chaos theory has been deployed in image encryption due to its characteristics like sensitivity to initial conditions, erogdicity, determinism, and periodicity. The chaos based image encryption has been successful in addressing many issues that traditional algorithms have failed to. Fridrich was the first to propose a chaos based image encryption. The chaotic map have been categorized as one dimensional, two dimensional, three dimensional, compound chaos map, hyper chaotic map[4]. Vinita Shadangi (2017) proposed a AES based image encryption in CBC mode using Arnold scrambling [5]. This scheme used multiple level of encryption that provided for the higher level of security against the eavesdropper. The technique involved the scrambling then confusion using Arnold map and then the

CBC mode based AES. The technique was time consuming due to AES yet it provided affirmative results. Traditional Advanced Encryption Standard (AES) algorithm is quite time consuming and memory intensive and hence not suitable for computers with less resource available. Ünal Çavusoglu et al (2018) made an attempt to optimize performance of AES using chaotic random number generator (RNG) [6]. The technique has added phase called added rows in combination to traditional AES stages. S-Box creation was based on RNG sequences produced using Zhong Tang chaotic system. The chaotic system was developed in 3 phases i.e. x, y and z phases. The results were compared with traditional AES and S-AES and demonstration suggested in affirmation. Alireza Arab in (2019) proposed an image encryption based on AES using Arnold chaos sequence [7].The Arnold chaos sequence obtained is used to control the AES encryption. CCAES (combined chaos AES) algorithms is different from AES as it has enhanced block operations. Yan-Ru Zhong, et al (2018) proposed a novel image encryption algorithm 2D SPLCM integrating Sine map and Piece wise Linear Chaotic map (PLCM) [8]. The image encryption involved a secret key based on initial conditions of 2D SPLCM, replacement operation and diffusion process. The algorithm on simulation proved to be robust. In [9] Shenil Zhu, et al (2019) proposed a technique based on compound Sine-Tent chaotic map and double S-box. The technique deployed the key sequences generated by a chaotic system for the generation of S-boxes and this successfully counterfeited some major attacks. Bhaskar Mondal, et al (2018) suggested a new image encryption based on 2D Baker Map [10]. Inverse permutation and inverse diffusion were the strength of the technique. The evaluation of the technique against several metrics suggested its effectiveness and robustness. Mohammad Javed Roustami, et al (2017) contrived encryption scheme using logistic map based chaotic window [11]. The technique employed logistic map five times to eliminate the demerits of logistic map like small key space, periodicity in chaotic behavior. The technique was efficient in terms of countering chosen plaintext attack, statistical attacks and differential attacks. It is superior in terms of time consumption M.Zarebina, et al (2019) proposed image encryption technique for gray scale images using hybrid chaotic systems [12]. The image was divided in blocks and then the subsequence generated using the combination chaotic systems were used to permute the images. 2D Arnold cat map and XOR operator encrypted the image. The last step of cyclic shift operation was used to get final encrypted image. The proposed technique was evaluated against the metrics of statistical attacks and differential attacks and results suggested their effectiveness. In [13] a novice image encryption based on Arnold3D cat map and pixel frequency was deployed. Pixel frequency was deployed as a source of random sequence generation at confusion phase and as a chaotic sequence generator in diffusion phase. The diffusion process was separately carried on rows and columns prior to cipher image generation. The plain image based key streams are used to for confusion and diffusion provided a high sensitivity to the slightest change in the image pixel. Hongyue Xiang and Lingfeng Liu (2020) contrived a technique to solve the limitations of logistic map in image encryption based on perturbation and feedback control [14]. Improved logistic map had higher randomness, higher ergodicity, wider range of chaotic behavior and better sensitivity to the initial conditions. The secret key employed had five components inclusive of both chaotic parameter and original image pixel values. The high technique was suitable for both grayscale and color images. The simulation demonstrated better security than contemporaries. Lingfeng Liu et al (2017) contrived an image encryption technique [15] where the authors first permutated the image using Arnold Map. Then the permutated image was divided in sub blocks. This division was controlled by Baker map. After blocking process, each sub image was substituted using logistic sequence generated using secret keys. The end result was obtained after the encryption of each individual blocks /sub image was complete using integer logistic map. Once the sub image encryption is complete they are combined to form final image. Most of the encryption techniques are either reliant on the original image or they are based on the key used rather than the original image. Thus there exists a vast gap between the key and the encryption process. In an attempt to bridge it a technique was proposed in [16] .The authors aimed to include a onetime pad characteristic in the encryption process. The image was first improved logistic map were used to scramble the image and then it is divided in the blocks and then the lower 4 bit matrix was used as the control parameter for the improved logistic map to provide for the sequence that was used in the scrambling of higher 4 bit matrix. The final stage of diffusion deployed XOR-ing of high 4 bit matrix with the chaotic sequence generated randomly. The improved logistic map was deployed to overcome the limited key space and limited chaotic behavior of the logistic maps. The technique allowed for encryption of the image in 4 bit low and 4 bit high bit planes based on the information present in the bit planes. The upper 4 bit planes had 94% of the information while remaining 6 % was present in the lower ones. The technique was unique and robust but only theoretical matrixes were evaluated. Syeda Iram Batool and Hafiz Muhammad Waseem (2019) proposed a Arnold map based technique [17]. The technique used Diffie Hellman key exchange to produce the secret key that was used to decide the number of epochs for the Arnold map and also set the starting value of Lucas series. The technique was found to be robust against adversary yet the periodicity of Arnold amp and the weakness of the Lucas series made the technique vulnerable to attacks. In 2019 Yuqin Luo et al contrived a technique using improved baker map and modified logistic map [18]. The technique relied on 2D baker map as the control parameter for the logistic map. The image was first shuffled using the logistic map and then the same logistic map was used to generate another chaotic sequence that was utilized for substitution. Chunyan Han (2019) propounded a novel image encryption scheme that defined a modified logistic map [19]. The modified map was used to generate a pseudorandom sequence which was used to generate the scrambling matrix and key matrix. The scrambling and diffusion model of was adopted in the technique. The second stage involved scrambling while the third stage provided for the diffusion. The results of the demonstration were quite a competition to the contemporaries.

Blockchain has garnered much of the interest in context of trust related issues over the past few years. Prince Waqas

Khan and Yungcheol Byun [20] propounded a blockchain based approach where the image was processed and a hashed transaction ID was allocated that was further used to design message digest. The salient feature of the approach was the security and robustness of hashed transaction ID. The technique was designed on permissioned blockchain thus the high cost of resources for mining that incur due to proof of work , etc was eliminated. Some drawbacks that were inherent were the admission control authority present / used to authenticate the users. Any attack on it would undermine the use of blockchain. Also the time of transmission of the image was proportional to the size of the image. The mining attack could easily forfeit the merits of the approach. Ruiping Li (2019) contrived a novel image encryption technique based on blockchain and fingerprint of the sender [21]. The keystreams used were independent of the original image rather dependent on the fingerprint of the sender. The blockchain used was to ensure that the image was transmitted without being tampered. The final stage was the use of anti-collusion code to merge the fingerprint of the distributor in the image. The technique scored for its robustness against Chosen-Plaintext attack. Zhao Feixiang, et al (2021), propounded a technique based on combination of Chaotic Restricted Boltzmann machine (CRBM) and blockchain [22]. The technique first deploys row permutation and then column permutation based on H´enon-zigzag map. Then the substitution was deployed using CRBM. Finally the transmission phase included the blockchain framework for allowing the detection of tampering of the encrypted image and also for the secure transfer to the authorized receiver. The key pair generated using blockchain SHA-256 algorithm was used for the authentication of the users. The technique was found to be robust against various attacks and efficacious against adversary.

In an attempt to solve the problem of key sharing in block ciphers like AES, Noor Kareem Jumma (2018) contrived and Linear Feedback Shift Register (LFSR) based approach for block cipher [23]. The technique used a 5-bit LFSR to produce 128 bits (6 bytes) key that was an input for the Advanced Encryption Standard Algorithm. The problem of key sharing was addressed by using the date of encryption as the seed for LFSR. Thus the decryptor just needed to know the date of sending/receiving the image and could easily get the required parameters. The demonstration suggested that algorithm was robust against adversary. Subhrajyoti Deb, et al (2019) put forward an algorithm based on Image randomization Logistics, Arnolds scrambling and word oriented feedback shift register (WFSR) [24]. The technique involved key sharing via Elliptical Curve Diffie Hellman (ECDH) approach, image randomization based on logistic map and Arnold's transform and WFSR. However, memory consumption is a cause of concern in case of chips, embedded systems. Sourav Saha, et al(2018) proposed an image encryption technique based on improved Linear feedback shift register (LFSR). The technique used a MUX for providing a randomization to the output of the LFSR. The MUX used has selector of the form of small LFSR probably of 3- bit. The technique relied on altering the tap sequence using small LFSR and these are chosen using 8*1 MUX. The bits are XOR-ed and output acts as input to LFSR. The encryption had two steps i.e. first a row wise permutation using LFSR sequence and them A column wise permutation using the sequence. And final step used XOR of both the images. The technique was robust and efficacious yet a time consuming affair. Shamama Anwar and Solleti Meghana (2019) proposed a technique based on pixel permutation [26] .The technique was an attempt in the direction that encrypted image appeared noise- like and hence was vulnerable. Thus the encrypted images were masqueraded by some other image. The techniques had three stages: First, replacing of the pixel values by some other pixel values i.e. pixel permutation using a variant of Arnold cat map. Second stage involved the XOR-ing of the normalized image with the obtained matrix. And the final stage involved the masquerading the obtained encrypted image using key image. The technique had infinite key space hence resistant towards brute force attack. But it was susceptible to chosen plaintext attack. Lu Xu et al propounded a block scrambling based image encryption with dynamic index based diffusion process [27]. The technique involved Logistic map based chaotic matrix that provided the scrambling effect. The scrambled images then underwent diffusion based on two dynamic indexed based diffusion algorithms. The technique was found suitable even for multiple image encryptions. Saiyma Fatima Raza and Vishal Satpute (2018) suggested an image encryption technique based on Rubiks cube and logistic map [28]. The approach involved Rubiks cube and logistic map for bit level permutation that provided diffusion. Confusion was present at two levels i.e. bit level and pixel level. The decisive parameter of the technique was the number of optimal rounds required for confusion and diffusion. The approach was demonstrated to be immune to statistical, differential and brute force attacks. M.Y. Mohamed Parvees, et al (2016) presented an approach based on color byte scrambling [29].This approach was composed of a Logistic map to generate a permutation sequence for shuffling the color bytes (confusion) and Ikeda map allowed the generation of a masking sequence for different color bytes (diffusion).

Table 1 gives the comparative analysis of different algorithms that have been studied.

2. PRELIMINARIES

2.1. Feedback Cary Shift Register(FCSR)

The commonly used pseudo random generator called LFSR (Linear Feedback Shift Register) has been a center of study in past few years. The short period of LFSR is the primary demerit of the pseudo random generator so developed. Saad Muhi Falih (2016) contrived a technique based on Linear Feedback Register (LFSR) and chaotic map [32].The monobit test, poker test, runs and long tests evaluated the effectiveness of the approach and even enhanced the LFSR's output using exclusive-OR (XOR) with stream bit. However the technique remains susceptible to correlation attack. To overcome such defects, Klapper and Goresky[31] propounded Feedback carry shift register. The architecture of FCSR is illustrated in Fig 1. The auxiliary memory *m* is a non negative integer. The tapped cells of the form (0or 1) are added to *m* and then added to form σ. The parity bit σ (mod 2) if fed back into the first cell and ($\llcorner \sigma/2 \lrcorner$) becomes the new value of the memory.

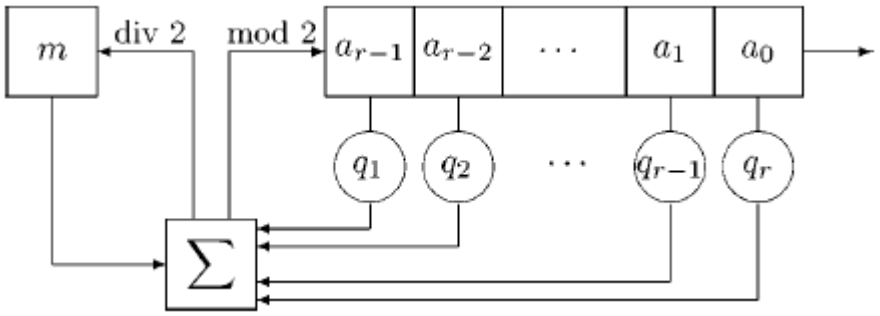

Figure 1: Feedback Carry Shift Register Architecture

The final output is denoted as:

$$\sigma = \sum_{i=1}^{m} q_i \, a_{m-i} \; + \; z \tag{1}$$

$$z_n = \; floor\left(\frac{\sigma_n}{N}\right) = \; \sigma_n(divN) \tag{2}$$

$$a_n = \; \sigma_n(modN) \tag{3}$$

$$m\,stage = floor(\log_N(q+1)) \tag{4}$$

Our technique involves the three FCSR sequence, 1 generated from random 37 bit value while other two generated from a mnemonic phrase that is 12 words phrases selected from the list of English words that has 2048 words based on 128 bit entropy. This has added advantage that sequence generation is typically dependent on the secure mnemonic that resides only with the encryptor. Also there is no key for the initial seed to be shared.

2.2. Arnold Map

Arnold Cat Map is an area preserving chaotic map that is employed to scramble the image there by reducing the correlation between the pixels of the image. The cat face scrambling is used in both stenography and encryption. The Arnold map is defined Equation 5:

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} mod\ N \tag{5}$$

Where (x_{i+1}, y_{i+1}) are the pixels of the new image produced after scrambling while (x_i, y_i) are the pixels of the original images. N is the size of the image. Opening this equation we have Equation 6 that is used to calculate the Arnold sequence.

$$\begin{cases} x_{i+1} = (x_i + by_i)\ mod\ N \\ y_{i+1} = (ax_i + (ab+1)y_i)\ mod\ N \end{cases} \tag{6}$$

The drawback of the Arnold map is that it's periodic. After certain number of iterations it returns the original image. For example for a grayscale image of 256 *256 it period is 192. This is quite a big loophole in the map as the adversary can easy try 192 iterations to get the original image back. The Arnold map leaves the grayscale values intact hence deciphering the original image from the scrambled image is quite an easy task. Some basic rules for the calculation of period of Arnold map are presented in [30].

Period τ of Arnold is stated as:

τ = 3n if and only if $n=2*5^k$ for k = 1, 2, 3, 4 ….. (1)

τ = 2n if and only if $n=5^k$ or $n=6*5^k$ for k=1, 2, 3, 4,…. (2)

τ ≤ (12n/7) for all other choices (3)

Other major drawback of the Arnold map is the requirement of square image, i.e. image of form M*M only. In our technique we propose modified Arnold Map to scramble the image there by eliminating such issues to an extent.

Step1: The proposed modification suggests the use of 37 bit random binary value as a seed for FCSR.

Step2: The generated sequence is a 128 bit sequence. Then checksum calculated is actually 128/32. This value is extracted from the sequence and appending it to the end. There by making it 132 bit value.

Step3: This value is then grouped in set of 11 bits each, thus there are in total 12 groups. The values are converted to decimal values. The decimal values so obtained are actually 12 decimal values.

Step4: Two sequences are generated from these 12 values. One is the summation of values at odd places and other is the summation of the values at even places.

$$l_1 = \sum_{i=1}^{12} odd\ index\ values \tag{7}$$

$$l_2 = \sum_{i=1}^{12} enen\ index\ values \tag{8}$$

Step 5: To normalize the two sequences obtained we calculate mod 256 of each as in Equation 9-10. These values will serve as the values in equation 6

$$y_1 = mod(l_1, N) \tag{9}$$

$$y_2 = mod(l_2, N) \tag{10}$$

Step 6: Assume two values of x. Let it be x_1=1 and x_2=2. In the next step we calculate *a* and *b* value required for substitution in equation 6. The values are obtained as in equation 6.

$$a = fix\left(x_1 + sqrt(y_1)\right) \quad (11)$$

$$b = fix\left(x_2 + sqrt(y_2)\right) \quad (12)$$

Step 7: We next substitute the values of calculated values of y, a, b and assumed values of x in equation 6. For the size of image in question we find two sequences s and r from the above parameters. The sequences obtained are next used for providing permutation effect.

2.3. Blockchain

Blockchain was initially developed for the purpose of cryptocurrency with the aim to remove the third party interference from the transactions. Bitcoin transaction is deeply based on blockchain framework. But now-a-days its impact on different industries can't be denied. Most of organizations are based on decentralized network of peers. Hence the chances of exposure of the sensitive data to the adversary are also higher. The trust issue of the mediators is a great cause of concern. Thus there is need of decentralized technique for equipping smart industries with the method to maintain the security and privacy of the image. Blockchain, in past decade, has emerged as a panacea for such situations. It provides with the distributed ledger that is immutable and hence the record of the transitions is secure and can't be tampered. The transactions once validated are then stored at the end of the blockchain. Thus to alter the block it is required that the chain of blocks following it must be altered. This involves a lot of computational power. Also the alterations made to the block are validated by majority vote system and only then are they recorded in all the nodes simultaneously. This increases the difficulty of attack on blockchain and in return ensures the security of the data. The transaction hash and the timestamp present in the record make this distributed ledger immutable. Every block has the hash of the previous block except the first block which is known as *Genesis Block*. Every block has the complete list of all transactions that are immutable and these accounts for its security. There are generally two types of the blockchain. Public blockchain like Bitcoin, Ethereum, etc. that can be used by all. Private Blockchain is especially customized for certain industries. The basic block structure is depicted in Fig 2.

Version defines the blockchain's version number. Timestamp is the time of block production. Merkel Root has a tree like structure with the leaf node containing the hash value of the transaction. Every transaction has an associated hash with itself and the sequential hash is not secure enough thus the tree like structure that has the transaction hash stored in the hashed form , i.e., the transaction hash of the blockchain are again hashed and then stored in tree form. Another important advantage of the Merkel Tree is that it allows for the verification of the blockchain data and also for the transfer of the data from one node to another. The MerkelRoot is the hash at the root of the Merkel Tree. Blockchain is highly secure as it uses both asymmetric and symmetric encryption. Asymmetric encryptions include the use of public and private key between the nodes in one-to-one fashion. Every node has a private key and a public key. While a node first signs its transaction using a key. Other node verifies the transaction by using the public key of the other. The cryptographic hash function used (SHA-256) is actually a collision resistance. Every block has the hash of the previous transaction associated with it. This linkage allows for the easy verification of the blocks. The Nonce value appended to very block [33].It stands for 'Number only used once' It is this number that if verified allows for the transaction to be verified. Miners solve the integrated puzzle for this number. Once solved miners are rewarded. Nonce is mined using a consensus model, generally Proof of Work (POW) or Proof of Stake (PoS). There are a few terminologies that seek explanation here to proceed.

• Mining: The consensus model used in blockchain requires that any block can be added to the chain only when verified by using a majority vote. The general process of this is called mining. The ultimate aim is that every miner has the equal responsibility of the transaction mined rather than a single block as in centralized system. The mining process requires a lot of computational power and hence the machines with adequate resources and genuine are a part of the blockchain.

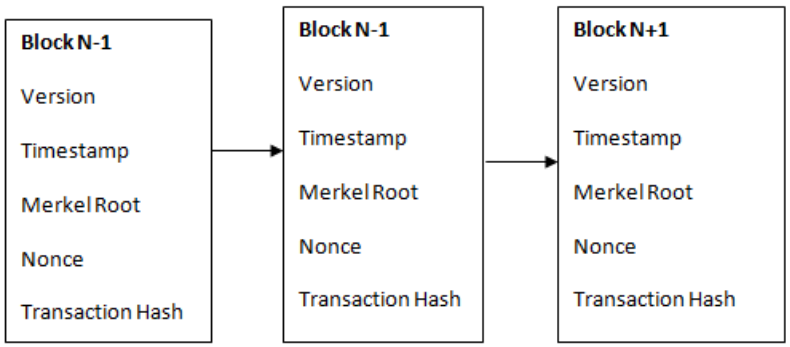

Figure 2: Blockchain Architecture

• Immutability: Every block has a transaction hash that cannot be altered and the data stored is also thus secure. As to alter the data one needs to mine to that hash block and the changed data would cause a complete different hash as previous and this would further require altering the hash of all the following blocks. This process is quite laborious and resource intensive.

• Proof Of Work: Blockchain relies on consensus mechanism to achieve an agreeement among nodes on which it manages the data being a distributed ledger. Proof Of Work (PoW) is one such consensus algorithm that is usd most widely and ensures security and confirmity of transactions. There are some 14 consensus algorithm. It is bassed on a complex mathematical puzzle that has the following three ingridents:

- Hash functions
- Integer factorization
- Guided puzzle tour

3. PROPOSED ALGORITHM

3.1. Blockchain workflow

For the purpose of this algorithm we are required to have a distributed blockchain using POW. We use a permissioned blockchain platform for creating a network to send the image in P2P manner.

The blockchain outlay is defined as:

Step1: Start the blockchain web service. This will provide with the active port number and 10 accounts for P2P network between the nodes.

Step2: A node generates the transaction to start with the genesis block. The genesis block generated will start the transaction at the port specified. The node will calculate a hash value through POW consensus algorithm.

The new generated block will be added to the blockchain.

Step3: We generate a contract address between different nodes. This will be used to mine the first block on blockchain. Also there is need of two mnemonic pass phrases that will be used as the membership authorization key for the sender and the user.

Step4: IPFS service daemon will store the values of IPFS hash on the blockchain web service. Hence would serve as the membership authentication service.

3.2. Proposed Algorithm

3.2.1. Encryption Algorithm

Step1: Generate a random 37 bit binary random sequence. Use this as seed in FCSR to generate FCSR sequence. The sequence generated would be as per Eq. (1).

Step2: Calculate the checksum of the sequence and append it to the end of the sequence. As the entropy is of 32 bits this checksum would be of 128/32 bits. Extract these many bits from the sequence and append them to the end of the sequence.

Step3: Calculate the values of *l1, l 2, y1, y2, a* and *b* as in Eq. (7)-(12). This will provide an Improved Arnold Map. The two sequences *s* and *r* are then normalized using the Eq. (13)-(14) to normalize the values in range of 0-255.

$$S = mod\big(floor\big((s * 100) * 10^{14}\big), 256\big) \quad (13)$$

$$R = mod\big(floor\big((r * 100) * 10^{14}\big), 256\big) \quad (14)$$

With the above sequences being generated we will provide for the permutation of the image.

Step1: Read the image and convert to grayscale. The colored image has three channels that are R, G, B. The encrypted image is sent over blockchain and hence the Merkel Root will record the transaction. If all the three channels are encrypted separately then the tree generation would be time intensive and hence would require extra computing resource.

Step2: Use *S* and *R* to provide row permutation and column permutation respectively. The shuffled image has sufficient amount of confusion but the gray values of the image are still intact i.e. there is still the correlation existing between the pixels, to remove these we use substitution process.

Step3: The parameters obtained from the diffusion phase i.e. values at odd places and values at even places are then used to generate two FCSR sequences. And two mnemonic pass phrases. The mnemonic pass phrases added over here

Step4: The sequences generated are then XOR-ed with each other bitwise. This will reduce any leakage of the information about the key. Also the mnemonic passphrase will be provided to only authenticate users after their blockchain membership has been analyzed.

Step5: The XOR-ed key is then used to substitute the values of the scrambled image. The diffusion process is required to remove any correlation between pixels. This process is iterated for the size of the image. The final result obtained is an encrypted image.

Step 6: The encrypted image is then sent over the IPFS network that would generate the transaction hash over the blockchain network. IPFS has been used for sending the image so as to leverage the blockchain from the load of large size images. The amount of computing power required for such transfer is less as compared to that one that are whole and solely made over the blockchain network.

The algorithm has been generated on the public blockchain, but in private blockchain like the one used in industries the customized resource applications are too much sensitive to resource usage and hence this must be kept in mind. So we have utilized a distributed storage called IPFS for the sake of restricted resource usage.

The complete process is illustrated in Fig. (3) as schematic diagram.

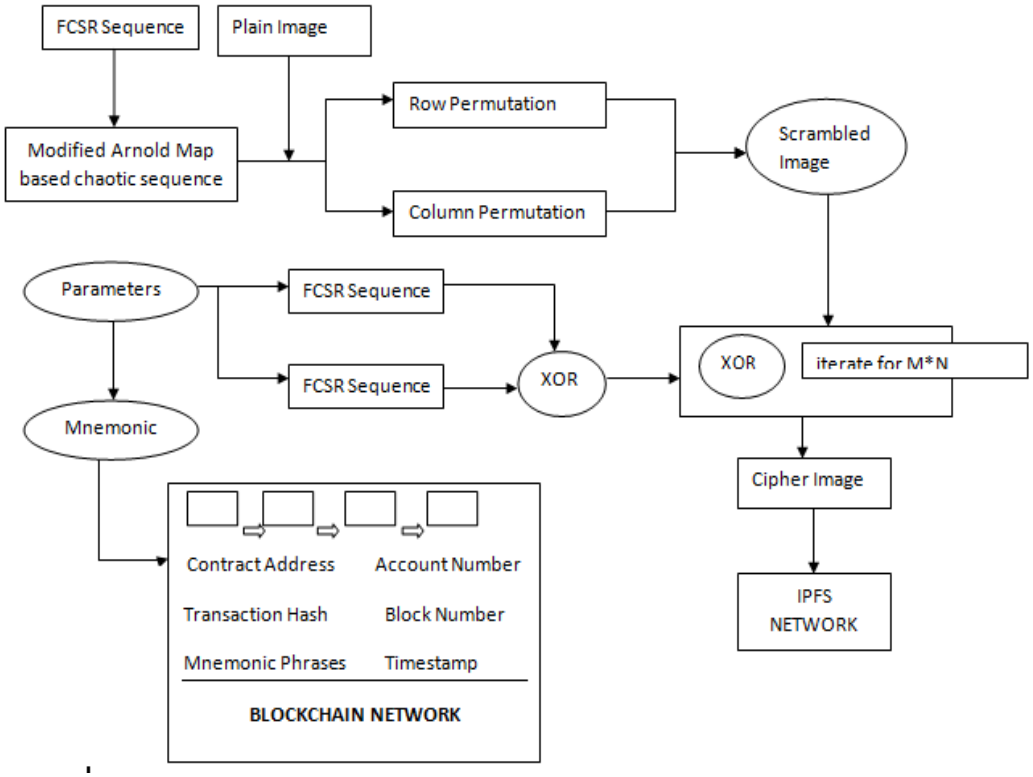

Figure 3: Schematic diagram of encryption process.

3.2.2. Decryption Algorithm

The decryption process is divided in two phases: a.) Authorization b.) Decryption. The authorization process is required to provide the access of the information only to the valid user. This process involves two phase authentication. The first phases is the contract address based authorization where only the valid ode can have the contract address created at the time of starting the blockchain. This serves as the node is legal or not authentication service. Any adversary that breaches the network would not be able to have the valid contract address. Also the validated node now gets the access only to IPFS hash to download the image. But the required key for decryption is yet to be missing. This will be only be present with the user that successfully validates itself in the second phase. In the second phase the user is validated for valid node in blockchain contract. This is based on the account number present with each node at the time of creation of blockchain. A node with successful dual authentication can then be provide by the mnemonic pass phrases that were stored in the blockchain.

With these two in hands actual process of decryption will start.

Step 1: Download the image.

Step2: Get the mnemonic codes and generate the respective FCSR sequences.

Step3: XOR the two sequences to get the respective keys.

Step4: Keys of step 3 are used for reverse diffusion. The resultant image still is scrambled image.

Step5: Inverse Arnold Map is used to unscramble the resultant image of step4. The parameters are generated using mnemonic passphrases provided.

The decryption process along with the authentication process is provided schematically in Fig. (4)-(5).

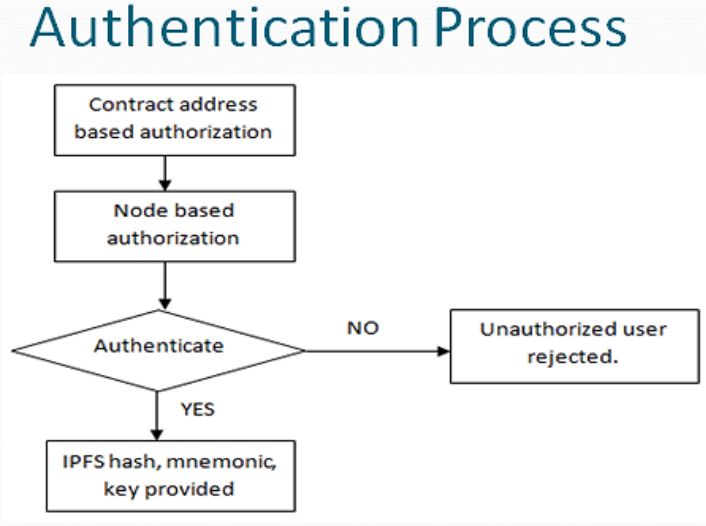

Figure 4: Schematic Diagram of Authentication Process

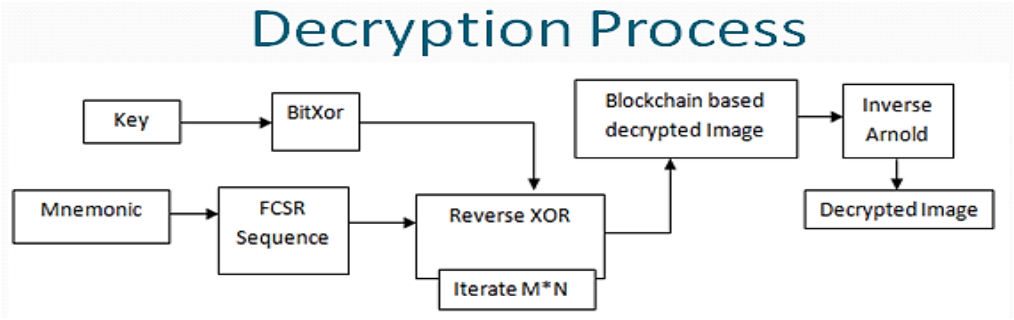

Figure 5: Schematic diagram of decryption process.

Table 1: Comparison of Techniques

Ref	Author	Year	Approach	Merit	Demrit
[24]	Subhrajyoti Deb, et al.	2019	Image randomization Logistics, Arnold's Map, WFSR	Better Security	More Space intensive
[32]	Saad Muhi Falih	2016	LFSR, Qudratic map, Logistic map	i)Eliminates Linearity and repetition in LFSR's Output. ii)Enhanced Key space	Susceptible to Correlation Attack
[29]	M.Y. Mohamed Parvees, et al	2016	Color Byte Scrambling , Logistic map, Ikeda map	Better Confusion and Diffusion using Logistic and Ikeda map	Permutation Sorting time increases as block size increases non linearly
[27]	Lu Xu et al.	2017	Block Scrambling, dynamic index based diffusion	High security, high key space, suitable for multiple image encryption	Complex and diffusion is time intensive.
[20]	Prince Waqas Khan and Yungcheol Byun	2019	Blockchain	Decentralised approach , use of Hashed transactioned ID	Memory intensive, Speed of transaction
[11]	Mohamad Javad Rostami, Abbas Shahba, Saeid Saryazdi, Hossein Nezamabadi-pour	2017	Chaotic window, pixel permutation	i)Secure, fast, robust, efficient. ii) Suitable for parallel processing	Higher dimensional image needs to be divided in larger blocks for better results.
[14]	Hongyue Xiang & Lingfeng Liu	2020	Improved Logistic map	Large Key space, Better security, Suitable for color as well as gray scale images	i)Time analysis required ii) Image compression required.
[26]	Shamama Anwar, Solleti Meghanna	2019	Pixel permutation, Arnold Cat map	i)Infinite key space ii)Visually eluding image transmission	Vulnerable to chosen plaintext attack.
[28]	Saiyma Fatima Raza and Vishal Satpute	2018	bit permutation , logistic map, rubics map	High key sensitivity, confusion at both bit level and pixel level	Limited chaotic range , Number of rounds should be less.

4. EXPERIMENT RESULTS

The algorithm was demonstrated using MATLAB2016a and a permissioned blockchain. The effectiveness of the proposed technique is demonstrated by applying it on some standard test images i.e. Lenna image, Cameramen image, peppers image and baboon image. The results are enumerated in following sections. The comparison of encryption of Lenna image using other technique is enumerated in Table 2-4.

4.1. Statistics Attack Analysis

4.1.1. Histogram Analysis

The histograms analysis produces the analysis of relative frequency of different pixel values. The histograms of the plain image present certain pattern while that of the encrypted image are uniform. More the uniformity in the histogram better is the resistance. The histograms produced after encryption demonstrates that the algorithm is robust against statistical attacks. The fig[6] to fig[7] juxtapose the histogram before and after the encryption.

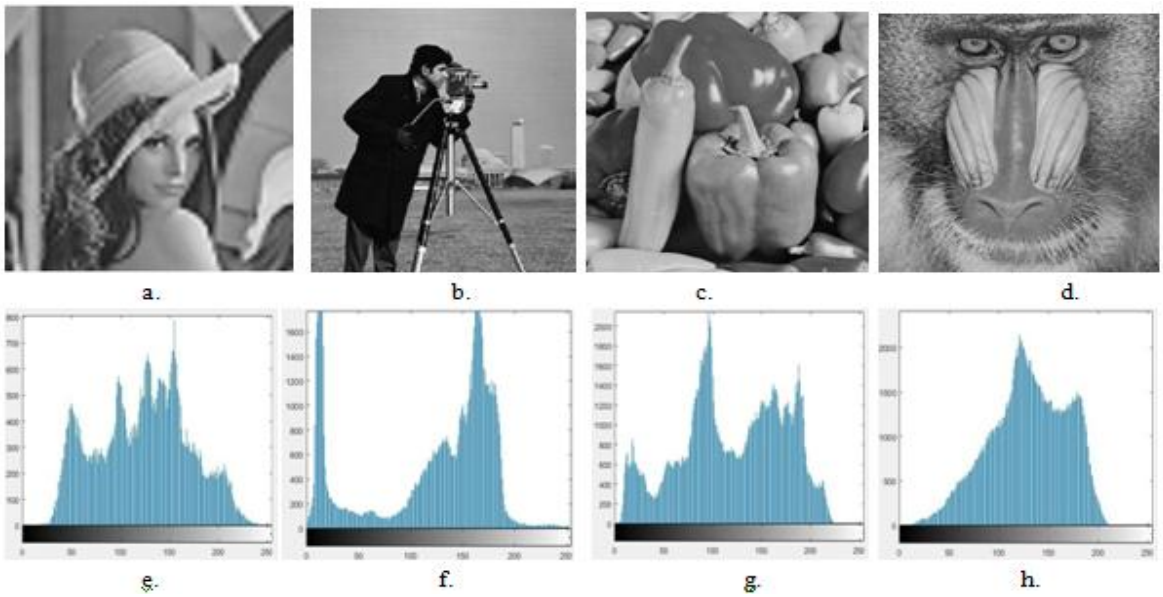

Figure 6: a.) Original Lenna Image. b.) Original Cammeramen Image. c.) Original Peppers Image. d.) Original Baboon Image. e.) Histogram of Lenna Image. f.) Histogram of Cameramen Image. g.) Histogram of Peppers Image. h.) Histogram of Baboon Image

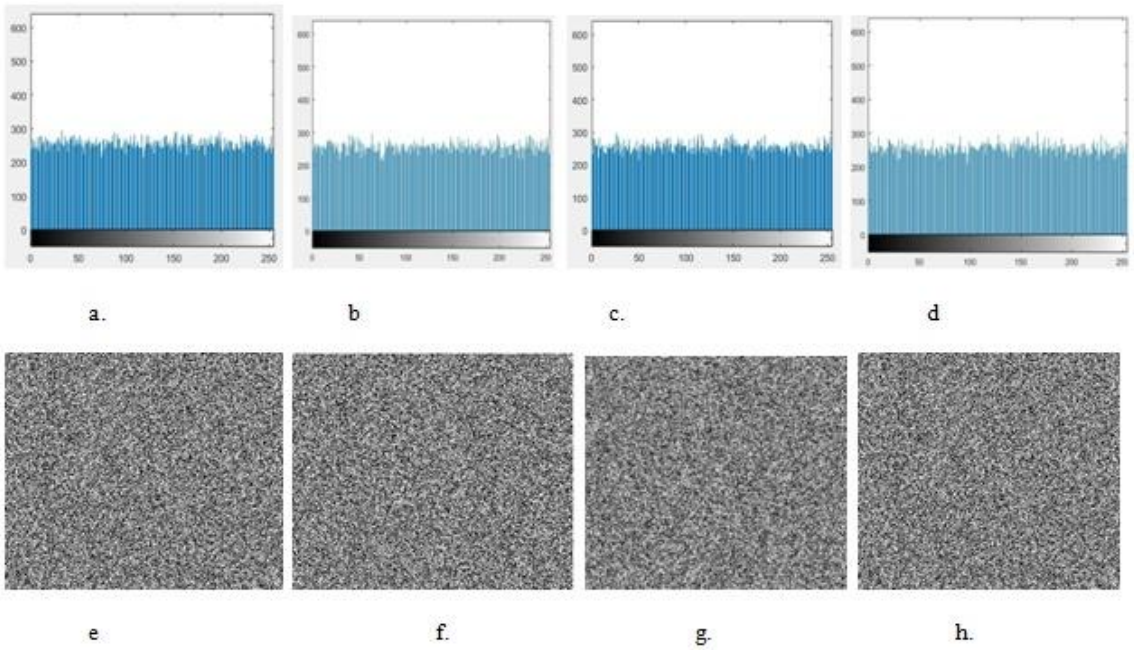

Figure 7: a.) Histogram of Lenna Image. b.) Histogram of Cameramen Image. c.) Histogram of Peppers Image. d.) Histogram of Baboon Image. e.) Encrypted Lenna Image. f.) Encrypted Cameraman Image. g.) Encrypted Peppers Image. h.) Encrypted Baboon Image.

4.1.2. Correlation Coefficients

The correlation coefficient analysis is used to measure the similarity between the encrypted and the plain image. The value is 1 if the image is an exact match while it's value must reside close to zero (< 0) for a better encryption algorithm. The equation 15 is used for the calculation of the correlation. The comparison of the correlation coefficients of the proposed technique and some other techniques for Lenna image is presented in Table 2. Let *J* pairs of pixels (x_i, y_i) in requisite direction then:

$$p = \frac{cov(x,y)}{\sqrt{var(x)} * \sqrt{var(y)}} \quad (15)$$

Where

$$cov(x,y) = \frac{1}{J}\sum_{i=1}^{J}(x_i - n_x)\left(y_i - n_y\right)$$

$$var(x) = \frac{1}{J}\sum_{i=1}^{J}(x_i - n_x)^2$$

$$n_x = \frac{1}{J}\sum_{i=1}^{J} x_i$$

Table 2: Comparison of Correlation Coefficient

Ref.No	Correlation Coefficient		
	Horizontal	Vertical	Diagonal
Proposed Technique	0.0033	0.0025	-0.0041
[11]	-0.0041	-0.0110	0.0011
[5]	0.9400	0.9693	0.9179
[22]	0.0058	0.0006	-0.00030
[24]	-0.0422	0.0367	-0.0582
[25]	-0.0067	0.0105	-0.0173

4.1.3. Entropy Analysis

The entropy is measured using Shannon's method. The entropy analysis demonstrates the randomness in the cipher image. The ideal value is 8 bits if there is equi-probability of the generation of 256 symbols. The equation 6 is used for the calculation of the entropy. The more the value closer to the 8 bits the better is the randomness of the cipher image. The comparison of the results of the various technique in [5],[11],[22],[23][24][25] are presented in Table 3. The proposed algorithm has a value close to 8 bit.

$$H(X) = -N \sum_{i=1}^{N} p(x_i)p(x_i) \quad (16)$$

Where N is the size of image, while x_i is the pixel of the image.

Table 3: Entropy values Comparisons

Ref.No	Entropy
Proposed	7.9986
[11]	7.9984
[5]	7.9975
[22]	7.9978
[23]	7.9972
[24]	7.9974
[25]	7.9992

4.2. Differential Attacks

4.2.1. Number of pixel change rate (NPCR)

NPCR metric measures the ability of algorithm to resist the differential attack. The equation 17 is used to calculate the NPCR. C_i and C_j are encrypted image of the same plain image differing by a value of the pixel. The results of the demonstration are compared with techniques in [5],[11],[22],[23][24][25] and presented in Table 4

$$NPCR = \frac{\sum_{i,j} D(i,j)}{N*M} * 100\ \% \quad (17)$$

4.2.2. Unified Average Changing Intensity (UACI)

It's the measure between the pixel intensity in plain image and cipher image. Equation 18 is used for the calculation of the UACI. The results of the comparisons of the various techniques in [5],[11],[22],[23][24][25] and presented in Table 4

$$UACI = \frac{1}{N*M}\sum_{i,j}\frac{C_1(i,j) - C_2(i,j)}{255} * 100\% \quad (18)$$

Where , $D(i,j) = \begin{cases} 1 & \text{if } (C_1(i,j)) = (C_2(i,j)) \\ 0 & \text{if } (C_1(i,j)) \neq (C_2(i,j)) \end{cases}$

Table 4: NPCR and UACI values.

Ref.No	NPCR	UACI
Proposed	99.69	33.45
[11]	99.42	31.71
[5]	99.64	30.52
[22]	99.60	33.49
[23]	99.58	33.36
[24]	99.60	33.41
[25]	99.61	33.44

5. CONCLUSIONS

The proposed technique employee FSCR sequence based improvement in Arnold Map. The FCSR sequence based Arnold map makes the period estimation of the map quite difficult hence the leakage of information is quite difficult. Also as the control parameters are the based on FCSR hence the iterations need not be dependent on the size of the image any more. This process allows for efficient scrambling and then the image undergoes the substitution process. The substitution process is again based on two FCSR sequences that have been generated based on the calculation so fthe odd and even places. This helps in further randomness of the sequences. The two FCSR sequences are then totally XOR-ed and finally used as the key for the image diffusion process. The final image thus generated is highly secure. And the transfer of this image takes place in IPFS network. The IPFS network provides for authenticated the transfer of the image. The results of the demonstration suggest that the image is robust against adversary. The statistical measures and the differential metrics both suggest the algorithm is efficacious. Blockchain network ensures that any tampering in the image will lead to detection as any transaction in the blockchain tampers the associated hash.

Declarations of Interests

Availability of data and material: Not applicable

Competing interests: Competing interests sections: The authors declare that they don't have any competing interests

Funding: Not applicable

Authors' contributions: The first author has propounded the enhanced Arnold map technique based on feedback carry shift register. Arnold map has demerit that it can only be used with square image and also is periodic . So it reveals the images when used. Thus for information security point of view it is required to remove these using feedback carry shift register. The co-author has contrived the idea of imbibing blockchain for providing the secure communications. The blockchain has been used for providing an authentication service for the users. Only the nodes authorized will be provided with the required mnemonic phrases required for decryption.

Acknowledgements: Not applicable

REFERENCES.

[1] Abd El-Samie, Fathi & Ahmed, Hossam & Elashry, Ibrahim & Shaheen, Mai & Faragallah, Osama & El-Rabaie, El-Sayed & Alshebeili, Saleh. (2013). Image Encryption: A Communication Perspective. 10.1201/b16309.

[2] MultiMedia Content enCryption Techniques and Applications Shiguo LianISBN:9781420065282, 1420065289 CRC Press

[3] "Chaos-based Cryptography Theory, Algorithms and Applications" Book ISBN978-3-642-20542-2DOI10.1007/978-3-642-20542-2. Springer-Verlag Berlin Heidelberg

[4] Artiles, J. A. P., Chaves, D. P. B., & Pimentel, C. (2019). *Image encryption using block cipher and chaotic sequences. Signal Processing: Image Communication, 79, 24–31*. doi:10.1016/ j.image. 2019.08.014

[5] Shadangi, Vinita & Choudhary, Siddharth & Abhimanyu, K & Patro, K Abhimanyu & Acharya, Bibhudendra. (2017). Novel Arnold Scrambling Based CBC-AES Image Encryption Novel Arnold Scrambling Based CBC-AES Image Encryption. International Journal of Control Theory and Applications. 10. 93 - 105.

[6] çavuşoğlu, Ünal & Kacar, S. & Zengin, Ahmet & Pehlivan, Ihsan. (2018). A novel hybrid encryption algorithm based on chaos and S-AES algorithm. Nonlinear Dynamics. 92. 10.1007/s11071-018-4159-4.

[7] Arab, A., Rostami, M.J. & Ghavami, B. An image encryption method based on chaos system and AES algorithm. *J Supercomput* 75, 6663–6682 (2019).https://doi.org/10.1007/s11227-019-02878-7

[8] Zhong, Yan-Ru & Liu, Hua-Yi & Sun, Xi-Yan & Lan, Ru-Shi & Luo, Xiao-Nan. (2018). Image Encryption Using 2D Sine-Piecewise Linear Chaotic Map. 72-77. 10.1109/ICWAPR.2018.8521240.

[9] Zhu, & Wang,. (2019). A Secure and Fast Image Encryption Scheme Based on Double Chaotic S-Boxes. Entropy. 21. 790. 10.3390/e21080790.

[10] Mondal, Bhaskar & Kumar, Prabhakar & Singh, Shrey. (2018). A chaotic permutation and diffusion based image encryption algorithm for secure communications. Multimedia Tools and Applications. 77. 10.1007/s11042-018-6214-z.

[11] Rostami, Mohamad & Shahba, Abbas & Saryazdi, Saeid & Nezamabadi-pour, Hossein. (2017). A novel parallel image encryption with chaotic windows based on logistic map. Computers & Electrical Engineering. 62. 10.1016/j.compeleceng.2017.04.004.

[12] Zarebnia, M. & Pakmanesh, Hosein & Parvaz, Reza. (2018). A fast multiple-image encryption algorithm based on hybrid chaotic systems for gray scale images. Optik. 179. 10.1016/j.ijleo.2018.10.025.

[13] Ye, Guodong & Huang, Xiaoling. (2018). Spatial image encryption algorithm based on chaotic map and pixel frequency. Science China Information Sciences. 61. 10.1007/s11432-017-9191-x

[14] Xiang, Hongyue & Liu, Lingfeng. (2020). An improved digital logistic map and its application in image encryption. Multimedia Tools and Applications. 79. 1-27. 10.1007/s11042-020-09595-x.

[15] Liu, Lingfeng & Hao, Shidi & Lin, Jun & Wang, Ze & Hu, Xinyi & Miao, Suoxia. (2017). Image block encryption algorithm based on chaotic maps. IET Signal Processing. 12. 10.1049/iet-spr.2016.0584.

[16] Liu, Jingyi & Yang, Dingding & Zhou, Hongbo & Chen, Shiqiang. (2018). A digital image encryption algorithm based on bit-planes and an improved logistic map. Multimedia Tools and Applications. 77. 10.1007/s11042-017-5406-2.

[17] Batool, Syeda & Hafiz, Waseem. (2019). A novel image encryption scheme based on Arnold scrambling and Lucas series. Multimedia Tools and Applications. 78. 10.1007/s11042-019-07881-x.

[18] Luo, Yuqin & Yu, Jin & Lai, Wenrui & Liu, Lingfeng. (2019). A novel chaotic image encryption algorithm based on improved baker map and logistic map. Multimedia Tools and Applications. 78. 22023-22043. 10.1007/s11042-019-7453-3.

[19] Han, Chunyan. (2018). An Image Encryption Algorithm Based on Modified Logistic Chaotic Map. Optik. 181. 10.1016/j.ijleo.2018.12.178.

[20] Khan, Prince Waqas & Byun, Yungcheol. (2020). A Blockchain-Based Secure Image Encryption Scheme for the Industrial Internet of Things. Entropy. 22. 175. 10.3390/e22020175.

[21]Li, Ruiping. (2020). Fingerprint-related chaotic image encryption scheme based on blockchain framework. Multimedia Tools and Applications. 10.1007/s11042-020-08802-z.

[22] Zhao, Feixiang & Mingzhe, Liu & Kun, Wang & Hong, Zhang. (2021). Color image encryption via Hénon-zigzag map and chaotic restricted Boltzmann machine over Blockchain. Optics & Laser Technology. 135. 106610. 10.1016/j.optlastec.2020.106610.

[23]Jumaa, Noor. (2018). Digital Image Encryption using AES and Random Number Generator. Iraqi Journal for Electrical and Electronic Engineering. 14. 80-89. 10.37917/ijeee.14.1.8.

[24] Deb, Subhrajyoti & Biswas, Bhaskar & Bhuyan, Bubu. (2019). Secure image encryption scheme using high efficiency word-oriented feedback shift register over finite field. Multimedia Tools and Applications. 78. 10.1007/s11042-019-08086-y.

[25] Saha, Sourav & Karsh, Ram & Amrohi, Mukul. (2018). Encryption and Decryption of Images Using Secure Linear Feedback Shift Registers. 0295-0298. 10.1109/ICCSP.2018.8523833.

[26] Anwar, Shamama & Meghana, Solleti. (2019). A pixel permutation based image encryption technique using chaotic map. Multimedia Tools and Applications. 78. 10.1007/s11042-019-07852-2.

[27] Xu, Lu & Gou, Xu & Li, Zhi & Li, Jian. (2017). A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion. Optics and Lasers in Engineering. 91. 10.1016/j.optlaseng.2016.10.012.

[28] Raza, Saiyma & Satpute, Vishal. (2019). A novel bit permutation-based image encryption algorithm. Nonlinear Dynamics. 95. 10.1007/s11071-018-4600-8.

[29] Parvees, Mohamed & Abdul Samath, Jabar & Raj, I.. (2016). A colour byte scrambling technique for efficient image encryption based on combined chaotic map: Image encryption using combined chaotic map. 1067-1072. 10.1109/ICEEOT.2016.7754851.

[30] Peterson, G.. "Arnold's Cat Map." (1997).

[31] Goresky, Mark & Klapper, Andrew. (2002). Fibonacci and Galois representations of feedback-with-carry shift registers. Information Theory, IEEE Transactions on. 48. 2826 - 2836. 10.1109/TIT.2002.804048.

[32] Falih, Saad. (2016). A Pseudorandom Binary Generator Based on Chaotic Linear Feedback Shift Register. 12. 155-160. 10.37917/ijeee.12.2.5.

[33] Nakamoto, Satoshi. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailing list at https://metzdowd.com