International Journal of Multidisciplinary Research and Growth Evaluation
ISSN: 2582-7138
Received: 06-05-2021; Accepted: 27-05-2021
www.allmultidisciplinaryjournal.com
Volume 2; Issue 3; May-June 2021; Page No. 477-488

Chaos based encryption on image with hash function implementation

G Vishnu Priya [1], K Prasad Babu [2]
[1] M Tech, Department of ECE, Dr. KVSRECW, Kurnool, Andhra Pradesh, India
[2] Assistant Professor, Department of ECE, Dr. KVSRECW, Kurnool, Andhra Pradesh, India
Corresponding Author: **G Vishnu Priya**

Abstract
Security of image information has always been important in the field of data. By using image encryption algorithms, the sender encrypts the plaintext into the Cipher-text. Only the authorized receiver could decrypt the Cipher-text with the secret key to obtain the plaintext. The encryption methods mainly include seven types. Among the reported approaches, the chaos-based ones suggest a promising direction owing to their optimal trade-off between security and efficiency. The existing approach presents a new chaos-based image cipher using a plaintext-related permutation. The cat map and Lorenz system are employed to shuffle the positions of image pixels and generate the diffusion key stream, respectively. The control parameters of the cat map, i.e. the permutation key, are determined by the murmur2 hash value of the original image. The entire process of encryption is carried out in the spatial domain. The attacker can hack acquire the information from the encrypted image easily. To overcome the drawbacks with the existing approach proposed a new image framework based on the Discrete Wavelet Transform, Arnold Transform. Here the proposed approach accomplished the DWT which represents the image in the frequency domain by which the attacker can't acquire the information easily.

Keywords: Image Encryption, DWT, Murmur2hash, Cat map, Arnold Transform

1. Introduction
During the last two decades, computer networks created a revolution in the use of information. Authorized people can send and receive information from a distance using computer networks. To be secured, information needs to be hidden from unauthorized access (confidentiality), protected from unauthorized change (integrity), and available to an authorized entity, when it is needed (availability). Transmitted information over computer networks nowadays is not only textual data, but also multimedia data such as audio, image, video and other multimedia types. The security of multimedia has matured in the last few years to provide a class of tool-sets and design insights for the protection and enhancement of digital media under a number of diverse attack scenarios. In such a setting, one natural question that arises is the security and confidentiality of a digital packet of multimedia information.

Image Encryption
The primary thought in the image encryption is to transmit the image safely over the system so no unapproved client can ready to decode the image. The image information has uncommon properties, for example, mass limit, high severance and high association among the pixels that forces exceptional prerequisites on any encryption procedure [1]. The most well-known system of secure the advanced pictures is to scramble the computerized information such that unique message of the archives ought not to be identified. There are a few methodologies to accomplish this for instance steganography, packing, advanced watermarking and cryptography. Here the emphasis is on the encryption methods of advanced digital images focused around the chaos mapping. Fundamentally image encryption is the methodology of changing data utilizing a algorithm to make it ambiguous to anybody with the exception of those having exceptional learning, normally alluded to as a key and the changing data utilizing "encryption algorithm" into a structure that can't be deciphered without a key of decryption. From the other point of view, decryption of image recovers the genuine data from the encrypted structure image. There are more than a few computerized image encryption frameworks to encode and decode the image information, and there is no single encryption calculation accessible that fulfills the distin.0ctive image sorts. The encryption strategies focused around the chaos mapping gives the encoded advanced images to hold the multilevel encryption strategy furthermore diminishes the computational difficulty of the encryption process.

A large portion of the algorithms particularly intended to scramble or encrypt computerized images are proposed in the mid-1990s. There are two significant assemblies of image encryption algorithms: (a) non-chaos selective methods and (b) Chaos-based selective or non-selective methods. The vast majority of these algorithms are intended for a particular image setup compacted or uncompressed, and some of them are even setup acquiescent.

There are systems that offer light encryption (degradation), although others compromise solid manifestation of encryption. A percentage of the algorithms are versatile and have different modes ranging from degradation to solid encryption [2]. The encryption methods focused around the chaos have distinctive sorts of uses in different zones, for illustrations ; the web correspondence, military, medicinal services, mapping and situating, picture informing applications on phones, interactive media frameworks, therapeutic imaging, Tele-pharmaceutical, protection and government archives and so forth. The advancement of image encryption procedure is moving towards a prospect of unlimited conceivable outcomes. On daily basis, new strategies for encryption methods are revealed [3].

Advanced Encryption Standard (AES) is a symmetric cryptosystem that proposed for content encryption by Rijmen and Daemen in 1999 [1] furthermore known as Rijndael algorithm, however a few scientists made functional use of this algorithm for image encryption likewise with a few changes in key generation and other requirements. Zeghid *et al.* [2] proposed an improved AES based algorithm by including a key stream generator (A5/1, W7) to AES to guarantee enhancing the encryption execution for image encryption process. Most of application does not provide a facility of a secure channel to transfer the private key or desire to keep the decryption key in secret, so we need to utilize public key cryptography. In the first place public key was circulated by Diffie and Hellman in 1976 [4]. It was a key trade down to earth strategy for making an imparted secret key over a verified correspondence channel without utilizing a former imparted secret. The greater part of conventional public key cryptosystems intended to encode printed information.

Compression procedures help us to lessen the transmission data transfer capacity or storage space. These procedures can be actualized in both spatial and frequency domain. Also frequency domain procedures are further effectual and consuming collective and widespread transforms such as DCT, DFT and DWT. Data compression lessons can be classified into two types.

- **Lossy:** Lossy methods compromise a definite loss for information in return with the high compression proportion. Usually lossy methods decline the superiority of the object so they are sought out for images, videos and audios for the reason of human observation. There lossy coding method also moreover categorized into the following types.
  a) Predictive coding
  b) Transform coding

- **Lossless:** On the other hand, some kinds of data could not accept any loss (e.g. Database records, executable files and word processing files and medical images), otherwise the data will be degraded, and here the lossless techniques play role. The Lossless coding technique also further classified into following categories.
  a) Run length encoding
  b) Huffman encoding
  c) Arithmetic encoding
  d) Entropy coding
  e) Area coding

Ordinary cryptosystems identifies with the compressed multimedia. Encryption and compressed multimedia are typically extremely contradictory and an exchange off depends between them. Encrypting the interactive media content before pressure uproots a ton of repetition and this result in an exceptionally poor compression proportion. Then again, encrypting the information after compression demolishes the codec design, which are the bases for the decoders to crash.

2. Literature survey

Amitava Nag *et al.* [5] Proposed a two phase encryption and decryption algorithms that is based on shuffling the image pixels using affine transform and they encrypting the resulting image using XOR operation in year 2011. With the help of four 8-bit key applied, the pixel values are redistributed on different location using affine transform technique. In the next stage the transformed image divided into 2 pixels x 2 pixels blocks and every block is encrypted using XOR operation by using four 8-bit keys. The key used in this algorithm is s 64 bit long. Their results proved that after the affine transform the correlation between pixel values was significantly decreased.

Yicong Zhou and SosAgaian [6] introduce a new method of applying the image steganography concept for image encryption. They used the concept of e PLIP (Parameterized Logarithmic Image Processing) addition to embed the scrambled original image into a selected cover image, it generates an encrypted image. The parameterized logarithmic image processing (PLIP) model is a mathematical framework based on set of precise operations that can be applied to the processing of intensity images valued in a bounded range. Result analysis shows that the algorithm has a very large key space and can withstand several common attacks.

In 2011 Yun sen and Gunayi Wang [7] proposed a modified chaotic map technique In order to improve the security of chaotic encryption algorithm. One of the advantage of their technique is that when we compared it with original logistic map, their proposed map makes it always be chaotic, and expands the iteration range from original (0, 1) to (0, 4λ) (λ>0.25). This is important for expanding key space of chaotic sequence and enhancing rate of change of chaotic signal. An encryption algorithm is designed based on this chaotic map and some analysis is presented to show its good efficiency. Experimental results show that the modified Logistic map possesses faster encryption, faster sequence generation rate, bigger key space and speed against the original logistic map in 2011.

In 2012 Qiudong Sun et.al. [8] Presented a random scrambling algorithm based on bit-planes decomposition of image. Their Algorithm starts by decomposing a gray image into bit-plane images, each image for separate bit plane. In the next step every bit plane image is shuffled by using a random scrambling algorithm. At last, all the shuffled bit plane images are merged according to their original levels on bit-planes and we obtained an encrypted image. Experimental results show that the proposed algorithm scrambled an image effectively as well as changed its histogram apparently. It has better efficiency and properties than the general random scrambling method. Therefore it has more stable scrambling degree than the classical method like Arnold transform.

In 2012 SukalyanSom and AtanuKotal [9] presented multiple chaotic maps based a new symmetric image encryption

algorithm. In the proposed algorithm, with the help of generalized Arnold Cat Map, the plain image is first scrambled. Further, the scrambled image at a particular iteration is encrypted using chaotic sequences generated by one dimensional Logistic Map after preprocessing them to integers. The results indicate that the proposed algorithm can successfully encrypt and decrypt grayscale images with secret keys. It also exhibit that the proposed method is secure, loss-less, and efficient.

In 2013 A. Kester [10] proposed a new technique that contribute to the general body of knowledge in the area of cryptography application by developing a new cipher algorithm for image encryption of m*n size by shuffling the RGB pixel values. With the help of RGB pixels, this algorithm ultimately encrypts and decrypts the images. The algorithm was implemented using MATLAB. In this method, neither the bit values of the pixel are affected and nor pixel expansion at the end of the encryption and the decryption process. In place of the numerical values are transposed, reshaped and concatenated with the RGB values, it shifted away from its respective positions and the RGB values interchanged in order to obtain the cipher image. This shows that, the total change in the sum of all values in the image is zero. Therefore there is no change in the total size of the image during encryption and decryption process. Advantage of their method is that the characteristic sizes of image will remain unchanged, while the encryption process is being performed.

In [11], the feasibility of selective image encryption on a bit plane is investigated. It is concluded that only selectively encrypting 50% of the whole image data can gain an acceptable security. Therefore, the encryption time is substantially reduced.

In [12-15], schemes with certain diffusion effect introduced in the permutation stage are proposed. As the pixel value mixing effect is contributed by both stages, the number of iteration rounds required by the diffusion procedure is reduced, and hence the performance of the cryptosystem is improved.

In [16], Wong *et al*. proposed a more efficient diffusion mechanism using simple table lookup and swapping techniques as a light-weight replacement of the 1D chaotic map iteration.

In [17], Wang *et al.* proposed a fast image encryption algorithm that combines the permutation and diffusion stages so that the pixel values are changed while the image blocks are being relocated. As a result, the image needs to be scanned only once in each encryption round, while conventional schemes separate the permutation and diffusion stages therefore require at least two image-scanning processes.

In [18], a fast image cipher using novel bidirectional diffusion is proposed. Theoretical analysis and simulation results indicate that a satisfactory level of security can be achieved with only one round of permutation and two rounds of diffusion operations.

Table 1: Comparisons of methods

Name	Methodology	Advantages	Disadvantages
A cryptographic Image Encryption technique based on the RGB PIXEL shuffling, 2013	Image encryption by shuffling the RGB pixel values.	effective in terms of the security analysis, increase of security of the image against all possible attacks	R, G, and B Pixels shuffling takes more times than other methods, Lot of confusion in process, Permutation process is too complex, Time taking and also chances of mistakes are high
Confusion and Diffusion of Grayscale Images Using Multiple Chaotic Maps, 2012	The plain image is first scrambled using generalized Arnold Cat Map. Further, the scrambled image at a particular iteration is encrypted using chaotic sequences generated by one dimensional Logistic Map	loss-less; secure and efficient; low correlation among pixels; a very large key space; high sensitivity to secret keys;	Time taking and risky, no changes in shuffled histogram, quality of encryption is low
Image Encryption Based on Bit-plane Decomposition and Random Scrambling, 2012	Decomposes a gray image into several bit-plane images Then shuffles them by a random scrambling algorithm separately. Lastly, merges the scrambled bit-plane images according to their original levels on bit-planes and gained an encrypted image	better efficiency, more stable scrambling degree than the classical method, image histogram is changed apparently,	Very time consuming, Some sort of security problem, Key is sensitive to crack. No specific technique is used for scrambling.
An Image Encryption Scheme Based on Modified Logistic Map, 2011	a modified chaotic map, which is based on the Logistic map, is used for image encryption	bigger key space, faster sequence generation rate, faster encryption speed	Due to its high-level simplicity, possible to decrypt image, correlation between pixels exists, sensitive to initial values.
Image Encryption Using the Image Steganography Concept and PLIP Model, 2011	To encrypt to original image it is embedded into the cover image, it fuses the scrambled original image with the cover image using the PLIP addition via specific parameters	Large key space, can withstand several common attacks	Due to lots of mathematical computational, it takes long time to encrypted the image, correlation between pixels still exists;
Image Encryption Using Affine Transform And XOR Operation, 2011	redistribute the pixel values to different location using affine transform technique transformed image is then encrypted using XOR operation	Better Solution and Correlation between pixels values significantly decreases	Lengthy, complicated, Time Consuming and chances of mistakes is high.
A Combination Of Permutation Technique Followed By Encryption, 2008	First pixels are shuffles based on permutation techniques used and then shuffled pixels are encrypted using Rijn Dael algorithm.	Higher Entropy and Correlation between image elements decreased	Permutation process is too complex, Time taking and also chances of mistakes are high
Encryption Image Encryption Using Block Based Transformation Algorithm, 2006	original image is divided into blocks, which are rearranged into a transformed image using a transformation algorithm presented, and then the transformed image was encrypted using the Blowfish algorithm	No key generator, correlation between image elements decreased and higher entropy.	Image loosing and lower Correlation, no standard technique is used for block transformation.

3. Implementation

Below figure represents existing method of encryption and decryption algorithms.

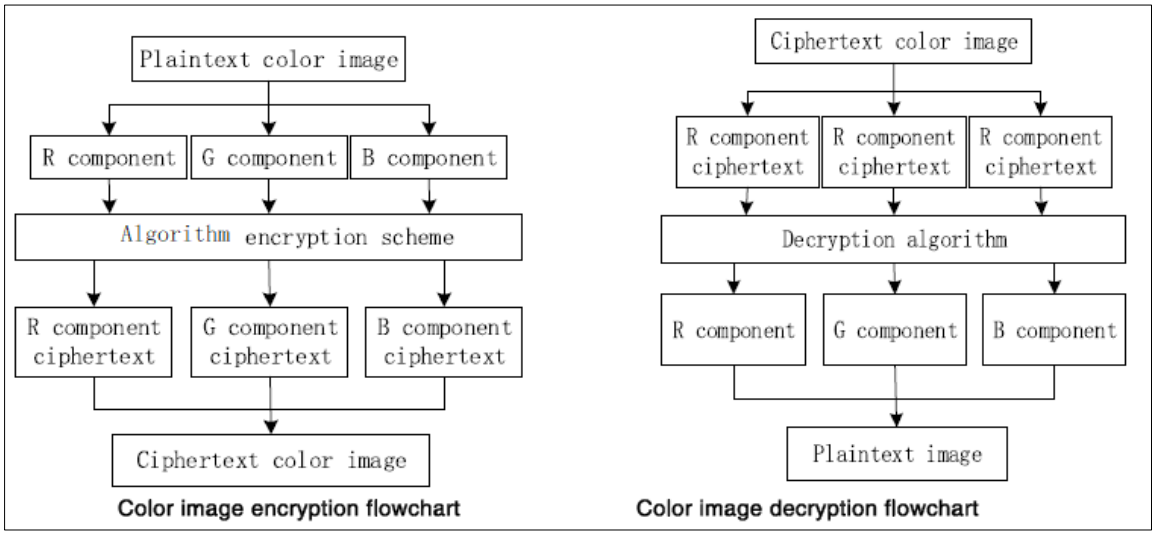


Fig 1: Existing System Design

In existing system, the color image encryption step is separating the R component, G component and B component of the color image, encrypting the three components separately using the proposed scheme for gray image encryption, and originally combining the cipher text image into a color cipher text image. The decryption algorithm is the inverse process of the encryption algorithm.

The proposed system is as shown below fig 2.

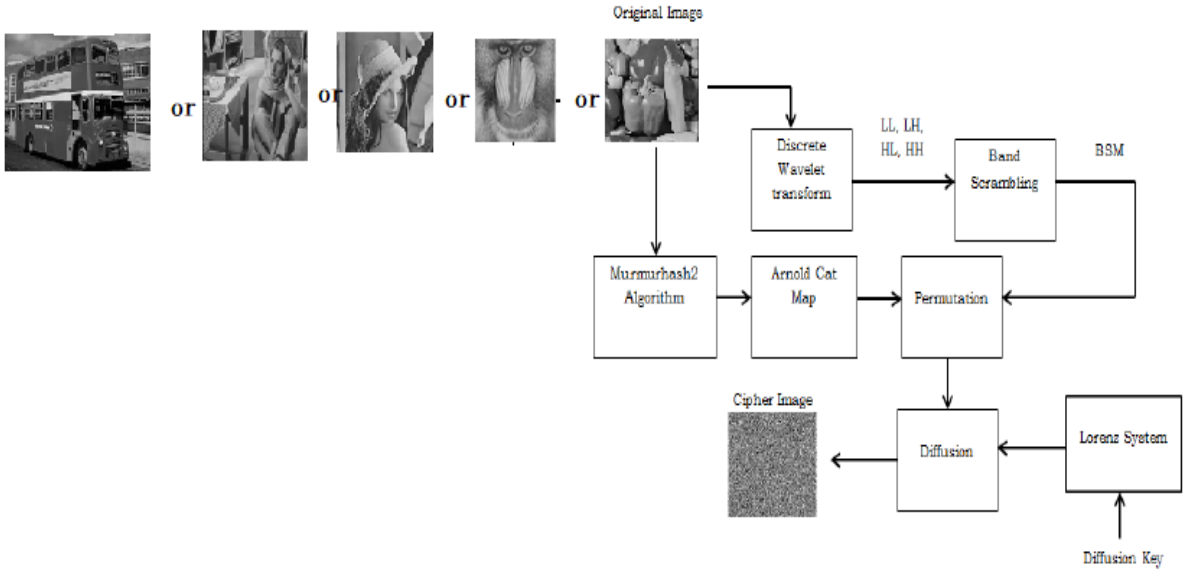


Fig 2: Proposed System Design

Under proposed structure, the original image is firstly decomposed through Discrete Wavelet transform into subbands. All the obtained frequency bands are formulated into a band scrambling matrix by the horizontal followed by vertical concatenation. Then the Band scrambling matrix is shuffled by using Arnold cat map, whose control parameters, i.e. the permutation key, are given by the hash value of the original image. As is known, the essential property of a hash function is that it almost surely produces different hash values for different messages. This means different images are rearranged in different ways and a satisfactory diffusion effect will be achieved with only one round of encryption. In our scheme, the 64-bit version Murmurhash2 algorithm, created by Austin Appleby in 2008, is employed. The algorithm outperforms most other ones because of its excellent distribution, avalanche behavior, collision resistance and performance. In the diffusion stage, the shuffled data are masked by a key stream extracted from the orbit of Lorenz system. A large key space is ensured as the three state variables of the Lorenz system are used as the diffusion key. The detailed DWT, permutation and diffusion operations are discussed as follows.

In wavelet transformation, a mother wavelet is selected, a function that is nonzero in some small interval, and it is used to explore the properties of the function f(t) in that interval. The mother wavelet is then translated to another interval of time and used in the same way. So with wavelet transforms, signals with sharp discontinuities can be approximated and also they provide a time-frequency representation of the signal. There are many wavelets discovered. The simplest one is the Haar wavelet. Information that is produced and analyzed in real-life situations is discrete. It comes in the form of numbers, rather than a continuous function. This is why the discrete rather than the continuous wavelet transform

is the one used in practice. When the input data consists of sequences of integers as in the case for images, wavelet transforms that map integers to integers can be used. Integer Wavelet Transform (IWT) is one such approach.

One of the most popular cover objects used for steganography is an image. Cover images may be grayscale images or color images. Color images have large space for information hiding and therefore color image steganography is more popular than gray scale image steganography. Color images can be represented in various formats such as RGB (Red Green Blue), HSV (Hue, Saturation, Value), YUV, YIQ, YCbCr (Luminance, Chrominance) etc3. Color image steganography can be done in any color space domain. When the wavelet transform is applied to a color image, the transformation coefficients are obtained for all the three channels in the corresponding representation.

Audio signals are analog signals. To use digital signal processing methods on an analog signal, it is sampled periodically in time. It produces sequence of samples. Audio files are stored in various file formats.WAV file is the simplest format. Unlike MP3 and other compressed formats, WAVs store samples "in the raw" where no pre-processing is required. MP3 is a popular audio signal format used everywhere. The MP3standard involves a coding technique that includes several methods namely, sub-band decomposition, filter bank analysis, transform coding, entropy coding, dynamic bit allocation and psychoacoustic analysis. The encoder operates on successive tracks of audio signal. Each track contains 1152 samples and one track is further divided into two pieces with 576 samples each. A hybrid filter bank is applied to enhance the frequency resolution4.When wavelet transform is applied to an image, it is decomposed into four sub-bands LL, LH, HL and HH. LL is the low frequency sub-band and contains approximation coefficients. The significant features of the image are contained in this sub-band. Other three sub-bands are high frequency sub-bands and contain less significant features. It is possible to reconstruct the image by considering only LL sub-band. When audio samples are transformed, approximation and detailed coefficients are produced. Approximation coefficients contain the most significant features. In this case also it is possible to reconstruct the audio signal by considering only approximation coefficients.

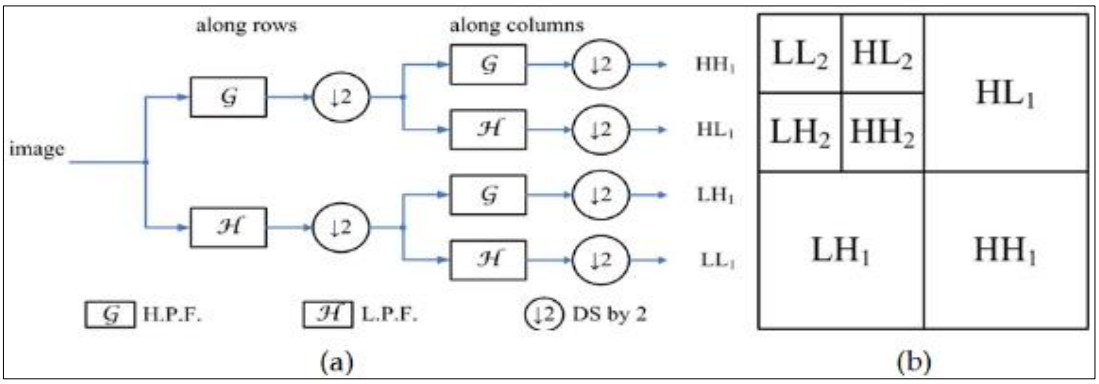


Fig 3: Diagrams of DWT image decomposition: a) The 1-L 2-D analysis DWT image decomposition process, b) The 2-L 2-D analysis DWT sub-band

Permutation Process

Arnold cat map

The Arnold cat map, described by Eq. (1), is a chaotic bijection of a unit square onto itself.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \ mod\ 1 \qquad (1)$$

Where p and q are control parameters, and x mod 1 means the fractional part of x for any real number x. To incorporate the map into image permutation that operated on a lattice of finite number of pixels, it has to be discretized. This can be done simply by changing the range of (x, y) from the unit square to the lattice $N \times N$, as follows.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \ mod\ N \qquad (2)$$

Where N is the number of pixels in one row (column). The inverse transform of the map is easily found to be given by.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} pq+1 & -p \\ -q & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \ mod\ N \qquad (3)$$

To determine the value of p and q, the 64-bit Murmur2hash value of the original image is firstly divided into two 32-bit parts, which are denoted by *hashl* and *hashr*, respectively. As the four-tuple $[1, (p+k1N), (q+k2N), (p+k3N)(q+k4N)+1]$ produce the same output as the four-tuple $[1, p, q, (pq+1)]$ forany $k1, k2, k3, k4 \in Z$, the two parameters are given by *mod*(*hashl*, *N*) and *mod*(*hashr*, *N*), respectively. The utilization of small parameters also speeds up the calculation. The pseudo code of the MrumurHash2 algorithm is listed below, where the argument *key* is a pointer that points to the image data. As can be seen from the pseudo code, the algorithm uses bitwise and integer multiplication operations to manipulate and update the hash value. As is known, the two operations are very efficient for hardware implementation, and thereby the computation cost of the hash algorithm is much lower than that of one round of diffusion operation, where the manipulations of real numbers are required.

Murmurhash2 algorithm

MurmurHash is a non-cryptographic hash function suitable for general hash-based lookup. It was created by Austin Appleby in 2008 and is currently hosted on Github along with its test suite named 'SMHasher'. It also exists in a number of variants, all of which have been released into the public domain. The name comes from two basic operations, multiply (MU) and rotate (R), used in its inner loop. Unlike cryptographic hash functions, it is not specifically designed to be difficult to reverse by an adversary, making it unsuitable for cryptographic purposes.

The older MurmurHash2 yields a 32-bit or 64-bit value. Slower versions of MurmurHash2 are available for big-

endian and aligned-only machines. The MurmurHash2A variant adds the Merkle-Damgård construction so that it can be called incrementally. There are two variants which generate 64-bit values; MurmurHash64A, which is optimized for 64-bit processors, and MurmurHash64B, for 32-bit ones. MurmurHash2-160 generates the 160-bit hash, and MurmurHash1 is obsolete. Hash functions can be vulnerable to attack if a user can choose input data in such as a way to intentionally cause hash collisions. Jean-Philippe Aumasson and Daniel J. Bernstein were able to show that even implementations of MurmurHash using a randomized seed are vulnerable to so-called Hash DoS attacks. With the use of differential cryptanalysis they were able to generate inputs that would lead to a hash collision. The authors of the attack recommend using their own Sip Hash instead.

Pseudocode of MrumurHash2 algorithm
Murmur2_64(key, len, seed) *m ←0xc6a4a7935bd1e995;* *r ← 47* *hash ← seed ^ (len* m)* *for each eight Byte Chunk of key* *k ← eight Byte Chunk* *k ← k × m* *k ← k XOR (k >> r)* *k ← k × m* *hash ← hash XOR k* *hash ← hash × m* *end for* *with any remaining Bytes In Key* *remaining Bytes ←* *Swap Endian Order Of (remaining Bytes In Key)* *// Note: Endian swapping is only necessary on big-endian machines.* *hash ← hash XOR remaining Bytes* *hash ← hash × m* *end with* *hash ← hash XOR (hash >> r)* *hash ← hash × m* *hash ← hash XOR (hash >> r)*

Diffusion Process

The well-known Lorenz system, developed by Edward Lorenz in 1963 for atmospheric convection, is described by.

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = x(\rho - z) - y \\ \dot{z} = xy - \beta z \end{cases} \quad (4)$$

Where t is time and σ, ρ, $\beta$are the system parameters. Thesystem is chaotic for the values of σ =10, ρ =8/3, β=28. The initial values of the state variables, ($x0$, $y0$, $z0$), are used as the diffusion key.

The detailed diffusion process is described as follows.

Step 1: Arrange the pixels of the shuffled image to a vector $p = \{p_0, p_1, \ldots p_{N\times N-1}\}$ in the order from left to right, top to bottom.

Step 2: Generate a key stream with length equal to p.

Step 2.1: Pre-iterate system (4) for I_0 times to the harmful effect of transitional procedure, where $I0$ is a constant. The fourth-order Runge-Kutta method is employed for solving the equation.

Step 2.2: Iterate system (4.4) for t times, where t =ceil ($N\times N/3$). For each iteration, the current values of the three state variables are appended to a vector $Ls = \{s_0, s_1, \ldots, s_{N\times N-1}\}$. Obviously, there are $r = (t\times 3\text{-}N\times N)$ redundant elements, which are discarded.

Step 2.3: Qualify a key stream $k = \{k_0, k_1, \ldots, k_{N\times N-1}\}$ from Ls according to

$$k_n = mod[sig_{N(abs(s_n))}, 2^L] \quad (5)$$

Where L is the color depth of the original image, $abs(x)$ returns the absolute value of x, and $sig\_n(x)$ returns the n most significant decimal digits of x, where n is the precision of x. In our scheme, all the variables are declared as double-precision type, which has a precision of 15 decimal digits.

Step 3: Calculate the cipher-pixels value according to Eq.(6).

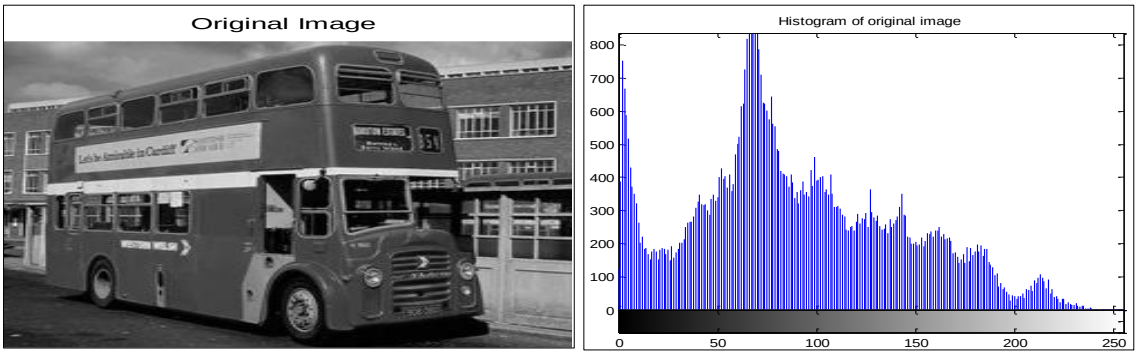
$$c_n = k_n \oplus \{[p_n + k_n] mod\ 2^L\} \oplus c_{n-1} \quad (6)$$

Where $c_n$and c_{n-1} are the output and previous cipher-pixels, respectively, and $\oplus$ performs bit-wise exclusive OR operation.One may set the initial value c_1 as a constant. The decipher procedure is the same as that of the encipher process described above except that the inverse of Eq. (6), described by Eq. (7), is employed.

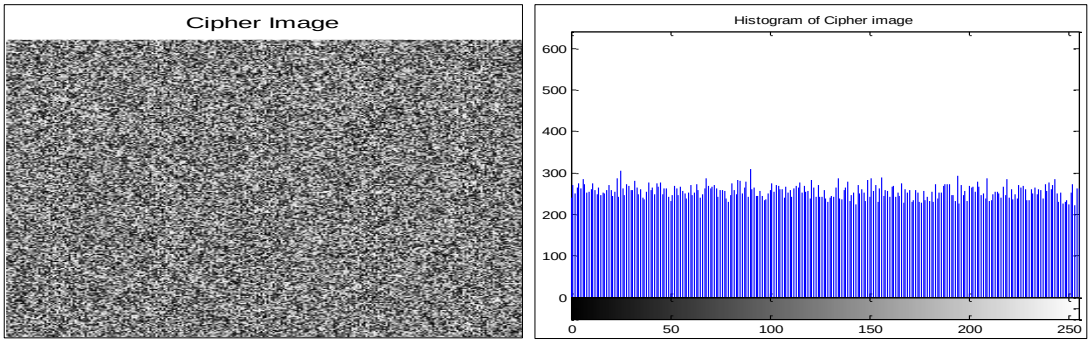
$$p_n = [k_n \oplus c_n \oplus c_{n-1} + 2^L - k_n] mod\ 2^L \quad (7)$$

4. Simulation results

Using matlab the results are obtained as shown below with the algorithms implemented



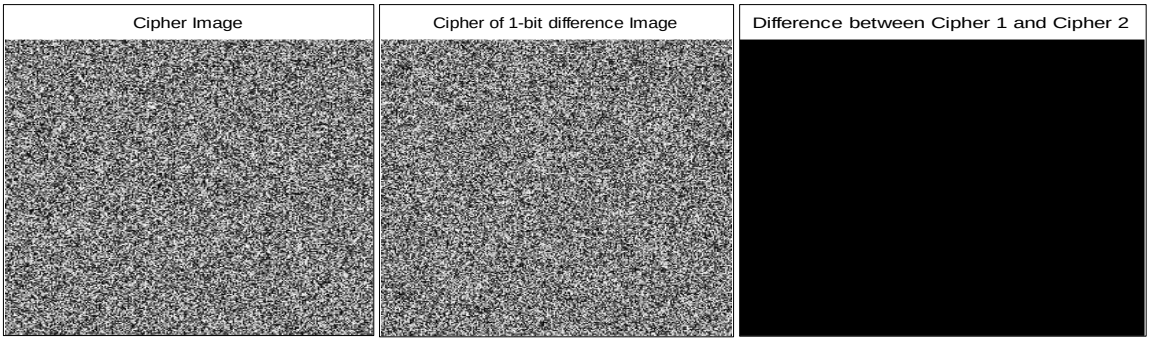
a) b)



c) d)

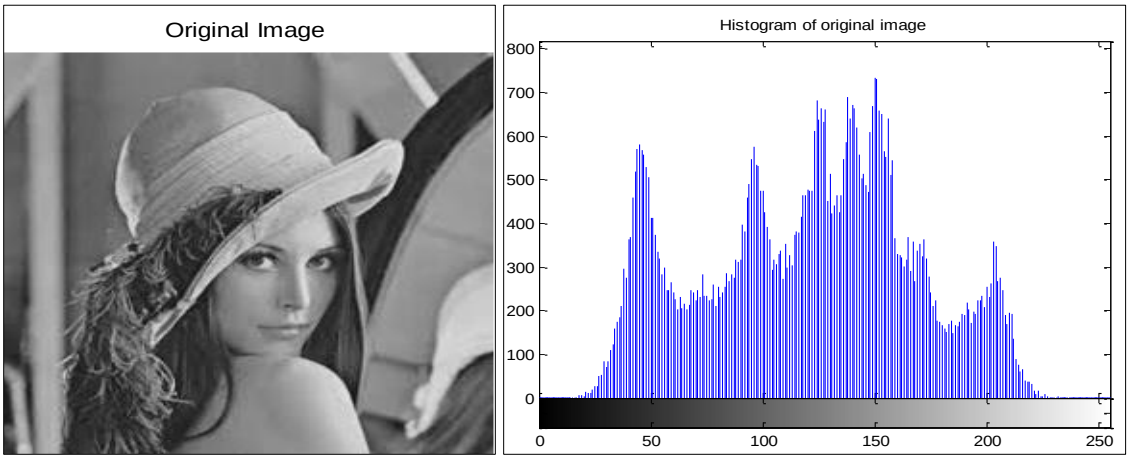
Fig 4: Histograms of the Bus test image and its output cipher image. a) The Bus test image, b) Histogram of a), c) Cipher image corresponding to a), d) Histogram of c).

a) b)

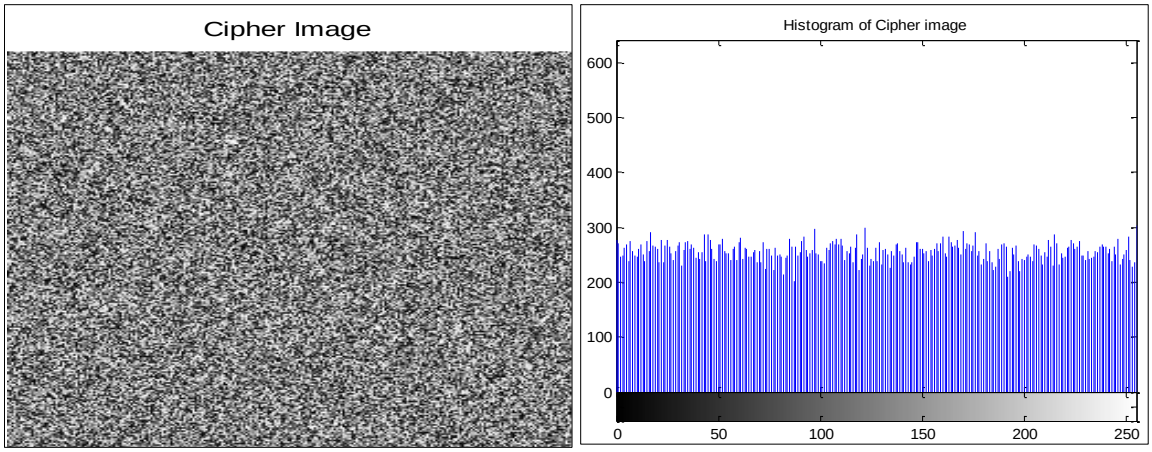


c) d) e)

Fig 5: The application of the proposed permutation algorithm. a) The original Lena test image, b) The image with 1-bit difference from a), c) The shuffled image corresponding to a), d) The shuffled image corresponding to b), e) The differential image between c) and d)

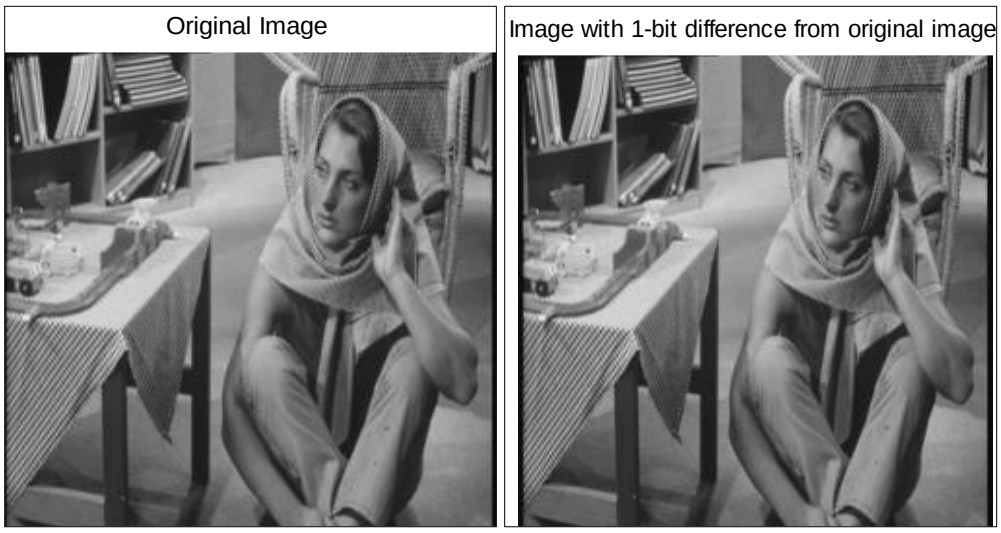


a) b)

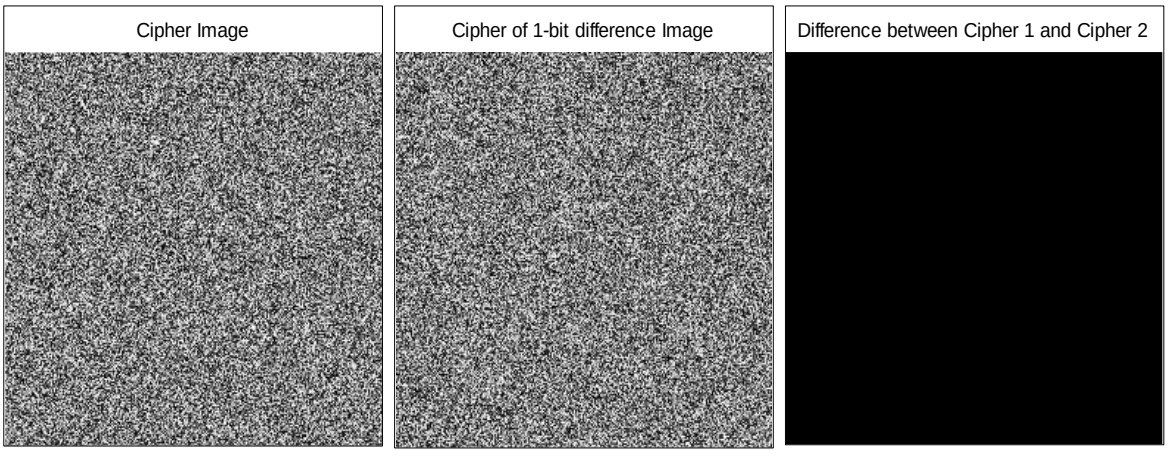


c) d)

Fig6: Histograms of the Lena test image and its output cipher image. a) The Lena test image, b) Histogram of a), c) Cipher image corresponding to a), d) Histogram of (c)



a) b)



c) d) e)

Fig 7: The application of the proposed permutation algorithm. a) The original Barbara test image, b) The image with 1-bit difference from a), c) The shuffled image corresponding to a), d) The shuffled image corresponding to b), e) The differential image between c) and d)

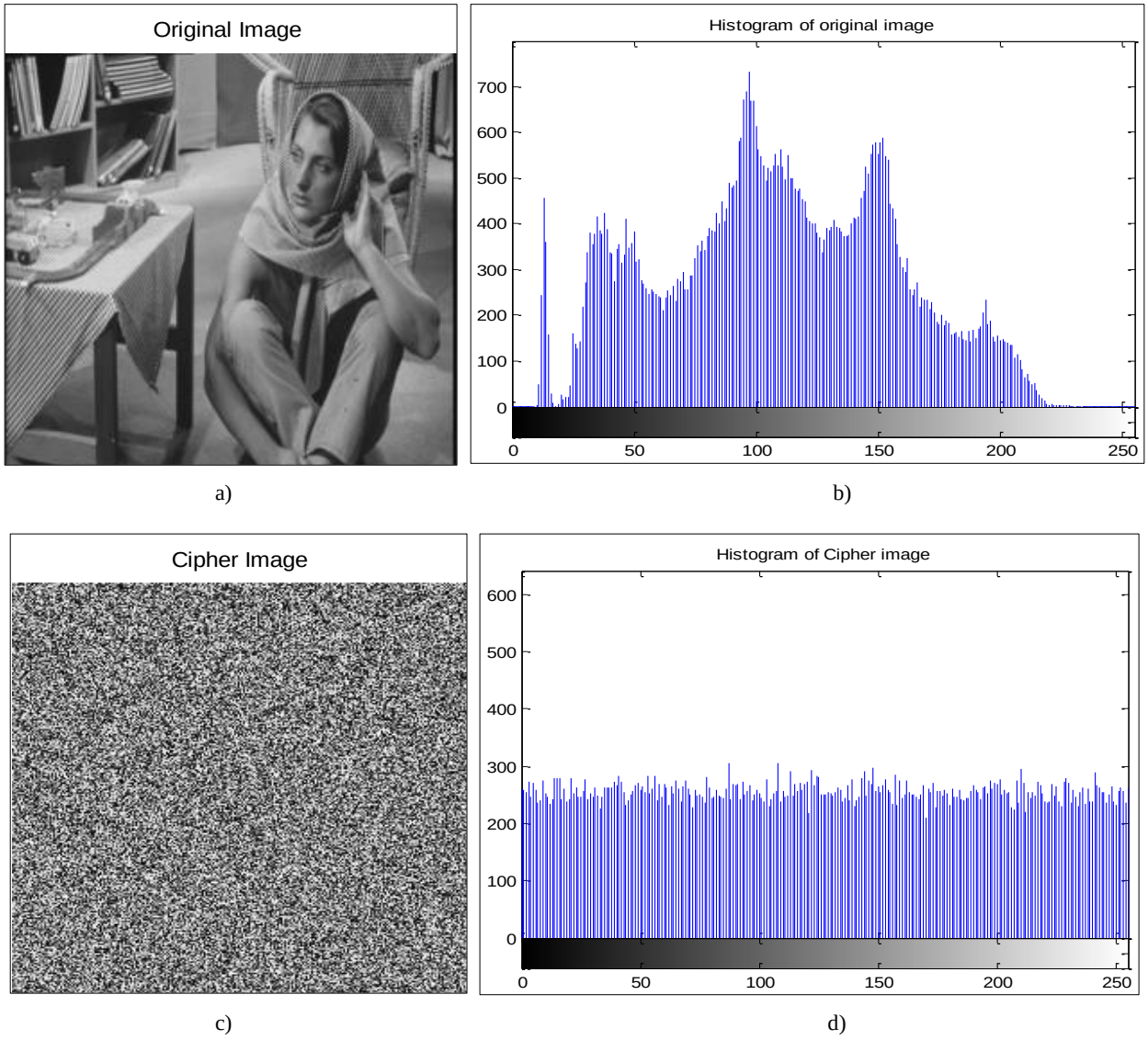
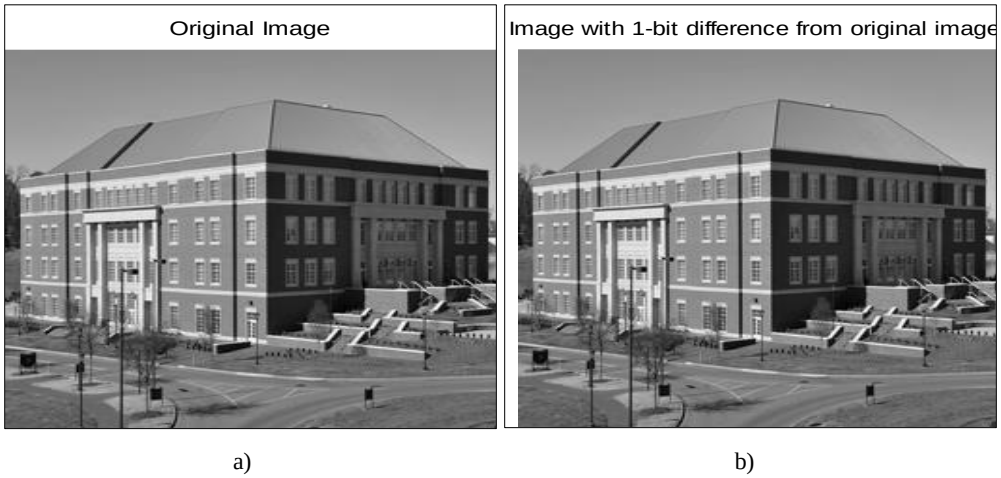
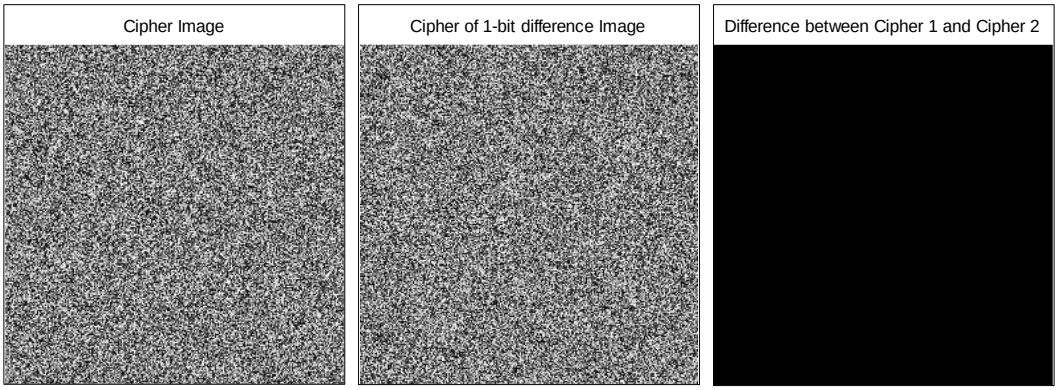


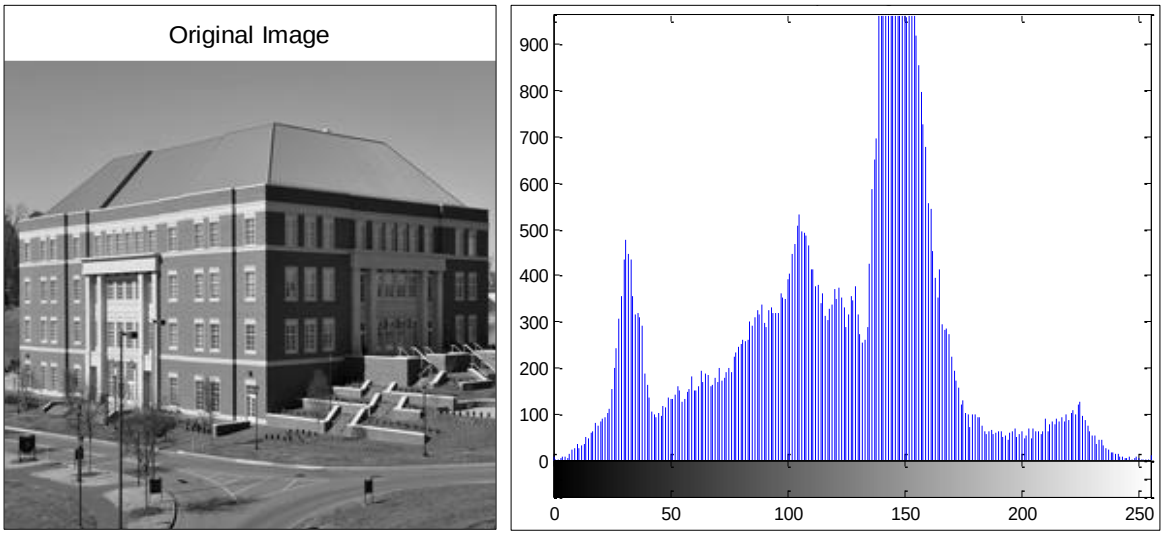
Fig 8: Histograms of the Barbara test image and its output cipher image. a) The Barbara test image, b) Histogram of a), c) Cipher image corresponding to a), d) Histogram of c)



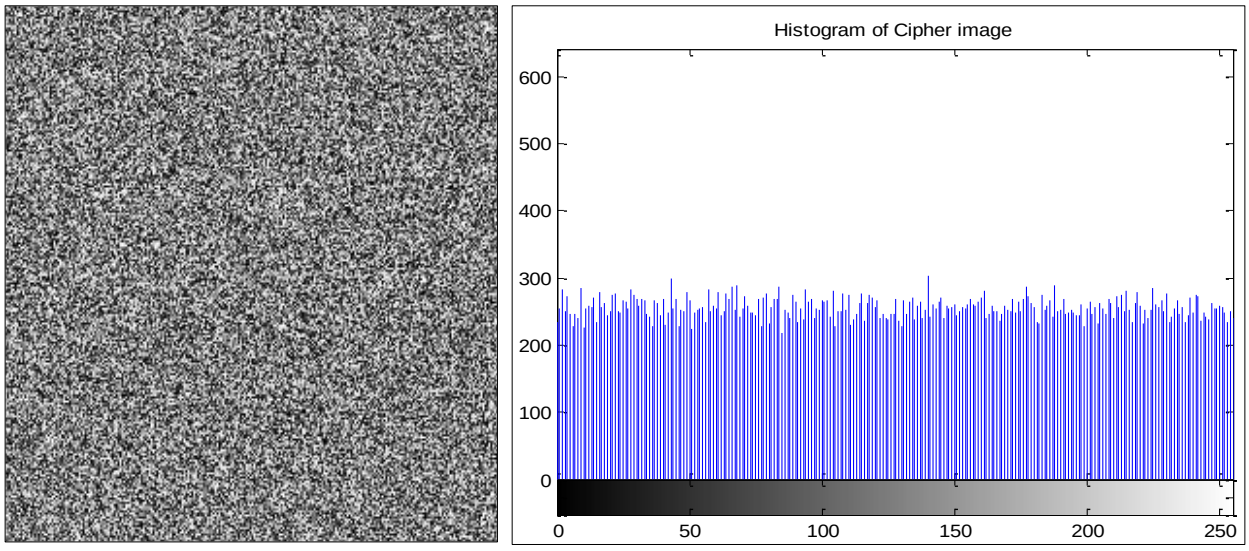


c) d) e)

Fig 9: The application of the proposed permutation algorithm. a) The original House test image, b) The image with 1-bit difference from a), c) The shuffled image corresponding to a), d) The shuffled image corresponding to b), e) The differential image between c) and d).



a) b)



c) d)

Fig 10: Histograms of the House test image and its output cipher image. a) The House test image, b) Histogram of a), c) Cipher image corresponding to a); d) Histogram of c)

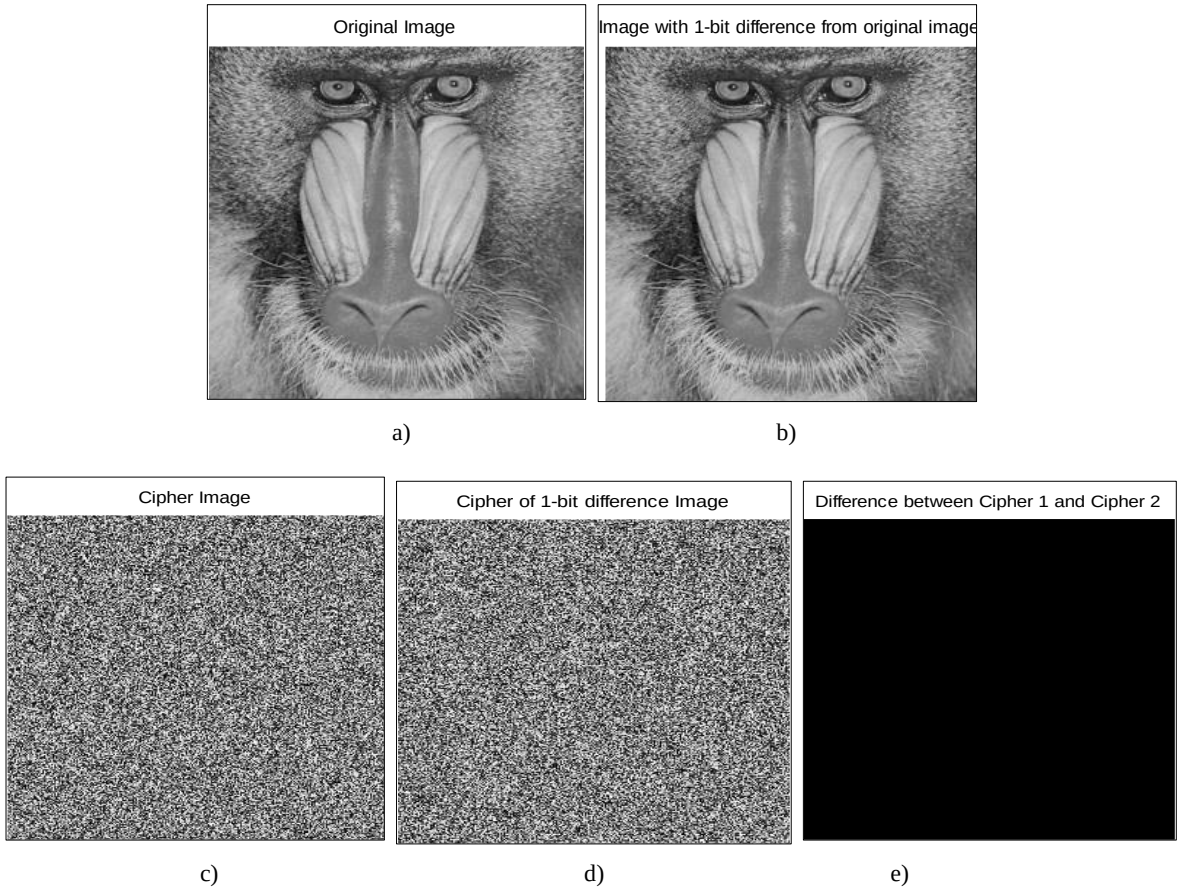


Fig 11: The application of the proposed permutation algorithm. a) The original Baboon test image, b) The image with 1-bit difference from a), c) The shuffled image corresponding to a), d) The shuffled image corresponding to b), e) The differential image between c) and d)

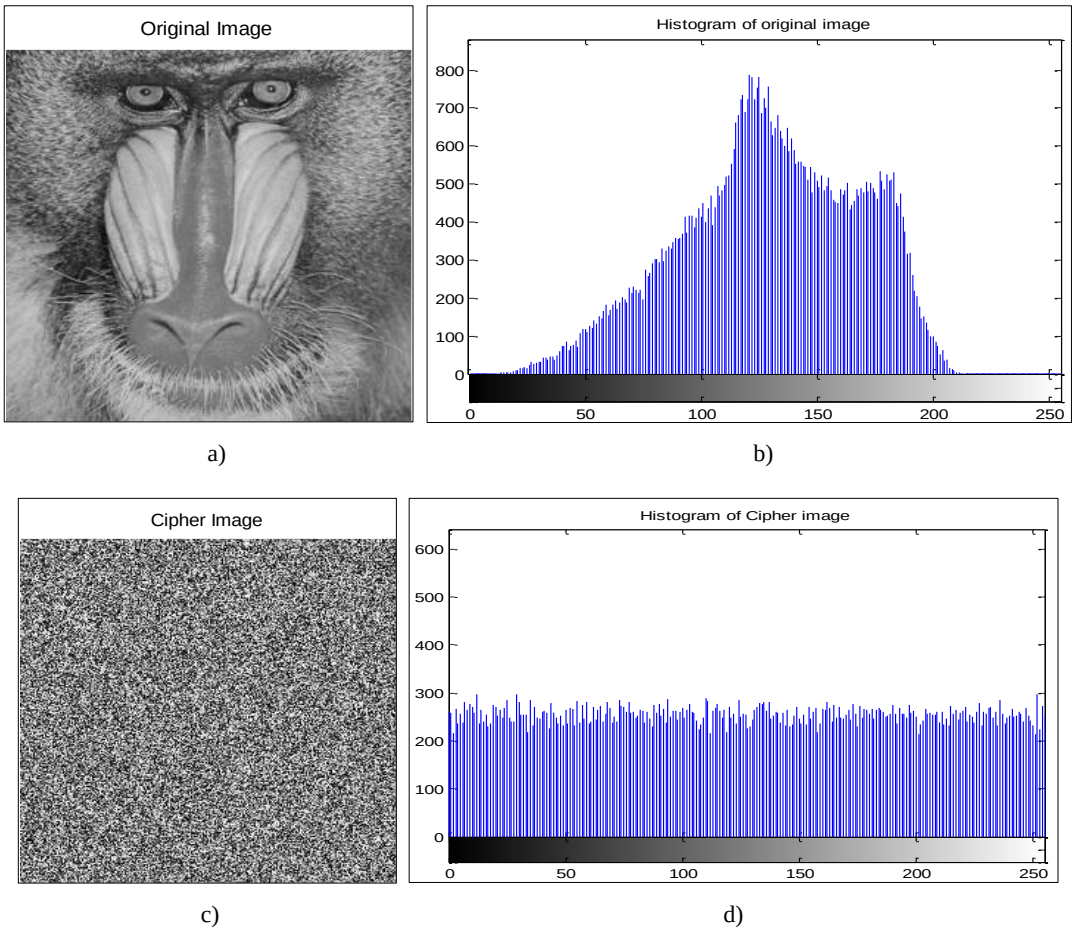


Fig 12: Histograms of the Baboon test image and its output cipher image. a) The Baboon test image, b) Histogram of a), c) Cipher image corresponding to a), d) Histogram of c)

Table2: Entropies of original and cipher images

Test Image	Entropy	
	Plain Image	Cipher Image
Peppers	7.5721	7.9969
Lena	7.4366	7.9970
Barbara	7.4838	7.9973
House	7.2743	7.9975
Baboon	7.2283	7.9970
Bus	7.5209	7.9973

As can been seen from Table 2,the entropy of all the output cipher images are very close to the theoretical value of 8. This means the proposed scheme produces outputs with perfect randomness and hence is robust against frequency analysis.

Table3: Correlation Coefficients for Adjacent Pixels in Five Test Images and Their Output Cipher Images

Test Image	Original			Ciphered		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Peppers	0.9654	0.9679	0.9142	-0.0034	-0.0030	-0.0997
Lena	0.9492	0.9744	0.9363	-0.0042	0.0021	0.0117
Barbara	0.9022	0.9485	0.9260	-0.0095	-0.0073	-0.0257
House	0.8952	0.8994	0.8403	0.0074	-0.0058	0.0653
Baboon	0.8742	0.8219	0.7549	0.0058	-0.0029	0.0178
Bus	0.9028	0.8847	0.7966	0.0030	-0.0060	-0.0101

5. Conclusion

This work has proposed a fast chaos-based image cipher with a permutation-diffusion structure using Discrete Wavelet transform. The cat map and Lorenz system are employed to transform the pixel positions and generate the diffusion key stream, respectively. In the permutation stage, the Murmur2 hash value of the original image is calculated to determine the control parameters of the cat map. Owing to the avalanche property of hash functions, completely different shuffled images will be produced even if there is a tiny difference between the original ones, and it helps accelerate the diffusion process.

Experimental results indicate that the proposed scheme requires only one and two cipher cycles to achieve an acceptable and a satisfactory level of security. Extensive security analysis has been carried out, including the most important ones like statistical analysis, and plaintext sensitivity analysis, which have demonstrated the satisfactory security of the new scheme.

6. References

1. Daemen J, Rijmen V. AES Proposal: Rijndael, AES Algorithm Submission, 1999.
2. Zeghid M, Machhout M, Khriji L, Baganne A, Tourki R. A Modified AES based algorithm for image encryption. World Academy of Science, Engineering & Technology, 2007.
3. Subramanyan B, Chhabria VM, Babu TGS. Image encryption based on AES key expansion. Second International IEEE Conference on Emerging Applications of Information Technology, 2011.
4. Diffie W, Hellman ME. New directions in cryptography. IEEE Transactions on Information Theory. 1976; 22(6).
5. Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, Sarkar Partha Pratim Sarkar D. Image Encryption using affine transform and XOR operation. IEEE International Conference on Signal Processing, Communication, Computing and Networking Technologies, 2011.
6. Yicong Zhou, SosAgaian. Image Encryption Using the Image Steganography Concept and PLIP Model. Proceedings of 2011 International Conference on System Science and Engineering, Macau, China, 2011.
7. Yue Sun, Guangyi Wang. An image encryption scheme based on modified logistic map. Fourth International Workshop on Chaos-Fractals Theories and Applications, 2011.
8. Qiudong Sun, Wenying Yan, Jiangwei Huang, Wenxin Ma. Image encryption based on Bit-plane decomposition and random scrambling. 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 2012.
9. Sukalyan Som, Atanu Kotal. Confusion and diffusion of grayscale images using multiple chaotic maps. National Conference on Computing and Communication Systems (NCCCS), 2012.
10. Quist-Aphetsi Kester. A cryptographic image encryption technique based on the RGB Pixel shuffling. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET). 2013; 2(2).
11. Xiang T, Wong KW, Liao X. Selective image encryption using a spatiotemporal chaotic system. Chaos: An Interdisciplinary Journal of Nonlinear Science. 2007; 17(2). Article no: 023115.
12. Wong KW, Kwok BSH, Law WS. A fast image encryption scheme based on chaotic standard map," Physics Letters A. 2008; 372(15):2645-2652.
13. Fu C, Lin BB, Miao YS, Liu X, Chen JJ. A novel chaos based bit-level permutation scheme for digital image encryption. Optics Communications. 2011; 284(23):5415-5423.
14. Fu C, Meng WH, Zhan YF, Zhu ZL, Lau FC, Chi KT, Ma HF. An efficient and secure medical image protection scheme based on chaotic maps. Computers in biology and medicine. 2013; 43(8):1000-1010.
15. Fu C, Huang JB, Wang NN, Hou QB, Lei WM. Asymmetric chaos-based image cipher with an improved bit-level permutation strategy. Entropy. 2014; 16(2):770-788.
16. Wong KW, Kwok BSH, Yuen CH. An efficient diffusion approach for chaos-based image encryption. Chaos, Solitons & Fractals. 2009; 41(5):2652-2663.
17. Wang Y, Wong KW, Liao X, Chen G. A new chaos-based fast image encryption algorithm. Applied soft computing. 2011; 11(1):514-522.
18. Fu C, Chen JJ, Zou H, Meng WH, Zhan YF, Yu YW. A chaos-based digital image encryption scheme with an improved diffusion strategy. Optics Express. 2012; 20(3):2363-2378.
19. Tao LI, Baoxiang DU, Xiaowen Liang. Image encryption algorithm based on logistic and two dimensional Lorenz. Special Section on Emerging Approaches to Cyber Security, IEEE Access. Doi: 10.1109/ACCESS.2020.2966264 [January 23, 2020]