International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 03 | March - 2021 ISSN: 2582-3930

A Bitwise Image Encryption Technique using Instant Key Generation

Jyoti Kansari1, Avinash Dhole2, Yogesh Rathore3

M.TECH student, Computer Science and Engineering 1

Raipur Institutes of Technology, Raipur, India1

Asst. Prof., Department of Computer Science and Engineering [2,3]

Raipur Institutes of Technology, Raipur, India [2,3]

Abstract - In data communication and multimedia application, security plays a crucial role for transmission of knowledge and pictures. In recent years, the latest encryption technology has improved the safety of multimedia data from unauthorized access. Multimedia encryption techniques converts original data to other form which is hard to recognized and is known as cipher-text. At the present, there are several conventional encoding algorithms are available like, AES, RSA and IDEA which are used for encryption of text and binary data.The essential methods have a fixed length of a key. However, the traditional algorithms are inefficient to use them directly in multimedia data and colour image encryption due to high correlation among pixels. Here in this paper, we have discussed various encryption techniques and trying to focus its merits and demerits on encryption of images. We have also find out the gaps of all major key generated encryption techniques and proposed their solutions through this paper. This paper may en light the path of new researcher who are working in image encryption using key generation method and bitwise operation.

Key Words: Confusion, Diffusion, Secret Key, bitwise transformation, Henon map, Chaos .

1.INTRODUCTION

Encryption is a process that transforms the first information into an unrecognizable form. The process that converts plaintext to cipher form is called encryption. The new form of the message is wholly different from the original message. An original massage is named as the plaintext, while the encoded message is named as cipher-text. The transmission from the cipher-text into plaintext is known as decryption process. This form of message is read and understood by a human or a computer. Many schemes are there that are used for encryption. Such a method is understood as a cryptographic scheme or a cipher. Schemes used for decrypting a message with none knowledge of the encrypted details falls under the world of cryptanalysis. The area of cryptography and cryptanalysis is jointly called cryptology [23].

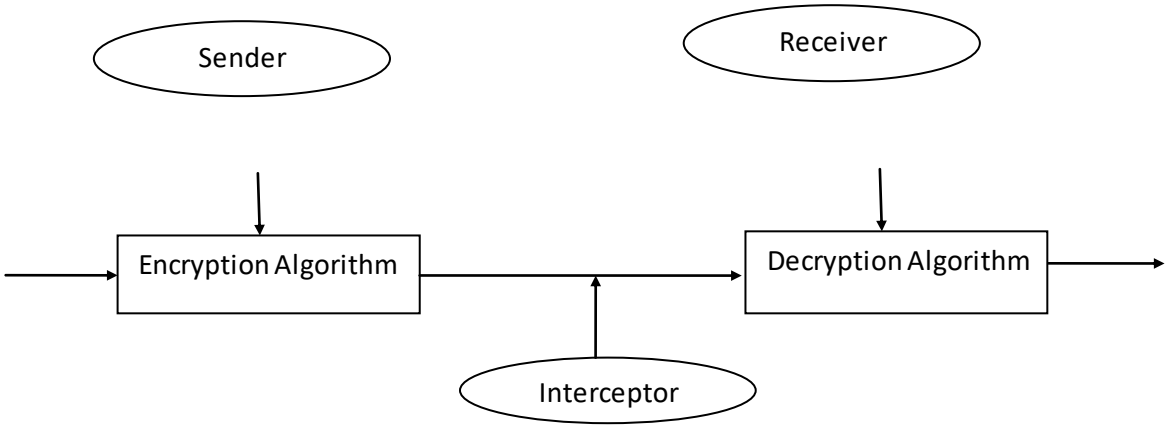


Figure 1: The Cryptography Model

Cryptography is typically mentioned because the learning of secret, while nowadays is all most related to the definition of encryption. Encryption is the process of adjusting information in such how on make it tedious to read by anyone excluding those who have special knowledge (usually mentioned as a "key") that permit them to change back to its original form, that can easily understood by all [24].

The concept of encryption is essential because it permit us to strongly protect data that we don't want to share with anyone else. Businesses use this concept to protect business/company secrets, government uses this concept to secure their confidential information, and numerous people use it to guard their personal information to guard against effects like fraud. As per our need we processed various transactions of our private information through the web, encoding the original things is an essential factor to any computer safety measures devices. One of the most reasons of encryption is to make safe our communication over internet. Keeping our data safe when using own computer may not be as easy as we suppose. Suppose we are transferring data at any time over the Internet, it is possible that third party can be access those data means it may be accessible by anyone else who is unauthorised or unauthenticated person. During transaction firstly the information is sent to local network then it is schedule to our internet service provider also called ISP, who can access our data. After this our data moves along different paths to reach to the internet service provider for the party that is tough to receive our data, ultimately, facts will be received by the intended person. As per above procedure, many person can access our personal data which we transferred. Here we can see the importance of encryption [24].

2. LITERATURE REVIEW

A successful encryption and decryption scheme has been presented in a research in which they used automatic encryption method to secure unseen secrete files, they have used this technique for cloud backup of the file available in mobile phones [1]. This new way of encryption technique has been implemented. This encryption method is the combination of S-box and chaotic sine-logistic map. This method shows excellent diffusion and confusion properties and shows secure behaviour against different attacks like plaintext that is original message, noise, and data loss attacks. This algorithm uses the symmetric security key to generate irregular, random, and non reiterate cipher images [2].A new encryption technique that is based on Hanon map with hybrid chaotic shift transform has been presented. The properties of Confusion and diffusion enhance the safety measures. A replacement of two dimensional modified Henon map which spring from the Henon map is presented. Presented algorithm provides more safety measures security as compared to conventional enciphering techniques such as Advanced Encryption Standard, RC4 and RC5 with required execution time. Hence this algorithm can be used in miscellaneous applications for making secure communication [3]. A DC recovery method for JPEG images has been introduced as new encryption technique, which may be wont to defend against the transaction error at the execution ends for everywhere systems. In this paper, encryption is performed in two steps first detecting the gray scale changing trends by brute force to presume the DC coefficients from all probable values. Secondly, analyse the result and tested this scheme. The outcome of recovery verifies the efficiency of DC coefficient recovery method and with previous method it is compared. This recovery method enhances the fault tolerance for JPEG image [4].The Text Encryption Character Jumbling method is used only for character encryption. This scheme tries to encipher facts for normal text messaging applications by performing shuffling on the top layer and the bottom layer. The constraint of character jumbling algorithm is that it has been applied only for alphabetic characters [5].An nonlinear S-box based on linear transformation is presented, which is structured by a particularly simple and direct algorithm. This scheme performs several tests on the basis of quality of an image and gives better result. Its confusion creating property is sort of high as compare to other S-box techniques. The numerical difficulty supported the partial sequential alteration provides ultimate results that make S-box genuine and reliable [6]. An optical image cryptosystem scheme has been presented which is based on Arnold's Cat map and the double random phase encoding. The Arnold's Cat map is used as a cover to enhance the security measures. As the optical image cryptosystem has simple and has good permutation and

diffusion in a sensible instance with huge resistance to noise that is an essential feature [7].A operation of a crypt-stego method for RGB image provides better confidentiality. In this method, the image encryption is performed with the Advanced Encryption Standard algorithm, and key is added to the enciphered image by using nearest-neighbour clustering and Least Significance Bit -M method. The experimental result proves the goodness of presented method as tested and compared to other schemes. The analysis of Structural similarity index measure, MSE, Peak signal to noise ratio, and histogram also ensure that this method gives enhanced result in terms of confidentiality and security against different attacks [8].A Secure Reversible Image Data Hiding (RIDH) approach has been presented that operates on the enciphered field. A strong two-class SVM classifier is used for decryption process to differentiate encrypted and non-encrypted image pieces. These methods also perform inclusive experiments to authenticate the greater embedding presentation of presented RIDH scheme on an encrypted domain [9].A new Hash based Encryption technique has been introduced for Diagnostic Hysteroscopy Key frames. In this technique the key frames are extracted from diagnostic hysteroscopy videos. This method analyse different parameter in terms of Number of Pixels Change Rate, Unified Average Changing Intensity values, correlation and speed. This result verifies the occurrence, safety measures, and competence of presented encryption scheme when compared to other encryption algorithms [10].A new encryption scheme is presented. This scheme is based on two algorithms Secure –Advanced Encryption Standard and Chaos. This scheme is practically tested and analyse that the RNG considered here passed all NIST test. This scheme can be utilized for security and speed. On the basis of Security and performance analyses it has been prove that the CS- Advanced Encryption Standard algorithm is safer and efficient [11].The FEC merged with double security scheme has been presented. In the presence of different noise and attack, this scheme analyse the multi-layer security algorithms with encoded transmitted packets. This algorithm ensures better security for responsive image throughout its transmission over AWGN wireless channel with different FEC method this, increases transmission consistency and also enhances the quality of extorted secret image [12].A new scheme that provides security of images has been presented. This scheme uses XOR method to encrypt data and make the secure. This paper performs analysis over different parameters like correlation value, histogram analysis, Peak signal to noise ratio and entropy [13].The encryption technique presented for image enciphering. The performance of this technique gives better outcomes. Hence it is observed that the presented method is effective and protected [14].A new S-box scheme combined with gingerbread man chaotic map has been implemented that provides security and has relatively less computational complexity. This method is proved good for real-time image encryption applications. This method enhance the security level by easily extending multiple chaotic maps to encipher an image [15].An efficient, safe, and fast image encryption technique is presented here. This method consists three parts: (i) dynamic key derivation, (ii) encryption, and (iii) decryption. It is concluded that this image encryption method gives better outcome to ensure security of an image [16].As analysed that S-box encryption cannot provide much security. So in order to improve this security level, an image encryption scheme has been presented which is very simple and effective. This method is combined approach of S-box with multiple iteration. The strength of this scheme is then analyzed over different parameters like computational cost comparison, NPCR, UACI, homogeneity, correlation analysis, contrast analysis, entropy analysis, histogram comparison etc [17]. A new binary image encryption technique has been presented. This algorithm is used for binary image or database of having same size binary image. This scheme is based on generation of key. This scheme is used to perform encryption not only on single image but also a dataset of binary image [18].Comparison among four different methods (Hyper+random, Hyper+Total Shuffle, Chen+random, Chen+Total shuffle) has been performed in terms of encryption quality, execution time, correlation coefficient, number of pixels change rate shorted as NPCR and unified average changing intensity that is UACI. These schemes were executed in Matlab platform and the results of each method were analyzed and compared. In this paper all four algorithms are applicable for all small size of images. These algorithms are providing better security to the digital data that are commonly used [19].A new encryption algorithm has been introduced by combining three different algorithms

that are RSA, Advanced Encryption Standard and Elliptic-Curve method. A software application is developed by this method. These methods perform analysis over different parameters like speediness, safety level, encrypted PEG image size, generation of key, tie required for encryption process, and throughput. After analysis it is concluded that the ECC gives best result as compare to the RSA and Advanced Encryption Standard and also ECC algorithm provides ore security as compare to RSA and Advanced Encryption Standard [20].A new scheme has been implemented to enhance the safety of system due to adding randomness to the typical DNA encryption. A new scheme has been implemented by combining the idea of random DNA encryption scheme, Huffman coding two-dimensional DCT steganography technique and RSA algorithm. This method provides three levels of safety [21].A combination of two methods that is an anti-counterfeiting method and digital watermarking has been implemented. An anti-counterfeiting method, combines the coding characteristics of the two-dimensional code and the digital watermarking is perform to improve the safety of the QR code. The experimental out forms can strongly ensure that this scheme is effective in terms of QR code security [22].

3. PROBLEM IDENTIFICATION

Table -1

Reference	Method Applied	Problem identified
[3]	2-Dimensional Modified Henon map.	The encryption scheme used in this paper has done more complex work. This paper gives higher value for PSNR (Peak signal to noise ratio).
[4]	Direct Cosine (DC) recovery method.	Need to improve way to calculate PSNR. This method gives higher value for PSNR.
[6]	S-box encryption technique.	This method concludes low value for Entropy.
[8]	Crypto-Stago method with the AES algorithm	This method is applied only on colour images. This scheme provides higher SSIM (Structural Similarity) value.
[11]	Chaos-based Advanced Encryption Algorithm (CS-AES).	This paper uses complex encryption structure. This paper analyse lower value of Entropy.
[12]	The data hiding Steganography combined with the encryption technique.	This method has complex steps to perform encryption. Applied only on gray scale images, and result as higher PSNR value.
[15]	A Substitution box with Gingerbreadman chaotic map and S8 permutations.	This method provides lower entropy value.
[16]	Two rounds of Substitution	The encryption scheme used in this

	and Diffusion method.	paper has done more complex work. This scheme provides higher SSIM(Structural Similarity) value.
[17]	Substitution-box with scrambling effect.	This method provides lower entropy value.
[18]	Binary image encryption	Result as higher PSNR value.
	method.	

After analysing different research papers, the performance of the algorithm has been tested using different quality benchmarks like PSNR, SSIM and Entropy. It is observed that analysed algorithm gives poor results. So after observation of performance of different encryption scheme it is concluded that there is always be a need of an algorithm that can produce good quality image after encryption.

4. METHODS

4.1 ADVANCED ENCRYPTION STANDARD ALGORITHM

The AES algorithm working is explained by following steps:

Step 1.Sub-byte Transformation: This transformation is a Substitution technique, that perform nonlinear transformation using S-box, this transformation is developed by Affine Transformation and multiplicative inverse.

Step 2.Shift rows transformation: This transformation performs row wise shift operation. This is an easy transposition technique in which the bytes of the last three rows are shifted randomly.

Step 3.Mix column transformation: This transformation is just like a matrix operation. Every column vector is multiplied by a matrix . The bytes must be treated as polynomials in its place of numbers.

Step 4.Add round key transformation: The Round key transformation is a simple XOR technique between the working state and the round key.

4.2 CS-AES TECHNIQUE

The new CS-AES is chaos-based RNG and S-Box generation technique.

The steps of the CS-AES Technique are as follows:

Encryption

1. The selected image will be processed as 128-bit blocks in every repetition for enciphering perpose.

2. The next step is to provide condition and system parameter required for the chaotic system.

3. The key is now sent to the recipient side for decryption process by applying RSA algorithm.

4. The next step is to performing logic encryption process. This process is done by using the values obtained from y and z phases of chaos-based RNG.

5. Create the round key using x and y phases of the chaos-based method.

6. Create S-Box using x and z phases.

7. To perform round operations such as add round key, sub-bytes, shift rows, mix rows, mix columns. here Mix columns are not present in the final round.

8. Finally we obtain a 128-bit enciphered block .

Decryption Process

1. The decryption is just a reverse process of encryption technique. In this process the conditions and system parameters used in the encryption process are received from the sender after the decryption.

2. Now 128-bit block is decrypted.

3. Next step is to generate round keys by using x and y phases and S-Box by using x and z phases to perfor decryption using chaos-based RNG.

4. Now perform round key operation in the deciphering process.

5. Next to Perform the round steps for the decryption process (Inv mix rows, Inv shift rows, Inv sub-bytes, add round key, Inv mix columns). In this process the Inv mix columns are not present in the final round.

6. The 128-bit block is used for logic operation. In this process each iteration is done using the y and z phases of RNG, and logic operation .

7. Finally we obtain a 128-bit deciphered block.

4.3 SUBSTITUTION–PERMUTATION BASED IMAGE ENCRYPTION ALGORITHM

The Substitution and Permutation based image encryption techniques enhance the range of chaotic technique in order to implement a new encryption technique. This process works as follows:

1. Firstly matrix of size [i, j] an original image is anticlockwise rotated through 90◦. The rotation of PxQ is performed by following equation:

$$M(i, j) = N(k, Q - n + 1) \quad (1)$$

2. According to Rijndael, next step is to replace each pixel value of rotated image with values of S-box matrix to get image of size A(i, j).

3. The next step is to get an arbitrary image B(i, j),We use an arbitrary row in image A(i, j) by using function Rand(j) as

$$B(i, j) \text{ is } (Q + 1) \times P \quad (2)$$

$$\text{Or, } B(i, j) = A(i - 1, j) \text{ for } i > 1 \quad (3)$$

4. A new matrix Cj of length (Q + 1) is implemented by transforming B (i, j) matrix into one-dimensional Column matrices. For transforming the equation is given as:

$$Cj(i) = B(i, j) \quad (4)$$

5. The next step is to change the pixel value for each column matrix Cj without affecting the first entry of matrix. This process is perform by the equation given as :

$$Rj(i) = Rj(i - 1) \text{ XOR } Cj(i) \text{ XOR\_\_} Ln(i, j) \times 1010 \bmod 256 \text{ for } 1 < i \leq (Q + 1) \quad (5)$$

For each Round of enciphering process an equivalent scheme Ln (i, j) is given as :

$$Ln(i, j) = \begin{cases} Ln - 1\ (0, P) & \text{for } i = 0,\ j = 0,\ n = 2, 4 \\ \_\ ST\ (ro, Ln\ (0, j - 1)) & \text{for } n > 0,\ j = 0 \\ \_TST\ (ri\ , Ln\ (i - 1, j)) & \text{for } n > 0,\ j > 0 \end{cases} \quad (6)$$

(6) This is the final step of first round of encryption process, in this step we get a two dimensional matrix by emerging all one dimensional Column vectors. In this step the first row of two dimensional matrix is discarded to add in the third step of encryption process. The given equations perform operation.

$$E(i, j) = Nj(i + 1)\ , i \leq Q \quad (7)$$

Here the two-dimensional matrix has size of Q × P. Equation (7) performed for all four rounds and after that we can obtain an encrypted image. To decrypt this image reverse process of encryption is perform by using keys..

Decryption process

1. In the first step of decryption process we have to add an arbitrary row in the encrypted image E(i, j) of size P × Q.

2. By using equation (4) of encryption process, the processed image is transformed into the column vectors

Rj (i) of length P + 1.

3. The next step is to transformed the column vectors Rj(i) into Cj (i) by using the inverse one-dimensional substitution. By applying the piecewise function we get the values of Ln (i, j) .

Cj (i) = Rj (i − 1) XOR Rj (i) XOR (Ln (i, j) × 1010 mod 256) (8)

4. Now, rejoin the one dimensional column vectors Cj (i) to obtain a two-dimensional matrix B (i, j).

5. The Next step is to substitute the pixels of the matrix B (i, j) by the converse s-box in order to get substituted matrix A (i, j). Now each pixel value is transformed into an 8 bits binary string. After converting the converse S-box into decimal form, the left four bits and right four bits are used to replace the substituted value from the converse S-box.

6. Finally, clockwise rotation of matrix A (i, j) by 90◦ is performed. After rotation of matrix the first column is leftover to obtain the image R (i, j). Hence by repeating these steps four times and by using exact key we get the original image.

4.4 2D-MODIFIED HENON MAP WITH HYBRID CHAOTIC SHIFT TRANSFORM TECHNIQUE

Input: Select original image I and two chaotic matrix A and B.

Output: The shuffled image T.

1. By ordering in xk and yk chaotic sequence construct the row and column shift matrix.

2. Repeat for i=1to N do

3. Do the following:

If (bi mod 2)=0 then perform cyclic shifting of the pixels in column i of I downwards with the step of ai

Else perform cyclic shifting of the pixels in column i of I upward with the size of ai

4. End if condition.

5. End for loop.

7. Signify the shifted image as Ti.

8. Repeat for i=1 to M

9. Do again

If the (ci mod 2)=0 then perform cyclic shifting of the pixels in row i to Ti by right including the size of bi

Else perform cyclic shifting of the pixels in row i of Ti by left with the size of bi

11. End if condition.

12. End for loop.

13. Signify the shifted image as T.

4.5 THE 2D LOGISTIC CHAOTIC MAP

The two-Dimensional logistic map is a distinct system with chaotic behaviour of the development of orbits and attractors. This is dynamic system. This system has more difficult behaviour as compare to one-dimensional chaotic behaviour.

Encryption Process

In this encryption is performed as firstly the system scans the key frame as RGB images, then we reshape the matrices into single matrix. Some arbitrary bits are formed using a real arbitrary value originator. Now, the obtained bits are combined using Bitwise-XOR operation with the whole key frame pixel values. It is important that the size of produced bits should have the same length as image. By testing and analysing it is confirmed that addition of random bits to the first key frame improves the protection level, primarily alongside differential attacks.

Here is the flowchart showing of the image encryption scheme:

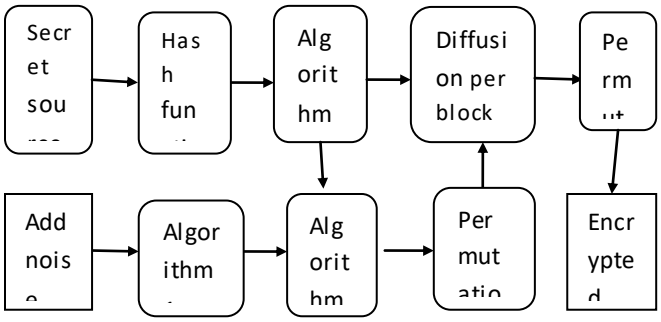


Figure 2: Image Encryption Scheme

Decryption Process

Decryption process performs reverse operation of encryption process in order to get the original data. Here Q is the original matrix and I is invertible matrix of Q. We have I as the, that means that I.Q = id16 and id16 is an [16, 16] that is an identical matrix.

4.6 2-DIMENSIONAL LOGISTIC MAP CHAOTIC ENCRYPTION TECHNIQUE

The 2-Dimensional logistic map is an extension of a 1-Dimensional logistic map. Due to dependency on control parameters it enhances the key space. It was popular in 1976 with name as Multimedia Tools. This logistic map is a one-dimensional chaotic map which is given below

$$X_{n+1} = eX_n(1-X_n)$$

Where Xn have range of zero and one. This is the simplest model that shows chaotic behaviour. There is a positive constant e having range from zero to four. Its value shows the behaviour of the map.This method of encryption enhances the security level. That means through this method the enciphered data is not extracted easily or cannot visualised by human eyes directly. This method uses the permutation substitution procedures. The confusion and diffusion property increases the complexity of an algorithm.

4.7 CHAOTIC TENT MAP

In Chaotic Tent Map, the chaotic tent map is used to develop the enciphering technique. This technique of image encryption has following step:

(1) Read original image (M×b) as input, take the size of M, for example, [a, b, c] to store number of dimensions of M, a x b x c = 256 x 256 x 3. Here we use control parameter represented by μ.

(2) The next step is to add key x0 to the algorithm. By repeating N times to the chaotic tent map we obtain the key array x(n) of size N.

(3) Now the next step is to perform encryption by mixing the key array x (n) with original image matrix (M×b).

(4) Finally we get encrypted image.

The flow chart of image enciphering method is represented as

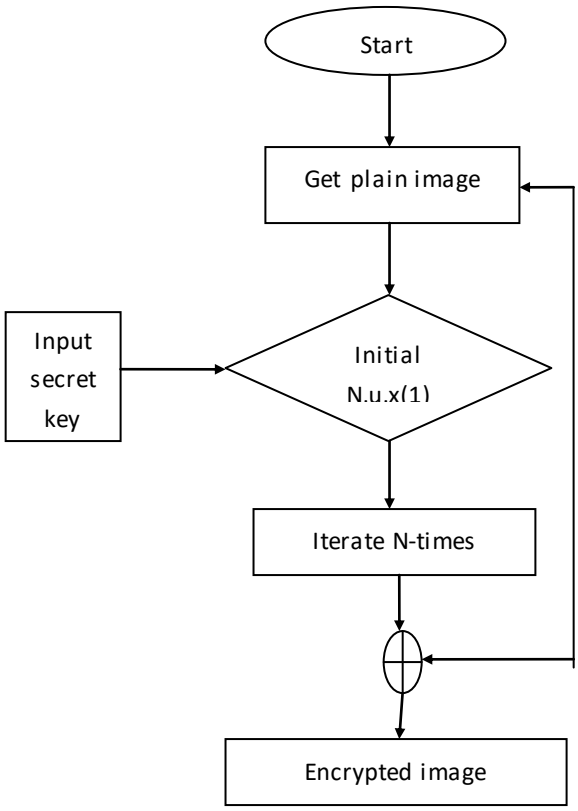


Figure 3: The image encryption method

Decryption procedure

For decryption we use the reverse operation of encryption. The decryption algorithm is performed by using following step:

(1) Read encrypted images matix (Ma×b), take the size of M, for example [a, b, c] to store the number of dimension of M, a x b x c = 256 x 256 x 3. After that initialize the control parameter represented a μ.

(2) Now decrypt the Input image using secret key x0. It is noted that the size of key x0 must have the same length as the encryption key, if both have different key we cannot get the plain image back. By repeating N times to the chaotic tent map we obtain the key array x(n) of size N.

(3) The next step is to perform decryption on matrix (Ma×b) by extracting the key array x(n) from the encrypted image (Ma×b).

(4) Finally we obtain the decrypted image which is the original image.

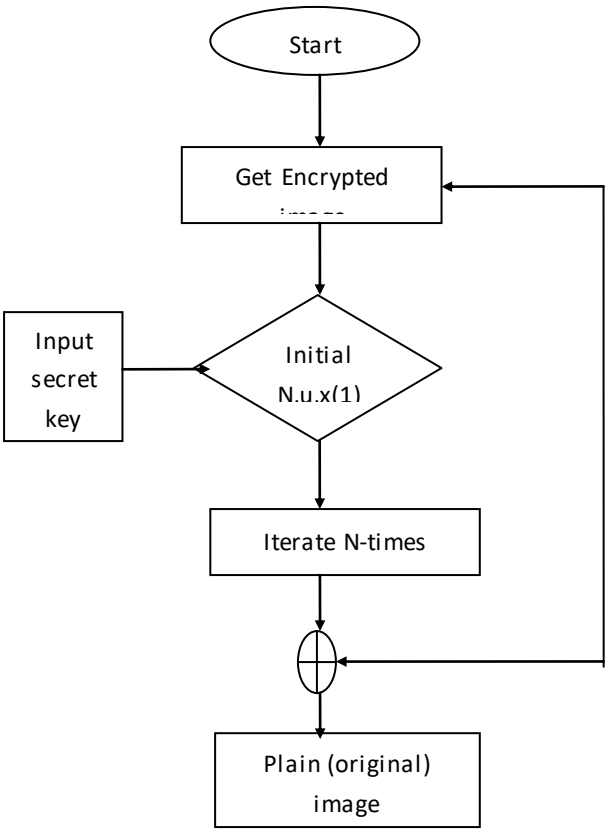


Figure 4: The image decryption algorithm

4.8 BINARY IMAGE ENCRYPTION ALGORITHM

Algorithm 1 : Binary image enciphering algorithm

Encryption process

Step 1: The first step is initialization. For initialization do the following:

a. Select an image as an Input image to encrypt.

b. Selected image is now breaking into d blocks.

c. Make the d block images equivalent size as input image.

Step 2: Process of generation of the key-matrix and enciphered image.

a. Calculate bj and bj.

b. Store bj as the key-image.

c. Store bj as the enciphered image.

Decryption

Step 1: The first step of decryption process is Initialization. For initialization do the following:

a. Select the key- matrix and enciphered images as an input image.

b. Return to the basis.

Step 2: Decryption procedure.

a. merge the spitted d-block image.

b. Display the deciphered image.

Algorithm 2 : Binary image encryption algorithm for database

Encryption

Step 1. Select the database (set of d images) to perform encryption.

Step 2. Next step is generation of the key-matrix and the enciphered images of the database.

a. Calculate aj and bj .

b. Store bj as the key image.

c. Store bj as the database of enciphered images.

Decryption

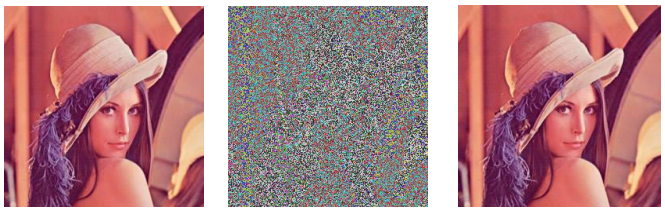
Step 1: Select the key-matrix and the enciphered images of the database as an input.

Step 2: Return to basis to recommend the deciphered images

5. RESULT

5.1 HISTOGRAM ANALYSIS

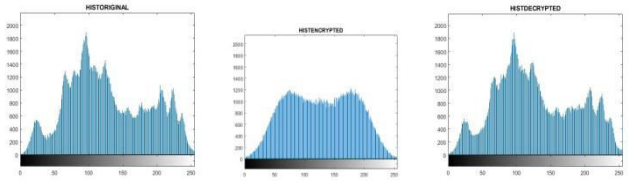
Histogram is a graphical representation of image pixels distribution at each intensity level. A good encryption technique requires significant difference in the histogram of the plain and encrypted image so that the original content could not be extracted. Different histograms of plain image, encrypted image and decrypted image are represented below. We also observed that, histograms of plain and decrypted images are almost similar to each other. The visual results obtained for histograms prove that our method is stable against the histogram based attacks.



a) Lena Plain Image b) Encrypted Image c) Decrypted Image

Figure 5 : Lena's plain image, encrypted image and decrypted image using our method. a) Plain image b) encrypted Image c) decrypted image.

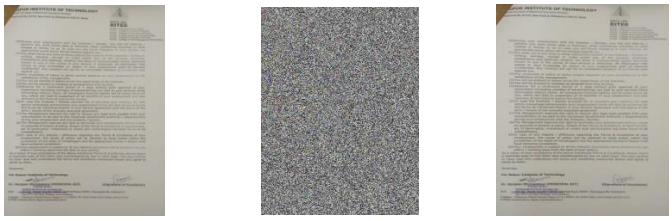
Figure 5 shows the output of encryption and decryption on applying lena image (color image), here we can observed that, encrypted image could not be easily identified by the human eyes. Hence, proposed method provides more security than compared ones. We also observed that, encrypted and decrypted images are almost similar to each other.



a) Histogram 1 b) Histogram 2 c) Histogram 3

Figure 6: The histogram of a) Lena's plain image b) Lena's encrypted image c) Lena's decrypted image.

Above Figure 6 represents the histograms of a) Lena's plain image b) Lena's encrypted image c) Lena's decrypted image. As illustrated, histogram of the original image (color image) is quietly different from the histogram of its corresponding cipher image. Cipher images follow a uniform distribution which is significantly different compared to the distribution of the plain images. Hence, histograms of the cipher images do not provide any clue to employ the statistical attack on the proposed encryption approach. We also observed that, histograms of plain and decrypted images are almost similar to each other. The visual results obtained for histograms prove that the proposed method is stable against the histogram based attacks.

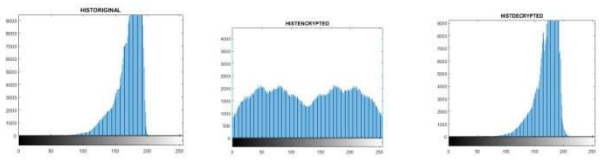


a) Doc1 Plain Image b) Encrypted Image c) Decrypted Image

Figure 7: Doc1's plain image, encrypted image and decrypted image using our method. a) Plain image b) encrypted Image c) decrypted image.

Figure 7 shows the output of encryption and decryption on applying Doc1 image (color image), here we can observed that, encrypted image could not be easily identified by the human eyes. Hence, proposed method provides more security

than compared ones. We also observed that, encrypted and decrypted images are almost similar to each other.



a) Histogram 1 b) Histogram 2 c) Histogram 3

Figure 8: The histogram of a) Doc1's plain image b) Doc1's encrypted image c) Doc1's decrypted image.

Above Figure 8 represents the histograms of a) Doc1's plain image b) Doc1's encrypted image c) Doc1's decrypted image. As illustrated, histogram of the original image (color image) is quietly different from the histogram of its corresponding cipher image. Cipher images follow a uniform distribution which is significantly different compared to the distribution of the plain images. Hence, histograms of the cipher images do not provide any clue to employ the statistical attack on the proposed encryption approach. We also observed that, histograms of plain and decrypted images are almost similar to each other. The visual results obtained for histograms prove that the proposed method is stable against the histogram based attacks.

2) Result Analysis Of Encryption Techniques

Table -2

			PROPERTIES						
S. NO.	METHODS	INPUT DATA	ENTROPY ORIGINAL IMAGE	ENTROPY ENCRYPTED IMAGE	PSNR	SSIM	NPCR	UACI	ELAPSED TIME
1	ImageEncryptionGUI	leena.jpg	7.2283	7.9560	8.9338	0.0088	33.1935	6.9227	24.1831
		leena256*256.jpg(color)	7.7599	7.7541	9.9759	0.0212	33.1794	4.1699	55.9426
		cameraman.jpg(color)	7.1048	7.9557	8.3931	0.0098	33.1894	5.7718	16.3071
		degree.jpg(color)	6.2823	7.9789	9.4234	0.0138	33.1833	2.3839	20.4945
		barbara.jpg	7.1674	7.9589	9.0613	0.0089	33.2032	5.8960	20.7665
		jyoti.jpg	7.5219	7.9733	8.1065	0.0106	33.1895	2.7195	299.3862
		doc1.jpg	6.0800	7.9695	9.4242	0.0134	33.1742	1.8354	26.1766
		baboon.jpg	7.2316	7.9567	9.7303	0.0128	33.2006	4.4115	18.6052
		onion.jpg	7.6197	7.8580	8.3149	0.0150	33.1716	7.5591	79.6436
		peppers.jpg	7.5925	7.9581	8.8526	0.0097	33.2020	5.4501	49.9451
2	Imageshuffle	leena.jpg	7.2283	7.4147	12.2358	0.0271	33.1019	3.2785	24.7383

		leena256*256.jpg(color)	7.7599	7.4700	10.8549	0.0157	33.1585	3.8865	37.2536
		cameraman.jpg(color)	7.1048	7.3545	9.1819	0.0153	33.0750	4.4775	19.8580
		degree.jpg(color)	6.2823	6.4864	16.2523	0.0747	32.8449	1.8643	23.9085
		barbara.jpg	7.1674	7.6103	11.3823	0.0204	33.1485	1.8643	17.9120
		jyoti.jpg	7.5219	7.3818	11.1352	0.0292	33.1592	3.6437	297.2427
		doc1.jpg	6.0800	5.8602	20.2123	0.1447	32.7364	3.7791	29.0230
		baboon.jpg	7.2316	6.8709	14.5720	0.0499	33.0677	1.2373	23.3591
		onion.jpg	7.6197	7.5659	9.7688	0.0171	3.1617	2.5123	28.7708
		peppers.jpg	7.5925	7.6825	10.4405	0.0185	33.1477	4.0589	31.2307
3	LshapeEncryption	leena.jpg	NA	NA	NA	NA	NA	NA	NA
		leena256*256.jpg(color)	7.7599	7.7954	9.7224	0.0589	33.1735	3.8171	26.8292
		cameraman.jpg(color)	NA	NA	NA	NA	NA	NA	NA
		degree.jpg(color)	6.2823	7.4124	12.8990	0.0442	33.0900	3.7683	35.7401
		barbara.jpg	NA	NA	NA	NA	NA	NA	NA
		jyoti.jpg	7.5219	7.6689	10.1498	0.0377	33.1702	3.6165	293.3821
		doc1.jpg	6.0800	7.1754	14.9966	0.0786	33.0500	3.4335	21.7099
		baboon.jpg	7.2316	7.8966	10.4742	0.0195	33.1777	4.1503	23.0984
		onion.jpg	7.6197	7.6860	9.2743	-0.0526	33.1708	5.1429	20.9937

3) COMPARISON TABLE

COMPARISION WITH EXISTING METHOD

The tests are done for the following parametric factors and the results are given in table.

5.3.1 Entropy Analysis

5.3.2 PSNR Analysis

5.3.3 SSIM Analysis

5.1.1 ENTROPY ANALYSIS

The strength of any encryption algorithm is measured quantatively in terms of information entropy which signifies the degree of randomness in the information content. For the 8 bit message, suppose if there are 256 possible outcomes with equal probability then the ideal value of entropy should be equal to 8. The entropy value of the good encryption algorithm should be close to ideal one which means that leakage of information is negligible during encryption

process. The information entropy of different ciphered images is given in Table 3. It can be observed from the table that the information entropy of ciphered image obtain by our method is much close to 8. This implies that the encryption algorithm results in random like ciphered images. Further, the comparison of this algorithm with other peer algorithms with respect to information entropy for Lena, Barbara and Peppers image are given in Table 3. The comparison results shows that the algorithm outperforms the method proposed in [6, 11, 15, 17]. Thus, the algorithm offers resistance against entropy based attacks.

Table-3 Entropy Analysis

S.NO.	REFERENCES	Leena.jpg	Barbara. Jpg	Peppers. Jpg
1	[6]	7.2415	NA	NA
2	[11]	NA	NA	7.9565
3	[15]	NA	NA	7.73018
4	[17]	NA	7.6015	7.5728
5	Our	7.9560	7.9589	7.9581

Table-3 exhibits entropy values calculated for different data set by proposed encryption technique and some other compared algorithms. Optimal values by proposed encryption technique are as follows: entropy for leena image is 7.9560, entropy for barbara image is 7.9589 and entropy for peppers image is 7.9581 An examination of Entropy values in Table-3 makes it clear that the encryption algorithm developed here gives better result than the compared ones.

5.2 PEAK SIGNAL TO NOISE RATIO (PSNR) ANALYSIS

PSNR evaluates the encryption algorithm objectively by considering the original image and encrypted image as a signal and noise respectively. The low value of the PSNR indicates the greater difference between the original and ciphered image. The PSNR values of different images are listed in Table 4. From the table results, it is clear that the encryption quality is good as the PSNR value of each image is very low. PSNR is a method traditionally used in comparative statistical analysis of images. It measures the quality of images in terms of PSNR (dB). It is calculated by dividing the signal strength by its mean squared error as given below

$PSNR=10\log10\ (MAXr^2/MSE)$

Where $MAXr2$ is the squared maximum pixel value that can exist in the image.

Table- 4 PSNR Analysis

S.NO.	REFERENCES	Leena.jpg	Barbara. Jpg	Peppers. Jpg	Cameraman. Jpg
1	[3]	9.2335	NA	9.0076	NA
2	[4]	NA	25.6400	NA	NA
3	[12]	NA	NA	NA	29.8
4	[18]	61.4000	NA	NA	NA
5	Our	8.9338	9.0613	8.8526	8.3931

Table-4 exhibits PSNR values calculated for different data set by proposed encryption technique and some other compared algorithms. Optimal values by proposed encryption technique are as follows: PSNR for leena image is 8.9338, PSNR for barbara image is 9.0613, PSNR for peppers image is 8.8526 and PSNR for cameraman image is 8.3931.An examination of PSNR values in Table-4 makes it clear that the encryption algorithm developed here gives better result than the compared ones.

5.3 STRUCTURAL SIMILARITY INDEX MEASURE (SSIM) ANALYSIS

SSIM is an important statistical method for measuring the similarity between two images, given that it tries to match the

human visual system's response rather than being a pixel-by-pixel objective comparison. The value of SSIM index is between [-1, 1] and the resultant value 1 indicate that both images are identical to each-other while a value of zero shows that there is no correlation between two images.

Table- 5 SSIM Analysis

S.NO.	REFERENCES	Leena. Jpg	Peppers. Jpg
1	[8]	NA	0.0200
4	[16]	0.0091	0.0100
3	Our	0.0088	0.0097

Table-5 exhibits SSIM values calculated for different data set by proposed encryption technique and some other compared algorithms. Optimal values by proposed encryption technique are as follows: SSIM for leena image is 0.0088 and SSIM for peppers image is 0.0097. An examination of SSIM values in Table-5 makes it clear that the encryption algorithm developed here gives better result than the compared ones.

6. CONCLUSION

From Table 2, we analyze different encryption techniques on the basis of different parameter like entropy of original image, entropy of encrypted image, PSNR,SSIM, NPCR,UACI, Elapsed Time. From Table 3 we can conclude that the algorithm developed here gives higher entropy result than the compared ones. From Table 4 we can conclude that the algorithm developed here gives lower PSNR result than the compared ones. From Table 5 we can conclude that the algorithm developed here gives lower SSIM result than the compared ones.

REFERENCES

[1] International Conference on Computing, Communication, and Automation (ICCCA2017) Abhishek Vichare, Tania Jose, Jagruti Tiwari, Uma Yadav, Data Security using Authenticated Encryption and Decryption Algorithm for Android Phones.

[2] Atta ullah, Sajjad shaukat Jamal, Tariq shah(2017), A novel scheme for image encryption using substitution box and chaotic system.

[3] S. J. Sheela1, K. V. Suresh1, Deepaknath Tandur2 (2018), Image encryption based on modified henon map using hybrid chaotic shift transform.

[4] Han qiu a, Gerard memmia, Xuan chen b, Jian xiong c, DC coefficient recovery for JPEG images in ubiquitous communication systems (2019).

[5] Rohit k. singh, Tajunnisa begum, Lawrence borah, Debabrata samanta, (ICISC-2017), Text Encryption - character jumbling.

[6] Shabieh Farwa1*, Tariq Shah2 and Lubna Idrees1, A highly nonlinear S-box based on a fractional linear transformation Farwa et al. SpringerPlus (2016).

[7] Ahmed M. Elshamy1,5 Fathi E. Abd El-Samie1 Osama S. Faragallah2,6 Elsayed M. Elshamy2 Hala S. El-sayed3 S. F. El-zoghdy4,6 Ahmed N. Z. Rashed1 Abd El-Naser A. Mohamed1 Ahmad Q. Alhamad5, Optical image cryptosystem using double random phase encoding and Arnold's Cat map (2017).

[8] Amna Shifa1, Muhammad S. Afgan1, Mamoona N. Asghar1, Martin Fleury2, Imran Memon3, Saima Abdullah1, and Nadia Rasheed4, Joint crypto-stego scheme for enhanced image protection with nearest-centroid clustering (2018).

[9] Jiantao Zhou, Member, IEEE, Weiwei Sun, Student Member, IEEE, Li Dong, Student Member, IEEE, Xianming Liu, Member, IEEE, Oscar C. Au, Fellow, IEEE, and Yuan Yan Tang, Fellow, IEEE, Secure Reversible Image Data Hiding Over Encrypted Domain via Key Modulation(2016).

[10]Rafik Hamza,Khan Muhammad, Arunkumar Nachiappan Gustavo Ramírez González, Hash based Encryption for Key-frames of Diagnostic Hysteroscopy.

[11] Unal cavu¸so˘glu, Sezgin kaçar, Ahmet zengin, Ihsan pehlivan, A novel hybrid encryption algorithm based on chaos and S-AES algorithm (2018).

[12] Mohsen A. M. El-bendary, FEC merged with double security approach based on encrypted image steganography for a different purpose in the presence of noise and different attacks (2016).

[13] Q. N. Natsheh*, B. Li, A. G. Gale, Security of multi-frame DICOM images using XOR encryption Approach (2016).

[14] Chunhu Li, Guangchun Luo, Ke Qin, Chunbao Li, An image encryption scheme based on chaotic tent map (2016).

[15] Majid Khan1, Zeeshan Asghar1, A novel construction of substitution box for image encryption applications with Gingerbread man chaotic map and S8 (2016).

[16] Zeinab Fawaz a, HassanNoura b, Ahmed Mostefaoui, An efficient and secure cipher scheme for images confidentiality preservation (2016).

[17] Shabieh Farwa, Nazeer Muhammad, Tariq Shah, Sohail Ahmad, A Novel Image Encryption Based on Algebraic S-box and Arnold Transform (2017).

[18] Amrane Houas, Zouhir Mokhtari, Kamal Eddine Melkemi, Abdel malik Boussaad, A novel binary image encryption algorithm supported diffuse Representation.

[19] Gaytri, Shelza suri, Dr. Ritu vijay, An implementation and performance evaluation of an improved chaotic image encryption approach (2016).

[20] Asma chaouch, Belgacem bouallegue, Ouni bouraouiSoftware, Application for simulation-based AES,RSA and Elliptic-Curve Algorithms (2016).

[21] Mumthas sa, Lijiya ab, Transform Domain Video Steganography Using RSA, Random DNA Encryption and Huffman Encoding (2017).

[22] Yijing Xun1, Zhijiang Li2(&), Xiaolu Zhong2, Sheng Li2, Jiawang Su2, and Ke Zhang2, Dual Anti-counterfeiting of QR Code Based on Information Encryption and Digital Watermarking (2019).

[23] Kahate, A. (2013). Cryptography and network security. Tata McGraw-Hill Education.

[24] Adamovic, S., Sarac, M., Stamenkovic, D., & Radovanovic, D. (2018). The importance of the using software tools for learning modern cryptography. Int. J. Eng. Educ., 34(1), 256-262.