International Journal of Computer Trends and Technology
ISSN: 2231 – 2803 / https://doi.org/10.14445/22312803/IJCTT-V69I3P110

Volume 69 Issue 3, 52-59, March, 2021

Review Article

A Survey on Block Cipher and Chaotic Based Encryption Techniques

Jyoti Kansari[1], Avinash Dhole[2], Yogesh Rathore[3]

[1]*M.TECH, Computer Science and Engineering, Raipur Institutes of Technology, Raipur, India*
[2,3]*Asst. Prof., Department of Computer Science and Engineering, Raipur Institutes of Technology, Raipur, India*

Received Date: 04 February 2021
Revised Date: 25 March 2021
Accepted Date: 27 March 2021

Abstract *- As we know the data transmission is the need for today's world. We cannot imagine our life without multimedia applications and data transmission. As we have seen, there are different attacks over data happening like information theft, hacking, phishing, vishing, smishing, etc. Here it is very important to make sure that transactions over media must be safe that means no attack can occur. Hence security becomes an essential task. The multimedia data includes text, image, and audio and video type data. There are several techniques for making our transaction secure are available. The newest enciphering technique has enhanced the safety of multimedia data from illegal operations. The multimedia enciphering method converts original data to others that are not visualized easily and are named as cipher-text. The process to convert a plain text to ciphered form is named as encryption process, and the inverting process of the encryption process that is transforming cipher-text to the original form is named as decryption process. Its numerous applications like multimedia transmission systems, telemedicine, military communication, and remedial imaging. Here, there are quite a lot of conventional encoding algorithms offered. Mainly three conventional algorithms are widely used. They are International Data Encryption Algorithm shorted as IDEA, RSA, and Advanced Encryption Standard shorted as AES. These algorithms are only applicable for the encryption of text and binary data. There is another method used for encryption in which encryption is performed by using a key. On the other hand, the typical algorithms are incompetent to use them in a direct way in multimedia data and color image encryption because of the high correlation among pixels. This paper analyzes different methods of encryption and decryption.*

Keyword *- Confusion, Diffusion, Secret Key, bitwise transformation, Henon map, Chaos.*

I. 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 message 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 the decryption process. This form of the 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 no knowledge of the encrypted details fall under the world of cryptanalysis. The area of cryptography and cryptanalysis is jointly called cryptology [23].

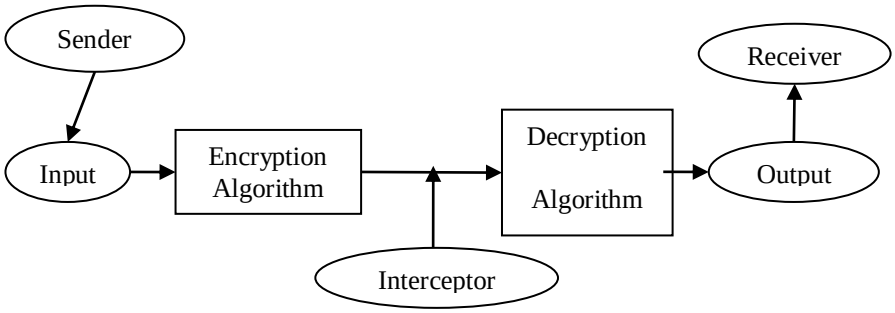

Fig. 1 The Cryptography Model

Cryptography is typically mentioned because of the learning of secret, while nowadays is 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 be understood by all [24].

The concept of encryption is essential because it permits us to strongly protect data that we don't want to share with anyone else. Businesses use this concept to protect business/company secrets, the government uses this concept to secure their confidential information, and numerous people use it to guard their personal information to guard against effects like a 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 for encryption is to make our communication safe over the Internet. Keeping our data safe when using our 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 a third party can access those data means it may be accessible by anyone else who is an unauthorized or unauthenticated person. During the transaction, firstly, the information is sent to the local network, then it is scheduled to our internet service provider, also called ISP, who can access our data. After this, our data moves along different paths to reach the internet service provider for the party that is tough to receive our data, and ultimately, facts will be received by the intended person. As per the above procedure, any person can access our personal data, which we transferred. Here we can see the importance of encryption [24].

II. 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 maps. This method shows excellent diffusion and confusion properties and shows secure behavior against different attacks like plaintext that is the 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 the 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 springs from the Henon map, is presented. The 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 a 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 grayscale changing trends by brute force to presume the DC coefficients from all probable values. Secondly, analyze the result and tested this scheme. The outcome of recovery verifies the efficiency of the DC coefficient recovery method, and with the previous method, it is compared. This recovery method enhances the fault tolerance for JPEG images [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 the character jumbling algorithm is that it has been applied only for alphabetic characters [5].A 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 the quality of an image and gives a 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].An operation of a crypt-stego method for RGB images provides better confidentiality. In this method, the image encryption is performed with the Advanced Encryption Standard algorithm, and a key is added to the enciphered image by using nearest-neighbor clustering and the Least Significance Bit -M method. The experimental result proves the goodness of the 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 results 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 the decryption process to differentiate encrypted and non-encrypted image pieces. These methods also perform inclusive experiments to authenticate the greater embedding presentation of the presented RIDH scheme on an encrypted domain [9].A new Hash-based Encryption technique has been introduced for Diagnostic Hysteroscopy Keyframes. In this technique, the keyframes are extracted from diagnostic hysteroscopy videos. This method analyses different parameters in terms of the Number of Pixels Change Rate, Unified Average Changing Intensity values, correlation, and speed. This result verifies the occurrence, safety measures, and competence of the 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 analyze that the RNG considered here passed all NIST tests. This scheme can be utilized for security and speed. On the basis of Security and performance analyses, it has been proving that the CS-Advanced Encryption Standard algorithm is safer and efficient [11].The FEC merged with a double security scheme has been presented. In the presence of different noise and attacks, this scheme analyses the multi-layer security algorithms with encoded, transmitted packets. This algorithm ensures better security for a responsive image throughout its transmission over AWGN wireless channel with different FEC methods. This increases transmission consistency and also enhances the quality of extorted secret images [12].A new scheme that provides the security of images has been presented. This scheme uses the XOR method to encrypt data and make them secure. This paper performs analysis over different parameters like correlation value, histogram analysis, Peak signal to noise ratio, and entropy [13].The encryption technique is 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 a 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 enhances 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 of three parts: (i) dynamic key derivation, (ii) encryption, and (iii) decryption. It is concluded that this image encryption method gives a better outcome to ensure the security of an image [16].As analyzed 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 a combined approach of S-box with multiple iterations. 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 images or databases of having same size binary image. This scheme is based on the generation of the key. This scheme is used to perform encryption not only one single image but also a dataset of binary images [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, the 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 the encryption process, and throughput. After analysis, it is concluded that the ECC gives the best result as compared to the RSA and Advanced Encryption Standard, and also ECC algorithm provides more security as compared to RSA and Advanced Encryption Standard [20].A new scheme has been implemented to enhance the safety of the 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 digital watermarking is performed 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].

III. PROBLEM IDENTIFICATION

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 a higher value for PSNR (Peak Signal to noise ratio).
[4]	Direct Cosine (DC) recovery method.	Need to improve the way to calculate PSNR. This method gives a 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 to color images. This scheme provides higher SSIM (Structural Similarity) value.
[11]	Chaos-based Advanced Encryption Algorithm (CS-AES).	This paper uses a complex encryption structure. This paper analyses the 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 grayscale images and result from a higher PSNR value.
[15]	A Substitution box with Gingerbreadman chaotic map and S8 permutations.	This method provides a lower entropy value.
[16]	Two rounds of Substitution and Diffusion method.	The encryption scheme used in this paper has done more complex work. This scheme provides a higher SSIM(Structural Similarity) value.
[17]	Substitution-box with scrambling effect.	This method provides a lower entropy value.
[18]	Binary image encryption method.	Result as higher PSNR value.

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

IV. METHODS

A. Advanced Encryption Standard Algorithm

The AES algorithm working is explained by the following steps:

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

Step 2.Shift rows transformation: This transformation performs a 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 their 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.

B. CS-AES Technique

The new CS-AES is a chaos-based RNG and S-Box generation technique.
The steps of the CS-AES Technique are as follows:
Encryption

- The selected image will be processed as 128-bit blocks in every repetition for enciphering purposes.
- The next step is to provide the condition and system parameter required for the chaotic system.
- The key is now sent to the recipient site for the decryption process by applying the RSA algorithm.
- The next step is to perform a logic encryption process. This process is done by using the values obtained from the y and z phases of chaos-based RNG.
- Create the round key using the x and y phases of the chaos-based method.
- Create S-Box using x and z phases.
- 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.
- Finally, we obtain a 128-bit enciphered block.

Decryption Process

- 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.
- Now, the 128-bit block is decrypted.
- Next step is to generate round keys by using x and y phases and S-Box by using x and z phases to perform decryption using chaos-based RNG.
- Now, perform the round key operation in the deciphering process.
- 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.
- 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.
- Finally, we obtain a 128-bit deciphered block.

C. Substitution–Permutation based image encryption algorithm

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

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

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

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

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

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

- 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:

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

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

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

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

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

- This is the final step of the first round of the 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 the two-dimensional matrix is discarded to add to the third step of the encryption process. The given equations perform the operation.

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

Here the two-dimensional matrix has a 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 performed by using keys.

Decryption process

- In the first step of the decryption process, we have to add an arbitrary row in the encrypted image E(i, j) of size P × Q.
- By using equation (4) of the encryption process, the processed image is transformed into the column vectors
- Rj (i) of length P + 1.
- The next step is to transformed the column vectors Rj(i) into Cj (i) by using the one-dimensional inverse 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)
- Now, rejoin the one-dimensional column vectors Cj (i) to obtain a two-dimensional matrix B (i, j).
- 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.
- Finally, the clockwise rotation of matrix A (i, j) by 90◦ is performed. After rotation of the matrix, the first column is leftover to obtain the image R (i, j). Hence by repeating these steps four times and by using the exact key, we get the original image.

D. 2D-Modified Henon map with Hybrid Chaotic Shift Transform technique

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

Output: The shuffled image T.

- By ordering in xk and yk chaotic sequence, construct the row and column shift matrix.
- Repeat for i=1to N do
- 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
- End if condition.
- End for a loop.
- Signify the shifted image as Ti.
- Repeat for i=1 to M
- 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
- End if condition.
- End for a loop.
- Signify the shifted image as T.

E. The 2D logistic chaotic map

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

Encryption Process

In this encryption is performed as firstly the system scans the keyframe as RGB images, then we reshape the matrices into a 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 keyframe pixel values. It is important that the size of produced bits should have the same length as the image. By testing and analyzing, it is confirmed that the addition of random bits to the first keyframe improves the protection level, primarily alongside differential attacks.

Here is the flowchart showing the image encryption scheme:

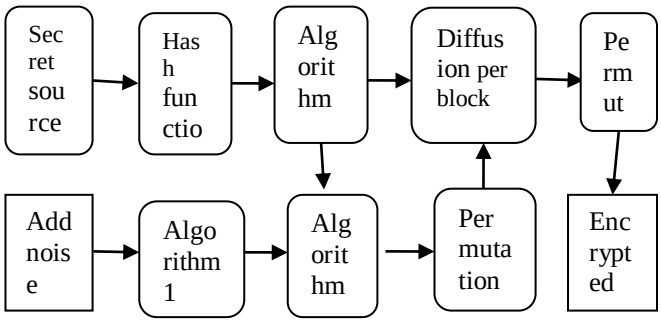

Fig. 2 Image Encryption Scheme

Decryption Process

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

F. 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 keyspace. It was popular in 1976 with name as Multimedia Tools. This logistic map is a one-dimensional chaotic map which is given below

Xn+1= eXn(1-Xn)

Where Xn has a range of zero and one, this is the simplest model that shows chaotic behavior. There is a positive constant e having a range from zero to four. Its value shows the behavior 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 be visualized by human eyes directly. This method uses the permutation substitution procedures. The confusion and diffusion property increase the complexity of an algorithm.

G. Chaotic Tent Map

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

- Read original image (Ma×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 the control parameter represented by μ.
- 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.
- Now, the next step is to perform encryption by mixing the key array x (n) with the original image matrix (Ma×b).
- Finally, we get the encrypted image.
- The flow chart of the image enciphering method is represented as

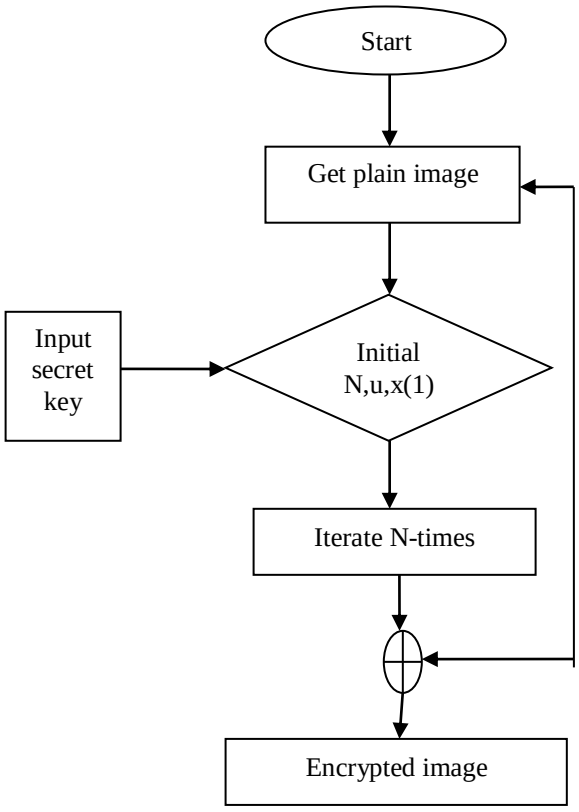

Fig. 3 The image encryption method

Decryption procedure

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

- 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.
- 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 a 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.
- The next step is to perform decryption on the matrix (Ma×b) by extracting the key array x(n) from the encrypted image (Ma×b).
- Finally, we obtain the decrypted image, which is the original image.

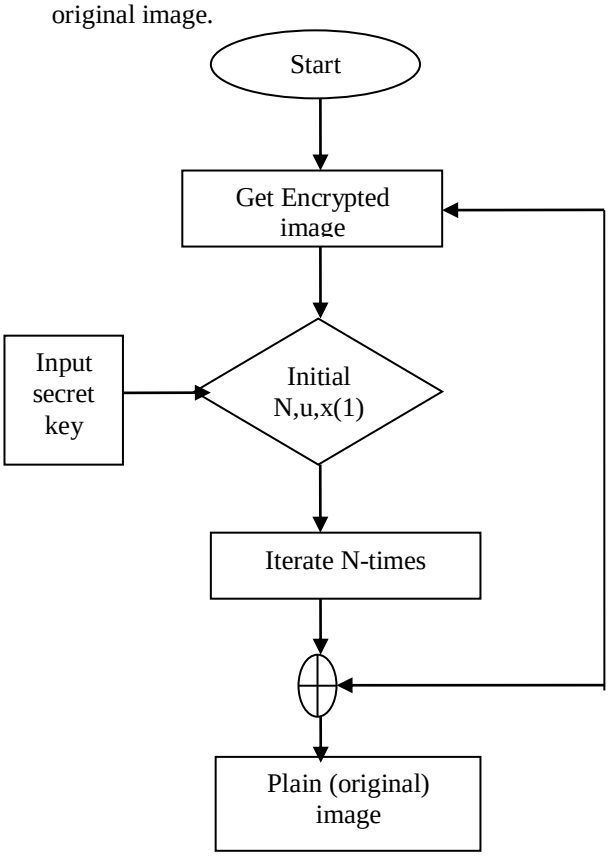

Fig. 4 The image decryption algorithm

H. Binary Image Encryption Algorithm

Algorithm 1: Binary image enciphering algorithm
Encryption process

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

- Select an image as an Input image to encrypt.
- Selected image is now breaking into d blocks.
- Make the d block images equivalent size as the input image.

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

- Calculate bj and bj.
- Store bj as the key-image.
- Store bj as the enciphered image.
-

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

- Select the key- matrix and enciphered images as an input image.
- Return to the basis.

Step 2: Decryption procedure.

- merge the spitted d-block image.
- 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. The next step is the generation of the key-matrix and the enciphered images of the database.

- Calculate aj and bj.
- Store bj as the key image.
- Store bj as the database of enciphered images.

Decryption
Step 1: Select the key-matrix and the enciphered images of the database as input.
Step 2: Return to basis to recommend the deciphered images.

V. CONCLUSION

After an analysis of twenty-two papers, we found the absolute best NPCR got 100% by using Binary Image Encryption Methodology on MATLAB inbuilt database images. THE highest UAIC found 33.8547 using Chaotic System alongside the Substitution, Box algorithm on MATLAB inbuilt database images also as self-created images. The very best Entropy found 7.9892 using the Chaotic System alongside the Substitution, Box algorithm, 7.999 using 2-Dimensional Modified Henon Map with Hybrid Chaotic shift Transform and 7.999 using Chaotic Tent Map algorithm. MATLAB inbuilt database images are used on all three papers for calculating Entropy.

And maintaining the IJCTT LaTeX style files which have been used in the preparation of this template. To see the list of contributors, please refer to the top of file IJCTT Tran. Cls in the IJCTT LaTeX distribution.

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, A novel scheme for image encryption using substitution box and chaotic system., (2017).

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

[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 Sbox 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 image 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 bouraoui Software, 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., Cryptography and network security. Tata McGraw-Hill Education., (2013).

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

[25] Kirti Sapra and Swati Kapoor, Modified Image Encryption Technique, SSRG International Journal of Electronics and Communication Engineering 1(6) (2014) 21-25.

[26] Subburaj.V, Srinivasan.M, Surendiran, R Sundaranarayanan, R. DDoS Defense Mechanism by Applying Stamps using Cryptography. International Journal of Computer Applications. 1(6) (2010) 48-52..ISSN: 0975 – 8887, DOI: 10.5120/143-262.