Image Cryptography: A State-Of-The-Art Survey on Image Encryption and Decryption Techniques

Hitesh Verma, Alka Choudhary, Jyotsna Parmar

Department of Computer Engineering, J. C. Bose University of Science and Technology YMCA, Faridabad, Haryana 121006, India

Corresponding Author: hitesh1425@gmail.com

Review Paper Received: 02.02.2021 Revised: 22.07.2021 Accepted: 24.08.2021

Abstract—In the present era of social media and smartphones, when almost all the smartphone users are clicking and posting their pictures on social media, then at this time the security of the transmitted images is of utmost importance. Colored images are widely used due to economically affordable gadgets as compared to the gray-scale images and moreover they contain more information in them. In this paper, a state-of-the-art survey of various techniques developed by various researchers in the area of image encryption is presented and a detailed comparison on various available techniques and algorithms in the area of image encryption is done. This paper also compares these techniques on the basis of their performance like NPCR, UACI, Correlation Coefficient, Entropy etc.

Keywords—Image encryption, Color image security, Chaotic cryptography, Multiple image encryption, Medical image security

1. Introduction

In today's world, when the technologies like Cloud Computing and Internet of Things are trending among researchers and are the real future technologies. Security of data still lies as the biggest challenge for their complete success. As the data on the internet is transmitted through different available communication networks, it makes it vulnerable to the hackers as they might eavesdrop or manipulate it while data is travelling on some medium. For textual data encryption, there are various strong algorithms such as BlowFish, Advanced Encryption Standard (AES), Embedded Image coding using Laplace transform [1], but these are found undesirable for images as images have high correlation among the data present in its pixels. Moreover, these algorithms lack speed in permutation and diffusion of image data, hence they are inefficient for images [2]. Also, the images captured using electronic devices are of very much of importance and they carry lots of information in them, so one of the best methods to save the image from the unethical elements is to convert it into an obscured image [3]. Majorly, images are classified into two types: gray-scale and colored images. Gray scale images have only one channel i.e., gray and colored images comprise of 3 channels Red, Green and Blue which together makes a pixel. In this paper, the focus is on the area of colored images as they are widely used and contains large amount of information which might be more sensitive than grey-scale contents. There are a lot of techniques

which have been already used for colored images based upon manipulating Red, Green and Blue channels and performing various operations on them and also using chaotic maps for pseudo random number generation [4,5,6].

Fig. 1: Lena image

Fig. 2: Red Channel

Fig. 3: Green Channel

Fig. 4: Blue Channel

A colored image has height H and width W so total WxH pixels. Pixel is nothing but a color dot. The value of each pixel is determined by the three channels namely Red, Green and Blue. To illustrate it, we have Fig. 1 that represents the colored Lena image while Fig. 2, Fig. 3 and Fig. 4 represents the respective Red, Green and Blue channels of the colored Lena image.

Image encryption is basically a process of making the input image unrecognizable so that a person cannot find the real image without the authorized access. Fig. 5 represents the image that is to be encrypted and Fig. 6 represents the given image after encryption. As shown in Fig. 6, the encrypted image is totally different and unrecognizable.

Fig. 5: Given Image

Fig. 6: Encrypted Image

There are many techniques of image encryption. One such technique uses chaotic cryptography. Chaotic cryptography is based upon mathematical chaos theory. It includes two prime steps, one is confusion stage and the other diffusion stage, both of which use sequences generated from chaotic maps [7]. Confusion part is just a method to change the pixel position based upon the index of chaotic sequence. It can also use the sequence for diffusion part also. Another method is DNA cryptography where there is a use of complementary rules of the DNA [8]. It has basically two stages- first one is DNA encoding, which is used to encode the input image as per the encoding rules of DNA and second stage involves DNA computing which is applying DNA operations like addition, subtraction and Ex-or on the image to obtain the encrypted image. Another method which is like DNA is RNA computing. Here RNA encoding rules can also be used with RNA computing rules just as it has used in the DNA. RNA is not totally alike DNA. It has amino acids of codons which can be further used in encryption of image [9]. One more method involves pixel scrambling processes which uses SCAN patterns like Spiral method, Zig-Zag method, Raster method for permuting the pixel positions [10]. Here the pixels are permuted first based upon one of the methods and then pseudo-

random sequences are produced using the chaotic maps that are used to diffuse the scrambled matrix. In most of the cases multiple images are sent over the network and single image encryption is inefficient for multiple images to be encrypted [11]. So, there is a need for algorithm for multiple image encryptions to encrypt multiple images in a single go. Basically, the multiple images are integrated into a one big image and then the permutation and diffusion are applied on them. Next section presents a state-of-the-art survey of various image encryption techniques. Section 3 gives the performance analysis of these techniques based on parameters which are used to evaluate an image encryption technique. Finally, section 4 provides the conclusion of the whole survey and its future scope.

2. Literature Review

A great amount of research has been done on Image encryption and decryption of images. Various techniques have been studied and read. Some of these techniques are: Chaotic techniques, DNA and RNA cryptography, Scrambling image technique, multiple image cryptography. In this section, a review of various schemes and methods available in the area of image encryption is presented and an effort is made to classify them as per their techniques and also about how they are applied and why it is advantageous to use them.

2.1. Image Encryption using Chaos based algorithms

Chaos is a state of disorder. In science, chaos is systematic and that is why called as deterministic chaos. A chaotic system is defined as a system which is highly dependent on initial conditions. Different conditions result in completely different results. Chaotic system is good when it comes to producing numbers in a pseudo-random manner and also, they are particularly very sensitive to the initial conditions given as their parameters [12]. Here the pseudo-random sequence produced using chaotic maps is used to permute the pixel positions and also at the same time is used in creation of diffusion matrix. To protect the image the sequence should be related to the plain image. There are various chaotic systems like Lorenz map, Arnold's cat map, Hénon map, Logistic map, Chen's Chaotic system, Tent and sine map etc. which are widely used in image encryption processes are.

Vidhya et al. [13] proposed a technique for colored images in which the plain image data is used to compute a seed and it is used as an initial vector for the Henon map and is iterated over and over in order to get the sequences. After this, the sequence is used for permuting rows and columns using Rubik's cube method. The same seed is applied for producing the key using the prime factorization method which is at last applied after permutation. The key generation process broadly involves two steps: first, prime factorization is done and then secondly these factors are used in the diffusion stage. On testing it is found that this technique was infeasible to brute force, statistical and differential attacks.

Teng et al [14] proposed a technique for colored images, using integrated bit-level where the given image was converted into their respective Red, Green and Blue planes and is combined into one bit level. Then chaotic map is used to get a pseudo-random sequence which is used to permute the bit level image multiple times in a row. And then the one bit level is converted back to its three planes and merged back into one. It is useful in decreasing the correlations among

the pixels while not using the diffusion operation saves time and makes the process time efficient.
Huang et al. [15]proposed a technique for gray and colored images where the permutation and diffusion operations are done in tandem to achieve a better security level. The permutation-diffusion operation happening at the same time reduces the clarity and makes it confusing, thus generating providing better security with higher efficiency. Here at first only single permutation-diffusion operation, where user randomly choose the location of the first encrypted pixel and set the values using both the values generated by key stream using 3D chaotic maps and then the value of the pixel in the plain image and the pixel that is encrypted is made to be dependent of value of previous pixel. The simple and clean permutation operations make it secure.
Patro et al [16] proposed a technique for colored images, which uses multiple piece-wise linear chaotic map systems. At start of the process, image blocks are rotationally permuted and then row column permutations are applied. After this the row, column and block diffusion techniques are applied to get the final encrypted image. It provides high security, simplicity, with the ability to withstand statistical attacks,
Wang et al. [17] proposed a technique for gray and colored images, where a random key is used to generate initial conditions for chaotic maps. Then SHA512 has algorithm is used to produce a key from the image. That key is used to produce a block positions and their divisions. Also, the chaotic maps and the key are used for the diffusion. It has better security and can withstand common attacks.
Mortajez et al. [18] proposed a technique for DICOM standard images which are used in medical science and its applications. At first, secret keys are extracted from all the pixels of the given plain image. Then permutation of the pixel position on the basis of random sequences and confusion algorithm is done. At last, permuted image pixels are diffused on the basis of sequences of logistic systems and the EX-or operator. It is resistant to differential attacks and exhaustive attacks.
Chaotic systems offer more key space, resistance to attacks and high speed and computationally cheap for encryption of images.
In the next subsection, DNA and RNA based image encryption techniques is reviewed.

2.2. Image Encryption using DNA and RNA based algorithms

In order to encode the three channels namely Red, Green and Blue, of the colored image and perform the DNA and RNA operations on them, one can use RNA and DNA rules as shown in Table 1 and Table 2. This subsection focuses on some techniques using DNA and RNA based algorithms.

TABLE 1: DNA encoding table

Rule	1	2	3	4	5	6	7	8
00	A	A	G	G	T	T	C	C
01	G	C	G	C	A	T	A	T
10	C	G	C	G	T	A	T	A
11	T	T	A	A	C	C	G	G

TABLE 2: RNA encoding table

Rule	1	2	3	4	5	6	7	8
00	A	A	G	G	U	U	C	C
01	G	C	G	C	A	U	A	U
10	C	G	C	G	U	A	U	A
11	U	U	A	A	C	C	G	G

Azimi et al [19] proposed a technique for colored images, where DNA encoding rules are used with the pair coupled chaotic maps to produce the encrypted image. First, decomposition of the colored image given to us in three components:

Red, Green, Blue is done. After that these three matrices are encoded using DNA encoding rules to make DNA matrices. In the next step, Red, Green and Blue components are added using DNA addition, and pair coupled chaotic maps are used to scramble the position of elements in the DNA sequence. We have a RGB encrypted image made after structuring and merging of R, G, and B components. It gives larger secret key space, high secret key sensitivity and resistance to statistical attacks.

Rehman et al. [20] proposed a technique for colored images, where the SHA-2 issued to produce the initial parameters for the chaotic maps. Then the R, G, B channels are first combined in a vector and then sorted as per Piecewise Linear Chaotic Map. After that R, G, B channel matrices are permuted independently using Lorrenze Chaotic map. After these steps the image pixels are encoded using DNA encoding rules and after that Ex-OR is done using DNA complimentary rules. This algorithm is found to resistant to plain image and differential attacks.

Wang et al. [21] proposed a novel chaotic image encryption algorithm for gray and colored images, which is based upon extended Zigzag confusion and RNA operation initially for gray images. Here a chaotic sequence is obtained using the SHA 512 hash function and Zig-Zag confusion is done based upon the chaotic sequence. Finally, the RNA encoding and RNA operations are applied as per amino acids and coding rules of RNA matrix controlled by the chaotic sequences we first generated.

Wu et al. [22] proposed a technique for gray images, where a 2D Hénon-Sine map is used for permutation of pixels. This map is used due to its wider range of chaos than other maps. For the permutation and diffusion process there is a use of DNA encoding process and then the DNA operations as it makes them efficient. For the diffusion part the DNA encoding and operations approach is used and for the permutation part the 2D Hénon-Sine map is used, which proves to be secure technique for the image. DNA-based encryption methods have large key space and low storage space and less costly in computation.

In the next subsection, scrambling based image encryption techniques are reviewed.

2.3. Image Encryption using Scrambling based algorithms

Scrambling of image is an important method for the preprocessing of image for various other encryption procedures. There are many scrambling methods like Arnold Cat map, Zig-Zag transformation method, Spiral transformation etc. This section reviews some of these techniques. Wang et al. [23] proposed

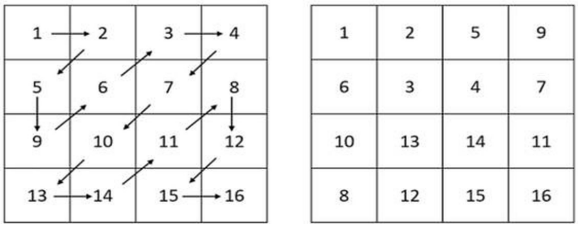

Fig. 7: Zig-Zag transform

a technique for gray and colored images, where Zig-Zag transformation method as shown in Fig.7 and LL compound chaotic system are used. In Zig-Zag method the matrix is traversed in “Z” letter shape and rearranged as per the traversal route. The LL compound chaotic map consists of Lü system and logistic chaotic map. The Lü system is nothing but a very easy circuit implementation of the third-order chaotic system. Here the Zig-Zag transformation and Lü system are used to permute block sub-channel

of the original image, and then complement of it is done by a sorting scrambling algorithm with identification values. Lü system and logistic chaotic map are integrated to get the LL compound chaotic system.
Xian et al. [24] proposed a technique for gray and colored images, where the plain image is first spiraled in blocks and then the blocks are scrambled depending upon the index matrix of block generated from the chaotic sequence. Then the two chaotic sequences are used to generate a matrix of size of plain image for the diffusion part. Chen's chaotic system is used for generation of chaotic sequences. This technique gives a higher key sensitivity and can effectively resist statistical, brute-force and differential attacks.
Hua et al. [25] proposed a technique for DICOM images, where at first the image is deliberately surrounded by the noise around the image matrix and after that a scrambled matrix is produced using the logistic chaotic map and their indexes and then the image matrix is scrambled based upon the scrambled matrix and after that the image matrix is diffused using the previous pixel value and new sequence generated from chaotic map. Scrambling methods are easily implementable and run efficiently and hence used in various image encryption techniques.

In the next subsection, multiple image encryption techniques are reviewed.

2.4. Image Encryption algorithms for multiple images

There are many techniques for single image but nowadays in real life, there are multiple images at a time. So, these images should be encrypted at a time and algorithms for single image are not sufficient for multiple images.
Zarebnia et al. [26] proposed a technique for gray images, where first the sub-blocks of the images are permuted independently and then the images are merged together in a big image and then that big image is permuted using chaotic maps. Arnold cat map is used to form a matrix and cyclic shifts are applied and then the image is diffused with it to get the encrypted image. This image is safe from differential attacks.
Enayatifar et al. [27] proposed a technique, where initially multiple plain- images given as input are combined together to make a single big image. After this, big image is converted into one dimensional array. Then the halves of the array indexes are utilized to permute positions of the big image pixels. While the process of permutation is happening, the same indexes are used and are made to associate with DNA sequence to diffuse the pixels gray level.

In the next subsection, non-chaotic maps based image encryption techniques are reviewed.

2.5. Image Encryption algorithms based upon non chaotic maps techniques

Chaotic maps are used for generating pseudo-random sequences but they have the disadvantage that there is a floating-point computation in chaotic iteration. So, in order to remove this advantage researcher came up with the non-chaotic image encryption algorithms and some of these are reviewed in this subsection.
Wang et al. [28] proposed a technique for colored images, where a combination of Logistic chaotic maps and Tent maps to process the initial key and after that the parameters are obtained for Arnold mapping using a function transformation which is required to permute the pixels of the plain

image. Hopfield chaotic neural network is used to create the self-diffusion chaotic matrix required for diffusion phase, and the key is produced using a function transformation; at last, the permuted image is EXORed with the key produced to obtain the final encrypted image.

Dawahdeh et al [29] proposed a technique for gray images, where Hill cipher algorithm was used for time efficient computations and to take care about its weak security, Elliptic curve cryptography is used. Here no chaotic maps are used to for generation of random numbers. Elliptic curve cryptology technique can work upon smaller key spaces and here the inverse of the matrix is not required but instead the same matrix is used in encryption. It is secure and resists various attacks.

Kandar et al [30] proposed a technique for gray images, where the random sequences are generated by the cyclic group. Cyclic groups form the basis of the technique. Here, at first pixel positions are permuted and after that pixels are permuted at the bit level. Then bits are shifted as per the transformation array and then pixels are added iteratively for diffusion.

Dhall et al. [31] proposed a technique for gray images, where the blocks can be customized for the encryption process. Here random bits are inserted after which two staged diffusion process is followed, the diffusion process involves Ex-OR. Addition of random bits makes the scheme probabilistic. The diffusion stage helps in increase of the entropy and will result in the uniform intensity distribution of cipher. Here the cipher text generated is double that of the plain text size.

Zhou et al [32] proposed a technique for colored images, where the 3d orthogonal Latin square technique in addition to matching matrix which is also orthogonal to the 3D-OLS is used. A Latin square is a matrix of size m x m containing 'm' different numbers each occurring exactly once in each row and exactly once in each column. Fig. 8 represents the Latin square matrix of order 4 where numbers from 1 to 4 occurs exactly once in each row and each column. In permutation process 3D orthogonal Latin square and matching matrix are used to permute the plain image. Then the process of block linking is executed and then cyclic shifting is done on matrix and then the final diffusion will take place.

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{bmatrix}$$

Fig. 8: Latin Square of order 4

2.6. Comparison of various Image Encryption algorithms

In this section, comparison of various image encryption algorithms has been done. The comparison of the techniques is essential as it gives readers the basic idea about it in short rather than reading the papers one by one.The Table 3 presents a comparison of different encryption schemes and methods already available in the literature to provide a brief review of them.

TABLE 3: Comparison table of various image encryption schemes and methods

S.No	Paper Name	Method Used	Advantages	Disadvantages
1.	Teng et al. [14]	Skew tent map, permutation, diffusion	Infeasible to brute force attacks, statistical attacks. No diffusion makes algorithm faster.	No diffusion in the process and simple chaotic maps makes it less secure too.
2.	Dawahdeh et al. [29]	Curve Cryptosystem with Hill Cipher	Resistance to statistical and exhaustive attacks.	UACI value is less than 33% which will lead to differential attacks.
3.	Azimi et al. [19]	DNA encoding, Pair coupled chaotic maps	Larger secret key space, resistant to statistical attacks and exhaustive attacks. high secret key sensitivity	Suffers from plain text attacks, and time consuming.
4.	Huang et al. [15]	Permutation-diffusion simultaneous operation	Resistant to plain text attacks, highly efficient, secure against statistical attacks and also brute-force resistant.	Suffers from differential attacks.
5.	Patro et al. [16]	Multiple piece-wise linear chaotic map.	Has a high key space and security and simplicity, can withstand statistical attacks.	Not safe from plain text attacks.
6.	Wang et al. [17]	Logistic chaotic maps, Tent Maps, Arnold Cat Map, Hopfield chaotic neural network	Resistant to statistical, differential attacks, shows good resistance to noise attacks,	After certain iteration, the plain image is obtained in Arnold Map.
7.	Wang et al. [23]	ZigZag transform, LL chaotic system	Resistant to exhaustive attacks, statistical attacks, resist the chosen plaintext attack.	Not resistant to differential image attack
8.	Kandar et al. [30]	Cyclic group, permutation, diffusion	Infeasible to brute-force attacks, also shows resistance to statistical and differential attacks	Chaotic maps are not used which makes it more time consuming
9.	Wang et al. [21]	ZigZag transform, RNA encoding and operations	Secure against exhaustive attacks, statistical attacks, chosen plain text attacks.	Suffers from differential attacks.
10.	Vidhya et al. [13]	Henon Map, Rubiks Cube algorithm, Prime factorization, Permutation, diffusion	Good key space, secure against statistical attacks, brute force resistant, effective against plain text attacks.	Increment vector used in the PF (prime factorization) process has to be sent over the network for every new encryption, PF process is computationally expensive.

Continuation of Table 3

S.No	Paper Name	Method Used	Advantages	Disadvantages
11.	Xian et al. [24]	Block scrambling, Chen's chaotic system	Nice range of key space, secure against differential attacks, brute force attacks, statistical attacks, noise attacks.	Not resistant to plain image attacks
12.	Wang et al. [17]	Chaotic maps, SHA512, permutation and diffusion	Larger secret key space, resistant to statistical attacks, resistant to exhaustive and differential attacks.	Time complexity high due to additional elements used while diffusing
13.	Rehman et al. [20]	SHA-2, Lorrenze Chaotic maps, DNA encoding rules	Resistant to brute force, statistical, differential and occlusion attack.	Not resistant to plain image attacks, and multiple diffusion operations increase time Complexity.
14.	Zarebnia et al. [26]	Arnold Cat map, block permutation and diffusion	Infeasible to brute-force, statistical, differential and plain text attacks	Arnold Cat map is used which gives the same value after some iteration.
15.	Dhall et al. [31]	Random bits insertion, block division and permutation	Secure against plain text attacks, brute force resistant, resistant to plain text attacks, large key space,	Suffers from differential attacks
16.	Zhou et al. [32]	3d orthogonal Latin square, permutation, diffusion	Resistant to statistical, plain text, differential, noise attacks, also resistant to brute force attacks.	Suffers from plain image attacks, and time consuming.
17.	Wu et al. [22]	2D Hénon-Sine map. DNA cryptosystem	Resistant to exhaustive attacks, statistical attacks, noise attacks, differential attacks	Suffers from plain image attacks.
18.	Mortajez et al. [18]	Logistic chaotic system, permutation	Efficient algorithm, resistant to differential attack, brute force attacks, statistical attacks, plain text attack	Suffers from noise attacks
19.	Enayatifar et al. [27]	DNA encoded diffusion, permutation	Resistant to exhaustive attacks, statistical attacks, plain text attack, time efficient	Not much secure from differential attack
20.	Hua et al. [25]	Scrambled matrix using Logistic chaotic map, diffusion	Resistant to exhaustive attacks, statistical attacks, differential attack, suited for medical images	Not secure from plain image attack

In next section, performance analysis of the image encryption techniques is done.

3. Performance Analysis

To determine and check the security and efficiency of an algorithm there are different parameters used to comprehensively evaluate them. The plain image needs to resist attacks like brute-force, differential, chosen plain text and statistical attack. Performance metrics of various techniques are shown in Table 4. The parameters which are generally used to evaluate the image encryption algorithms are summarized in this section.

3.1. Histogram Analysis

Histograms are used to tell us about the statistical information of the image and also the intensity of gray level. If the histogram is non-uniform, then there is a high probability of histogram attack. But if the histogram is uniform then it is difficult to predict the information [5].

3.2. Correlation Analysis

In images you will see that there is a strong relation among the adjacent pixels horizontally, vertically and diagonally. The maximum value of the correlation coefficient is 1 and the minimum value of the correlation coefficient is 0 [33]. The Eq. (1)-(4) are used to calculate the correlation coefficient of the horizontal, vertical and diagonal pixels. The value closer to 0 for encrypted image is considered as good encryption technique.

$$R_{xy} = \frac{cov(x,y)}{\sqrt{/D(x)}\sqrt{D(y)}} \tag{1}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{2}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{3}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{4}$$

In the above relations, N represents the number of pixels in a NxN image, y represents the horizontal pixel adjacent to x, E(x) is the mean,$\sqrt{D(x)}$ is the standard deviation.

In next subsection information entropy analysis of encrypted image is done.

3.3. Information Entropy Analysis

Entropy analysis informs about the randomness of the system and computes the spread of gray level in each of the Red, Green, Blue channels. Entropy values nearer to 8 means they are harder to predict. It is depicted by Eq. (5) [34]

$$H(m) = -\sum_{i=0}^{N-1} P(m_i) log_2 P(m_i) \tag{5}$$

where, m denotes the source of information used and the probability of occurring of symbol m in the source is denoted by P (m). The value 8 is considered to be the ideal value.

In next subsection, the analysis of NPCR and UACI of encrypted image is done.

3.4. NPCR and UACI Analysis

NPCR stands for number of pixels change rate when one of the pixels is changed in the image. The value of NPCR nearer to 100% the more the encrypted image is dependent upon the plain image and better it is resistant to plain text attacks. UACI stands for Unified Average Changed Intensity which informs about the average intensity of differences between the plain image and encrypted image. The UACI value is generally preferred above 33% for effective algorithm and higher the value of the UACI, the more effective it is against differential attack. The ideal value of NPCR and UACI are 99.61% and 33.46% , respectively [35]. The Eq. (6) gives us the formula for calculating NPCR.

$$NPCR = \sum \frac{D(i,j)}{M \times N} \times 100\% \tag{6}$$

where the length and breadth of the random images is denoted by M and N and the value of D(i, j) is calculated using Eq. (7) where X_1 and X_2 shows the encrypted images before and after change of one pixel in the plain image.

$$D(i,j) = f(x) = \begin{cases} 1, \text{if} X_1(i,j) \neq X_2(i,j) \\ 0, \text{otherwise} \end{cases} \tag{7}$$

Eq. (8) is used to calculate UACI value

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{X_1(i,j) - X_2(i,j)}{255}\right] \tag{8}$$

In next subsection, an occlusion noise attack on encrypted image is studied.

3.5. Occlusion Noise Attack

Sometimes during encryption, some portion of the encrypted image might be lost, so the technique used should be capable to handle it while decrypting. This can be tested by partially removing a part of the image or its channel and then try to decrypt it. It should be capable of decrypting lossy image [20]. In next subsection, differential attacks on the encrypted image are studied.

3.6. Differential Attack

In the differential attack, the attacker has the means of access to the encryption machine and tries to encrypt the image with very small change in input image and observes the changes in the output image. The attacker will make various attempts to find the key used for encryption. Hence the key should be dependent on image to avoid differential attacks in general [36]. In next subsection, the chosen plain text attacks on the encrypted image are studied.

3.7. Chosen plain text attacks

In plain text attacks, the attacker tries to make uniform or special input images like all input pixels black or white. Using these attacker tries to find the key used or find the relation between plain image and encrypted image. Hence, the key should be dependent on image to avoid these attacks in general [37].

3.8. Performance based comparison of various Image Encryption algorithms

In this section, various image encryption algorithms are compared on the parameters. Table 4 compares the performance of various encryption methods on the basis of Correlation Analysis, entropy of the image, key space, NPCR and UACI. For calculating parameters, Zhou [32], Vidhya [13], Wang [21], Azimi [19], Huang [15], Patro [16], Wang [23], Wang [28], Teng [14],

TABLE 4: Various techniques and their performances

SNo.	Authors/ Reference	Year	Average Correlation Analysis			Entropy	Key Space	NPCR	UACI
			Horizontal	Vertical	Diagonal				
1.	Mortajez et al. [18]	2020	0.0013	0.0021	-0.0037	7.9994	10^{56}	99.6124	33.549
2.	Zhou et al. [32]	2020	0.00063	0.0058	-0.0051	7.9973	2^{300}	99.6278	33.5052
3.	Xian et al. [24]	2020	0.0014	0.0016	- 0.00882	7.9973	$>2^{156}$	99.6105	33.4656
4.	Vidhya et al. [13]	2020	0.000027	0.00045	0.00081	7.9953	10^{114}	99.6261	33.4670
5.	Wang et al. [21]	2020	- 0.008824	−0.0004	0.0028	7.9972	10^{140}	99.6002	33.4592
6.	Azimi et al. [19]	2019	0.00267	-0.0835	-0.0722	7.9988	10^{450}	-	-
7.	Huang et al. [15]	2019	-0.0015	-0.00056	0.002	7.9994	2^{170}	99.6094	33.4635
8.	Patro et al. [16]	2019	0.0031	0.0005	-0.0041	7.9997	1.2219×2^{626}	99.6314	33.5513
9.	Wang et al. [23]	2019	-0.0034	0.0019	-0.0134	7.9993	2^{128}	99.61	33.4766
10.	Wang et al. [28]	2019	-0.0034	0.0019	-0.0134	7.9987	10^{102}	99.6233	33.4766
11.	Kandar et al. [30]	2019	0.00094	0.00084	0.0027	7.9993	2^{148}	99.6944	33.4162
12.	Zarebnia et al. [26]	2019	−0.003644	0.00262	0.001239	7.9995	10^{195}	99.6059	33.4173
13.	Enayatifar et al. [27]	2019	0.0017	0.0029	0.0009	7.9992	-	99.1841	33.5284
14.	Teng et al. [14]	2018	-0.011701			7.9942	10^{128}	99.6282	33.4795
15.	Dawahdeh et al. [29]	2018	-	-	-	7.9970	-	-	30.4814
16.	Wang et al. [17]	2018	0.001787	0.001203	0.001497	7.9028	1.4742×10^{236}	99.6105	33.4539
17.	Rehman et al. [20]	2018	-0.0041	0.0016	0.00206	7.9968	10^{94}	99.6073	33.4254
18.	Dhall et al. [31]	2018	-5.6521×10^{-05}			7.9987	2^{256}	99.5808	33.4413
19.	Wu et al. [22]	2018	0.0056	0.0037	0.0032	7.9976	10^{112}	99.6200	33.4169
20.	Hua et al. [25]	2018	-	-	-	7.9977	2^{256}	Close to 99.9985	Close to 33.3338

Dawahdeh [29], Wang [17], Rehman [20], Dhall [31], Hua [25] has used Lena image of size 256 x 256. Kandar [30] has used Lena image of size 512 x 512. Wu [22] has used gray Lena image of size 256 x 256. Zarebnia [26] has used Elaine image of size 256 x 256. Enayatifar [27] has used four random images of size256 x 256 each. Xian [24] has used random images of size 256 x 256. Mortajez et al. [18] and Hua et al. [25] has used DICOM standard medical images of size 512 x 512.

In Dhall [31] a single value for correlation coefficient was only given. In Hua[25] MIE-BX method for entropy and MIE-BX and MIE-MA used on DICOM images is considered for parameter values. We have studied various techniques in image encryption like Chaos based, DNA and RNA based, Scrambling based, Multiple images based and Non-chaotic maps based. It is found that the chaos based techniques are found to be better in terms of NPCR, UACI, Entropy as compared to others but suffers in key space as it has low key space than other techniques. The DNA and RNA techniques which are reviewed are bound by a set of rules for the operations which makes the randomization in the values of the encrypted image low but efficient in terms of computation and storage, thus providing a low cost alternative. The scrambling encryption techniques reviewed are found to be good in terms of speed and entropy but they suffer from the occlusion attack and will not be able to get the plain image if the encrypted image was added with noise. Multiple image encrypting algorithms were found to be better to encrypt all images together at once rather than one by one but the problem in these techniques is that they can process the images if all of them are of one particular size only rather than different ones. Non chaotic maps techniques give a different way of generating random sequences as they don't involve floating points like chaotic maps but this causes increase computation time as compared to chaotic maps techniques. Researchers should use a combination of various techniques to solve the problems of the other technique. It has been found that use of techniques in combination will give better results and also better security and will also root out the deficiency of other.

4. Conclusion

The subject of paramount importance in today's world is of image security especially when there are networking technologies used for sending and receiving the images. In today's world, the use of images is frequent especially in online learning which has been ameliorated in COVID time, defense, advertising, engineering etc. While much attention is given to storage space and efficient transfer for images, there should also be concern for the integrity and safety of the images. Various techniques majorly for colored images than gray images are discussed due to more data and wide use. Many of these techniques suffered from the differential, noise and plain text attacks. Some of these techniques which are resistant to these attacks are not time efficient or had security issue while transferring the secret key. In this paper, many techniques and methods are discussed with their resistance to various attacks possible on image. A performance analysis of the techniques based upon the various performance parameters is shown. Based upon these, future research schemes can be designed for images. The direction for ongoing research should be designing a technique which should be resistant to attacks and also efficient. There are various methods which are reviewed; the integration of two or more

methods can be used for better performance and security.

5. Acknowledgments

The authors would like to thank the reviewers for their inputs in the form of review that led to the improvement of the review paper.

References

[1] M.T. Gencoglu, "Embedded image coding using Laplace transform for Turkish letters," Multimedia Tools and Applications, vol. 78, no. 13, pp. 17521–17534, 2019.

[2] S.M. Seyedzadeh and S. Mirzakuchaki, "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map," Signal Processing, vol. 92, no. 5, pp. 1202–1215, 2012.

[3] X. Wu, K. Wang, X. Wang, H. Kan and J. Kurths, "Color image DNA encryption using nca map based cml and one-time keys," Signal Processing, vol. 148, pp. 272–287, 2018.

[4] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," Computers & Mathematics with Applications, vol. 59, no. 10, pp. 3320–3327, 2010.

[5] M. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R.M López-Gutiérrez and O.A. Del Campo, "A RGB image encryption algorithm based on total plain image characteristics and chaos," Signal Processing, vol. 109, pp. 119–131, 2015.

[6] B. Norouzi and S. Mirzakuchaki, "A fast color image encryption algorithm based on hyper-chaotic systems," Non Linear Dynamics, vol. 78, no. 2, pp. 995–1015, 2014.

[7] G. Jacob and A. Murugan, "DNA based cryptography: An overview and analysis," International Journal of Emerging Sciences, vol. 3, pp. 36–42, 2013.

[8] H. Liu and X. Wang, "Image encryption using DNA complementary rule and chaotic maps," Applied Soft Computing, vol. 12, no. 5, pp. 1457–1466, 2020.

[9] M. Mahmud, M. Lee and J.Y. Choi, "Evolutionary-based image encryption using RNA codons truth table," Optics & Laser Technology, vol. 121, p. 105818, 2020.

[10] S.S. Maniccam and N.G. Bourbakis, "Lossless image compression and encryption using SCAN," Pattern Recognition, vol. 34, no. 6, pp. 1229–1245, 2001.

[11] Z. Gan, X. Chai, M. Zhang and Y. Lu, "A double color image encryption scheme based on three-dimensional Brownian motion," Multimedia Tools and Application, vol. 77, no. 21, pp. 27919–27953, 2018.

[12] Y. Li,C. Wang and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," Optics & Lasers Engineering, vol. 90, pp. 238–246, 2017.

[13] R. Vidhya and M. Brindha, "A chaos based image encryption algorithm using Rubik's cube and prime factorization process (CIERPF)," Journal of King Saud University-Computer and Information Sciences, in press, 2021.

[14] L. Teng, X. Wang, J. Meng, "A chaotic color image encryption using integrated bit-level permutation," Multimedia Tools and Application, vol. 77, no. 6, pp. 6883–6896, 2018.

[15] L. Huang, S. Cai, X. Xiong and M. Xiao, "On symmetric color image encryption system with permutation-diffusion simultaneous operation," Optics and Lasers Engineering, vol. 115, pp. 7–20, 2019.

[16] K. Patro and B. Acharya, "An efficient colour image encryption scheme based on 1-D chaotic maps," Journal of Information Security and Application, vol. 46, pp. 23-41, 2019.

[17] M. Wang, X. Wang, Y. Zhang and Z. Gao, "A novel chaotic encryption scheme based on image segmentation and multiple diffusion models," Optics and Laser Technology, vol. 108, pp. 558-573, 2018.

[18] S. Mortajez, M. Tahmasbi, J. Zarei and A. Jamshidnezhad, "A novel chaotic encryption scheme based on efficient secret keys and confusion technique for confidential of DICOM images," Informatics in Medicine Unlocked, vol. 20, p. 100396, 2020.

[19] Z. Azimi and S. Ahadpour, "Color image encryption based on DNA encoding and pair coupled chaotic maps," Multimedia Tools and Application, vol. 79, pp. 1727–1744, 2020.

[20] A. Rehman, X. Liao, R. Ashraf, S. Ullah and H. Wang, "A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2," Optik, vol. 159, pp. 348-367, 2018.

[21] X. Wang and N. Guan, "A novel chaotic image encryption algorithm based on extended Zigzag confusion and RNA operation," Optics and Laser Technology, vol. 131, p. 106366, 2020.

[22] J. Wu, X. Liao and B. Yang, "Image encryption using 2D Hénon-Sine map and DNA approach," Signal Processing, vol. 153, pp. 11-23, 2018.

[23] X. Wang, J. Zhan and G. Cao, "An image encryption algorithm based on ZigZag transform and LL compound chaotic system," Optics and Laser Technology, vol. 119, p. 105581, 2019.

[24] Y. Xian, X. Wang, X. Yan, Q. Li and X. Wang, "Image Encryption Based on Chaotic Sub-Block Scrambling and Chaotic Digit Selection Diffusion," Optics and Lasers in Engineering, vol. 134, p. 106202, 2020.

[25] Z. Hua, S. Yi and Y. Zhou, "Medical image encryption

using high-speed scrambling and pixel adaptive diffusion," Signal Processing, vol. 144, pp. 134-144, 2017.

[26] M. Zarebnia, H. Pakmanesh and R. Parvaz, "A fast multiple-image encryption algorithm based on hybrid chaotic systems for gray scale images," Optik, vol. 179, pp. 761-773, 2018.

[27] R. Enayatifar, F. Guimarães and P. Siarry, "Index-based permutation-diffusion in multiple-image encryption using DNA sequence," Optics and Lasers in Engineering, vol. 115, pp. 131-140, 2018.

[28] X.Y. Wang and Z.M. Li, "A color image encryption algorithm based on hopfield chaotic neural network," Optics and Lasers Engineering, vol. 115, pp. 107–118, 2019.

[29] Z. Dawahdeh, S. Yaakob and R. Othman, "A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher," Journal of King Saud University-Computer and Information Sciences, vol. 30, no. 3, pp. 349-355, 2019.

[30] S. Kandar, D. Chaudhuri, A. Bhattacharjee and B.C. Dhara, "Image encryption using sequence generated by cyclic group," Journal of Information Security and Applications, vol. 44, pp. 117-129, February 2019.

[31] S. Dhall, S. Pal and K. Sharma, "A chaos-based probabilistic block cipher for image encryption," Journal of King Saud University-Computer and Information Sciences, vol. 511, pp.1-11, 2018.

[32] J. Zhou, N. Zhou and L. Gong, "Fast color image encryption scheme based on 3D orthogonal Latin squares and matching matrix," Optics and Laser Technology, vol. 131, pp. 106437, 2020.

[33] S.S. Raja and V. Mohan, "A review on various image encryption techniques for secure image transmission," International Journal of Advances in Engineering Research, vol. 8, pp. 1–14, 2014.

[34] N.A. Abbas, "Image encryption based on independent component analysis and arnold's cat map," Egyptian Informatics Journal, vol. 17, no. 1, pp. 139–146, 2016.

[35] E.H. Bensikaddour, Y. Bentoutou and N. Taleb, "Embedded implementation of multispectral satellite image encryption using a chaos-based block cipher," Journal of King Saud University-Computer and Information Sciences, vol. 3, pp. 1–7, 2018.

[36] L. Chen, B. Ma, X. Zhao and S. Wang, "Differential cryptanalysis of a novel image encryption algorithm based on chaos and line map," Non Linear Dynamics, vol. 87, no. 3, pp. 1797-1807, 2016.

[37] Y. Zhou, L. Bao and C. Chen, "A new 1D chaotic system for image encryption," Signal Processing, vol. 97, pp. 172–182, 2014.