IS_check1

by Diet Buddy

Submission date: 13-Jun-2022 10:27AM (UTC+0530)
Submission ID: 1855803550
File name: IS_RESESARCH_PAPER_3.pdf (3.12M)
Word count: 8731
Character count: 43507

Image Encryption using Efficient Dice Algorithm

1st Hartik Suhagiya
Department of Computer Engineering,
D.J. Sanghvi College of Engineering,
University of Mumbai, India
hartiksuhagiya10@gmail.com

2nd Dhruv Mehta
Department of Computer Engineering,
D.J. Sanghvi College of Engineering,
University of Mumbai, India
mehtadhruv933@gmail.com

3rd Manish Jha
Department of Computer Engineering,
D.J. Sanghvi College of Engineering,
University of Mumbai, India
manishjha5410@gmail.com

4th Prof. Ramchandra Mangrulkar
Department of Computer Engineering,
D.J. Sanghvi College of Engineering,
University of Mumbai, India
ramchandra.mangrulkar@djsce.ac.in

***Abstract*—Color photographs are widely made and kept in today's world for a number of purposes by organisations. Due to their pattern appearance and high computational cost, standard encryption techniques such as AES or DES are not well suited for encrypting multimedia data. Many methods for encrypting grayscale photos have been presented. However, in the literature, only a few methods for encrypting colour images have been proposed. DieRoll Encryption is a new method for encrypting colour photographs that is based on a novel key generation process disclosed in this study. This paper explains the unique key generation which involves different stages of dividing and scrambling the key followed by using the fair die to do transposition and then reintegrating to form one whole key. This key is used to then securely and robustly encrypt the RGB colored image. The paper shows comparative studies with other algorithms and substantiates that it is on par if not better than other algorithms. Various visual and quantitative evaluations are carried out to demonstrate the method's resistance against modern-day threats.**

***Index Terms*—image encryption; image security; dice; scrambling; substitution; security analysis; cryptography; diffusion.**

I. Introduction

Images and videos have become an effective means of processing information and transmission in computer systems in recent years as a result of the rapid improvement and expanding acceptance of network technologies and online digital systems around the world. Network security issues, on the other hand, have long been a significant element impeding and limiting network technology growth. How to provide data protection safety in a computer system is a critical content and research path in network security and data security, particularly in the context of government and the public data sources.

Due to their temporal complexity and pattern appearance, typical techniques viz as Rivest, Shamir, Adleman (RSA),ECB,CBC, Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Hill Cipher Yang et al. (2019) are not very well suited for photo encryption, according to Wadi and Zainal (2014). Researchers have proposed various photo encryption algorithms in the research. Because they are based on complicated mathematics and trapdoor functions, these algorithms are difficult to decipher. Deep learning is another area that is utilized to produce an image compression and encryption approach. Among these initiatives are Maniyath and Thanikaiselvan (2020), Hu et al. (2016), and Hu et al. (2017). section II delves more into each of these masterpieces.

In today's world, communication by transfer of data has exalted. Out of all types of data, the data in the form of an image is transferred at a huge rate like the multimedia data such as videos, images, etc. gets viral within a fraction of a second. Hence, with the huge transfer of confidential data, privacy becomes our primary concern. So cryptography is the way by which the data can be encrypted and decrypted. Image encryption has shown to be a critical topic in terms of the safe transmission of private information involving images. So to deal with the active and passive attackers there are various methods that were used in the past and also used in present, such as image steganography.

A wide variety of research contributed to the field of cryptography and more specifically to image encryption with different thesis, different levels of efficiency, and various possible complexities. Various standard algorithms had been developed for image and video encryption which were efficient during their time as can be seen in Abdmouleh et al. (2017), Wen et al. (2016), Tabeidi et al. (2020). There are more advanced algorithms that are based on standard algorithms, Data Encryption Standard (DES),ECB, CCB, Rivest, Shamir, Adleman (RSA), Advanced Encryption Standard (AES) algorithms such as DES Gaur et al. (2021), Elliptic curve cryptography (ECC) Sasikaladevi et al. (2018), AES Zhang et al. (2017).

Researchers have devised methods such as steganography to hide data in images by adding extra bits or changing the LSB bits of an RGB value. Kamil et al. (2018) introduced a Video steganography technique, which achieved nearly 0% variation and very limited calculation time, as well as hiding secret bits in both complemented and non-complemented forms.

In this research, we have introduced an innovative approach and tried extending image encryption by implementing it on real data. The algorithm we introduced in this paper is highly efficient and quite impregnable to attack, even if the attacker

has access to extensive resource power too. A new image encryption method is proposed for 3-channel Red, Green, and Blue (RGB) pictures called DieRoll Encryption. This method has 2 stages, wherein the first stage includes effective key generation where the algorithm divides the user key into multiple parts and several operations are performed on each of the blocks that are created by dividing the key. These functions performed on every block of the divided keys use a Fair Die which will be explained further in the later section VI. In stage 2, the encryption algorithm is applied to each and every pixel of an image to get the ciphered image.

II. Related works

The authors of this study, Abdmouleh et al. (2017), offer a compressive sensing-based visually meaningful photo encryption technique. The proposed image encryption technique includes three processes: compression, encryption, and concealment. Wen et al. (2016) describe a salient areas encryption system for visually meaningful secret text production. First, in the compressed domain, a subspace detection method efficiently extracts salient regions. Then, using a chaos-based encryption technique, we pre-encrypt these key regions. Zhao et al. (2019) proposed a partial-duplicate picture-based coverless image steganography technique. They also presented a chaotic maps-based encryption algorithm for partial duplicate picture retrieval, which helps restrict the size of image blocks. Pan et al. (2018) propose Digital Photo Encryption using Dual Logistic Method in their research paper.

With the use of the Möbius transformation, Lin (2012) presents a new technique of transmission and cryptography. The method of modulation technique in the Chen-Mobius communication network, which is considerably different from the usual one, is based on the Möbius transformation and is used in picture transfer and encryption. A turtle-shell matrix optimisation scheme proposed by Qiu et al. (2020) used a greedy algorithm.

Their proposed greedy method is better than the particle swarm optimisation scheme at finding a near-optimal matrix and achieving better stego-image hiding. Chen et al. (2020a) reversible data hiding scheme based on exploiting modification direction (EMD) method. In this scheme, two 5-ary secret numbers are embedded into each pixel pair in the cover image according to the EMD method to generate two pairs of stego pixels. Tripathy et al. (2019) proposed method based on musical notes and dice which lead them to efficient encryption and decryption with high security.

With the use of cloud computing idea the authors Chen et al. (2020b) are trying to encrypt an RGB Image based on feature extraction which is a bit longer process. Yadav and Singh (2018) proposed unique key generation that first scrambles the location of the pixels and then applies a chaotic map by using a 32 bit symmetric key that changes the pixel values of the image. The authors Elkamchouchi et al. (2019) are trying to encrypt images using key permutation which can be harmful as attacker might knows the pattern of key. Beloucif and Noui (2018) authors are build a way for lossless encryption scheme that can be used for digital images based on combination of matrix transformations and XOR operation. The authors Zhao et al. (2020) are trying to adjust a large key space which is then send to Androl transform for scrambling of images. A novel cloud encryption based algorithm is implemented Fan et al. (2018) in which they are adding a new AES based encryption which boost up the performance with normal Cloud Server. Computation time leverage can be seen on RSA algorithm implemented by Researchers Wei et al. (2015). Researchers Luo et al. (2016) are trying to build a novel idea based on HMCPABE and CP-ABE for mobile dicovery pattern.

Demonstrating how IDEA (International Data Encryption Algorithm) can be used for photo encryption before changing the plaintext can be utilised to employ one of the strongest uncan bedisclosed key block cyphers. On IDEA, Upadhyay et al. (2016) created a block cypher that uses 64-bit plaintext blocks and generates 64-bit cypher text blocks using a 128-bit key. They used the picture pixels to encrypt the image.

Because chaotic maps can generate a randomly generated sequence of numbers, they have been used extensively in picture encryption research. These numbers are used for confusion and diffusion processes to encrypt images, according to Shannon (1949). Researchers have also attempted to combine chaotic mapping with other areas for encryption. Few of these works include Chai et al. (2017a), Qiuqiong et al. (2020).

III. ENCRYPTION PATTERN

By default, the data gets stored in plaintext, which is a readable format. The plaintext is vulnerable to unauthorized and perhaps malicious access when transferred over a network. The encryption process is a digital coding scheme designed to keep data private and secure. It's used to convert unencrypted data into a secure, unreadable format. Encryption technology frequently employs a standardised procedure known as a cypher to turn plaintext data into encrypted data, also known as ciphertext. Apart from basic metadata, such as message length and creation date, ciphertext access does not reveal the original plaintext material. When plaintext data is encrypted, it is associated with an encryption key, which is a string of characters. The key for encryption is used. The key use for encryption is also used for decryption.

IV. Scrambling Method

The Scrambling Method is an encryption algorithm used in DVB digital television broadcasting. In May 1994, ETSI specified CSA, which was then accepted by the DVB consortium. CSA was kept a closely guarded secret until 2002. The patent documents provided some suggestions, but key features such as the layout of the so-called S-boxes were kept hidden. It was impossible to implement the method without these free implementations. CSA was supposed to be implemented entirely in hardware at first, which would have made reverse engineering current implementations difficult. Frederic,

a software implementation of CSA, was released in 2002. Although it was only available in binary form, disassembly revealed the missing features and allowed the technique to be reimplemented in higher-level languages. Text scrambling is a type of encryption in which the original message's locations are jumbled according to the place replacement, resulting in a cipher text that is a permutation of the original message. When working with fractions, the scrambling text is most useful. The scrambling technique was employed by Kumar et al. However, the message organization was done in two-dimensional regions. In comparison to three-dimensional and cubical spaces, this two-dimensional space may not pose as much of a challenge to hackers when it comes to cryptanalysis. This method necessitates a greater number of row or column transformations to produce a more secure cipher text, which takes longer to encrypt and decrypt.

When cryptanalysis is compared to three-dimensional and cubical spaces, this two-dimensional environment may not present as much of a barrier to hackers. To produce a more secure cipher text, this method demands a larger number of row or column modifications, which takes a bit longer to encrypt or decrypt. The use of text in the scrambling method resulted in effective variance in the original message scrambling. This research supports the suggested effort in which text is rotated as a six-sided Dice cube to scramble the original meaning.

V. Security Analysis of the DieRoll Encryption

In most circumstances, visual inspection alone is insufficient to evaluate an image encryption scheme. As a result, rather than depending exclusively on visual elements, the encrypted images are examined using standard scientifically proved parameters to identify any performance or security-related flaws. The algorithm is analyzed in detail using 10 different parameters, which are presented in this part. The advantages of the DieRoll image encryption technique can be assessed using a range of analysis and performance metrics frequently used for image encryption algorithms.

A. Analysis of the Histogram

The histogram shows how the intensity values of pixels in an image are distributed. It's possible to interpret the intensity distribution in it. Histograms graphically display the pixel value at each level. The same image in its encrypted form, when plotted as a histogram, should have a uniform or nearly equal intensity distribution to defend itself against various statistical attacks. To protect the encrypted image from statistical attacks, it must have a histogram with a uniform distribution. Table IX present shows the histograms of various plain photographs and their matching with encrypted images made using Die Roll. As can be seen, the encrypted photographs have a rather consistent distribution.

B. Average value Analysis

The simple difference of the colour contribution to form an image can easily be noticed with the help of the average colour value analysis. In this analysis, the average/Mean of the Red, Green, and Blue values for any image is calculated. As a result, in cryptography, we calculate the mean value of all RGB colours in both the original and encrypted images. After calculating the average values in both images, we can see the difference by showing a bar graph to make the data more visible. So this analysis is done and the output of it is also shown in the figure at the bottom of the paper. where the average values of 3 colours are not uniform and it is more for some colours and less for some colours. Whereas in the encrypted image the average of RGB values is uniform that is consistent hence the encrypted image is uniform and the attacker cannot interpret anything from this image. So, the algorithm made is secure in terms of encrypting and decrypting the image.

Avg intensity of an color =

$$\frac{1}{EH}\sum_{a=1}^{E}\sum_{b=1}^{H} I_i(a,b) \tag{1}$$

where,
E = Height of an image,
H = Width of an image,
I_i(a,b)= Intensity value for particular color,
i belongs (red, green, blue)

C. Information Entropy Analysis

Cryptographic functions are built on the foundation of entropy. In Cryptography, entropy is a measure of a data-generating function's randomness or diversity. Data with 100% entropy is fully random, with no discernible patterns. Low entropy data allows you to forecast the values that will be generated in the future. The entropy of a cryptographic function's output is one way to assess its quality. Encryption and hashing algorithms require highly ephemeral algorithms.

$$IE(a) = \sum_{m=0}^{n-1} P(x_m) log(1/P(a_m)) \tag{2}$$

Where,
IE(a) = information entropy for the message source a
n = bit length of a symbol $a_m \epsilon a$
$P(a_m)$ = probability of occurrence for a symbol s_m

According to Xu and Tian (2019), the value of information entropy should be near 8 for a reliable and valid encryption scheme. The closer it gets to 8, the less it matters. The cryptosystem's proclivity towards leaking any information to the outside world attackers. Information entropy values for various photographs Table I shows the results. Image comparisons with Lena. Table II includes more approaches. As can be observed, the DieRoll encryption works well in comparison. Its information entropy value is higher than that of other algorithms, which is around is 7.9996, and is closer to the number eight than other approaches.

D. Analysis of the key space

A wide keyspace is required in encryption algorithm to withstand a wide brute force attacks. Because the DieRoll starts with a 192-bit key, there are 2^{192} potential permutations. This 192-bit key is then broken into 24-bit blocks, each of which has 2^{24} potential combinations. This keyspace is large enough to keep brute-force attacks at bay. If an attacker tries to find the plain image by exploiting any intermediary phase, the number of combinations and computations increases much more. For example, while encrypting an image of size 256 256 3, every pixel can go from 0-255 and thus be of 8 bits. As a result, the suggested approach's key size is adequate to survive contemporary brute force attacks.

E. Analysis of the effect of differential attacks

Attacker tries to make an tiny alteration in orignal image to guess the key this is a common method known as differential attack. To anticipate the keys, the attacker does cryptography analysis on the encrypted photos and studies the changes that occur in these encrypted files. To protect against a small amount of change in the plain image, differential attacks must induce a significant change in the secret image. Only one pixel in the original Baboon image was changed to study the DieRoll encryption reaction to differential assaults. The two photographs that were encrypted were compared. This success is visually demonstrated and validated by the graph. The Number of Pixel Change Rate (NPCR) & Unified Average Changing Intensity (UACI) and the are used for quantification. NPCR and UACI are specified by Equation 3 and Equation 4, respectively.

$$NPCR = \frac{1}{EH}\sum_{o=1}^{E}\sum_{n=1}^{H} D(o,n) * 100 \tag{3}$$

$$UACI = \frac{1}{EH}\sum_{o=1}^{E}\sum_{n=1}^{H} \frac{|C_1(o,n) - C_2(o,n)|}{L-1} \tag{4}$$

where,

$$D(g,h) = \begin{cases} 1, & if(C_1(g,h) = C_2(g,h)) \\ 0, & otherwise \end{cases} \tag{5}$$

Wu et al. (2011) proposed strict NPCR and UACI values in their work. Equation 6 is used to calculate the crucial NPCR score given a significance level α.

$$N_\alpha = \frac{T - \phi^{-1}(\alpha)(T/R)^{1/2}}{T+1} \tag{6}$$

If the encrypted image's NPCR value is bigger than Nα, the technique gives more security against differential assaults. The critical UACI scores (U_α^-, U_α^+) with the given α can be obtained as follows:

$$\begin{cases} U_\alpha^- = \mu_\mu - \phi^{-1}(\alpha/2)\sigma_\mu \\ U_\alpha^+ = \mu_\mu - \phi^{+1}(\alpha/2)\sigma_\mu \end{cases}$$

where,

$$\mu_\mu = \frac{E+2}{3E+3} \tag{7}$$

and

$$\sigma_\mu = \frac{(E+2)(E^2+2E+3)}{3E+3} \tag{8}$$

If calculated UACI value is in range (U_α^-, U_α^+) then the algorithm passes the test. As recommended by Wu et. al, the significance level α is normally set to 0.05. Thus, for an image of size 256 × 256, the obtained N0.05 = 99.56936%, and (U_α^-, U_α^+) = (33.28243%, 33.64473%), and for an image of size 512 × 512, the obtained N0.05 = 99.58933%, and (U_α^-, U_α^+) = (33.37303%, 33.55413%). Table III shows that the total values for images are well within these limits, indicating that the DieRoll passes this test. We also compared those results to those obtained using other approaches. The results of these comparisons are shown in Table IV and Table V. DieRoll's performance is at least comparable to that of other techniques, as seen in the tables.

F. Time Complexity Analysis

Let's assume an RGB colour image of dimension M × N × 3. In stage 1, there is a key generation process which is done over by rolling a die. In stage 2, it performs pixel by pixel XOR operation. How it works is that initially, it does a 24-bit rearrangement which is constant, then we have an XOR operation which is again constant and finally, we do a rearrangement again. Thus, the time complexity becomes O(M × N × 72). With small modifications to the original image, it can be used for an M × N size RGB image O(M × N) would become a possible time complexity. The time needed to encrypt or decrypt an image increases as the size of the image increases and hence they are positively correlated. Through several experiments of the algorithm, we found out that the proposed scheme takes about 1.79 seconds to encrypt and 1.84 seconds to decrypt the image. Thus, encryption and decryption times are almost similar.

G. Key Sensitivity Analysis

An encryption algorithm's sensitivity to keys is a critical and necessary criterion. As a result, even the tiniest key modification should cause a fragile modification in secret key, ensuring that the true image is accurately concealed. To encrypt the image, the suggested system's initial 192-bit key is utilised. Only the last portion of the key (K1) has been modified; the rest of the key has remained the same. With the key, we encrypt the image once more. When we look at the two encrypted photographs side by side, it's evident that even a minor adjustment in the key resulted in a drastically different encrypted image. Because of the several key production processes contained at various levels in this approach, a slight change in the initial key causes an increasing number of changes in the subsequent parameters generated, resulting in a large change.

H. Analysis of Degree of Scrambling

To estimate the change in each pixel's position and change in the nearby pixel's value we use DoS (Degree of Scrambling). The relatively closed pixels are used to evaluate DoS

TABLE I
PLAIN TEXT IMAGES AND ENCRYPTED IMAGE INFORMATION ENTROPY

Image	Lena	Babbon	MRI	Cat
Plain Image	7.594	7.706	6.164	7.807
Encrypted Image	7.9983	7.816	7.782	7.834

TABLE II
INFORMATION ENTROPY FOR LENA IMAGE

DieRoll	Roy et al. (2021)	Arpacı et al. (2020)	Kaur et al. (2020)	Chai et al. (2017b)
7.689	7.9983	7.9945	7.9938	7.9993

which can be defined using Equation 9. The values of DoS for encrypted images are mentioned in Table VIII.

$$DoS = \frac{\sum_{a=1}^{O-2}\sum_{b=1}^{N-2} R_{ab}}{255^2(O-2)(N-2)} \tag{9}$$

where,

$$R_{eh} = F_1(r,s) + F_2(r,s) + F_3(r,s) + F_4(r,s) \tag{10}$$

and

$$\begin{cases} F_1(r,s) = |[C(r-1,s) - C(r,s)]^2 - [P(r-1,s) - P(r,s)]^2| \\ F_2(r,s) = |[C(r+1,s) - C(r,s)]^2 - [P(r+1,s) - P(r,s)]^2| \\ F_3(r,s) = |[C(r,s-1) - C(r,s)]^2 - [P(r,s-1) - P(r,s)]^2| \\ F_4(r,s) = |[C(r,s+1) - C(r,s)]^2 - [P(r,s+1) - P(r,s)]^2| \end{cases}$$

I. Analysis of correlation coefficients

Adjoining pixels in a basic image have a high degree of connection. To avoid the plain image from being decrypted, it is necessary to break this encryption correlation. 7000 to 8000 neighbouring pixels from the Baboon image were chosen at random and evaluated in horizontal, vertical, and diagonal orientations using various plots. The basic image has a substantial association, as seen in the Table XIII at the end of the study, with the majority of the plotted pairs falling along the diagonal line. This indicates that the intensity values of adjacent pixels are similar. After encrypting and graphing these pairs, the Table XIII shows there is a lot of volatility. The graphs in Table XIII above show how the data is graphically represented. The correlation coefficient in Equation 11 below are used to quantitatively check relationships in horizontal, vertical, and diagonal orientations.

$$corr(e,h) = \frac{cov(e,h)}{\sqrt{D(e)}\sqrt{D(h)}} \tag{11}$$

where, e and h = intensity values of two adjacent pixels

$$cov(e,h) = \frac{1}{C_{pairs}} \sum_{a=1}^{C_{pairs}} ((x_a - E(e))(y_i - E(h))) \tag{12}$$

$$D(a) = \frac{1}{C_{pairs}} \sum_{a=1}^{C_{pairs}} (x_a - E(x_a))^2 \tag{13}$$

$$E(b) = \frac{1}{C_{pairs}} \sum_{b=1}^{C_{pairs}} z_b \tag{14}$$

The correlation coefficient can be anything between -1 and +1. According to Zhang et al. (2017), a value of 1 implies a strong positive association. As a result, for the encrypted image, a correlation of 0 is preferable. Table 6 shows the image correlation coefficients after encryption. The encrypted photos have a desirable correlation of close to 0.

In addition, Table 5 compares the suggested method to previous approaches for the Lena image. Here it can be shown that the DieRoll produces secret Lena Photo and correlation coefficients that are extremely close to the intended value, i.e. zero. As a result, it is either superior to or comparable to other methods.

J. MSE and SSIM Analysis

Following Equation 15 represent the Mean Squared Error (MSE) between encrypted image and orignal image.

$$MSE = \frac{1}{ON} \sum_{a=0}^{O-1} \sum_{b=0}^{N-1} [I(a,b) - K(a,b)]^2 \tag{15}$$

where, I = unencrypted image K = Encrypted image. An MSE of 0 indicates perfect similarity. The encrypted and original photos are less comparable if the MSE value is higher. This value will rise as the gap between pixel intensities grows. One of MSE's flaws is that the values aren't relative to each other. As a result, the Structural Similarity Index (SSIM), a new statistic, is used. The SSIM between two pictures can be calculated using Equation 16

$$SSIM(n,o) = \frac{(2\mu_n\mu_o + c_1)(2\sigma_{no} + c_2)}{(\mu_n^2 + \mu_o^2 + c_1)(\sigma_n^2 + \sigma_o^2 + c_2)} \tag{16}$$

SSIM, unlike MSE, may compare two windows instead of the complete image. This aids in identifying changes in the image's structure rather than just apparent change. The SSIM value ranges from -1 to 1, with 1 representing perfect similarity. As a result, a value of 0 for the encrypted image is preferable. The MSE and SSIM values for the original and encrypted photos are shown in Table VIII.

VI. DICE ALGORITHM FOR IMAGE CRYPTOGRAPHY

In this section VI we are trying to explain our Die Roll Working with algorithm and diagrammatic representation, this part is further explained in detail in the following subsections.

TABLE III
UACI AND NPCR VALUES FOR ENCRYPTED IMAGES

Image	Image Size	NPCR R-Channel	NPCR G-Channel	NPCR B-Channel	NPCR Overall	UACI R-Channel	UACI G-Channel	UACI B-Channel	UACI Overall
Lena	512*512*3	99.969863	99.970881	99.970881	99.970541	0.30136	0.39118	0.392549	0.361696
Baboon	320*320*3	99.597168	99.635315	99.647522	99.626668	0.335099	0.331115	0.337337	0.334516
Cat	509*520*3	99.624969	99.62302	99.621813	99.621813	0.334341	0.33431	0.335427	0.334692
MRI	233*206*3	99.7342	99.7241	99.7252	99.72783	0.335431	0.356342	0.34255	0.344774

TABLE IV
COMPARISON OF NPCR WITH OTHER APPROACHES

Image	DieRoll	Arpacı et al. (2020)	Kaur et al. (2020)	Yan et al. (2021)
Lena	99.61	99.62	99.60	99.61
Cat	99.62	99.62	99.61	99.63

TABLE V
COMPARISON OF UACI WITH OTHER APPROACHES

Image	DieRoll	Arpacı et al. (2020)	Kaur et al. (2020)	Yan et al. (2021)
Lena	33.58	33.44	33.64	33.54
Peppers	33.89	33.44	32.93	33.48

TABLE VI
CORRELATION COEFFICIENTS FOR ENCRYPTED IMAGES WERE OBTAINED IN THE HORIZONTAL, VERTICAL, AND DIAGONAL DIRECTIONS.

Images	Horizontal	Vertical	Diagonal
Lena	0.00007631	0.00017738	-0.00220529
Baboon	-0.00029362	0.00197253	-0.00300302
MRI	-0.00078982	0.00283848	0.00167262
Cat	0.00256111	-0.00166877	0.00043290

A. *Working of Die Roll*

The input image of any size with any valid image extensions such as jpeg/jpg/png, etc. can be given as input to the algorithm. The source image could be either with RGB colour or it can be a grayscale image. Since the images or pictures taken are in 2D format; Firstly, the algorithm will convert the image into the 2D matrix with a tuple having Red, Green, and Blue (RGB) values; As a result, each pixel in a picture is represented as a 2D matrix, with the pixel's value in RGB format. The intensity of each colour ranges from 0 to 255 so, the next step is to convert those values into the 8-bit binary number. So we transformed the decimal value into a binary number and stored it in a matrix. Hence the result is a matrix of binary values.

Now, we also require a key for encryption so the key is supposed to be 192 bits that is the input value for the key should be 192 bits, 192 bits to strengthen the algorithm that is to make the decryption with the brute force or any other method very difficult for the attackers.

Next, the 192-bit key is divided into a total of 8 parts each having 24 bits. Then further the 24 bits are divided into 2 parts each with an 8-bit number. So till here, the algorithm will generate 24 parts of 8 bits each. After this, we still divide the 8 bit into 2 parts of 4bit each. So now here we have a total of 48 parts of 4 bits each and then we divide these 2 parts into 2 bits each.

Now the actual innovation algorithm comes. So as we know that the Rolling dice with 6 faces have values ranging from 1 to 6. So let's consider that dice currently has the top face as 1 and the face adjacent and below the top face is 2 and the face adjacent and rightward is 3 and the face upward is 4 and the face leftward is 5 and the face on the ground is 6.

In the last step we divided the 4 bits into 2 bits each now, the bit can either be 0 or 1. so if the 1 st bit of the first 2 bits is 1 then the algorithm will rotate the die towards the right and if it is 0 then the rotation will be towards left. So the 2 digit decimal is generated from the 2-bit binary number.

Now for the next 2 bits, the algorithm does a similar thin and generates 2 digit decimal number. So in the next 2 bits if the first bit is 1 then we rotate the top and if the bit is 0 then the die will rotate downward So, we get 2 digit number from these 2 binary bits too. Hence after appending the 2digit number of the 2nd part we get 4 digit decimal number for our 4-bit number where each value is ranging from 1 to 6. Similarly, for all 4 binary bits, the 4 digit decimal number is generated.
Then we combine the 4 digit decimal numbers and generate 8 digit decimal numbers and then we combine the 3, 8 digit numbers to generate 24 numbers, then we merge all the 24 digit decimal numbers to get the final key. So finally, for our 192 bit key the key generation algorithm will generate 192 digit decimal number.

TABLE VII
COMAPARISON OF CORRELATION COEFFICIENTS WITH OTHER APPROACHES FOR LENA IMAGE

Method	DieRoll	Roy et al. (2021)	Yan et al. (2021)	Ali and Ali (2020)
Horizontal	0.00007	-0.00005	-0.0016	-0.00217
Vertical	0.00017	0.0082	0.0043	0.001
Diagonal	0.001	0.001	0.001	0.0012

B. Diagrammatic representation

1) Source image:

The source/original image that is to be encrypted is taken as input in jpg/png/jpeg or any other universally accepted image file extensions.

2) Dice Pattern:

We are diving the input keys in binary form to the decimal numbers.

3) Key generator:

The entire process of key generation is descripted in the figure given below and the brief overview of it is also given below. Add Figure

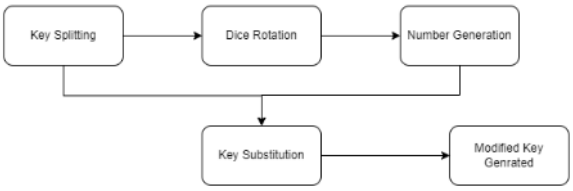
Consider a 4 bit text in which bitPos is the position of the bit in a .number

$$R = \begin{cases} bitPos = 0 \ \ or \ \ bitPos = 1, & f(x) \\ bitPos = 2 \ \ or \ \ bitPos = 3, & g(x) \end{cases}$$

$$f(x) = \begin{cases} Rotate\ Dice\ Left, & bit = 0 \\ Rotate\ Dice\ Right, & bit = 1 \end{cases}$$

$$g(x) = \begin{cases} Rotate\ Dice\ Bottom, & bit = 0 \\ Rotate\ Dice\ Top, & bit = 1 \end{cases}$$

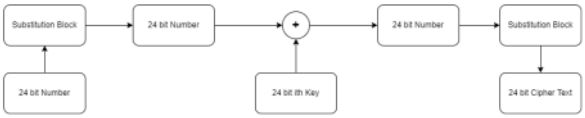
Where, bitPos = Position of bit in text, bit is the bit at bitPos in text, R = Top Face of the dice after rotation.



Above Image is the workflow of DiceRoll Key Generation Algorithm

4) Encrypted image

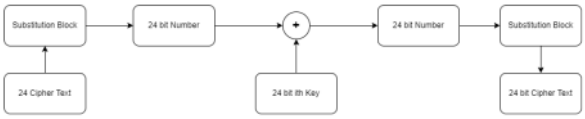
Encryption is done using the modified key generated from above result



In the above Diagram the 24 bit ith key is one of the part of 192bit modified key

5) Decrypted image

Encryption is done using the modified key generated from above result



In the above Diagram the 24 bit ith key is a part of 192bit modified key

C. Vital Components

We have a 192-bit key initially which would be known by the sender and the receiver. We divide the 192-bit key into 8, 24-bit keys. These 24-bit keys are then divided into 6, 4-bit keys. We perform crystal function on these 4-bit keys.
let, key = 192 bit key

1) Key Generation

Split the 192 bit keys into smaller keys of 4 bit. Perform Crystal Function on a key of 4 bit each. Combine all 4 digit number into 192 digit number. Store the 192 digit number into modified key. Perform Scrambling algorithm. Return output received from Scramble algorithm

2) Crystal Function

Generate a 3*3 matrix with initial values as 1,2,3,4 and 5. Split the 4 bit key into 2bit key of 2 parts. Take first 2 bit key If the bit is 1 then rotate dice right. If the bit is 0 rotate dice left. Take a second 2 bit key and if the bit is 1 then rotate the dice top else if the bit is 0 then rotate dice towards bottom. Record the top face of dice after each rotation. Return the 4 digit number.

3) Scrambling Algorithm

Split 192 bit key into a smaller key of 6 bit. Split 192 modified bit keys into smaller keys of 6 bit. Create empty new key Shift each bit of key as per the position of modified key Store into new key Return new key

Input img = source/original image which is to be encrypted

4) Encrypting algorithm

Generate the image matrix (M × N) of the source image and store it in imgmatrix. M = height and N = width Convert all values in the image matrix from decimal to its equivalent eight bits binary form. Split 192 bit key into 24 bit keys and store it into key_arr Initialize i as 0

Repeat N*M times let RGB tuple = image matrix[i] Combine all bit of RGB tuple into one Plain Text Perform Substitution let Key = key_arr[iIncrement i Split 24 bit Key into smaller key of 6 bit Split Substituted plainText into 6 smaller tuple Perform Xor Operation of each Plain Text with key tuple Combine all the result Perform Substitution Store the substituted Result into cipherText

Recombine all cipherText and store it in encryptedimg variable. Convert all values in the variable(encryptedimg) from binary to its equivalent decimal form.

5) Output

Encryptedimg = the encrypted image data.

D. Algorithm

We have a 192-bit key initially which would be known by the sender and the receiver. We divide the 192-bit key into 8, 24-bit keys. These 24-bit keys are then divided into 6, 4 bit keys. We perform crystal function on these 4-bit keys. let, key = 192-bit key

1) Key Generation

Split the 192-bit keys into smaller keys of 4-bit. Perform Crystal Function on each 4-bit key. Combine all 4 digit number into 192 digit number. Store the 192 digit number into modified key. Perform Scrambling algorithm. Return output received from Scramble algorithm

a) Crystal Function

Generate a 3*3 matrix with initial values as 1,2,3,4 and 5. Split the 4 bit key into 2 bit key of 2 parts. Take first 2 bit key If the bit is 1 then rotate dice right. If the bit is 0 rotate dice left. Take second 2 bit key If the bit is 1 then rotate the dice top. If the bit is 0 rotate dice bottom. Record the top face of dice after each rotation. Return the 4 digit number.

b) Scrambling Algorithm

Split 192 bit key into smaller key of 6 bit. Split 192 modified bit keys into smaller keys of 6 bit. Create empty new key Shift each bit of key as per the position of modified key Store into new key Return new key Input img = source/original image which is to be encrypted

2) Encrypting algorithm

Generate the image matrix (M × N) of the source image and store it in imgmatrix. let, X = height and Y = width, convert all the values in the image matrix from decimal to its equivalent eight bits binary form. Split 192 bit key into 24 bit keys and store it into key_arr Initialize i as 0

Repeat N*M times let RGB tuple = image matrix[i] Combine all bit of RGB tuple into one Plain Text Perform Substitution let Key = key_arr[iIncrement i Split 24 bit Key into smaller key of 6 bit Split Substituted plainText into 6 smaller tuple Perform Xor Operation of each Plain Text with key tuple Combine all the result Perform Substitution Store the substituted Result into cipherText

Recombine all cipherText and store it in encryptedimg. Convert all values in encryptedimg from binary to its equivalent decimal form.

3) Output

Encryptedimg = the encrypted image data.

VII. Case Study

We use an example as a case study and solve it to retrieve the secret version of a source photo to have a better grasp of the Dice method. Consider that the input/source/original image has a 3 x 3 image matrix having the following pixel intensity values of 3 channels in the range of 0 to 255. And take the input key of 192 bit.

010001101011111101100001	101011001011010100101111	010011110110001011110111
001000100011010000101001	000010101111110111100100	010011011111000101010011
101100100011110010000011	100011001001000111101100	

Considering 1st block for key generation and dividing it into 3 parts each of 8 bits.

01000110	10111111	01100001

Considering 1st block for key generation and dividing it into 2 parts each of 4 bits.

0100	0110

Considering 1st block for key generation and dividing it into 2 parts each of 2 bits.

01	00

Generating numbers as 1,2,4 and 6 based on the bits.

Bit Position	0	1	2	3
Bit value	0	1	0	0
Top value of dice	4	1	2	6

Similarly the 24 digit value from key generation can obtained: Lets say New key is 412641513156365141514626 And our original key is 010001101011111101100001

Divide the original key into a chunk of 6

010001	101011	111101	100001

Divide the New key into a chunk of 6

412641	513156	365141	514626

Bit value	0	1	0	0	0	1
Bit position	1	2	3	4	5	6
New Key value	4	1	2	6	4	1
Shifted position	0	0	1	1	0	0

After shifting the bits we get the part of a final key We will be generating all parts of the key in a similar manner and final we will get the 192 bit key. So the final key for our case study is: 00110011 11111101 11010101

TABLE VIII
MSE, SSIM AND DOS VALUES OBTAINED FOR THE ENCRYPTED IMAGES

Image	MSE	SSIM	DoS
Lena	26639.7	0.01009632	0.66203
Baboon	24400.3	0.00947997	0.64968
MRI	25000.4	0.020512	0.5999
Cat	30948.2	0.0091772	0.66053

A. *Image Encryption:*

Lets say we have our input image of dimension 3 * 3 * 3 Image Matrix

(13, 14, 15)	(10, 12, 15)	(20, 10, 4)
(15, 5, 12)	(13, 16, 2)	(0,0,0)
(0,5,7)	(6, 9, 6)	(9,0,2)

Now we have to convert each block into its binary form lets consider example of one block

(00000000, 00000101, 00000111)	(00000110, 00001001, 00000110)	(00001001, 00000000, 00000010)

So the rest of blocks also be converted as shown.

00001101 00001110 00001111	00001010 00001100 00001111	00010100 00001010 00000100
00001111 00000101 00001100	00001101 00001000 00000100	00000000 00000000 00000000
00000000 00000101 00000111	00000110 00001001 00000110	00001001 00000000 00000010

Now we apply substitution on block 1 therefore we get 011001010000101000101011
Know apply XOR Operation with key therefore we get Applying substitute block on cell 1:

$$\begin{array}{r} 01100101\ 00001010\ 00101011 \\ \oplus\ 00110011\ 11111101\ 11010101 \\ \hline 011010000000010000100100 \end{array}$$

Applying substitution block having reverse of the above substitution block is : 010010000000100010011000

Final Cipher for Block 1: 010010000000100010011000

Similarly we apply the key_part1 to pixel 1, key_part2 to pixel 2, key_part3 to pixel 3 and so on in a circular manner.

VIII. APPLICATIONS OF DICE ALGORITHM AND ITS WORKING SCOPE

With petabytes of data generated every day, the bulk of which is unstructured multimedia data, securing it while delivering it across unsecure routes or keeping it in the cloud is critical.

To maintain privacy, it is essential to safeguard the contents of photographs and videos when distributing them through the public domain. Because RGB images are so ubiquitous in today's world, it's critical to utilise a technique that is tailored to them. The proposed DieRoll Image Encryption Scheme can be used in a wide range of businesses. The approach can be used in a variety of industries, including healthcare, banking, defence, and cloud computing. For healthcare facilities that keep a big number of patients' X-Ray, HRCT, and MRI scans in the cloud or locally in their databases, encrypting images before uploading or storing them can be useful. Financial organisations can utilise this encryption technique to securely store and transfer customer photos and scanned documents. Users can use this approach to encrypt individual private photographs before saving them in the cloud. The most essential application of this strategy could be in defence. Images taken from satellites or covert cameras may be stored or transmitted by governments as long as they are not intercepted by opponents. The scheme's huge keyspace contributes significantly to this. Furthermore, with simple tweaks, this system can be utilised for grayscale photos as well. For added security, advanced non-linear dynamics could be used to improve the method. As a result, the proposed DieRoll encryption has a wide range of real-world applications across several industries, giving it a strong influence.

IX. CONCLUSIONS AND FUTURE SCOPE

DieRoll, a revolutionary image encryption method for colour images, is introduced in this research. This method encrypts color photos using scrambling and a fair die in multiple phases. The approach uses a sophisticated scrambling and divides the key into equal parts of 24 bits in the first stage. Next we gain divide these 24-bit parts into 8-bit parts and then into 4-bits. The dice is then used to perform certain operations on the 4-bit parts in the next stage, which generates various new number sequences. To obtain the encrypted image and make the approach resilient, the final stage combines the divided and operated 4-bit parts into 8 and then 24 and finally a 192-bit key is produced. DieRoll then robustly and reliably encrypts the plaintext or image with the produced key. DieRoll uses a 192-bit key size, and the encrypted image can be recovered in its entirety. Various investigations and experiments show that the DieRoll is more resistant to modern-day attacks than other works. Therefore, DieRoll can be adopted for various applications in real life. It can be used in every possible cryptography related fields. In Future the key generation part can be made more dynamic and pseud random number can be used for the key generation to generate a high secure key.

REFERENCES

Hongyu Yang, Yuguang Ning, and Yue Wang. Research on rsa and hill hybrid encryption algorithm. *International Journal of Computational Science and Engineering*, 20(1): 1–6, 2019.

Salim Muhsin Wadi and Nasharuddin Zainal. High definition image encryption algorithm based on aes modification. *Wireless personal communications*, 79(2):811–829, 2014.

Shima Ramesh Maniyath and V Thanikaiselvan. An efficient image encryption using deep neural network and chaotic map. *Microprocessors and Microsystems*, 77:103134, 2020.

Fei Hu, Changjiu Pu, Haowei Gao, Mengzi Tang, and Li Li. An image compression and encryption scheme based on

deep learning. *CoRR*, abs/1608.05001, 2016. URL http://arxiv.org/abs/1608.05001.

Fei Hu, Jingyuan Wang, Xiaofei Xu, Changjiu Pu, and Tao Peng. Batch image encryption using generated deep features based on stacked autoencoder network. *Mathematical Problems in Engineering*, 2017:1–12, 02 2017. doi: 10.1155/2017/3675459.

Med Karim Abdmouleh, Ali Khalfallah, and Med Salim Bouhlel. A novel selective encryption dwt-based algorithm for medical images. In *2017 14th International conference on computer graphics, imaging and visualization*, pages 79–84. IEEE, 2017.

Wenying Wen, Yushu Zhang, Yuming Fang, and Zhijun Fang. A novel selective image encryption method based on saliency detection. In *2016 Visual Communications and Image Processing (VCIP)*, pages 1–4. IEEE, 2016.

Rania A Tabeidi, Hanaa F Morse, Samia M Masaad, Reem H Al-shammari, and Dalia M Alsaffar. Create a hybrid algorithm by combining hill and advanced encryption standard algorithms to enhance efficiency of rgb image encryption. In *International Conference on Soft Computing and Pattern Recognition*, pages 749–757. Springer, 2020.

Ghanshyam Gaur, Janki Ballabh Sharma, and Lokesh Tharani. Verilog implementation of biometric-based transmission of fused images using data encryption standards algorithm. In *Nanoelectronics, Circuits and Communication Systems*, pages 455–467. Springer, 2021.

N Sasikaladevi, N Mahalakshmi, and N Archana. Leach-genus 2 hyper elliptic curve based secured light-weight visual cryptography for highly sensitive images. In *International Conference on Advances in Computing and Data Sciences*, pages 302–311. Springer, 2018.

Yong Zhang, Xueqian Li, and Wengang Hou. A fast image encryption scheme based on aes. In *2017 2nd International Conference on Image, Vision and Computing (ICIVC)*, pages 624–628. IEEE, 2017.

Samar Kamil, Masri Ayob, Siti Norul Huda Sheikh Abdullah, and Zulkifli Ahmad. Optimized data hiding in complemented or non-complemented form in video steganography. In *2018 Cyber Resilience Conference (CRC)*, pages 1–4. IEEE, 2018.

Ningsheng Zhao, Zhili Zhou, and Lingzhi Liao. Partial-duplicate image retrieval based on hsv colour space for coverless information hiding. *International Journal of Computational Science and Engineering*, 19(1):15–24, 2019.

Hailan Pan, Yongmei Lei, and Chen Jian. Research on digital image encryption algorithm based on double logistic chaotic map. *EURASIP Journal on Image and Video Processing*, 2018(1):1–10, 2018.

ShunDa Lin. Image transmission and cryptography on the basis of mobius transform. In *2012 5th International Congress on Image and Signal Processing*, pages 258–261. IEEE, 2012.

Guo-Hua Qiu, Chin-Feng Lee, and Chin-Chen Chang. Greedy algorithm for image quality optimisation based on turtle-shell steganography. *International Journal of Computational Science and Engineering*, 23(1):50–62, 2020.

Yu Chen, Jiangyi Lin, Chin-Chen Chang, and Yu-Chen Hu. Reversibly hiding data using dual images scheme based on emd data hiding method. *International Journal of Computational Science and Engineering*, 21(4):583–592, 2020a.

AK Tripathy et al. Data cryptography based on musical notes on a fingerboard along with a dice. *Indones. J. Electr. Eng. Comput. Sci*, 14:1286–1290, 2019.

Jianhua Chen, Jiaohua Qin, Xuyu Xiang, and Yun Tan. A new encrypted image retrieval method based on feature fusion in cloud computing. *International Journal of Computational Science and Engineering*, 22(1):114–123, 2020b.

Sudeept Singh Yadav and Yashpal Singh. Image encryption based on random scrambling and chaotic logistic map. *International Journal of Grid and Utility Computing*, 9(3):228–234, 2018.

Hassan Elkamchouchi, Wessam M Salama, and Yasmine Abouelseoud. Armtfr: a new permutation-based image encryption scheme. *International Journal of Electronic Security and Digital Forensics*, 11(1):1–28, 2019.

Assia Beloucif and Lemnouar Noui. A lossless image encryption algorithm using matrix transformations and xor operation. *International Journal of Information and Communication Technology*, 13(1):99–113, 2018.

Jian-Feng Zhao, Shu-Ying Wang, Li-Tao Zhang, and Xian-Feng Li. Image encryption scheme based on a novel fractional order compound chaotic attractor. *International Journal of Information and Computer Security*, 13(2):166–186, 2020.

Wenjie Fan, Lifeng Li, Xiaowan Chen, Hai Jiang, Zhongwen Li, and Kuan-Ching Li. Deploying parallelised ciphertext-policy attributed-based encryption in clouds. *International Journal of Computational Science and Engineering*, 16(3):321–333, 2018.

Fushan Wei, Jianfeng Ma, Chuangui Ma, and Xinghua Li. A two-factor authenticated key exchange protocol based on rsa with dynamic passwords. *International Journal of Embedded Systems*, 7(3-4):257–265, 2015.

Entao Luo, Qin Liu, and Guojun Wang. Hierarchical multi-authority and attribute-based encryption friend discovery scheme in mobile social networks. *IEEE Communications Letters*, 20:1772–1775, 2016.

Sandeep Upadhyay, Drashti Dave, and Gourav Sharma. Image encryption by using block-based symmetric transformation algorithm (international data encryption algorithm). In *Proceedings of International Conference on ICT for Sustainable Development*, pages 531–539. Springer, 2016.

Claude E Shannon. Communication theory of secrecy systems. *The Bell system technical journal*, 28(4):656–715, 1949.

Xiuli Chai, Yiran Chen, and Lucie Broyde. A novel chaos-based image encryption algorithm using dna sequence operations. *Optics and Lasers in engineering*, 88:197–213, 2017a.

Chen Qiuqiong, Dai Yao, and Niu Zhiyong. An image encryption algorithm based on combination of chaos and dna

encoding. In *2020 International Conference on Computer Vision, Image and Deep Learning (CVIDL)*, pages 182–185. IEEE, 2020.

Ming Xu and Zihong Tian. A novel image cipher based on 3d bit matrix and latin cubes. *Information Sciences*, 478: 1–14, 2019.

Yue Wu, Joseph P Noonan, Sos Agaian, et al. Npcr and uaci randomness tests for image encryption. *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, 1(2): 31–38, 2011.

Mousomi Roy, Shouvik Chakraborty, and Kalyani Mali. The msk: a simple and robust image encryption method. *Multimedia Tools and Applications*, 80, 06 2021. doi: 10.1007/s11042-021-10761-y.

Batuhan Arpacı, Erol Kurt, and Kayhan Çelik. A new algorithm for the colored image encryption via the modified chua's circuit. *Engineering Science and Technology, an International Journal*, 23(3):595–604, 2020. ISSN 2215-0986. doi: https://doi.org/10.1016/j.jestch.2019.09.001.

Gurpreet Kaur, Rekha Agarwal, and Vinod Patidar. Chaos based multiple order optical transform for 2d image encryption. *Engineering Science and Technology, an International Journal*, 23(5):998–1014, 2020. ISSN 2215-0986. doi: https://doi.org/10.1016/j.jestch.2020.02.007.

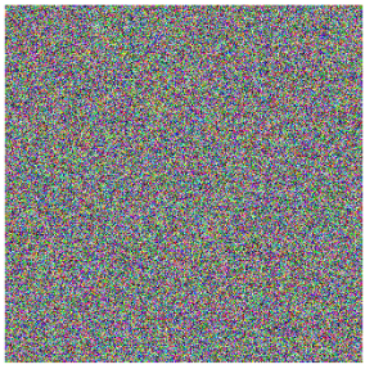
Xiuli Chai, Yiran Chen, and Lucie Broyde. A novel chaos-based image encryption algorithm using dna sequence operations. *Optics and Lasers in Engineering*, 88:197–213, 2017b. ISSN 0143-8166. doi: https://doi.org/10.1016/j.optlaseng.2016.08.009.

Xiaopeng Yan, Xingyuan Wang, and Yongjin Xian. Chaotic image encryption algorithm based on arithmetic sequence scrambling model and dna encoding operation. *Multimedia Tools and Applications*, 80:1–35, 03 2021. doi: 10.1007/s11042-020-10218-8.

Tahir Ali and Rashid Ali. A new chaos based color image encryption algorithm using permutation substitution and boolean operation. *Multimedia Tools and Applications*, 79, 07 2020. doi: 10.1007/s11042-020-08850-5.

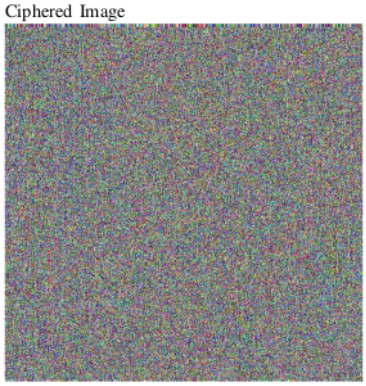
TABLE IX
IMAGE ENCRYPTION ON BASIS OF PLAIN IMAGE


Plain input Image

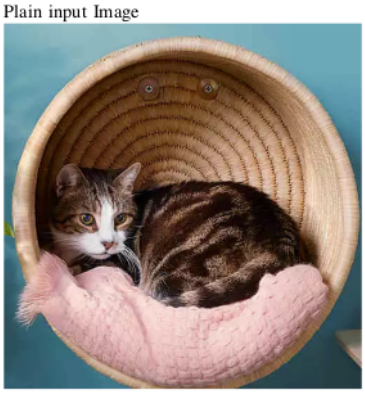

Ciphered Image

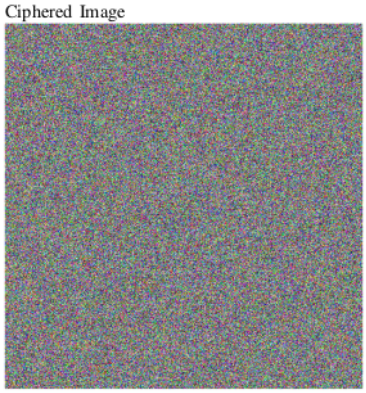

Deciphered Image


Plain input Image

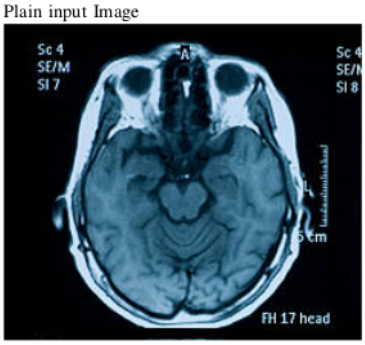

Ciphered Image


Deciphered Image

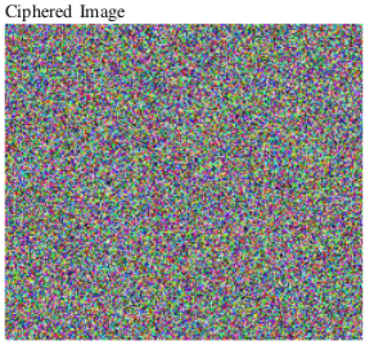

Plain input Image

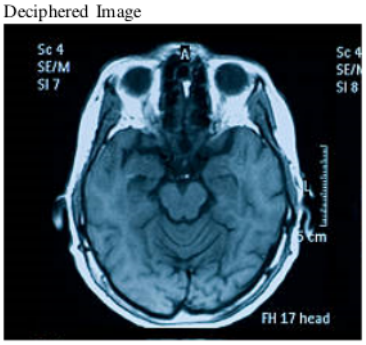

Ciphered Image


Deciphered Image



Plain input Image


Ciphered Image



Deciphered Image

TABLE X
HISTOGRAM ANALYSIS OF ENCRYPTED IMAGE

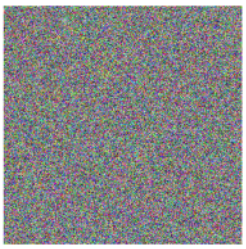
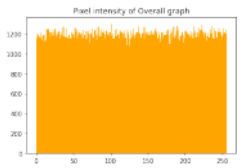
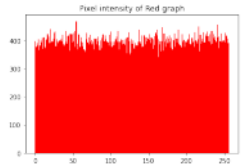
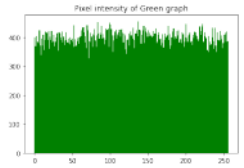
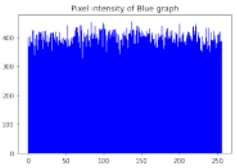
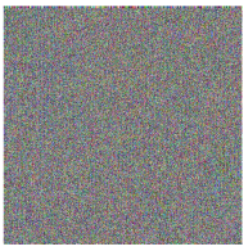
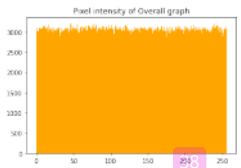
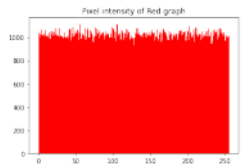
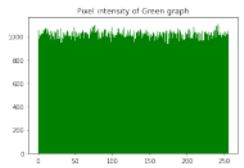
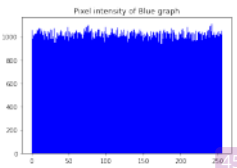
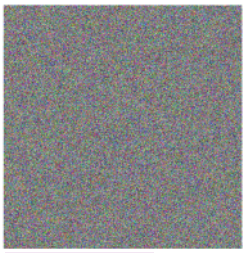
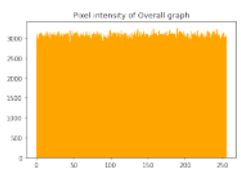
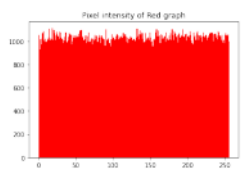
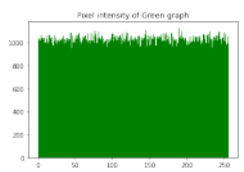
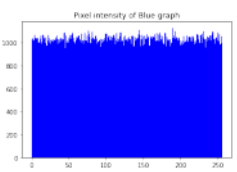
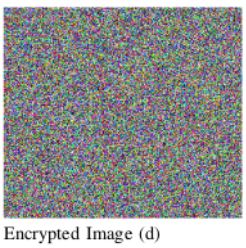
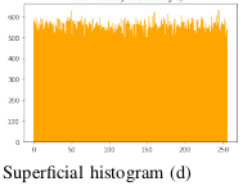
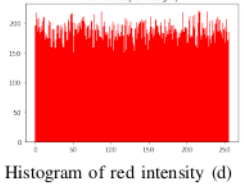
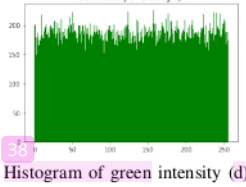
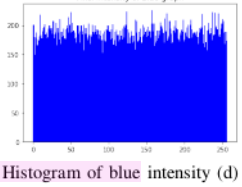
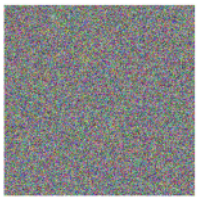
				
Encrypted image (a)	Superficial histogram (a)	Histogram of red intensity (a)	Histogram of green intensity (a)	Histogram of blue intensity (a)
				
Encrypted Image (b)	Superficial histogram (b)	Histogram of red intensity (b)	Histogram of green intensity (b)	Histogram of blue intensity (b)
				
Encrypted Image (c)	Superficial histogram (c)	Histogram of red intensity (c)	Histogram of green intensity (c)	Histogram of blue intensity (c)
				
Encrypted Image (d)	Superficial histogram (d)	Histogram of red intensity (d)	Histogram of green intensity (d)	Histogram of blue intensity (d)

TABLE XI
CHANGES ON IMAGE SENSITIVITY VIA DIFFERENT MANIPULATION

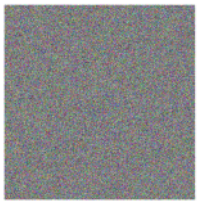

Initial Image (a)

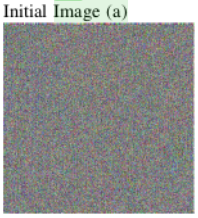

Encrypted Image of a (b)


Small change of a (b)

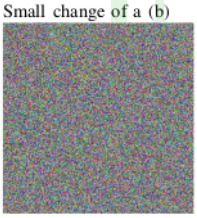

Encrypted Image of (c)

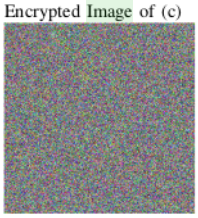

Variance between (a) and (c)

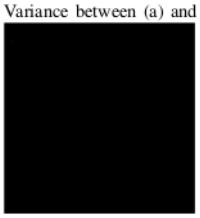

Variance between (b) and (d)


Enciphered Image (g)


Decrypted Image of g (h)


Small change in g (i)


Decrypted image of (j)


Variance between (g) and (i)

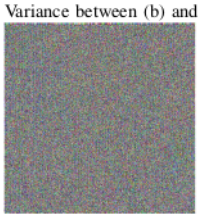
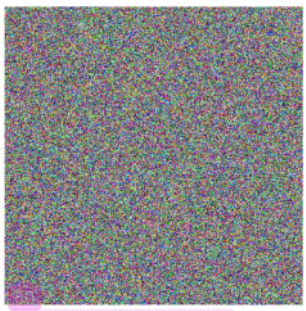
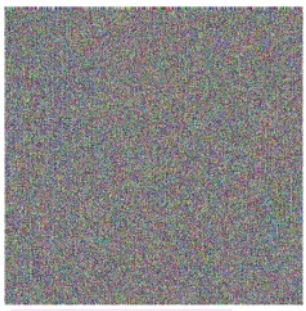

Variance between (h) and (j)

TABLE XII
KEY SENSITIVITY ANALYSIS FOR LENA IMAGE (KEY K1 WAS OBTAINED WHEN ONE BIT WAS CHANGED IN KEY K0)


(a)Initial Lena Image (f)


(b) Ciphered Image using key K0


(c) Ciphered Image using key K1

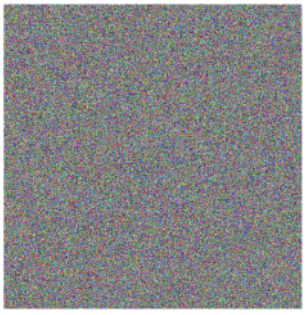
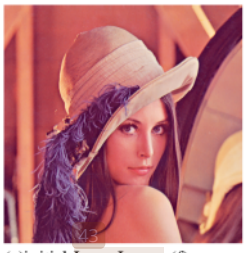
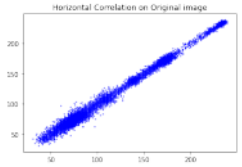

variance between (b) and (c) (d)

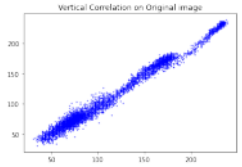
TABLE XIII
VISUALIZATION OF THE CORRELATIONS ALONG DIFFERENT DIRECTIONS FOR ORIGINAL AND ENCRYPTED LENA IMAGE



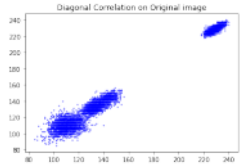
(a)initial Lena Image (f)



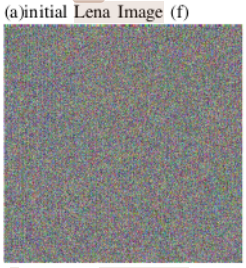
(b) Horizontal Correlation



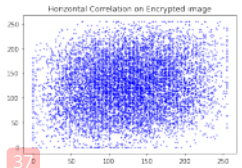
(c) Vertical correlation



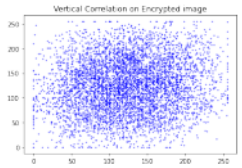
(d) Diagonal correlation



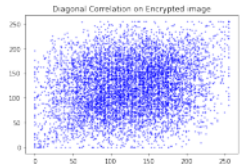
(a)Ciphered Lena Image (f)



(b) Horizontal Correlation



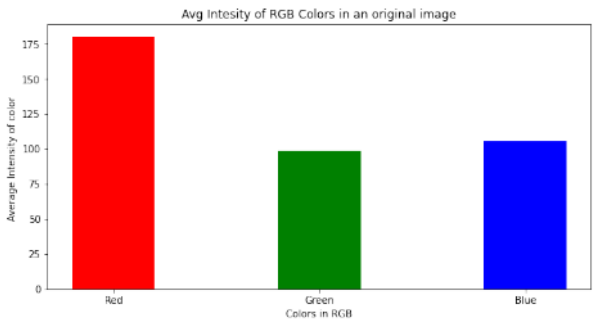
(c) Vertical correlation



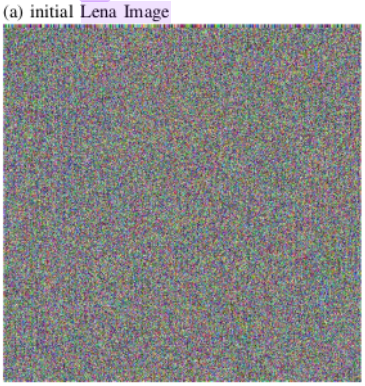
(d) Diagonal correlation

TABLE XIV
AVERAGE ANALYSIS OF LENA'S REAL AND ENCIPHERED IMAGES

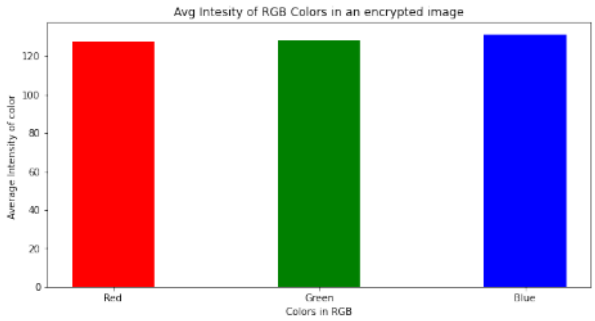
(a) initial Lena Image



(b) Intensity level (original image)



(a)Encrypted Lena Image



(b) Intensity level (encrypted image)

IS_check1

ORIGINALITY REPORT

18%	14%	16%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	dblp.dagstuhl.de Internet Source	1%
2	www.inderscience.com Internet Source	1%
3	scholar.ppu.edu Internet Source	1%
4	researchr.org Internet Source	1%
5	Rahul Patanwadia, Ramchandra Mangrulkar. "Divide and Scramble - A Recursive Image Scrambling algorithm utilizing Rubik's Cube", 2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT), 2021 Publication	<1%
6	www.springerprofessional.de Internet Source	<1%
7	Shah, Manali D., Shrenik N. Gala, and Narendra M. Shekokar. "Lightweight authentication protocol used in Wireless	<1%

Sensor Network", 2014 International Conference on Circuits Systems Communication and Information Technology Applications (CSCITA), 2014.
Publication

8	dblp.uni-trier.de Internet Source	<1 %
9	www.hindawi.com Internet Source	<1 %
10	Farhan Musanna, Sanjeev Kumar. "Generating visually coherent encrypted images with reversible data hiding in wavelet domain by fusing chaos and pairing function", Computer Communications, 2020 Publication	<1 %
11	Ali Mansouri, Xingyuan Wang. "Image encryption using shuffled Arnold map and multiple values manipulations", The Visual Computer, 2020 Publication	<1 %
12	dblp2.uni-trier.de Internet Source	<1 %
13	tel.archives-ouvertes.fr Internet Source	<1 %
14	S.Mahaboob Basha, P. Mathivanan, A. Balaji Ganesh. "Bit Level Color Image Encryption	<1 %

using Logistic-Sine-Tent-Chebyshev (LSTC) map", Optik, 2022
Publication

15	Guo Hua Qiu, Chin Feng Lee, Chin Chen Chang. "Greedy algorithm for image quality optimisation based on turtle-shell steganography", International Journal of Computational Science and Engineering, 2020 Publication	<1 %
16	K. Jaspin, Shirley Selvan, S Sahana, G Thanmai. "Efficient and Secure File Transfer in Cloud Through Double Encryption Using AES and RSA Algorithm", 2021 International Conference on Emerging Smart Computing and Informatics (ESCI), 2021 Publication	<1 %
17	csie.pu.edu.tw Internet Source	<1 %
18	Submitted to National Institute of Technology Warangal Student Paper	<1 %
19	Shun-da Lin. "A new method for image de-noising on the basis of Chen-Mobius transform", 2013 IEEE International Conference on Imaging Systems and Techniques (IST), 2013 Publication	<1 %

20	www.ijrte.org Internet Source	<1 %
21	Mousomi Roy, Shouvik Chakraborty, Kalyani Mali. "The MSK: a simple and robust image encryption method", Multimedia Tools and Applications, 2021 Publication	<1 %
22	ukmsarjana.ukm.my Internet Source	<1 %
23	www.bmvc2021-virtualconference.com Internet Source	<1 %
24	www.sciencegate.app Internet Source	<1 %
25	Lei Zhou, Entao Luo, Guojun Wang, Shui Yu. "Secure fine-grained friend-making scheme based on hierarchical management in mobile social networks", Information Sciences, 2021 Publication	<1 %
26	Hengxiao Chi, Chin-Chen Chang, Yanjun Liu. "An SMVQ compressed data hiding scheme based on multiple linear regression prediction", Connection Science, 2020 Publication	<1 %
27	dblp.org Internet Source	<1 %
	publiweb.femto-st.fr	

28	Internet Source	<1%
29	Submitted to Uttar Pradesh Technical University Student Paper	<1%
30	ijece.iaescore.com Internet Source	<1%
31	Bin Wu, Dong Xie, Fulong Chen, Xueli Wang, Yangyang Zeng. "A multi-party secure encryption-sharing hybrid scheme for image data base on compressed sensing", Digital Signal Processing, 2022 Publication	<1%
32	dokumen.pub Internet Source	<1%
33	hal.archives-ouvertes.fr Internet Source	<1%
34	www.pua.edu.eg Internet Source	<1%
35	jips-k.org Internet Source	<1%
36	Submitted to IIT Delhi Student Paper	<1%
37	link.springer.com Internet Source	<1%

38	Jian Feng Zhao, Shu Ying Wang, Li Tao Zhang, Xian Feng Li. "Image encryption scheme based on a novel fractional order compound chaotic attractor", International Journal of Information and Computer Security, 2020 Publication	<1 %
39	Submitted to University of Philadelphia - Jordan Student Paper	<1 %
40	Wen-Sheng Chen, Xiya Ge, Binbin Pan. "A novel general kernel-based non-negative matrix factorisation approach for face recognition", Connection Science, 2021 Publication	<1 %
41	Nadeem Iqbal, Muhammad Hanif, Sagheer Abbas, Muhammad Adnan Khan, Sultan H. Almotiri, Mohammed A. Al Ghamdi. "DNA Strands Level Scrambling Based Color Image Encryption Scheme", IEEE Access, 2020 Publication	<1 %
42	export.arxiv.org Internet Source	<1 %
43	journals.plos.org Internet Source	<1 %
44	uis.brage.unit.no Internet Source	<1 %

45	Submitted to Indian Institute of Technology, Madras Student Paper	<1%
46	herald.kibit.edu.ua Internet Source	<1%
47	Nadeem Iqbal, Muhammad Hanif, Sagheer Abbas, Muhammad Adnan Khan, Sultan H. Almotiri, Mohammed A. Al Ghamdi. "DNA strands level scrambling based color image encryption scheme", IEEE Access, 2020 Publication	<1%
48	Tarek Azizi, Zouhour Kaddachi, Moufida Ben Karoui, Ala Eddinne Touihri, Rached Gharbi. " Electrical Characterization and Efficiency Enhancement of Dye Sensitized Solar Cell Using Natural Sensitizer and TiO Nanoparticles Deposited by Electrophoretic Technique ", IEEE Journal of Photovoltaics, 2021 Publication	<1%
49	"Innovations in Bio-Inspired Computing and Applications", Springer Science and Business Media LLC, 2021 Publication	<1%
50	Fu, Chong, Wei-hong Meng, Yong-feng Zhan, Zhi-liang Zhu, Francis C.M. Lau, Chi K. Tse, and Hong-feng Ma. "An efficient and secure	<1%

medical image protection scheme based on chaotic maps", Computers in Biology and Medicine, 2013.
Publication

51	Mohammad Kamrul Hasan, Samar Kamil, Muhammad Shafiq, Yuvaraj S, E. Saravana Kumar, Rajiv Vincent, Nazmus Shaker Nafi. "An improved watermarking algorithm for robustness and imperceptibility of data protection in the perception layer of internet of things", Pattern Recognition Letters, 2021 Publication	<1 %
52	vdocument.in Internet Source	<1 %
53	Mingxu Wang, Xingyuan Wang, Yingqian Zhang, Zhenguo Gao. "A novel chaotic encryption scheme based on image segmentation and multiple diffusion models", Optics & Laser Technology, 2018 Publication	<1 %
54	aclanthology.org Internet Source	<1 %
55	piaf.loria.fr Internet Source	<1 %
56	visionbib.com Internet Source	<1 %

140.112.30.160

57	Internet Source	<1%
58	Huishan Wu, Hongyang Zhu, Guodong Ye. "Public key image encryption algorithm based on pixel information and random number insertion", Physica Scripta, 2021 Publication	<1%
59	Ichraf Aouissaoui, Toufik Bakir, Anis Sakly. "Robustly correlated key ‐ medical image for DNA ‐ chaos based encryption", IET Image Processing, 2021 Publication	<1%
60	Qusay Kanaan Kadhim, Basman M. Al-Nedawe, Emad Majeed Hameed. "Encryption and Decryption of Images using GGH Algorithm: Proposed", IOP Conference Series: Materials Science and Engineering, 2021 Publication	<1%
61	S Geetha, P Punithavathi, A Magnus Infanteena, S Siva Sivatha Sindhu. "A Literature Review on Image Encryption Techniques", International Journal of Information Security and Privacy, 2018 Publication	<1%
62	Sujarani Rajendran, Kannan Krithivasan, Manivannan Doraipandian. "A novel cross cosine map based medical image	<1%

	cryptosystem using dynamic bit-level diffusion", Multimedia Tools and Applications, 2021 Publication	
63	cb66109b-0e0b-4dac-8f11-8c6697985f7e.filesusr.com Internet Source	<1 %
64	downloads.hindawi.com Internet Source	<1 %
65	mdpi-res.com Internet Source	<1 %
66	www.jisikworld.com Internet Source	<1 %
67	"Advances in Computing and Data Sciences", Springer Science and Business Media LLC, 2018 Publication	<1 %
68	"Nanoelectronics, Circuits and Communication Systems", Springer Science and Business Media LLC, 2021 Publication	<1 %
69	Advances in Intelligent Systems and Computing, 2016. Publication	<1 %
70	Nehal Abd El-Salam Mohamed, Aliaa Youssif, Hala Abdel-Galil El-Sayed. "Fast and Robust Image Encryption Scheme Based on Quantum	<1 %

Logistic Map and Hyperchaotic System", Complexity, 2022
Publication

71	S. Mahaboob Basha, P. Mathivanan, A. Balaji Ganesh. "Bit level color image encryption using Logistic-Sine-Tent-Chebyshev (LSTC) map", Optik, 2022 Publication	<1 %
72	G. Kapinesh, K. Sachin Kumaran, Konduru Gayatri, Thilak Mohan, V. Thanikaiselvan, S. Subashanthini, R. Amirtharajan. "New Image Encryption Method using Multiple Chaotic Map Computation and Irregular Diffusion Process", Journal of Uncertain Systems, 2022 Publication	<1 %
73	Gregory Gaspari. "Construction and application of covariance functions with variable length-fields", Quarterly Journal of the Royal Meteorological Society, 07/2006 Publication	<1 %
74	Guo Hua Qiu, Chin Feng Lee, Chin Chen Chang. "Turtle-shell data embedding method with high image fidelity", International Journal of Embedded Systems, 2021 Publication	<1 %
75	Majid Khan, Hafiz Muhammad Waseem. "A novel image encryption scheme based on	<1 %

quantum dynamical spinning and rotations",
PLOS ONE, 2018
Publication

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		