A Mathematical Interpretation of Images and Image Encryption

Ratheesh Kumar R[#1], Jabin Mathew[*2]

[#1] *Ratheesh Kumar R, MTech (CSE) Scholar, Govt. Engineering College, Idukki, Kerala, India*
[*2] *Jabin Mathew, Assistant Professor, Dept. of Computer Science & Engg., Govt. Engineering College, Idukki*

Abstract *— This paper gives us the idea that how the images are stored, accessed, and processed, and how the image encryption is implemented. Images are merely matrices of pixels and image encryption is just a technical 'game' or mathematical 'puzzle' that involves the matrix of pixels. A plain-image and its cipher-image of an image encryption system are two different matrices, but they have a hidden relationship. That mathematical relationship is the essence of that encryption algorithm. Not only the images, their encryption and decryption, and their security and performance analyses are also complex mathematical operations on the image matrices.*

Keywords — *Gray-scale and Color Images, Matrices, Pixels, Encryption, Security Attacks, Analysis, Key.*

I. INTRODUCTION

Visualizing and realizing a problem in terms of a mathematical entity is very helpful for finding its solution. Then, the overall problem-and-solution will be a mathematical model. This is the main reason for the fact that there are a large number of image encryption techniques and a very large number of image encryption systems. The numbers are still growing. Security and performance of the image encryption progress with the latest encryptions due to the characteristics of viewing the encryption as a mathematical model. All the aspects of image encryption can be interpreted mathematically, i.e., the images, the image encryption, the decryption, and analyses can be represented and performed as mathematical entities and operations.

II. MATHEMATICAL INTERPRETATION

A. Matrix Representation of Images

The smallest element of an image is a pixel (picture element). An image is represented by a matrix of pixels. A grayscale image contains various shades of the combination of black and white colors. A pixel or an element in the grayscale image matrix is 8-bit with that having 2^8 combinations of shades of gray. A pixel in a grayscale image or an element in the matrix is an integer value (0-255). A color image is usually a combination of three matrices, one each for the three colors RED (R), GREEN (G), and BLUE (B). Here, a pixel is 24-bit that 8 bits of Red, 8 bits of Green, 8 bits for Blue information. It can create 2^{24} color combinations. Each color (R/G/B) matrix has elements having values (0-255). [21]

B. Process of Image encryption

Valuable meaningful images are converted into visually meaningless cipher-images using encryption, for security. This is done at the sender-side. On the receiver-side, the cipher-image is converted back to the original image using decryption. Normally the decryption is just the reverse of the encryption process. An image cryptosystem has both encryption and decryption. There exist numerous image encryption systems, and fall into two classes, namely traditional techniques and alternative techniques. AES, 3DES, RSA, ECC, etc. and their combinations belong to the traditional techniques, and DNA, Chaos, and the combinations are considered as the alternative techniques.

Whatever the technique used for image encryption the underlying process is nothing but a complex mathematical operation that performed on the image matrix. This complex mathematical operation is a combination of several simple mathematical operations such as arithmetic, relational, logical, conversion, mixing, grouping, scrambling, or related mathematical operations.

Since all the traditional image encryption techniques are international standards, they are well-defined mathematical models. The underlying principles and processes of them are pre-defined and universally acceptable. Their modified versions and the combinations can also be easily defined mathematically. But the traditional techniques are not best suited for image encryption. This is because they cannot address the special characteristics of the images over text such as the huge data volume, 2D spatial distribution of pixels, multiple data redundancy, and high correlation between adjacent pixels. Therefore, the traditional techniques are sluggish in execution.

On the other hand, alternative techniques like DNA and Chaos have no pre-defined principles and processes. Even though they lack the standard model, they are well suited for image encryption. The reason for this is that

they can address the abovesaid special features of the images. Therefore, there is a lot of research in the alternative techniques of image encryption.

The chaotic theory is a field of mathematics that gives a new dimension in image encryption. It gives the behavior and characteristics of a specific non-linear dynamic system that shows dynamics under certain conditions that are deterministic and unpredictable. A chaotic map is a mathematical map or function that exhibits chaotic behavior, i.e., the outputs of these maps are unpredictable pseudorandom numbers (PRNs). The purpose of these mathematical maps is PRNG (Pseudo-random number generation). Different types of maps are Lorenz, Arnold, Logistic, etc, and multiple dimensional maps are possible. These maps generate pseudo-random numbers which can be used as keys and intermediate values for the encryption. The relationship between chaotic theory and cryptography is as follows [21]:

Chaotic feature	Cryptographic feature	Explanation
Ergodicity	Confusion	The outputs have the same distribution for all inputs.
Sensitivity to initial conditions	Diffusion with a small change in the plain-text/secret key	Even a small deviation in the input results in a large change at the output.
Mixing property	Diffusion with a small change in one plain-block of the whole plain-text	Even a small deviation in the local area can cause a large change in the whole space.
Deterministic dynamics	Deterministic pseudo-randomness	A deterministic process has a random-like behavior.
Structure complexity	Algorithm complexity	Even a simple process has very high complexity.

DNA cryptography is evolving; it performs operations on techniques of DNA computing and exploits the properties of the biological structure of deoxyribonucleic acid (DNA) that contains nucleotides - Adenine (A), Guanine (G), Cytosine (C), and Thymine (T). DNA focuses on utilizing DNA sequences to encode binary data in a certain kind or another. It is hiding of data in terms of DNA sequences. The various operations such as DNA addition and DNA subtraction can be possible with DNA sequences [21]. We have to define the rules for DNA addition and subtraction.

We can also club relational and logical operations like XOR with traditional and alternative techniques. Therefore, we can conclude that image encryption is a complex mathematical operation that performed on the image matrix. An image encryption algorithm possesses a permutation and diffusion structure (PDS) for the process.

C. Security and Performance Analyses

Here, we are presenting the various analyses and their mathematical definitions and interpretations. Cipher-image, histogram, statistical attack, differential attack, brute-force attack, noise attack, information loss, PSNR, robustness, perceptual, key sensitivity, speed, and complexity analyses are the analyses used to evaluate the security and performance of the image encryption system. Histograms of the input-images or plain-images and the cipher-images or encrypted images explain and reveal the distribution of pixel values by finding the count of each value.

Variance Analysis: Variance of a histogram of a plain-image or a cipher-image can be defined as a statistic to quantify the distribution uniformity of pixels. The lower variance indicates the higher uniformity of the image. The variance of a histogram is mathematically defined as:

$$Var(X) = \frac{1}{256^2} \sum_{i=1}^{256} \sum_{j=1}^{256} \frac{1}{2} (x_i - x_j)^2$$

where X is the vector of the histogram values, and $X=\{x_1,x_2,...,x_{256}\}$. x_i and x_j are the numbers of pixels which values are equal to *i* and *j* respectively. [14]

Chi-square (χ2) Analysis: We can also use χ2 analyses to verify whether the histogram distribution is uniform, and the value of χ2 is computed by:

$$c^2 = \sum_{i=0}^{255} \frac{(v_i - v_e)^2}{v_e}$$

where *i* represents pixel value, the value of *i* is an integer between 0 and 255. v_i represents the times of the pixel value *i* appears in the image. v_e is the expected frequency of a pixel value *i*, v_e = (P×Q)/256, where PxQ is the dimension of image matrix. Assumptions: commonly used significant level is α = 0.05, and $\chi^2_{0.05}$ = 293.24783. Hence, we think that the histogram distribution is uniform in the case of the significant horizontal α = 0.05.

Different differential attack positions are selected and the above equation is used to detect the $\chi 2$ value of input image and the $\chi 2$ value of encrypted image. [20]

Correlation Analysis: For good quality images, adjacent pixels are very close to each other. Therefore, the correlation of the visual image is very high. The encrypted image by a good image encryption system must exhibit a low correlation of two adjacent pixels. The correlation coefficient is a numerical measure to assess a statistical relationship between two variables. Correlation coefficient is defined mathematically as:

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

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

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

$$f_{xy} = \frac{C(x,y)}{\sqrt{M(x)}\sqrt{M(y)}}$$

where *x, y* are values of adjacent pixels. *N* is the number of pixels selected from the image. *E(x)* is the estimation of mathematical expectation of *x* and *M(x)* is the estimation of the variance of *x*. *C(x,y)* is the estimation of the covariance between *x* and *y*. f_{xy} represents the correlation coefficient of the image. Correlation distributions of input-images are concentrated whereas that of encrypted images is fairly uniform. [14]

Information Entropy Analysis: The entropy of the ensemble is defined as a sensible measure of the ensemble's average information content. Information entropy can be considered as an important parameter to measure the intensity of the symmetric cryptosystem. The mathematical definition of entropy is given as:

$$I(x) = -\sum_{i=0}^{2^n-1} p(x_i)\log_2 p(x_i)$$

where $p(x_i)$ is the probability of the symbol x_i. The ideal information entropy is equal to 8 for the cipher-image with 2^8 gray-levels. Larger information entropy means less information content. [14]

Differential Attack Analysis: Differential attack can be viewed as an efficient cryptanalytic method to use pairs of input-images related by a constant difference and compare the difference of the corresponding encrypted-images for statistical patterns in their distribution. Usually, attackers make a tiny change in the input-image and use the encryption algorithm to encrypt the image before and after any changes. Then they try to find out the relationship between the input-image and the encrypted image. The differential analysis aims to assess sensitivity to the input-image. Number of pixels change rate (NPCR) and unified average changing intensity (UACI) are two parameters to measure the difference between two encrypted images of the same image. NPCR calculates the percentage of different pixel numbers between two encrypted images. UACI calculates the average intensity of difference between two encrypted images [14]. NPCR and UACI are defined as:

$$B(i,j) = \begin{cases} 0, & C(i,j) = C'(i,j) \\ 1, & C(i,j) \neq C'(i,j) \end{cases}$$

$$NPCR = \frac{\sum_{i,j} B(i,j)}{P \times Q} \times 100\%$$

$$UACI = \frac{1}{P \times Q} \times \sum_{i,j} \frac{|C(i,j) - C'(i,j)|}{255} \times 100\%$$

where P×Q is the size of encrypted images C and C'. The following table reports results of NPCR and UACI which are closer to reference values.

Key Sensitivity Analysis: As a common attack, key sensitivity uses pairs of security keys related by a slight difference to encrypt input-images and calculates the differences of the corresponding encrypted-images for statistical clues. High key sensitivity is that the cryptosystem with two slightly distinct keys encrypts the same input-image and gets utterly different encrypted images. The difference can be quantified by the parameters NPCR and UACI [14].

Noise and Information Loss Analyses:

Noise Analysis: Peak Signal to Noise Ratio is defined as the ratio between the maximum power possible of the signal and the power of the corrupted signal due to noise. PSNR is given as:

$$PSNR = 20\log_{10}(255/\sqrt{MSE})$$

where *MSE* is the mean square error value. For good encryption, PSNR between plain-image and cipher must be a low value. It is also used for evaluating information loss; high PSNR between plain-image and decrypted image means less information loss. [21]

Information Loss Analysis: A good encryption system should be free from information loss due to noise or algorithm while encryption and/or decryption. To verify whether the information loss has occurred or not, we must perform the analyses of HSL (hue, saturation, luminosity), resolution, aspect ratio, RGB content, energy, contrast, etc. [21]

The mathematical definitions of hue, saturation, and luminosity are complex, but they are calculated by the mathematical operations on the image matrix. There are library functions in image processing languages for computing hue, saturation, and luminosity of the pixels.

R(Red) value of a particular pixel is the value of the corresponding element in the R matrix of the image. G(Green) value of that particular pixel is the value of the corresponding element in the G matrix of the image. B(Blue) value of a particular pixel is the value of the corresponding element in the B matrix of the image.

The resolution of an image is the dimension of the image matrix, i.e., the number of rows x the number of columns in the image matrix. Example: A color image has a resolution of 400x300x3; 400 is the number of rows, 300 is the number of columns, and 3 is the number of color channels. If the image is color, then the R, G, and B matrices have the same dimension.

The aspect ratio of an image is the number of rows in the image matrix (M) divided by the number of columns (N) in the image matrix.

$$Aspect\text{-}Ratio = M/N$$

The contrast of an image is the difference of the maximum pixel (or element) value in the image matrix and the minimum pixel value.

$$Contrast = maximum(I) - minimum(I),$$ where I is the image.

The energy of an image is defined as the sum of all the pixel values in the image matrix (I).

$$Energy = sum(I)$$

Robustness Analysis: Due to noise or the related, images may suffer from occlusion and clipping attacks. A good encryption scheme has a provision for restoring and reclaiming the information lost. That is, robustness is an important property of image encryption methods. Robustness is an important index to verify the anti-interference ability of cryptography. In the process of transmitting images, the information may be lost or polluted by noise, so it is necessary to design an encryption algorithm, with strong mathematical properties in mind. Even if part of the information is lost, the part of the plain-image information can be obtained by decrypting the program [20]. The systems with scrambling and descrambling help maximizing the robustness. Robustness is the outcome of the mathematical properties of the encryption.

Perceptual Analysis: A good algorithm must be sensitive to the secret key of the process. That is, a small change in the secret key will produce a completely different result.

Example: key = (0.111111111111111, 0.111111111111110)
The last bit has been changed to generate a new key: new key = (0.111111111111111, 0.111111111111111)
The correct key produces the image back, whereas the wrong key does not produce the image. This is due to the mathematical characteristics of the encryption. [20]

Keyspace, Algorithmic Complexity, and Speed Analyses: Keyspace is the number of possible key combinations. If the keyspace of an algorithm is greater than 2^{100}, then the algorithm is a good image encryption which can resists brute force attacks. For example, a cryptosystem has a key with 6 variables, the algorithm has a keyspace which is > 2^{300}. Therefore, we can say that the example system can resist brute-force attacks. Algorithmic complexity is the total number of vital iterations in the algorithm. It is the measure of an algorithm's time and speed. Encryption efficiency analysis assesses the running performance of encryption. Encryption efficiency is an important measure to assess the running performance of the encryption scheme. For

analyses of chaotic encryption schemes, the time-consuming part in computations is the operations of multiplying floating point numbers. [14] The speed or data rate of the encryption can be computed by the size of the image divided by the execution speed.

III. CONCLUSION

People, who are involving in the activities of cryptography and cryptanalysis, always want to visualize and realize the images, encryption, and analyses as mathematical models. Mathematical models of images, encryption, and analyses give them flexibility and easiness in the development of algorithms, the provision for prior simulations, and the ability to verify the correctness, security, and performance of the encryption systems under consideration. We hope this paper provides the readers with the idea of mathematical interpretations of the various concepts of the images and encryption, and this will help them to correct and extend the existing ideas and device new encryption systems with more security and performance.

REFERENCES

[1] Priyanka and Deepika Arora, *"Survey and Analysis of Current Methods of Image Encryption Algorithm Based on DNA Sequencing"*, IJCST, vol. 9, pp. 34-41, 2018.

[2] Ahmed A. Abd El-Latif, Bassem Abd-El-Atty, and Muhammad Talha, "Robust Encryption of Quantum Medical Images", IEEE Access, vol. 6, pp. 1073 – 1081, Feb. 2018.

[3] Ramya Princess Mary, P Eswaran, and K Shankar, "Multi Secret Image Sharing Scheme Based on DNA Cryptography with XOR", Pure and Applied Mathematics, vol. 118, No. 7, pp. 393-398, Feb. 2018.

[4] Tian Tian Zhang, Shan Jun Yan, Cheng Yan Gu, Ran Ren, and Kai Xin Liao, "Research on Image Encryption Based on DNA Sequence and Chaos Theory", Physics: Conf. Series, vol. 1004, pp. 1–6, 2018.

[5] Xing-Quan Fu, Bo-Cheng Liu, Yi-Yuan Xie, Wei Li, and Yong Liu, "Image Encryption-Then-Transmission Using DNA Encryption Algorithm and The Double Chaos", IEEE Photonics, vol. 10, no. 3, June 2018.

[6] Osama S. Faragallah, Mohammed A. Alzain, Hala S. El-Sayed, Jehad F. Al-Amri, Walid El-Shafai, Ashraf Afifi, Ensherah A. Naeem, and Ben Soh, "Block-Based Optical Color Image Encryption Based on Double Random Phase Encoding", IEEE Access, vol. 7, pp. 4184 - 4194, Jan. 2019.

[7] Xingbin Liu, Di Xiao, and Yanping Xiang, "Quantum Image Encryption Using Intra and Inter Bit Permutation Based on Logistic Map", IEEE Access, vol. 7, pp. 6937 - 6946, Jan. 2019.

[8] *Zhenjun Tang, Ye Yang, Shijie Xu, Chunqiang Yu, and Xianquan Zhang, "Image Encryption with Double Spiral Scans and Chaotic Maps", Hindawi Sec. and Comm. Networks, vol. 2019, pp. 1-15, Jan. 2019.*

[9] Xinsheng Li, Zhilong Xie, Jiang Wu, and Taiyong Li, "Image Encryption Based on Dynamic Filtering and Bit Cuboid Operations", Hindawi Complexity, vol. 2019, pp. 1-16, Feb. 2019.

[10] Taiyong Li, Jiayi Shi, Xinsheng Li, Jiang Wu, and Fan Pan, "Image Encryption Based on Pixel-Level Diffusion with Dynamic Filtering and DNA-Level Permutation with 3D Latin Cubes", Entropy, vol. 21, no. 319, pp. 1-21, 2019.

[11] Yuling Luo, Xue Ouyang, Junxiu Liu, and Lvchen Cao, "An Image Encryption Method Based on Elliptic Curve Elgamal Encryption and Chaotic Systems", IEEE Access, vol. 7, pp. 38507–38522, Mar. 2019.

[12] *Fazal Noorbasha, S. Mohit Srinath, SK. Khadir Bhasha, P. Jagadish, and K Hari Kishore, "FPGA Based DNA Cryptography System for Medical Image Data Analysis Process", Innovative Technology and Exploring Engineering, vol. 8, No. 6S, pp. 128-131, Apr. 2019.*

[13] *Akram Belazi, Muhammad Talha, Sofiane Kharbech, and Wei Xiang, "Novel Medical Image Encryption Scheme Based on Chaos and DNA Encoding", IEEE Access, vol. 7, pp. 36667–36681, Mar. 2019.*

[14] *Hui Liu, Bo Zhao, and Linquan Huang, "A Remote-Sensing Image Encryption Scheme Using DNA Bases Probability and Two-Dimensional Logistic Map", IEEE Access, vol. 7, pp. 65450–65459, May 2019.*

[15] *Shikha Jaryal and Chetan Marwaha, "Comparative Analysis of Various İmage Encryption Techniques", Computational Intelligence Research, vol. 13, No. 2, pp. 273-284, 2017.*

[16] *Bin Wang, Yingjie Xie, Shihua Zhou, Xuedong Zheng, and Changjun Zhou, "Correcting Errors in Image Encryption Based on DNA Coding", Molecules, vol. 23, pp. 1-13, 2018.*

[17] *Chunhu Li, Guangchun Luo, and Chunbao Li, "An Image Encryption Scheme Based on The Three-dimensional Chaotic Logistic Map", Network Security, vol.21, No.1, PP.22-29, 2019.*

[18] *Omar Farook Mohammad, Mohd Shafry Mohd Rahim, Subhi Rafeeq Mohammed Zeebaree and Falah Y.H. Ahmed, "A Survey and Analysis of the Image Encryption Methods", Applied Engineering Research, vol. 12, no. 23, pp.13265-13280, 2017.*

[19] *Zhijuan Deng and Shaojun Zhong, "A digital image encryption algorithm based on chaotic mapping", Algorithms Computational Technology, vol. 13, pp. 1 – 11, 2019.*

[20] *Xingyuan Wang, Suo Gao, Longjiao Yu, Yuming Sun, and Huaihuai Sun, "Chaotic Image Encryption Algorithm Based on Bit-Combination Scrambling in Decimal System and Dynamic Diffusion", IEEE Access, vol. 7, pp. 103662-103677, 2019.*

[21] *Ratheesh Kumar R and Jabin Mathew, "Image Encryption: Traditional Methods vs Alternative Methods", IEEE, Proceedings of the Fourth International Conference on Computing Methodologies and Communication (ICCMC 2020), pp. 619-625, March 2020.*

[22] *Shuqin Zhu, Congxu Zhu, and Wenhong Wang, "A New Image Encryption Algorithm Based on Chaos and Secure Hash SHA-256", Entropy, Sep 2018, 20, 716, pp. 1-18.*

[23] *Anupam Kumar, Aman Kumar, Sahil Jain, P Kiranmai, "Performance Comparison of Cryptanalysis Techniques over DES", IJRASET, May 2016, vol. 4, pp. 1-13.*

[24] *Xiaoqiang Di, Jinqing Li, Hui Qi, Ligang Cong, and Huamin Yang: "A semi-symmetric image encryption scheme based on the function projective synchronization of two hyperchaotic systems", PLOS ONE, Sep 14, 2017, pp 1-29.*

[25] *K W Wong, W S Yap, B M Goi, and Denis C K Wong: "Differential Cryptanalysis on Chaotic Based Image Encryption Scheme", IOP Conf. Series, 2019, vol. 495 (2019) 012041, pp.1-11.*

[26] A. ChandraSekhar, D. Chaya Kumari, S. Ashok Kumar, *"Symmetric Key Cryptosystem for Multiple Encryptions", International Journal of Mathematics Trends and Technology (IJMTT).* V29(2):140-144 January 2016. ISSN:2231-5373.

[27] Meena Bairola, Dr.A.S.Uniyal, *"Application of Advanced Cryptographic System", International Journal of Mathematics Trends and Technology (IJMTT).* V55(4):311-316, March 2018. ISSN:2231-5373.