IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 12, December 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212049 |

The Math of Images and Image Encryption in Computer Science

Shibi. M. S, Shajahan S

Lecturer in Computer Engineering, Government Polytechnic College, Neyyattinkara, Kerala, India

Lecturer in Computer Engineering, Department of Computer Hardware Engineering, Govt Polytechnic College, Nedumangad, Kerala, India

ABSTRACT: The paper delves into the technical aspects of image storage, encryption, and processing, highlighting that images are fundamentally grids of pixels, organized in matrices. The process of encrypting an image involves treating this pixel matrix as a puzzle or a game, wherein encryption is the act of transforming the plain, easily readable image matrix into a cipher-image, making it unreadable without the decryption key. The core idea lies in the relationship between these two matrices—the original plain-image matrix and its encrypted counterpart. This relationship is established through complex mathematical operations that form the encryption algorithm. This algorithm defines how the plain image is transformed into the cipher-image and vice versa during decryption. Furthermore, this emphasizes that the encryption and decryption processes, along with assessing the security and performance of these methods, involve intricate mathematical operations applied to these image matrices. Security analysis aims to ensure that the encrypted image remains unreadable without the proper decryption key, while performance analysis assesses how efficiently and effectively these encryption and decryption operations can be carried out. Overall, the paper underscores the mathematical foundation behind image encryption, where the manipulation of pixel matrices forms the basis of the security measures implemented to protect images from unauthorized access.

KEYWORDS: images, image encryption, pixel, variance, histogram, chi-square, correlation, entropy, PSNR

I. INTRODUCTION

The idea expressed here centers on the significance of conceptualizing problems in terms of mathematical entities to facilitate their resolution. When a problem is visualized and formulated in mathematical terms, it becomes more manageable to find a solution. This approach often results in an overarching problem-and-solution framework that constitutes a mathematical model. In the context of image encryption, this mathematical perspective has led to the proliferation of numerous encryption techniques and systems. The continual growth in their numbers is attributed to the effectiveness of viewing encryption as a mathematical model. This viewpoint allows for the development of diverse and innovative encryption methods that enhance both the security and performance of image encryption processes. The core reason behind the ongoing evolution of image encryption lies in perceiving encryption as a mathematical model. By embracing this perspective, various aspects of image encryption—such as the images themselves, the encryption and decryption procedures, as well as the analyses conducted on these processes—can all be translated and understood as mathematical entities and operations. This mathematical interpretation facilitates a deeper comprehension of image encryption techniques, enabling researchers and developers to refine existing methods or create new ones by leveraging mathematical principles. Consequently, the continuous advancement of image encryption methods is fueled by this mathematical framework, allowing for improvements in both the security and efficiency of protecting digital images.

II. MATHEMATICS OF IMAGES

(i) Representation of Images: Images, whether grayscale or color, are essentially comprised of pixels, which are the smallest components. The representation of an image in digital form is based on a matrix, with each element of the matrix corresponding to a pixel.

Grayscale Images: In a grayscale image, various shades between black and white are represented. Each pixel in a grayscale image matrix is typically 8 bits, allowing for 2^8 (or 256) combinations of shades of gray. This means each pixel's value ranges from 0 to 255, with 0 representing black and 255 representing white.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212049 |

Color Images: Color images are usually composed of three matrices, one for each primary color: RED (R), GREEN (G), and BLUE (B), often referred to as the RGB format. Each pixel in a color image is 24 bits, comprising 8 bits for each of the primary colors—Red, Green, and Blue. This configuration enables 2^24 (or 16,777,216) possible color combinations. Each color matrix (R/G/B) consists of elements, i.e., pixels, where each pixel's value ranges from 0 to 255 for intensity levels of each color component. Therefore, when we're dealing with a color image represented digitally, each pixel's value in the matrix for a particular color channel (R, G, or B) determines the intensity or contribution of that color to the overall color of that pixel. The combination of these RGB values across all pixels creates the full-color image we perceive.

This matrix-based representation of images forms the foundation for digital image processing and manipulation, allowing for various transformations, enhancements, and algorithms to be applied to images in both grayscale and color formats.

(ii) Image Encryption: The process of image encryption involves transforming meaningful images into visually unintelligible cipher-images using encryption techniques. This transformation is carried out at the sender-side to ensure the security of the transmitted information. On the receiver-side, decryption is performed to convert the cipher-image back to its original form. Typically, decryption is the inverse of the encryption process. There are numerous image encryption systems classified into two main classes: traditional techniques and alternative techniques. Traditional techniques like AES, 3DES, RSA, ECC, etc., and their combinations are well-defined international standards, relying on established mathematical models. These methods are based on complex mathematical operations involving arithmetic, relational, logical, conversion, mixing, grouping, scrambling, or similar mathematical operations applied to the image matrix. However, traditional techniques struggle with handling specific characteristics unique to images, such as their large data volume, 2D spatial distribution of pixels, redundancy, and high pixel correlation. Consequently, they tend to be slower in execution for image encryption due to these limitations.

On the other hand, alternative techniques such as DNA and Chaos lack predefined principles and processes. Despite this, they excel in addressing the unique features of images that traditional methods struggle with. For instance, Chaos theory introduces non-linear dynamic systems and chaotic maps, generating unpredictable pseudorandom numbers that can be used for encryption keys and intermediate values. DNA cryptography leverages DNA computing techniques, exploiting the properties of DNA's biological structure and sequences (Adenine, Guanine, Cytosine, and Thymine) to encode binary data. Operations such as DNA addition and subtraction are defined within this framework. The integration of relational and logical operations, such as XOR, with both traditional and alternative techniques is also possible, creating hybrid encryption approaches. Image encryption involves intricate mathematical operations performed on the image matrix. An encryption algorithm typically follows a permutation and diffusion structure (PDS) to ensure security and transform the original image into an encrypted form, either using well-established traditional methods or innovative alternative approaches that cater better to the unique characteristics of images.

(iii) Security and Performance Analyses of Image Encryption: The various analyses used to evaluate the security and performance of an image encryption system are:

Cipher-Image Analysis: This involves examining the encrypted image, which appears visually meaningless, to assess the extent of its encryption. The goal is to ensure that the encrypted image is not susceptible to unauthorized decryption.

Histogram Analysis: Histograms are graphical representations that illustrate the distribution of pixel values within an image. By analyzing the histograms of both the original (plain) and encrypted (cipher) images, one can gain insights into how pixel values are distributed. Any significant alteration in the pixel value distribution post-encryption indicates a change in the image content.

Statistical Attacks and Analysis: These attacks involve using statistical methods to analyze patterns or irregularities in the encrypted image. Statistical analysis might reveal correlations, biases, or patterns that could potentially weaken the encryption and compromise security.
Differential Attacks and Analysis: These attacks involve comparing differences between encrypted versions of similar or related images. If patterns or similarities emerge in the encrypted data, it could lead to vulnerabilities in the encryption method.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212049 |

Brute-Force Attacks and Analysis: This involves systematically trying all possible decryption keys to break the encryption. Analyzing the system's resilience against such attacks helps determine its security level.

Noise Attack Analysis: Assessing how well the encryption system handles or resists external noise or interference is crucial for evaluating its robustness.

Information Loss Analysis: It involves measuring any loss of information during the encryption process. A good encryption system should retain the essential information while making it unintelligible to unauthorized users.

PSNR (Peak Signal-to-Noise Ratio): PSNR quantifies the quality of the recovered image concerning the original one. It measures the level of noise introduced during encryption and decryption, thus reflecting the fidelity of the decrypted image.

Robustness and Perceptual Analysis: These analyses focus on evaluating how well the encrypted image withstands attacks and how closely the decrypted image resembles the original visually.

Key Sensitivity: Assessing the impact of changes in encryption keys on the security and quality of encrypted images is crucial to understanding the system's vulnerability to key-related attacks.

Speed and Complexity Analysis: These evaluations consider the computational speed and complexity of the encryption and decryption processes. A good system balances robust security measures with efficient processing.

These analyses, often approached from a mathematical perspective, provide comprehensive evaluations of image encryption systems, covering various aspects of security, fidelity, robustness, and computational efficiency. They help in gauging the strength and performance of an encryption system and aid in refining or choosing the most suitable techniques for securing image data.

(a) Variance Analysis: Variance analysis, in the context of image processing and encryption, involves the statistical evaluation of pixel distribution within an image's histogram. Variance itself is a measure of how spreads out the values in a dataset are relative to the mean or average value. For a histogram—a graphical representation of the frequency distribution of pixel values in an image—the variance quantifies the uniformity or spread of these pixel values across the image.

In the case of a plain-image or a cipher-image, their respective histograms showcase the distribution of pixel values. By calculating the variance of these histograms, one can assess the uniformity or diversity of pixel values present in the image. A lower variance in the histogram implies that the pixel values are closer together or more concentrated around the mean value. This suggests a higher level of uniformity in the image, where the range of pixel values is narrower and less varied. Consequently, images with lower variance tend to exhibit more consistent or uniform pixel distributions across the image. Conversely, a higher variance indicates a broader spread of pixel values, suggesting greater diversity in the intensity or color distribution within the image. This could signify regions of high contrast or more diverse color/shade variations throughout the image.

In the context of image encryption, changes in the variance of the histogram before and after encryption can indicate alterations in the distribution of pixel values. Significant shifts in variance post-encryption may signal modifications in the uniformity or spread of pixel values, which could potentially reveal changes in image content or characteristics.
Therefore, variance analysis provides a quantitative measure to assess the uniformity or variability of pixel values in an image's histogram, aiding in evaluating changes or patterns in pixel distributions before and after encryption or during any image processing.

The variance of a histogram is mathematically defined as:

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

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212049 |

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.

(b) Chi-square (χ2) Analysis: χ2 analyses can also be used 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, $v_e = (P \times Q)/256$, where PxQ is the dimension of image matrix.

The concept here refers to using the Chi-square test as a statistical method to assess the uniformity of a histogram's distribution. When conducting a Chi-square test for histogram analysis, a significance level (α) is chosen to determine the threshold for accepting or rejecting the null hypothesis. In this case, a commonly used significance level is $\alpha = 0.05$, implying that there is a 5% chance of rejecting the null hypothesis when it is actually true. The Chi-square test involves comparing observed and expected frequencies within different categories or bins of a histogram. For image analysis, the pixel values are often binned, and the observed frequencies of these values are compared against the expected frequencies (assuming a uniform distribution). The critical value of Chi-square (χ^2) at a significance level of 0.05 with degrees of freedom (d_f) determines the threshold for uniformity. The formula to calculate the critical value for a Chi-square distribution involves the significance level and degrees of freedom. For example, if the degrees of freedom are 20 (which could be related to the number of bins in the histogram), $\chi^2_{0.05}$ with 20 degrees of freedom is determined to be approximately 29.324783.

In the context of differential attacks on image encryption, different positions or alterations in the encrypted image are made. The Chi-square test is then used to compute the χ^2 values of the input (original) image and the χ^2 values of the encrypted image. By comparing these values, one can assess if there are significant deviations in the distribution of pixel values between the original and encrypted images. If the computed Chi-square value exceeds the critical value (e.g., 29.324783 with a significance level of 0.05 and 20 degrees of freedom), it suggests that the pixel distribution in the encrypted image differs significantly from what would be expected in a uniform distribution. This could indicate potential vulnerabilities in the encryption method, where alterations made during a differential attack can be detected through deviations in the pixel value distribution as captured by the Chi-square test.

The Chi-square test serves as a tool to quantify and detect deviations in the distribution of pixel values, aiding in assessing the effectiveness and robustness of an image encryption system against differential attacks.

(c) Correlation Analysis: Correlation analysis in the context of image encryption involves assessing the relationship between adjacent pixels in an image, both in the original (plain) image and in its encrypted form. In high-quality images, adjacent pixels tend to exhibit a strong correlation or relationship. This correlation implies that neighboring pixels have similar values, creating smoother transitions and more coherent visual information. This correlation could manifest in various ways, such as similar color intensities or grayscale values in neighboring regions. However, for a robust image encryption system, it's desirable that the encrypted image presents a low correlation between adjacent pixels. This low correlation means that neighboring pixels in the encrypted image should not have predictable or related values, rendering the encrypted data more complex and less susceptible to analysis. Correlation coefficient is mathematically defined as:

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

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

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212049 |

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

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

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.

The correlation coefficient is a statistical measure that quantifies the strength and direction of a relationship between two variables. In this case, the variables are the pixel values of adjacent pixels in an image. The correlation coefficient can range from -1 to 1:

- A correlation coefficient close to 1 indicates a strong positive correlation, where adjacent pixel values tend to move together in the same direction.
- A correlation coefficient close to -1 indicates a strong negative correlation, where adjacent pixel values tend to move in opposite directions.
- A correlation coefficient close to 0 suggests a weak or no linear relationship between adjacent pixel values.

In the context of image encryption, a good encryption system aims to disrupt or reduce the correlation between adjacent pixels in the encrypted image. Achieving a low correlation coefficient signifies that neighboring pixels in the encrypted image have less predictability or statistical relationship, making it harder for an attacker to decipher or extract meaningful information from the encrypted data.

Correlation analysis serves as a valuable tool to evaluate the quality and effectiveness of an image encryption system by quantifying the relationship between adjacent pixels, where a low correlation in the encrypted image indicates enhanced security against attempts to exploit pixel value patterns for decryption purposes.

(d) Information Entropy Analysis: Information entropy serves as a fundamental concept in assessing the uncertainty or unpredictability present in a system or dataset. In the context of cryptography and image encryption, information entropy analysis offers insights into the level of disorder or randomness within the encrypted data. The entropy of an ensemble—or a set of data—is a measure that quantifies the average information content within that ensemble. In other words, it gauges the amount of unpredictability or uncertainty within a given dataset. 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.

In cryptography, particularly symmetric cryptosystems used in image encryption, information entropy plays a crucial role in evaluating the strength and robustness of the encryption method. Higher entropy in the encrypted image implies a higher degree of disorder or randomness, making it more challenging for an attacker to extract meaningful information or discern any patterns within the encrypted data. Entropy, measured in bits or Shannons, represents the average amount of information or surprise associated with each element in the dataset. High entropy signifies greater unpredictability, suggesting a higher level of security in the encryption process. If an encrypted image has high entropy, it means that the pixel values are distributed in a more random or unpredictable manner, making it more resistant to decryption attempts. When analyzing an image encryption system, assessing the information entropy of the encrypted image provides valuable insights into the strength of the encryption algorithm. Higher entropy indicates a higher level of disorder and complexity, which are desirable traits in encryption as they make it more difficult for unauthorized entities to decipher the encrypted content. Information entropy analysis serves as an important parameter for evaluating

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212049 |

the quality and effectiveness of symmetric cryptosystems in image encryption, with higher entropy suggesting a higher level of security and unpredictability within the encrypted data.

(e) Differential Attack Analysis: This is a method used by cryptanalysts to exploit weaknesses in encryption algorithms, particularly in their sensitivity to small changes made in input data. This analysis aims to understand and detect patterns or relationships between plaintext and ciphertext when minimal alterations are introduced to the input data. In differential attacks, cryptanalysts work with pairs of related input-images that differ by a constant value. They encrypt these pairs and compare the differences in their corresponding encrypted-images, looking for statistical patterns or regularities in the distribution of these differences. The goal is to uncover any vulnerability that might allow an attacker to infer information about the encryption or the plaintext data. Attackers typically introduce subtle changes to the input-image and encrypt both the original and modified versions. By comparing these encrypted images, they aim to reveal any discernible relationships or patterns that may assist in breaking the encryption scheme. To quantitatively measure the differences between two encrypted images resulting from changes in the input-image, two parameters are commonly used:

1. **Number of Pixels Change Rate (NPCR):** This parameter calculates the percentage of pixels that differ between two encrypted images of the same original image. A higher NPCR suggests a greater variation between the encrypted images, indicating increased sensitivity to changes in the input data.
2. **Unified Average Changing Intensity (UACI):** UACI measures the average intensity or magnitude of the differences between corresponding pixels in the two encrypted images. It quantifies the overall change or discrepancy between the encrypted versions. Higher UACI values indicate more significant variations between the encrypted images resulting from changes in the input data.

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'.
These parameters serve as quantitative measures to assess the vulnerability of an encryption algorithm to differential attacks. A higher NPCR or UACI signifies greater sensitivity of the encryption system to changes in the input, which may suggest weaknesses that attackers could potentially exploit to gain insights into the encryption process or extract information from encrypted data. This analysis involves manipulating input data, encrypting the altered and original versions, and comparing the resulting encrypted images to identify potential vulnerabilities or patterns that could compromise the security of the encryption algorithm. Parameters like NPCR and UACI help quantify the differences between encrypted images resulting from changes in the input data, aiding in the assessment of encryption system robustness against differential attacks.

(f) Key Sensitivity Analysis: This assesses how encryption algorithms respond to slight variations or changes in the encryption keys. Attackers exploit key sensitivity to uncover vulnerabilities in encryption systems by examining how small differences in keys impact the encryption of input data. In this analysis, pairs of security keys that are related by a slight difference are used to encrypt the same input-images. By comparing the resulting encrypted images derived from these related keys, cryptanalysts aim to detect any statistical patterns or clues that could indicate weaknesses in the encryption scheme.

A robust encryption system should exhibit high key sensitivity, meaning that even a slight difference in the keys should lead to vastly different encrypted images for the same input. If the encrypted images significantly differ with minute variations in the keys, it implies that the encryption system is highly sensitive to key changes. This sensitivity is desirable as it prevents attackers from predicting or inferring relationships between keys and their corresponding encrypted data.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212049 |

To quantitatively assess key sensitivity, similar to differential attack analysis, parameters like Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are utilized:

1. **NPCR (Number of Pixels Change Rate):** Measures the percentage of different pixels between two encrypted images derived from slightly varied keys. A higher NPCR indicates greater differences between the encrypted images due to key variations.
2. **UACI (Unified Average Changing Intensity):** Quantifies the average intensity of differences between corresponding pixels in the encrypted images. Higher UACI values indicate more substantial variations resulting from slight changes in the keys.

The goal of key sensitivity analysis is to evaluate the extent to which an encryption system exhibits sensitivity to variations in keys. A cryptosystem with high key sensitivity will produce vastly different encrypted images when using slightly different keys to encrypt the same input. This robust behavior enhances security by making it difficult for attackers to exploit key relationships or predict the encrypted output based on slight changes in the encryption keys.

(g) Noise Analysis: Peak Signal-to-Noise Ratio (PSNR) is a measure used to evaluate the quality of a signal or an image corrupted by noise. It compares the original or uncorrupted signal's maximum power to the power of the noise-distorted or corrupted signal. The PSNR is calculated using the following formula:

$PSNR=10\times\log_{10}(MAX^2/MSE)$

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

where MAX represents the maximum possible pixel value of the image (for example, 255 in an 8-bit grayscale image or 1 in a normalized image). MSE (Mean Squared Error) is the average of the squared differences between the original and noisy signal or image. That is, 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.

The PSNR value is usually expressed in decibels (dB) and serves as a metric to quantify the quality of an image or signal after being affected by noise. A higher PSNR value indicates less distortion or noise in the corrupted signal compared to the original signal. In image processing and analysis, a higher PSNR suggests that the differences between the original image and the noisy image are relatively small or negligible to the human eye. Conversely, a lower PSNR value signifies more significant distortion or noise present in the corrupted image compared to the original. This measure is particularly useful in assessing the fidelity of an image after it has undergone various transformations, compression, or encryption processes that might introduce noise or distortions. In the context of noise analysis for image encryption, evaluating the PSNR helps to determine the extent of information loss or degradation in the encrypted image compared to the original, aiding in understanding the impact of encryption on image quality.

(h) Information Loss Analysis: This is crucial in evaluating the impact of encryption processes on image data. A good encryption system should maintain data integrity and prevent loss or degradation of information while encrypting or decrypting images. Various parameters and characteristics of the image are analyzed to assess if any loss or alteration of information has occurred due to encryption. These parameters include:

1. **Hue, Saturation, and Luminosity (HSL):** These parameters describe the color space of an image. Hue represents the type of color (e.g., red, blue), saturation measures the purity or intensity of the color, and luminosity defines the brightness. Mathematical operations on the image matrix compute these values.
2. **Resolution:** It refers to the dimensions of the image matrix, typically measured by the number of rows and columns in the matrix. For example, a color image with a resolution of 400x300x3 has 400 rows, 300 columns, and 3 color channels (R, G, B).
3. **Aspect Ratio:** This is the ratio of the number of rows to the number of columns in the image matrix, representing the image's proportions. A higher or lower aspect ratio might distort the image's shape.
4. **Contrast:** It measures the difference between the maximum and minimum pixel values in the image matrix. Higher contrast typically indicates a greater difference between light and dark areas in the image.
5. **Energy:** Defined as the sum of all pixel values in the image matrix, energy represents the overall intensity or magnitude of the image.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212049 |

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.

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

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

$$\text{Contrast} = \text{maximum}(I) - \text{minimum}(I), \quad \text{where I is the image.}$$

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

$$\text{Energy} = \text{sum}(I)$$

Performing analyses on these parameters enables the assessment of potential information loss or alterations that might occur during encryption and decryption processes. Changes in these characteristics compared to the original image could indicate degradation or loss of information caused by the encryption algorithm. By applying mathematical operations on the image matrix or using specific functions available in image processing libraries, these parameters can be computed and compared between the original and encrypted images. This analysis helps ensure that the encryption process maintains the integrity and fidelity of the image data, minimizing any potential loss or distortion during encryption and decryption operations.

(i) Robustness Analysis: Robustness analysis in image encryption focuses on assessing an encryption scheme's ability to withstand various attacks; including noise, occlusion, or clipping, and its capability to recover lost or altered information during transmission or storage. In the context of image encryption, robustness signifies the encryption method's resilience against data corruption, loss, or attacks that could occur during image transmission or processing. A robust encryption scheme should possess features that allow for the restoration or recovery of the original information, even if parts of it are lost, damaged, or affected by interference.

Key aspects of robustness analysis in image encryption include:

1. **Anti-Interference Ability:** Robustness serves as an important indicator of an encryption algorithm's resistance to interference, such as noise or transmission errors. Strong mathematical properties in the encryption method are essential to ensure that even if the image data is corrupted or partially lost during transmission, the decryption process can recover as much of the original information as possible.
2. **Information Recovery:** A robust encryption scheme should enable the recovery of the plain-image information despite data loss or corruption. This means that even if parts of the image are missing or damaged, the decryption process should still retrieve meaningful information from the encrypted data.
3. **Scrambling and Descrambling:** Encryption systems employing scrambling and descrambling techniques enhance robustness by introducing complexity and non-linearity in the encryption process. These techniques help maximize the encryption method's resistance to attacks or alterations while enabling efficient recovery of the original information during decryption.
4. **Mathematical Properties:** The robustness of an encryption system is deeply rooted in its underlying mathematical properties. Strong mathematical foundations and algorithms are crucial for ensuring that the encrypted data remains secure and recoverable despite potential attacks or data corruption.

Robustness analysis assesses how well an encryption scheme handles challenges such as noise, data loss, or deliberate attacks without compromising the integrity or recoverability of the encrypted information. Evaluating the algorithm's ability to restore information despite interference ensures that the encryption method can reliably protect and recover image data under adverse conditions, thereby reinforcing its effectiveness and reliability in real-world applications.

(j) Perceptual Analysis: Perceptual analysis in the context of image encryption delves into the visual and interpretative aspects of the encrypted images concerning the secret key used in the encryption process. A good encryption algorithm must exhibit sensitivity to changes in the secret key. Even a minor alteration in the secret key should result in a completely different output or encrypted image. This sensitivity ensures that the encrypted data is highly secure and that without the correct key, decrypting the data to recover the original image becomes extremely challenging or practically impossible.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212049 |

For instance, consider a scenario where a secret key is slightly modified:
Original key: (0.111111111111111, 0.111111111111110)
Modified key: (0.111111111111111, 0.111111111111111)
Despite the minute change in the last bit of the key, it results in a new and completely different key. This small alteration in the key generates a vastly different encryption, leading to a significantly distinct encrypted image.

The perceptual analysis of this scenario demonstrates that the correct key is crucial for accurately decrypting the encrypted image. With the correct key, the decryption should successfully restore the original image. However, even a slight change in the key—such as a single bit—results in a completely different decryption outcome. The wrong key fails to produce the original image due to the mathematical intricacies and sensitivity of the encryption algorithm. This level of sensitivity to the secret key is a fundamental characteristic of robust encryption systems. It ensures that without precise knowledge of the correct key, unauthorized decryption becomes exceedingly difficult, reinforcing the security and confidentiality of the encrypted image data.

(k) Keyspace, Algorithmic Complexity, and Speed Analyses: Keyspace, algorithmic complexity, and speed analyses are critical factors in evaluating the strength, efficiency, and security of image encryption algorithms.

1. **Keyspace:** Keyspace refers to the total number of possible unique keys that an encryption algorithm can generate. A larger keyspace implies a greater number of potential key combinations, making brute-force attacks more challenging for attackers. Brute-force attacks involve trying every possible key combination until the correct one is found. If the keyspace of an algorithm is significantly large, say greater than 2^100, it's considered robust against brute-force attacks because trying every possible key becomes computationally infeasible due to the vast number of combinations.
2. **Algorithmic Complexity:** Algorithmic complexity measures the number of essential iterations or operations required by an algorithm to execute a particular task. It gauges an algorithm's time complexity and speed. A lower algorithmic complexity often indicates faster execution and lower computational requirements, which are favorable attributes for efficient encryption algorithms.
3. **Encryption Efficiency:** Encryption efficiency assesses the running performance of an encryption scheme. It's a crucial measure to determine how efficiently an algorithm encrypts data concerning its execution time, computational resources, and speed. Efficiency can be evaluated based on factors such as the time taken to encrypt an image, the computational resources utilized, and the resulting data rate or speed of the encryption process. For chaotic encryption schemes specifically, the time-consuming computational operations often involve multiplying floating-point numbers. These operations significantly impact the time required for encryption.
4. **Speed or Data Rate:** The speed or data rate of encryption is computed by dividing the size of the image (in bits or bytes) by the execution speed of the encryption process. This metric quantifies how quickly an encryption algorithm can process and encrypt image data, providing insights into its efficiency in handling large amounts of data.

Analyzing keyspace, algorithmic complexity, and speed helps in comprehensively evaluating an encryption algorithm's strength, resistance to attacks, computational efficiency, and overall performance in securely encrypting image data. A balance between a large keyspace for security and efficient algorithmic complexity for speed and efficiency is essential in designing robust image encryption systems.

III. CONCLUSION

Visualizing and understanding cryptography and cryptanalysis through mathematical models is fundamental for professionals in these fields. Mathematical models provide a structured and flexible framework to comprehend the complexities of images, encryption techniques, and analysis methods. Mathematical models serve as blueprints for creating encryption algorithms. They provide a systematic way to conceptualize the encryption process, allowing developers to design algorithms with defined steps, logical operations, and mathematical functions. Models enable prior simulations and testing of encryption systems. Cryptographers can simulate various scenarios, manipulate parameters, and analyze the behavior of encryption algorithms under different conditions. This helps in understanding how the algorithms perform and behave before actual implementation. Mathematical models allow for rigorous verification of the correctness, security, and performance of encryption systems. By subjecting these models to mathematical analysis and scrutiny, cryptographers can verify their soundness and assess their security against potential attacks. Understanding cryptographic concepts through mathematical models enables experts to identify flaws, correct errors, and enhance existing encryption techniques. It provides a framework to build upon and develop new and more robust

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212049 |

encryption systems with improved security and performance. The use of mathematical interpretations facilitates a deeper understanding of image encryption concepts, allowing cryptographers to explore innovative ideas, devise novel encryption systems, and enhance the security and efficiency of cryptographic algorithms. This mathematical approach provides a solid foundation for continual advancement and innovation in the field of cryptography and contributes to the development of more secure and reliable encryption methods.

REFERENCES

[1] Bowen Zhang and Lingfeng Liu, "Chaos-Based Image Encryption: Review, Application, and Challenges", MDPI Mathematics 2023, 11, 2585, pp. 1-39.
[2] Unsub Zia, Mark McCartney, Bryan Scotney, Jorge Martinez, Mamun AbuTair, Jamshed Memon, Ali Sajjad, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains", International Journal of Information Security (2022) 21:917–935
[3] Sajitha A.S., A. Shobha Rekh, "Review on various image encryption schemes", Materials Today: Proceedings 58 (2022) 529–534
[4] 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 17, 2019.
[5] 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, July 25, 2019.
[6] Ratheesh Kumar R and Jabin Mathew, "Image Encryption: Traditional Methods vs Alternative methods",IEEE, Proceedings of the Fourth In-ternational Conference on Computing Methodologies and Commu-nication (ICCMC 2020), pp. 619-625, March 2020.
[7] Ratheesh Kumar R and Jabin Mathew, "How to Evaluate the Security and Performance of an Image Encryption System",International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Vol. 7 Issue 3, pp. 302-311, May-June 2020.
[8] Ratheesh Kumar R and Jabin Mathew, "A Mathematical Interpretation of Images and Image Encryption",International Journal ofMathematics Trends and Technology (IJMTT), Vol. 66.6 (2020):190-194.
[9] Ratheesh Kumar R and Jabin Mathew, "A System with 5-Level Security for Cloud Data and a Comparison of AES and 3DES", International Journal of Advanced Research in Engineering and Technology (IJARET), Volume 11, Issue 6, pp. 1046-1055, 2020.
[10] Ratheesh Kumar R and Jabin Mathew, "An Image Encryption Using Dynamic DNA Coding, Chaotic Map, And The Provision For Improved Robustness", Advances in Mathematics: Scientific Journal 9 (2020), no.10, pp. 8957–8967.
[11] Ratheesh Kumar R, "A Comparison of Two Image Encryption Algorithms with Chaotic Maps", International Journal of Scientific & Engineering Research Volume 12, Issue 12, December-2021, pp. 70-74.
[12] Ratheesh Kumar R, "A Comparison of Six DNA-based Cryptographic Methods", Science, Technology and Development, Volume X Issue XII DECEMBER 2021, pp. 358-361.
[13] 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, 2017.
[14] 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.
[15] 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, 2018.
[16] Xingbin Liu, Di Xiao, and Yanping Xiang, "Quantum Image Encryption Using Intra and Inter Bit Permutation Based on Logistic Map", IEEE Ac-cess, vol. 7, pp. 6937-6946, 2019.
[17] 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, 2019.
[18] Yuling Luo, Xue Ouyang, Junxiu Liu, and Lvchen Cao, "An Image Encryption Method Based on Elliptic Curve Elgamal Encryption and Cha-otic Systems", IEEE Access, vol. 7, pp. 38507–38522, 2019.
[19] Akram Belazi, Muhammad Talha, Sofiane Kharbech, and Wei Xiang, "Novel Medical Image Encryption Scheme Based on Chaos and DNA En-coding", IEEE Access, vol. 7, pp. 36667–36681, 2019.
[20] Chunhu Li, Guangchun Luo, and Chunbao Li, "An Image Encryption Scheme Based on The Three-dimensional Chaotic LogisticMap", Network Security, vol. 21, No.1, PP.22-29, 2019.
[21] Zhijuan Deng and Shaojun Zhong, "A Digital Image Encryption Algo-rithm Based on Chaotic Mapping", Algorithms Computational Technol-ogy, vol. 13, pp. 1–11, 2019.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 12, December 2023 ||

| DOI:10.15680/IJIRSET.2023.1212049 |

[22] Shikha Jaryal and Chetan Marwaha, "Comparative Analysis of Various ˙Image Encryption Techniques", Computational Intelligence Research, vol. 13, No. 2, pp. 273-284, 2017.
[23] 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.
[24] 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.
[25] 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.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details