International Journal of Scientific Research in Science, Engineering and Technology (www.ijsrset.com)
© 2020 IJSRSET | Volume 7 | Issue 3 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
DOI : https://doi.org/10.32628/IJSRSET207372

# How to Evaluate the Security and Performance of an Image Encryption System

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

## ABSTRACT

Almost all technical people know about images and image encryption, but some of them are not aware of the security and performance of the encryption systems. All image encryption systems are capable of encrypting the images, but some are not so secure. However, the question is how to evaluate the encryption systems. This paper gives you what are the analyses that are possible for evaluating the security and performance of the encryption systems. We hope this paper gives you an insight into Images, Image encryption, Security attacks, Noise and information loss, Evaluation Criteria, Analysis, Resistance, Key, Speed, Complexity, and other parameters.

**Keywords:** Plain-image, Encryption, Cipher, Security Attack, Noise, Occlusion, Robustness, Analysis, Key.

## I. INTRODUCTION

Security of images is an important practical issue because transmissions of images suffer from various security attacks and threats. Military images, medical images, remote-sensing images, etc. are of great worth both in money and content. Evaluating various image encryptions is always difficult. Subjectivity, lack of values of the analytical parameters, the algorithms' complexity levels, loss of information, the versatility of the domains, too many concepts related to keys, permutation and diffusion structures (PDS), etc., and time constraints make it complex [21].

There are various traditional image encryption techniques such as 3DES, AES, RSA, and ECC, various alternative techniques such as Chaos and DNA, and combinations of them. Traditional techniques are not so suitable for image encryption because they are sluggish, and cannot address the special features of images over text such as the huge data volume, 2D spatial distribution of pixels, multiple data redundancy, and high correlation between adjacent pixels. Alternative techniques such as Chaos, DNA, and the combinations can meet these requirements of the performance of the image encryption. But whatever the technique is used for the image encryption, we have to evaluate the security and performance of the encryption system. The history and evolution of images and image encryption have developed various analyses for the evaluation of image encryption systems.

These analyses are used as standards for comparing the image encryption systems. While some analyses apply to all image encryption systems, one analysis (NIST SP800-22 test) applies to chaotic image encryption systems. Security analyses are more important than the performance analyses because the security is superior to the performance. The systems without scrambling of pixels in the process do not have much robustness. From these ideas, we can say

that the image encryption systems with the combinations of DNA, Chaos, and scrambling can outperform all the other techniques of image encryption.

We have collected the information regarding the various analyses, used by the different scientists, that are scattered in the image encryption world, and are presenting here with the details and the examples. We hope the exemplification of analyses will provide the readers, the ideas of images, encryption, security, and performance, in depth.

## II. BACKGROUND

### A. Images

Pixel (Picture Element) is the smallest component of an image. Matrices of pixels are used to represent images. A grayscale image has the shades of the combination of black and white colors. A grayscale image has 8-bit pixels with 256 combinations of shades of gray. A color image has usually 24-bit pixels with 8 bits of Red (R), 8 bits of Green (G), 8 bits for Blue (B) information. RGB can create $2^{24}$ combinations of color. [21]

### B. Image encryption

Applications of valuable images include medical, military, and remote-sensing. The images may contain secret information, so security is essential to secure images from security threats and attacks, ensure integrity, and avoiding information loss. A good encryption system resists security attacks like brute-force, statistical, and differential attacks, tackles noise, occlusion, and information loss problems [21]. 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. Alternative techniques are superior to traditional techniques in image encryption. Whatever the technique used the whole image encryption problem and solution can be defined and viewed as a mathematical model. A good image encryption system will be free from cryptanalysis. This can be evaluated by comparing the plain-images, the cipher-images, and the decrypted images, and analysing the image encryption and decryption algorithms. The fields of image cryptography and image cryptanalysis improve their abilities to fight the other. Therefore, the evaluation is so important for image cryptography to defeat the image cryptanalysis.

### C. Attacks, Issues, and Concerns of Encryption

Images and image encryption techniques are prone to different security attacks, noise problems, occlusion or clipping menace, information loss, encryption or decryption speed, secret key issues, etc. Therefore, those who are dealing with images and image encryption must be very aware of these attacks, issues, and concerns. The following subsections explain the various attacks, issues, and concerns of the image encryption.

### D. Security Attacks

Mainly, there are three security attacks with images and image encryption, namely brute-force, statistical, and differential security attacks. Brute-force attacks - as its name implies the deduction of plain-image is based on trying all the possible combinations of keys. This approach is gaining popularity due to continuously increasing computational power which makes it easy to try all combinations in less time [23].

Statistical attacks - attackers try to derive and infer the meaningful information out of the cipher-images, i.e., they try to find the statistical relationship

between the pixels in the cipher-image, and between cipher-image and plain-image. Differential attacks - these can be considered as chosen plaintext attacks, where the attacker is given access to choose pairs of inputs and outputs of a cipher. The concept of difference can be varied and interpreted in many ways. For an encryption system, security is the prime concern. Therefore, security analyses are very important. There are keyspace analysis for verifying brute-force attacks, histogram, variance, chi-square, correlation, and information entropy analyses for verifying statistical attacks, and UACI and NPCR analyses for verifying differential attacks.

### E. Noise and Occlusion Attacks

When an image is encrypted or decrypted, or transmitted over the channel, certain information loss is inevitably caused by noise or network environment. Noise may result in information loss, and occlusion or clipping. PSNR, information loss, and robustness analyses are used to check the noise and occlusion attacks.

### F. Performance Issues of Key, Complexity, and Speed

'How much a key is sensitive in encryption?' is a core question in the encryption field. Another question is 'How fast the proposed encryption system?'. For analysing key, key sensitivity, and perceptual analyses are used. Computation of algorithmic complexity, and encryption and decryption times help evaluate the speed.

### G. Randomness Issue

An image encryption system is said to be very good encryption if the key possesses randomness to a greater extent. For this, NIST SP800-22 test helps and verifies the random numbers generated by the encryption.

## III. ANALYSES

Here, we are presenting the various analyses and their details. For better understanding and visualization, examples and their results are given. Tables and figures are shown to substantiate the analyses, and these tables and figures are real, i.e., they are the results of some recent image encryptions.

### A. Cipher-image Analysis

The following figure (Fig. 1) gives the visualization of the images of an example. In the figure, the images (named grayimage1, colorimage1, grayimage2, and colorimage2) in the first column are the plain-images (input). The first and the second images are grayscale and color images equivalent, and the third and the fourth images are grayscale and color images equivalent. Their dimensions are 128×128, 128×128, 200×200, and 200×200 respectively. The images in the second column are the cipher-images of the respective plain-images. The attacker cannot get any meaningful information from the cipher-images. The images in the third column are the decrypted images of the cipher-images.

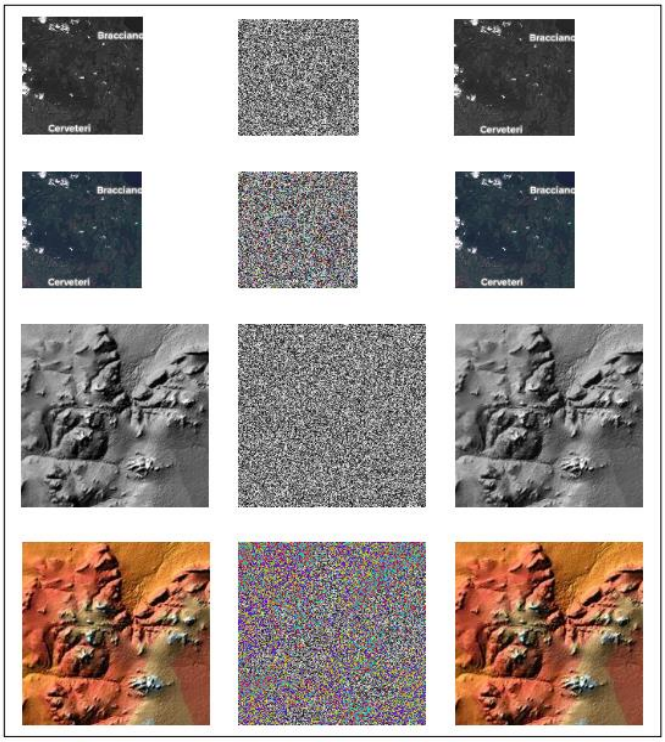


Fig. 1: Plain-images, cipher-images and decrypted images

### B. Histogram Analysis

Image histogram reveals the pixel value distribution by counting the number of each gray-level value. The ideal image encryption guarantees the uniform frequency distribution of the cipher-image, which

provides as little statistical information as possible for the attacker [21].

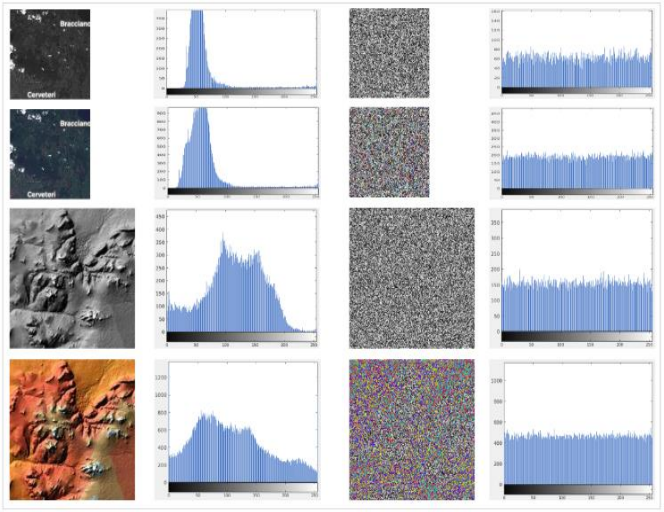


Fig. 2: Plain-images, cipher-images and their histograms

Example: The above figure (Fig. 2) shows plain-images have the concentration on some pixel values while cipher-images have a fairly uniform distribution.

### C. Variance Analysis

The variance of histograms is 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 defined as:

$$var(Z) = \frac{1}{256^2}\sum_{i=1}^{256}\sum_{j=1}^{256}\frac{1}{2}(z_i - z_j)^2$$

where Z is the vector of the histogram values, and $Z=\{z_1,z_2,...,z_{256}\}$. $z_i$ and $z_j$ are the numbers of pixels which values are equal to $i$ and $j$ respectively [14].
Example: we calculate variances of histograms of plain-images and their cipher-images and report them in the following tables.

| | Variance Values for grayimage2 | |
|---|---|---|
| | Plain-image | Cipher-image |
| | 11843 | 144 |

| | Variance Values for colorimage2 | |
|---|---|---|
| | Plain-image | Cipher-image |
| R | 8482 | 155 |
| G | 16844 | 136 |
| B | 47988 | 130 |

Variances of ciphers are much smaller than those of plain-images. Therefore, we conclude that the example cryptosystem can resist statistical attacks.

### D. Chi-square (χ2) Analysis

We can also use χ2 tests to verify whether the histogram distribution is uniform, and the χ2 value is calculated by:

$$\chi^2 = \sum_{i=0}^{255}\frac{(v_i - v_0)^2}{v_0}$$

$i$ 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. $v_0$ is the expected frequency of a pixel value $i$, $v_0 = (P\times Q)/256$.

Note: commonly used significant level is $\alpha = 0.05$, and $\chi^2_{0.05} = 293.24783$. Therefore, we think that the histogram distribution is uniform in the case of significant horizontal $\alpha = 0.05$. Various differential attack positions are selected and the above equation is used to detect the χ2 value of plaintext image and the χ2 value of ciphertext image. [20]

Example: two set of test results are shown in the following tables.

| | $\chi^2$ Values of grayimage2 | |
|---|---|---|
| | Plain-image | Cipher-image |
| | 19404 | 252 |

| | $\chi^2$ Values of colorimage2 | |
|---|---|---|
| | Plain-image | Cipher-image |
| R | 13897 | 255 |
| G | 27597 | 223 |
| B | 78624 | 212 |

From the tables, the χ2 value of plain-image is very large, but through the usual encryptions, the χ2 value of cipher is very small. Under the confidence level $\alpha = 0.05$, the χ2 values are all less than 293.24783, so we conclude that the histogram distribution is uniform under the confidence level $\alpha = 0.05$.

### E. Correlation Analysis

For high-quality images, adjacent pixels are very close to each other. Therefore, the correlation of the visual image is very high. The cipher encrypted by a good cryptosystem should exhibit a very low correlation of two adjacent pixels. Correlation coefficient is a numerical measure to assess a statistical relationship between variables. The correlation coefficient can be defined as:

$$EM = \frac{1}{N}\sum_{i=1}^{N} a_i$$

$$EV(a) = \frac{1}{N}\sum_{i=1}^{N}(a_i - EM(a))^2$$

$$EC(a,b) = \frac{1}{N}\sum_{i=1}^{N}(a_i - EM(a))(b_i - EM(b))$$

$$cc_{ab} = \frac{EC(a,b)}{\sqrt{EV(a)}\sqrt{EV(b)}}$$

where *a, b* are values of adjacent pixels. *N* is the number of pixels selected from the plain-/cipher-image. *EM* is the estimation of mathematical expectation and *EV(a)* is the estimation of the variance of *a*. *EC(a,b)* is the estimation of co-variance between *a* and *b*. $cc_{ab}$ represents the correlation coefficient of the image. Correlation distributions of plain-images are concentrated, and those of ciphers are fairly uniform. [21] A good cryptosystem can effectively reduce the correlation between two adjacent pixels along three different directions. We have the coefficients for the images and their ciphers of an example cryptosystem along with horizontal, vertical, and diagonal directions; results are listed in the table.

| | Correlation Coefficients | | | | | |
|---|---|---|---|---|---|---|
| | Plain-image | | | Cipher-image | | |
| Image | CC-D | CC-H | CC-V | CC-D | CC-H | CC-V |
| grayimage1 | 0.6801 | 0.7716 | 0.7666 | 0.0004 | 0.0014 | 0.0078 |
| colorimage1 | 0.6929 | 0.7764 | 0.7835 | -0.0013 | -0.0015 | -0.0027 |
| grayimage2 | 0.7323 | 0.8766 | 0.8666 | -0.0021 | -0.0134 | 0.0025 |
| colorimage2 | 0.8334 | 0.9219 | 0.9170 | -0.0008 | -0.0012 | 0.0010 |

Correlation coefficients of plain-images are closer to 1, on the other hand, those of ciphers are closer to 0. Therefore, the attacker cannot get useful correlation information to break up the cryptosystem.

### F. Information Entropy Analysis

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

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

where $p(x_i)$ is the probability of the symbol $x_i$. The ideal entropy is equal to 8 for the cipher-image with $2^8$ or 256 gray-levels. Larger entropy indicates less information content. [21]

| | Information Entropy | |
|---|---|---|
| Image | Plain-image | Cipher-image |
| grayimage1 | 5.9419 | 7.9872 |
| colorimage1 | 6.4109 | 7.9958 |
| grayimage2 | 7.5853 | 7.9954 |
| colorimage2 | 7.8076 | 7.9985 |

Example: the above table reports information entropy of plain-images and their ciphers encrypted by the image cryptosystem. Results show that the cryptosystem barely reveals any image information.

### G. Differential Analysis

The differential attack is an efficient method to use pairs of plain-images related by a constant difference and compare the difference of the corresponding ciphers for statistical patterns in their distribution. Usually, attackers make a tiny change in the plain-image and use the algorithm to encrypt the image before and after any changes. Then they try to find out the relationship between the plain image and the cipher. The differential analysis assesses sensitivity to the plain-image. Number of pixels change rate (NPCR) and unified average changing intensity (UACI) are two parameters to measure the difference between ciphers. NPCR calculates the percentage of different pixel numbers between two images. UACI calculates the average intensity of the difference between the two images. NPCR and UACI are defined as:

$$B(i,j) = \begin{cases} 0, & C_1(i,j)=C_2(i,j) \\ 1, & C_1(i,j)\neq C_2(i,j) \end{cases}$$

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

$$UACI = \frac{1}{P \times Q} \times \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%$$

where $P \times Q$ is the size of images $C_1$ and $C_2$. The following table reports results of NPCR and UACI which are closer to reference values [21].

| Differential Attack Analysis | | |
|---|---|---|
| Image | NPCR | UACI |
| grayimage1 | 0.9957 | 0.3304 |
| colorimage1 | 0.9963 | 0.3347 |
| grayimage2 | 0.9963 | 0.3365 |
| colorimage2 | 0.9961 | 0.3341 |

Results show that the example algorithm can resist differential attack, since the reference values of NPCR and UACI are 99.6093% and 33.4635% respectively.

### H. Key Sensitivity Analysis

As a common attack technique, key sensitivity analysis uses pairs of security keys related by a slight difference to encrypt images and calculates the differences of the corresponding ciphers for statistical clues. High key-sensitivity means, the cryptosystem with two slightly different keys encrypts the same image and gets utterly different ciphers. The differences can be quantified by NPCR and UACI [14]. Example: results of NPCR and UACI for key sensitivity analysis are reported in the following table, which indicates the significant difference between two ciphers.

| Key Sensitivity Analysis | | |
|---|---|---|
| Image | NPCR | UACI |
| grayimage2 | 0.9962 | 0.3319 |

### I. Noise and Information Loss Analysis

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

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

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 system must not suffer from information loss due to noise or algorithm while encryption and/or decryption. To check whether the information loss has occurred or not, we have to perform the analysis of hue, saturation, luminosity, RGB, resolution, aspect ratio, energy, contrast, etc. [21].

The definitions of hue, saturation, and luminosity are complex. There are libraries in image processing languages to compute HSL 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 300x200x3; 300 is the number of rows, 200 is the number of columns, and 3 is the number of color channels. If the image is color, 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 divided by the number of columns.

$$AR = M/N$$

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

$C = max(I) - min(I)$, where I is the image.

Energy of an image is the total sum of all the pixel values in the image matrix.

$$E=sum(I)$$

Example: The following table gives the noise and information loss analyses for colorimage2. From these values, we can say that the cryptosystem has no noise and information loss problems in encryption and decryption.

**Noise and Information Loss Analyses**

| | Hue | Saturation | Luminosity | R | G | B | Resolution | Aspect ratio |
|---|---|---|---|---|---|---|---|---|
| **Plain-image** | 0.0667 | 0.7143 | 0.8235 | 210 | 120 | 60 | 200x200x3 | 1 |
| **Cipher-image** | 0.5488 | 0.9216 | 0.8 | 16 | 149 | 204 | 200x200x3 | 1 |
| **Decrypted image** | 0.0667 | 0.7143 | 0.8235 | 210 | 120 | 60 | 200x200x3 | 1 |

| | PSNR of image | Contrast | Energy | PSNR (img/img) |
|---|---|---|---|---|
| **Plain-image** | 11.9341 | 255 | $1.2737x10^7$ | P/C : 8.1040 |
| **Cipher-image** | 10.761 | 255 | $1.5322x10^7$ | P/D : ∞ |
| **Decrypted image** | 11.9341 | 255 | $1.2737x10^7$ | D/C : 8.1040 |

## J. Robustness Analysis

Images may suffer from occlusion or clipping attacks. A good encryption scheme has a provision for restoring and reclaiming the information lost. That is, robustness is an important characteristic of image encryption methods. Robustness is an important index to test the anti-interference ability of cryptography.

In the process of transmission, the information may be lost or polluted by noise, so it is necessary to design an encryption algorithm to address this issue. Even if part of the information is lost, the part of the plain-image information can be obtained by decrypting the program. We detect the robustness of the example method by clipping attack and noise pollution.

Example: The following figure shows a different degree of clipping attack in grayimage2, we can see that although the cipher-image has lost some information, some plain-image information can also be obtained through the decryption algorithm, i.e., the algorithm supports robustness to some extent. [20]

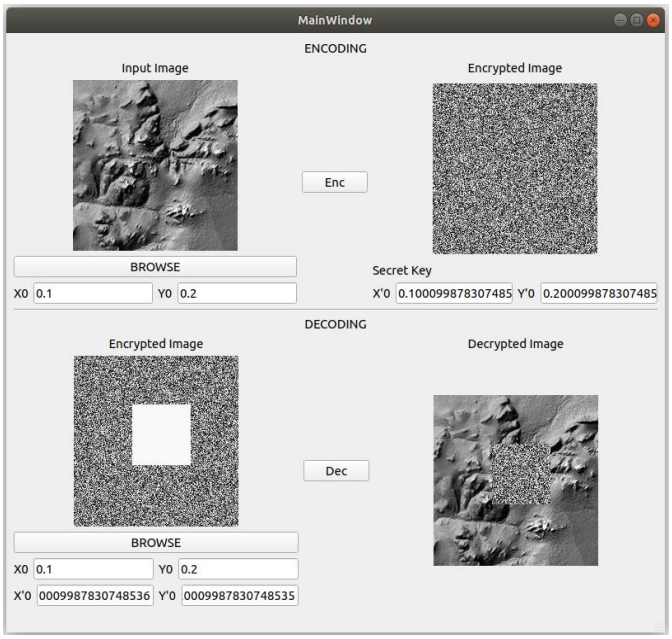



Fig. 3: Robustness Analysis

In the examples below, the systems with scrambling and descrambling help maximizing the robustness.

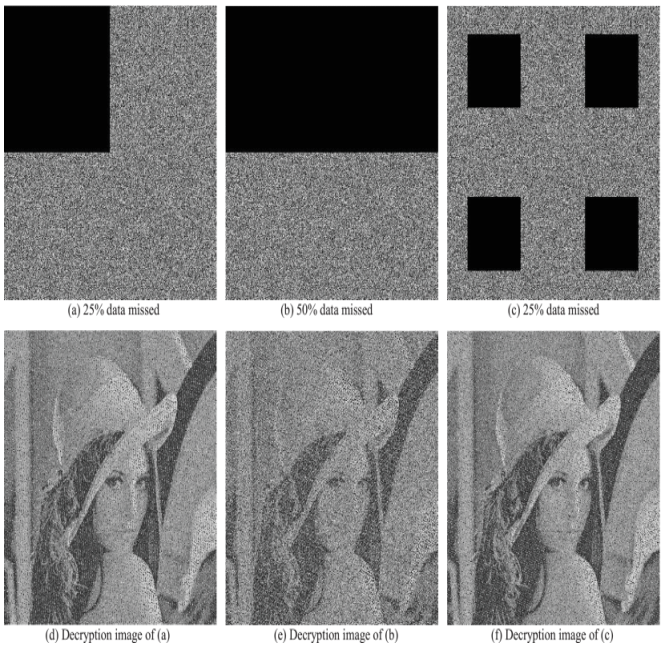



Fig. 4: Robustness Analysis (Image courtesy: [20])

Another example: the maximum robustness can be achieved and viewed as follows:

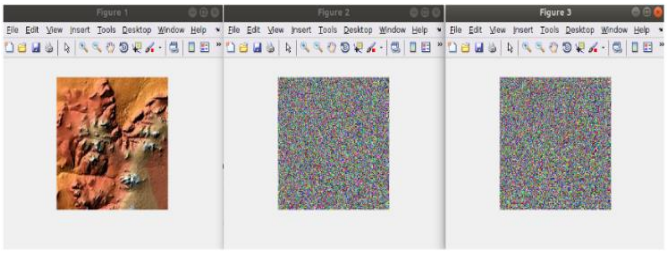


Fig. 5: Plain-image, cipher-image, scrambled cipher

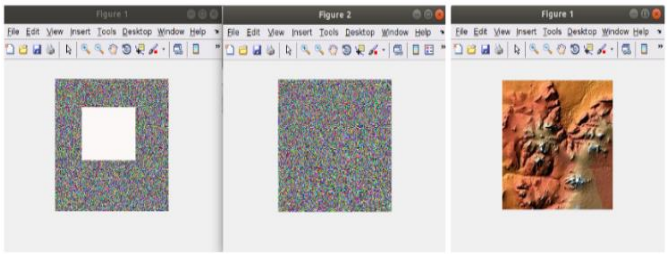


Fig. 6: Clipped cipher, descrambled cipher, decrypted image

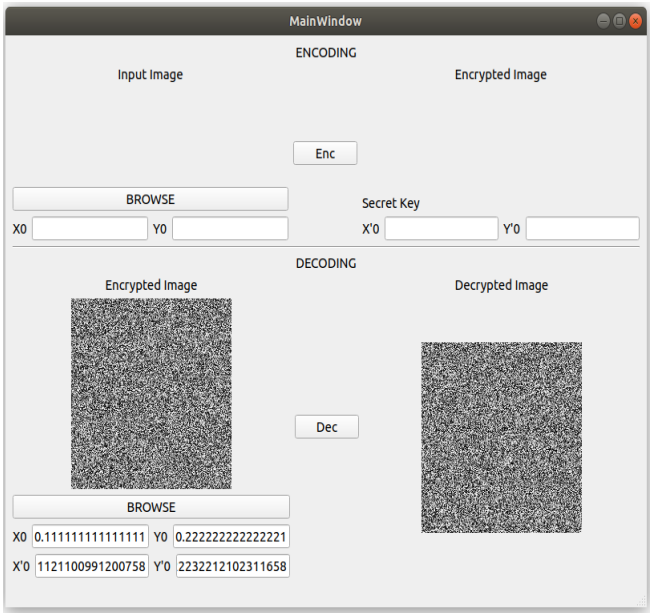



Fig. 7: Perceptual Analysis

## K. Perceptual Analysis

A good algorithm is sensitive to the secret key. To make a small change in the key, and then restore, we get a different result.

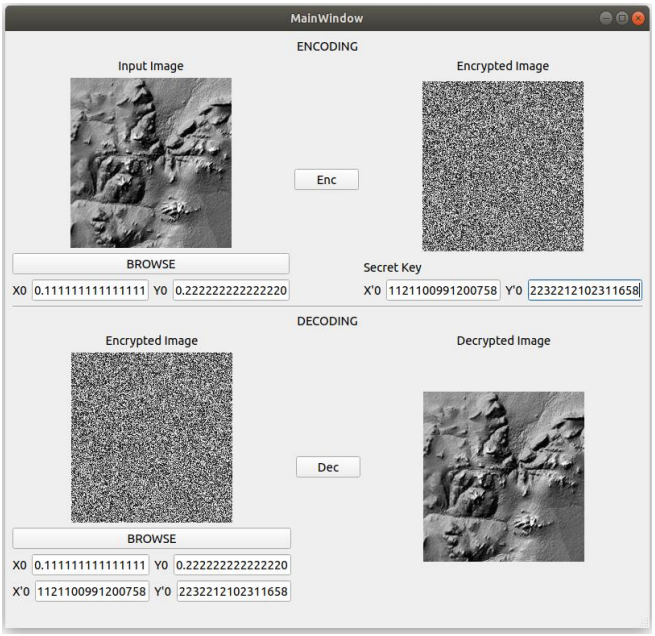
Example: key is selected to change one bit,

key = (0.111111111111111, 0.222222222222220)

Change the last bit of the key to generate a new key:

new key = (0.111111111111111, 0.222222222222221)

Restore by the correct secret key and the wrong secret key, respectively, and the results are shown in the following figure. The wrong key does not produce the image back.




## L. Keyspace, Complexity and Speed Analyses

The keyspace is the number of key combinations. An image encryption scheme is said to be good if its keyspace is greater than $2^{100}$. Example: in a cryptosystem, the key has 6 variables, the algorithm has a keyspace which is $> 2^{300}$. Therefore, the system can resist brute-force attacks. Complexity is the number of vital iterations. It is the measure of an algorithm's speed. Encryption efficiency analysis assesses the running performance of encryption. Efficiency is an important measure to assess the running performance of the encryption. For analyses of chaos-based encryptions, the time-consuming part in computations is the operation of multiplying floating point numbers [14].

The algorithm also must have an acceptable running speed. We can find the execution times for encryption and decryption, and analyse them. Example: The keyspace, complexity, and speed (grayimage2 and colorimage2) are shown in the table.

| Keyspace | Complexity | | Speed (200x200 images) | | | |
|---|---|---|---|---|---|---|
| | Grayscale SS | Color SS | Grayscale SS | | Color SS | |
| | | | Enc | Dec | Enc | Dec |
| $> 2^{300}$ | $6 \times M \times N$ | $18 \times M \times N$ | 70s | 50s | 175s | 164s |

## M. NIST SP800-22 Test

To measure the randomness of the CPRNG sequences, we can use the NIST SP800–22 statistical test suite,

which consists of 15 statistical tests. Each test result is converted to a p-value for judgment, and when applying the NIST test suite, a significance level $\alpha = 0.01$ is chosen for testing. If the p-value $\geq \alpha$, then the test sequence is considered to be pseudo-random [22]. The following test result is an example, with image courtesy.

| Test name | | P-value | Result |
|---|---|---|---|
| Frequency | | 0.9801 | Success |
| Block-frequency | | 0.2775 | Success |
| Runs | | 0.3160 | Success |
| Long runs of ones | | 0.3954 | Success |
| Rank | | 0.0296 | Success |
| Spectral DFT | | 0.1550 | Success |
| No overlapping templates | | 0.9967 | Success |
| Overlapping templates | | 0.4514 | Success |
| Universal | | 0.6556 | Success |
| Linear complexity | | 0.9056 | Success |
| Serial | P-value1 | 0.9266 | Success |
| Serial | P-value2 | 0.7865 | Success |
| Approximate entropy | | 0.6375 | Success |
| Cumulative sums forward | | 0.5436 | Success |
| Cumulative sums reverse | | 0.5651 | Success |
| Random excursions | X = -4 | 0.7220 | Success |
| | X = -3 | 0.7752 | Success |
| | X = -2 | 0.2677 | Success |
| | X = -1 | 0.2656 | Success |
| | X = 1 | 0.1007 | Success |
| | X = 2 | 0.3482 | Success |
| | X = 3 | 0.4977 | Success |
| | X = 4 | 0.5168 | Success |
| Random excursions variant | X = -9 | 0.2492 | Success |
| | X = -8 | 0.1723 | Success |
| | X = -7 | 0.2026 | Success |
| | X = -6 | 0.4146 | Success |
| | X = -5 | 0.4073 | Success |
| | X = -4 | 0.3178 | Success |
| | X = -3 | 0.3753 | Success |
| | X = -2 | 0.6367 | Success |
| | X = -1 | 0.4315 | Success |
| | X = 1 | 0.6596 | Success |
| | X = 2 | 0.7163 | Success |
| | X = 3 | 0.6525 | Success |
| | X = 4 | 0.4903 | Success |
| | X = 5 | 0.3089 | Success |
| | X = 6 | 0.2110 | Success |
| | X = 7 | 0.1905 | Success |
| | X = 8 | 0.1267 | Success |
| | X = 9 | 0.1269 | Success |

https://doi.org/10.1371/journal.pone.0184586.t009

## IV. CONCLUSION

The analyses and their examples and results explained above provide us an insight into the images, encryption, and security. This may help us to discover more analyses to evaluate image encryption systems. We hope more image encryption systems with easier and cheaper implementation but with high security and performance will emerge.

## V. 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, 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, 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, 21-319, 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, 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.

**Cite this article as :**

Ratheesh Kumar R, 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), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 7 Issue 3, pp. 302-311, May-June 2020. Available at doi : https://doi.org/10.32628/IJSRSET207372
Journal URL : http://ijsrset.com/IJSRSET207372