Artificial & Computational Intelligence / Published Online : March 2020
https://acors.org/ijacoi/VOL1_ISSUE2_08.pdf

Artificial & Computational Intelligence

# A Comprehensive Review on Various Image Encryption Techniques Using Different Parameters

Gaurav Mittal[1], Manish Gupta[2]
Department of Computer Science and Engineering
[1]gauravmittal2903@gmail.com, [2]manishgupta.2007@gmail.com
VITM, Gwalior, India

**Abstract**

Nowadays the uses of internet and social media plateforms are increases day-by-day. This is because of the increases use of smart phones. Most of the communications via smart phones are in the form of images. So there is a need of lightweight, secure and fast image encryption algorithm. This work presents a comprehensive study of various image encryption techniques on different parameters such as NPCR, UACI, horizontal correlation, vertical correlation, diagonal correlation and entropy. This work concludes by discussing the major advancements in the field of image cryptography and future challenges.

**Keywords:** Image Encryption, Image Decryption, NPCR, UACI, Entropy, Histogram.

## 1. Introduction

With the advent of the Internet and the World Wide Web, the amount of digital information to be stored and communicated has grown exponentially beyond imagination. This digital information not only comprises text but also has a large volume of an image, audio/video, and multimedia data, which comparatively is very bulky than the textual information. The images as on date have become an integral and vital component of any useful data and are widely used in several important applications. Few of these crucial applications include Military Image Database & Message Communication, Confidential Video Conferencing, Medical Imaging System & Telemedicine, Online Personal Photograph Albums, Natural Disaster or Catastrophe Alarming Systems, Online Image Identification and Authentication, Reflection Seismology, Electronic Surveillance Systems, Document Imaging, Image 'CAPTCHA', Image Registration, Geographic Information System, etc.

The uses of smartphones are increasing day by day and a lot of images are transmitted regularly to thousands of people via social media websites and apps. So an exchange of secure images over the communication network becomes a serious issue [1]. Various traditional encryption algorithms such as RSA, AES, IDEA, Diffie-Hellman, etc have been developed, but the efficiency of these algorithms for image encryption is less due to higher redundancy and higher correlation among pixels.

## 2. Evaluation Measures

Evaluation measures are the pillars of any image encryption technique. This section explores the following measures for checking the randomness of various techniques discussed here.

### a) NPCR and UACI

The following formula is used to measure the value of NPCR-

$$\text{NPCR} = \frac{\sum_{j,i} D(j,i)}{H \times W} * 100\ \%$$

Where W represents width and H represents the Height of the image.

D(j, i) is defined as

$$D(j,i) = \begin{cases} 0, & \text{if } C1(j,i) = C2(j,i) \\ 1, & \text{Otherwise} \end{cases}$$

While UACI is measured by using the following formula:

$$UACI = \frac{1}{H\,X\,W} \sum_{i,j} \left[ \frac{C1(j,i) - C2(j,i)}{255} \right] * 255 )$$

**b) Correlation analysis**

The following formulas are used to calculate horizontal, vertical and diagonal correlation –

$$Cov(x,y) = E\big(x - E(X)\big)\big(y - E(y)\big)$$

$$R_{xy} = \frac{Cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

The following three formulas are used in numerical computations, where x and y are the values of two adjacent pixels in the image.

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

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

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

**c) Entropy:**

It is a statistical measure of randomness that can be used to characterize the texture of the input image. For calculating entropy, the following formula is used –

$$E(m) = \sum_{j=0}^{M-1} p(m_j) \log \frac{1}{p(m_j)}$$

## 3. Performance Analysis:

This section desribes the performance analysis on various measures described above. For performance analysis of vaious image encryption techniques, a well known Lenna image is considered. Table 1 shows the comparitive study of various existing image encryption techniques on different parameters.

## 4. Conclusion

This work presents comprehensive review on latest image encryption techniques using different parameters. It has been obsered that still security becomes the major issue behind researchers. These techniques performs well on various randomness parameters but are not lightweight, secure and fast. In coming days, The uses of IoT enabled devices are increasing exponentially and these devices use only those applications which are fast, secure and light weight. The future challenge is to design a robust algorithm that is fast, secure and requies less memory in IoT enabled devices.

**References**


[1] Usman, M., Ahmed, I., Aslam, M., Khan S. and Shah, U., SIT: A Lightweight Encryption Algorithm for Secure Internet of Things. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 1, 2017.

[2] Xiao S, Yu Z, Deng Y. Design and analysis of a novel chaos-based image encryption algorithm via switch control mechanism. Security and Communication Networks (2020). https://doi.org/10.1155/2020/7913061.

[3] Premkumar R, Anand S. Secured and compounded 3-D chaos image encryption using hybrid mutation and crossover operator. Multimedia tools and Appl (2018). https://doi.org/10.1007/s11042-018-6534-z

[4] Liu H, Zhao B, Huang L. A novel quantum image encryption algorithm based on crossover operation and mutation operation. Multimedia Tools and Appl (2019). https://doi.org/10.1007/s11042-019-7186-3.

[5] Li C, Luo G, Li C (2018) A parallel image encryption algorithm based on chaotic Duffing oscillators. Multimed Tools Appl 77(15):19193–19208.

[6] Chai X, Gan Z, Zhang M (2017) A fast chaos-based image encryption scheme with a novel plain image-related swapping block permutation and block diffusion. Multimed Tools Appl 76(14):15561–15585

[7] Zhang Y, Tang Y (2017) A plaintext-related image encryption algorithm based on chaos. Multimed Tools Appl 77:1–23

[8] Huang X, Ye G (2018) An image encryption algorithm based on irregular wave representation. Multimed Tools Appl 77(2):2611–2628

[9] Chai X, Yang K, Gan Z (2017) A new chaos-based

image encryption algorithm with dynamic key selection mechanisms. Multimed Tools Appl 76(7):9907–9927

[10] Chai X (2017) An image encryption algorithm based on bit level brownian motion and new chaotic systems. Multimed Tools Appl 76(1):1159–1175

[11] Mollaeefar M, Sharif A, Nazari M (2017) A novel encryption scheme for colored image based on high level chaotic maps. Multimed Tools Appl 76(1):607–629

[12] Tang Z, Wang F, Zhang X (2017) Image encryption based on random projection partition and chaotic system. Multimed Tools Appl 76(6):8257–8283

[13] Liu L, Miao S (2017) An image encryption algorithm based on baker map with varying parameter. Multimed Tools Appl 76(15):16511–16527

[14] Zhu J, Yang X, Meng X, Wang Y, Yin Y, Sun X, Dong G (2018) Optical image encryption scheme with multiple light paths based on compressive ghost imaging. J Mod Opt 65(3):306–313.

[15] Wu J, Zhang M, Zhou N (2017) Image encryption scheme based on random fractional discrete cosine transform and dependent scrambling and diffusion. J Mod Opt 64(4):334–346

[16] Li H, Wang Y (2008) Double-image encryption by iterative phase retrieval algorithm in fractional Fourier domain. J Mod Opt 55(21):3601–3609

[17] Wang X, Teng L, Qin X (2012) A novel colour image encryption algorithm based on chaos. Signal Process 92(4):1101–1108

Table 1 shows the performance analysis of various image encryption techniques on Lenna Image

| Existing techniques | NPCR | UACI | Diagonal correlation | Vertical coorelation | Horizontal correlation | Entropy |
|---|---|---|---|---|---|---|
| Ref [2] | 99.6063 | 33.4621 | 0.0005 | 0.0014 | -0.0011 | 7.9974 |
| Ref [3] | 99.7453 | 33.4021 | -0.0015 | 0.0001 | -0.0002 | 7.924 |
| Ref [4] | 99.6102 | 33.3915 | 0.000019 | 0.000108 | 0.000882 | 7.9974 |
| Ref [5] | 99.629 | 38.572 | 0.0006 | 0.0019 | 0.0021 | 7.9986 |
| Ref [6] | 99.730 | 33.55 | 0.0012 | 0.0151 | 0.0044 | 7.9984 |
| Ref [7] | 99.609 | 33.463 | -0.0193 | -0.0226 | -0.0245 | 7.9899 |
| Ref [8] | 99.6090 | 33.429 | 0.0277 | 0.0039 | 0.0172 | 7.9917 |
| Ref [9] | 99.419 | 33.641 | 8.3962e-04 | -1.8380e-04 | 0.0210 | 7.9973 |
| Ref [10] | 99.620 | 33.450 | 0.0277 | 0.0039 | 0.0172 | 7.9993 |
| Ref [11] | 99.683 | 33.530 | 0.0009 | 0.0025 | 0.0030 | 7.9973 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Ref [12] | 99.589 | 33.526 | 0.0003 | 0.0002 | 0.0003 | 7.9971 |
| Ref [13] | 99.690 | 33.510 | 0.0043 | 0.0021 | 0.0042 | 7.9995 |
| Ref [14] | 93.790 | 16.780 | 0.0259 | 0.0232 | 0.0012 | 7.9959 |
| Ref [15] | 98.798 | 33.648 | 0.0007 | 0.0011 | 0.0021 | 7.9972 |
| Ref [16] | 99.683 | 33.530 | 0.0009 | 0.0025 | 0.0030 | 7.9973 |
| Ref [17] | 99.610 | 33.550 | -0.0125 | -0.0102 | -0.0086 | 7.9991 |