IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 4, April 2021

DOI: 10.17148/IARJSET.2021.8463

# Comparative Study of Image Encryption Techniques

**Malika Acharya[1], Rama Shankar Sharma[2]**

Master of Technology, Department of Computer Science, Rajasthan Technical University, Kota, India[1]

Associate Professor, Department of Computer Science, Rajasthan Technical University, Kota, India[2]

**Abstract**: Internet has made the path of information easy and convenient, yet it has put security of information at stake. The use of critical information by adversary can be catastrophic and hence security of information is rather a necessity than the facade. Images play an indispensable part in information exchange. Their role in the field of military, architecture, medicine, communication cannot be undermined. Image information hiding is broadly divided in two categories , first, image watermarking and second image cryptography. Over recent years, image encryption has gained much attention. The paper gives a brief insight of different image encryption techniques that have been proposed in recent years.

**Keywords**: Image encryption, chaotic maps, pseudo random generators, blockchain, block ciphers, stream ciphers.

## I. INTRODUCTION

With the development of multimedia technology, images occupy copious fractions in the storage and transmission sphere. Their stakes in the field of communication especially in military, medical, government offices etc, is indelible. Also the hitherto unreliable network poses an alarming concern with respect to their confidentiality and security. In the past decade it has become a hotspot for researchers. Images have unique properties of bulk data capacity, high correlation among pixels, high redundancy. Image encryption has successfully garnered researcher's attention owing to some differences in image and text data encryption.

Image encryption techniques called naïve algorithms tend to convert two dimensional image format to one dimensional stream These algorithms have proven their worth in many applications but they also pose some critical issues [1], like bulk data capacity, high correlation between pixels. The traditional algorithms are slow in speed Secondly, compression after encryption or compression before encryption. Encryption algorithms sought are desired to meet the following requirements [2]:

1. Reduced computational complexity
2. Compression ratio
3. Format compliance
4. Bit error tolerance

This paper is further accentuated in sections with section II dealing with various evaluation metrics, section III dwells on background study of the various image encryption techniques, section IV is a brief discussion of our inference from the study and section V concludes the review.

## II. EVALUATION METRICS

Images are of two types: a.)Gray scale images. B.)Color images. Gray scale images, (monochrome images/one-color) require 8 bits/pixel data i.e. 256 values in the range [0-255], which is generally called intensity of pixel. They require less information for the pixel representation. Binary image is a special case of gray scale image that requires only 1 binary digit for pixel representation (i.e. black /white, or 0/1). Hence they are also called as 1-bit images. They are obtained via threshold operation. Color images (three-band monochrome images) each band corresponds to different colors. Commonly used color space is RGB color space that uses 24 bits/pixel (8 bits for each color). Multispectral images are images outside human perceptual range for example, infrared, ultraviolet, X-ray, acoustic radar etc. Their information is not directly perceptible but could be deduced on careful mapping with RGB components.

Image encryption can be complete encryption or partial encryption. Complete Encryption encrypts image as complete. The symmetric encryption is preferred for encryption of raw/ compressed data. The schematic diagram of complete encryption is shown in Fig1.The partial encryption deals with encrypting only a part of the image and the rest of the content remain unchanged. The schematic diagram of the partial encryption is illustrated in Fig2. Partial domain involves majorly two categories: a.) Region based encryption. b.)Bit plane encryption. While in region based encryption, the region of interest is first selected then the part is encrypted, the bit plane based technique involves the division of the image into bit-planes and then encryption of only some bit-planes. The combination of encrypted and decrypted regions form the resultant output as in **[Figure-2]**.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 4, April 2021

DOI: 10.17148/IARJSET.2021.8463

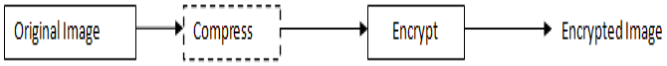


Fig1: Complete Encryption Process.

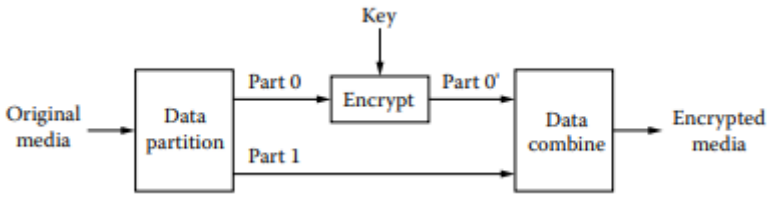


Fig2: Partial Encryption Process.

A. **Statistical Attacks**

1. **Key Space**:

All admissible permutation of keys is called key space. A robust algorithm relies on the large key space as it inhibits the adversary from brute force attack. Also as the key space is large, the truly random key can be selected from the permutations thereby reducing the chances of choice of an anticipated key.

2. **Key Sensitivity**:

Key sensitivity should be high, that means an iota of alteration in the key causes a drastic change in image. The key sensitivity is subdivided in 2 classes

3. **Shannon Entropy**:

Shannon Entropy measures randomness in encrypted images as a whole. Ideal value is 8 bits. Use (1) to calculate Entropy.

$$H(X) = -N \sum_{i=1}^{N} \log_{N}(x_i) p(x_i) \qquad \textbf{(1)}$$

Where $p(x_i)$ denote the probability of pixel with gray value $m_i$ and N is number of gray values.

4. **Local Entropy** :

This metric is a variant of the Shannon Entropy. It is calculated over the local blocks rather than the entire image. We use (2) to calculate it.

$$H_{\{k,T_b\}} = \sum_{i=1}^{k} \frac{H_i}{k} \qquad \textbf{(2)}$$

where $H_i$ for i= 1,.....k is defined as Shannon Entropy for the image with $T_b$ pixels.

**5. Histogram Analysis:**

This involves the better the uniformity of the histograms the better the algorithm as it successfully veils the pixel correlation.

**6. Correlation coefficient:**

It measures the correlation between the pixels especially in horizontal, vertical, and diagonal direction. Let *J* pairs of pixels $(x_i, y_i)$ in requisite direction and use (3) for the calculation.

$$p = \frac{cov(x,y)}{\sqrt{var(x)} * \sqrt{var(y)}} \qquad \textbf{(3)}$$

Where

$$cov(x,y) = \frac{1}{J}\sum_{i=1}^{J}(x_i - n_x)\left(y_i - n_y\right)$$

$$var(x) = \frac{1}{J}\sum_{i=1}^{J}(x_i - n_x)^2$$

$$n_x = \frac{1}{J}\sum_{i=1}^{J} x_i$$

B. **Differential Attacks**

**1. NPCR (Number of Pixel Change rate ) And UACI(Unified Average Changing Intensity:**

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 4, April 2021

DOI: 10.17148/IARJSET.2021.8463

NPCR measures the change in cipher with a single bit change in the original image. NPCR and UACI are calculated using (4) and (5). The metrics are crucial in calculation of robustness against differential attacks. The critical value of NPCR is approx 99.5 and for UACI the value should be greater than 33.3. The larger the value for the algorithm devised the better is the algorithm. Let $C_1$ and $C_2$ be two encrypted image each with M*N dimensions, then the values are calculated as below

$$NPCR = \frac{\sum_{i,j} D(i,j)}{N*M} * 100\ \% \quad \textbf{(4)}$$

$$UACI = \frac{1}{N*M} \sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255} * 100\% \quad \textbf{(5)}$$

Where , D(i,j) = 1 if $(C_1(i,j)) = (C_2(i,j))$
1 if $(C_1(i,j)) \neq (C_2(i,))$

C. **Noise Attack Analysis**

Presence of any disturbing altercations in course of image transmission is termed as noise. The two common types of noises interleaved are discussed below:

1. Gaussian Noise:

When the image pixels fluctuate randomly, it's called Gaussian noise or Electronic noise. The noise is modeled by adding random values to the image and then the respective strength of the decryption is evaluated.

2. Salt and Pepper:

When the image signal appears with random white and black pixels over it, is called Salt and pepper noise or (Impulse noise).

D. **Occlusion Attack**

The dissipation of parts of image intentionally or unintentionally is called an occlusion attack. To measure the strength of the image encryption scheme the encrypted image is ingested with varied levels of occlusion values and then analyzed.

**1. Peak Signal to Noise Ratio (PSNR) :**

It's the ratio between the power of the signal and the power of the noise distortions. The mathematical equation for PSNR is (6). For a good encryption technique the ratio should be small. Similarly there is another metric called Mean Square Error(MSE) that can be calculated as (7).

$$PSNR = \left(\frac{L^2}{MSE}\right) \quad \textbf{(6)}$$

$$MSE = \frac{1}{M^2} \sum_{i=1}^{M} \sum_{j=1}^{M} \left(I'(i,j) - I(i,j)\right)^2 \quad \textbf{(7)}$$

Where M*M is size of image ,
I'(i,j) is Encrypted image pixel value,
I(i,j) is Original value pixel value , MSE is Mean Squared Error
and L is Number of gray levels

## II. LITERATURE REVIEW

Yan-Ru Zhong, et al (2018) proposed a novel image encryption algorithm 2D SPLCM integrating Sine map and Piece wise Linear Chaotic map (PLCM) [3]. The image encryption involved a secret key based on initial conditions of 2D SPLCM, replacement operation and diffusion process. The algorithm on simulation proved to be robust against adversary José A.P. Artiles,et al (2019) proposed an image encryption technique based on AES and Logistic map [4]. Here AES s-box generation based on fixed number of chaotic bits i.e. 3. was proposed. The method was robust against different attacks yet limited chaotic range was the biggest demerit. Vinita Shadangi (2017) proposed a AES based image encryption in CBC mode using Arnold scrambling [5]. The scrambled image was then encrypted using AES. Better confusion –diffusion model was proposed for better security and effectivenss. Ünal Çavusoglu et al (2018) made optimized AES based on chaotic random number generator (RNG) i.e. Zhong Tang chaotic system. AES had one more phases in this technique that is added rows phase [6]. Jan Sher Khan, et al (2018) proposed an image encryption technique in [7] based on correlation coefficient and chaos system. Image was divided in blocks and correlation coefficients were calculated and then exclusive –OR (XOR) of the maximum correlation coefficient with the pseudo random sequence generated from the tent map. M.Y. Mohamed Parvees, et al (2016) presented a new color byte scrambling based image encryption approach [8]. This approach was composed of a Logistic map to generate a permutation sequence for shuffling the color bytes (confusion) and Ikeda map allowed the generation of a masking sequence for different color bytes (diffusion). The technique was effective against the adversary. Umar Hayat, et al (2018) designed a novel image encryption scheme based on total order on the elliptical curve [9].In the technique S-box generation(confusion) were generated via Ordered Elliptical curve (OEC) and pseudo random number generation

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 4, April 2021

DOI: 10.17148/IARJSET.2021.8463

(PRN). However, the above process is computationally intensive and more time consuming. Saleh Ibrahim, et al Ayman Alharbi (2017) proposed a unique image encryption technique to enhance substitution boxes (S-box). [10]. The technique relied on Substitution box generation using Henon map, the hash function for the key stream generation and Elliptical Curve Cryptography for the secure transmission of the key. The technique although proved to be effective yet it was time consuming and computational intensiveness. In [11] W. M. Abd-Elhafiez1, et al(2020) proposed two algorithms based on logistic map, Henon map, and Elliptical curve cryptography (ECC). The proposed cryptosystem relied on key generation based on logistic map and then XOR-ing the resultant with the image. Chunlei Fan and Qun Ding (2018) in [12] proposed an image encryption based on a self synchronous chaotic stream cipher generated using 4D hyperchaotic cryptosystems. The technique deployed the wavelet transform alongside Arnold's map. Nitin Rawat, et al (2015) proposed a technique for image encryption based on compressive sensing, structurally random matrix es and Arnold's Transform[13]. At first the image was reduced in dimensions and then it underwent Arnold's transform. Then the original image with a double random phase encoding process was deployed to provide encryption. The keys used were generated based on fractional Fourier transform. The simulation of the image suggested that the technique is highly robust to adversary and provides better security than its contemporaries. Fu Jie, et al (2019) recommended a method based compressive sensing and wavelet transform [14]. The image included 2D-LASM for pixel permutation. The outcomes of the experiment indicated that the recommended method was feasible and provided efficient encryption. Amit Chatterjee, et al (2017) recommended a new image encryption system on the basis of virtual optical method, Fourier transform phase retrieval algorithm and RSA public key exchange [15]. The outcomes of simulation indicated that the recommended technique was authentic and robust against potential attacks. The RMSE was computed amid the original image and retrieved image for determining the precision of information retrieved through the recommended system. This system was also capable of validating the information. P.Jeya Bright, et al (2019) introduced a Block Truncation code (BTC) based approach [16].The compressed image was encrypted using pseudo random sequence. The key was shared between sender and receiver. The technique was successful but it led to poor quality of image on reconstruction. Lingfeng Liu, et al(2017) contrived an image encryption technique that meant for blocks division of image[17]. Then each individual block was separately encrypted. The diffusion process included Arnold map and logistic map then the baker map was used to provide the required diffusion. The technique was evaluated to be secure against adversary. In [18] another technique based on 2D baker map and 1 D logistic map was proposed. This technique involved baker map chaotic behavior of logistic map. The limited chaotic range and limited key space were two prominent demerits of the technique that were addressed in this approach. In [19] blockchain based image encryption was proposed that was used to provide the security against the attacker when the image in transmit. This technique was found to be effective against chosen plaintext text attack and provided good results in statistical and differential attack. [20]proposed a technique based on fingerprint of the encryptor to be embedded in the encrypted image and the encrypted image was then transmitted over the blockchain. The technique provided secuirty against leakage of information to the unauthorized user as only valid user will have the fingerprint of the user. In [21] another authors (2020) designed a technique based on a combination of chaotic tent map. Diffusion was provided by tent map. The key stream depends on the original image. Zhao Feixiang, et al (2021), propounded a technique based on combination of Chaotic Restricted Boltzmann machine (CRBM) and blockchain [22]. Blockchain SHA-256 algorithm authenticated users. The technique was robust. In [23]an image encryption technique based on improved Linear feedback shift register (LFSR) was proposed. The technique used a MUX ,small LFSR probably of 3- bit, 8*1 MUX.At first a row wise permutation then a column wise permutation was deployed. The technique was robust time consuming affair. M.Y. Mohamed Parvees, et al (2016) presented an approach based on color byte scrambling [24].This approach was composed of a Logistic map to generate a permutation sequence for shuffling the color bytes (confusion) and Ikeda map allowed the generation of a masking sequence for different color bytes (diffusion). A technique based on pixel permutation was proposed in [25] .The encrypted images were masqueraded by some other image using key image. The technique had infinite key space but it was susceptible to chosen plaintext attack. In [26] Symmetric chaos based technique was proposed based on bit planes. The technique was found to be robust against several attacks as it increased the chaotic range of the map. Bit plain was first sliced to provide a D bit plane and the finally XOR-ed with bit matrix. Authors in [27] contrived a technique based on swapping block diffusion. At first the image was divided in blocks and then hash value was calculated for the image. This value was then used as key to LSS system. This was used to provide confusion and diffusion . The technique was robust against different attacks and also efficacious against adversary.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 4, April 2021

DOI: 10.17148/IARJSET.2021.8463

TABLE: Comparisons between various techniques.

| Ref NO | Authors | Year | Approach | Advantages | Disadvantages |
|---|---|---|---|---|---|
| [24] | Subhrajyoti Deb, et al. | 2019 | Image randomization Logistics, Arnold's Map, WFSR | Better Security | More Space intensive |
| [32] | Saad Muhi Falih | 2016 | LFSR, Qudratic map, Logistic map | i)Eliminates Linearity and repetition in LFSR's Output. ii)Enhanced Key space | Susceptible to Correlation Attack |
| [29] | M.Y. Mohamed Parvees, et al | 2016 | Color Byte Scrambling , Logistic map, Ikeda map | Better Confusion and Diffusion using Logistic and Ikeda map | Permutation Sorting time increases as block size increases non linearly |
| [27] | Lu Xu et al. | 2017 | Block Scrambling, dynamic index based diffusion | High security, high key space, suitable for multiple image encryption | Complex and diffusion is time intensive. |
| [4] | José A.P. Artiles , Daniel P.B. Chaves, Cecilio Pimentel | 2019 | AES, Logistic map | Improved AES. | Time consuming, Logistic map has a limited range |

## III. CONCLUSION

An acute review of the present image encryption techniques suggests that the field although quite developed yet some loopholes exist. The persistent security issues, limited key space, tuning parameters, computational speed, execution time, etc. are some impediments that still seek remedy. These have also opened new avenues for the future revenues. There are some fields like meta-heuristics that still have limited literature available. On other hand the recent researches have seen an unprecedented rise in the chaos based encryption. In this wake they tend to forget the computational complexity of the higher ordered chaotic maps. The above review evinces that the field of image encryption is still in premature phase and there are lots of avenues like hyper-spectral, 3D imaging that are yet to be explored.

## REFERENCES

[1] Abd El-Samie, Fathi & Ahmed, Hossam & Elashry, Ibrahim & Shaheen, Mai & Faragallah, Osama & El-Rabaie, El-Sayed & Alshebeili, Saleh. (2013). Image Encryption: A Communication Perspective. 10.1201/b16309.

[2] MultiMedia Content enCryption Techniques and Applications Shiguo LianISBN:9781420065282, 1420065289 CRC Press

[3] "Chaos-based Cryptography Theory, Algorithms and Applications" Book ISBN978-3-642-20542-2DOI10.1007/978-3-642-20542-2. Springer-Verlag Berlin Heidelberg

[4] "Chaos-based Cryptography Theory, Algorithms and Applications" Book ISBN978-3-642-20542-2DOI10.1007/978-3-642-20542-2. Springer-Verlag Berlin Heidelberg

[5] Artiles, J. A. P., Chaves, D. P. B., & Pimentel, C. (2019). *Image encryption using block cipher and chaotic sequences. Signal Processing: Image Communication, 79, 24–31.* doi:10.1016/ j.image. 2019.08.014

[6] Shadangi, Vinita & Choudhary, Siddharth & Abhimanyu, K & Patro, K Abhimanyu & Acharya, Bibhudendra. (2017). Novel Arnold Scrambling Based CBC-AES Image Encryption Novel Arnold Scrambling Based CBC-AES Image Encryption. International Journal of Control Theory and Applications. 10. 93 - 105.

[7] çavuşoğlu, Ünal & Kacar, S. & Zengin, Ahmet & Pehlivan, Ihsan. (2018). A novel hybrid encryption algorithm based on chaos and S-AES algorithm. Nonlinear Dynamics. 92. 10.1007/s11071-018-4159-4.

[8] Arab, A., Rostami, M.J. & Ghavami, B. An image encryption method based on chaos system and AES algorithm. *J Supercomput* **75,** 6663–6682 (2019).https://doi.org/10.1007/s11227-019-02878-7

[9] hong, Yan-Ru & Liu, Hua-Yi & Sun, Xi-Yan & Lan, Ru-Shi & Luo, Xiao-Nan. (2018). Image Encryption Using 2D Sine-Piecewise Linear Chaotic Map. 72-77. 10.1109/ICWAPR.2018.8521240.

[10] Zhu, & Wang,. (2019). A Secure and Fast Image Encryption Scheme Based on Double Chaotic S-Boxes. Entropy. 21. 790. 10.3390/e21080790.

[11] Mondal, Bhaskar & Kumar, Prabhakar & Singh, Shrey. (2018). A chaotic permutation and diffusion based image encryption algorithm for secure communications. Multimedia Tools and Applications. 77. 10.1007/s11042-018-6214-z.

[12] Rostami, Mohamad & Shahba, Abbas & Saryazdi, Saeid & Nezamabadi-pour, Hossein. (2017). A novel parallel image encryption with chaotic windows based on logistic map. Computers & Electrical Engineering. 62. 10.1016/j.compeleceng.2017.04.004.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 4, April 2021

DOI: 10.17148/IARJSET.2021.8463

[13] Zarebnia, M. & Pakmanesh, Hosein & Parvaz, Reza. (2018). A fast multiple-image encryption algorithm based on hybrid chaotic systems for gray scale images. Optik. 179. 10.1016/j.ijleo.2018.10.025.
[14] Ye, Guodong & Huang, Xiaoling. (2018). Spatial image encryption algorithm based on chaotic map and pixel frequency. Science China Information Sciences. 61. 10.1007/s11432-017-9191-x
[15] Xiang, Hongyue & Liu, Lingfeng. (2020). An improved digital logistic map and its application in image encryption. Multimedia Tools and Applications. 79. 1-27. 10.1007/s11042-020-09595-x.
[16] Liu, Lingfeng & Hao, Shidi & Lin, Jun & Wang, Ze & Hu, Xinyi & Miao, Suoxia. (2017). Image block encryption algorithm based on chaotic maps. IET Signal Processing. 12. 10.1049/iet-spr.2016.0584.
[17] Liu, Jingyi & Yang, Dingding & Zhou, Hongbo & Chen, Shiqiang. (2018). A digital image encryption algorithm based on bit-planes and an improved logistic map. Multimedia Tools and Applications. 77. 10.1007/s11042-017-5406-2.
[18] Batool, Syeda & Hafiz, Waseem. (2019). A novel image encryption scheme based on Arnold scrambling and Lucas series. Multimedia Tools and Applications. 78. 10.1007/s11042-019-07881-x.
[19] Luo, Yuqin & Yu, Jin & Lai, Wenrui & Liu, Lingfeng. (2019). A novel chaotic image encryption algorithm based on improved baker map and logistic map. Multimedia Tools and Applications. 78. 22023-22043. 10.1007/s11042-019-7453-3.
[20] Han, Chunyan. (2018). An Image Encryption Algorithm Based on Modified Logistic Chaotic Map. Optik. 181. 10.1016/j.ijleo.2018.12.178.
[21] Khan, Prince Waqas & Byun, Yungcheol. (2020). A Blockchain-Based Secure Image Encryption Scheme for the Industrial Internet of Things. Entropy. 22. 175. 10.3390/e22020175.
[22] Li, Ruiping. (2020). Fingerprint-related chaotic image encryption scheme based on blockchain framework. Multimedia Tools and Applications. 10.1007/s11042-020-08802-z.
[23] Zhao, Feixiang & Mingzhe, Liu & Kun, Wang & Hong, Zhang. (2021). Color image encryption via Hénon-zigzag map and chaotic restricted Boltzmann machine over Blockchain. Optics & Laser Technology. 135. 106610. 10.1016/j.optlastec.2020.106610.
[24] Deb, Subhrajyoti & Biswas, Bhaskar & Bhuyan, Bubu. (2019). Secure image encryption scheme using high efficiency word-oriented feedback shift register over finite field. Multimedia Tools and Applications. 78. 10.1007/s11042-019-08086-y.
[25] Saha, Sourav & Karsh, Ram & Amrohi, Mukul. (2018). Encryption and Decryption of Images Using Secure Linear Feedback Shift Registers. 0295-0298. 10.1109/ICCSP.2018.8523833.
[26] Anwar, Shamama & Meghana, Solleti. (2019). A pixel permutation based image encryption technique using chaotic map. Multimedia Tools and Applications. 78. 10.1007/s11042-019-07852-2.
[27] Parvees, Mohamed & Abdul Samath, Jabar & Raj, I.. (2016). A colour byte scrambling technique for efficient image encryption based on combined chaotic map: Image encryption using combined chaotic map. 1067-1072. 10.1109/ICEEOT.2016.7754851.