**Chaotic maps provide the most secured image encryption**

**Abstract-**

To cope up with the emerging security threats it became urgency for the researchers to find out the best and effective encryption methods. Moreover, securing images are most important as images are very sensitive in terms of privacy. Images are used in almost every sector for different purposes. Therefore, the demand of secured image encryption has emerged. There are many techniques have been invented for image encryption. This paper will discuss about some techniques of image encryption by researchers and will determine how chaotic maps provide the most secured image encryption.

**Introduction-**

Providing best security of the data and information is the main goal of modern cryptography. Data, images must be encrypted in a secured way. Researches are going on to find out the most secured encryption method. Exchange of images for different purposes has increased. As a result threats against security of images have also emerged. Researchers applied different techniques for image encryption. Among the techniques, using chaotic maps is the most secured system as it has satisfied most of the image security parameters. Chaotic maps are maps that exhibit some sort of chaotic behavior which obey certain rules of mathematical equation in terms of chaotic theory. Comparing with other techniques with chaotic maps regarding image encryption has shown that, using different chaotic maps is the most secured way for image encryption.

**Paper organization**-

The content of the paper has four sections. It will discuss about the image security parameters’; the techniques of image encryption using affine transform and XOR proposed by Nag, Singh, Khan, Biswas, D.Sarkar, P.sarkar; the technique of image encryption based on one dimensional random scrambling proposed by Sun, Guan, Yongping and Xue; And technique for image encryption based on hybrid chaotic maps proposed by N. Abdullah and A. Abdullah.

**Content-**

**Section 1- Image security parameters-**

There are six major image security parameters. And these are large key space, Key sensitivity, uniform image histogram, information entropy, co relation analysis and differential analysis.

**Large key space**- For secured image encryption large key space is required to function against Brute force attack.

**Key sensitivity**- It ensures that the system will generate completely opposite outcomes despite a small change in key. Thus image encryption has to be key sensitive.

**Uniform image histogram**-It refers the frequency distribution of continuous pixels and it shows density estimation. Pixels are the small elements of an image. Cipher image must have uniform histogram to be secure from known plain text attack.

**Information entropy**-It identifies uniform distribution in the system and the degree of uncertainty.

**Co-relation analysis**- It focus on the correlation between the encrypted image and two joining pixel of plain image. The cipher image must have very low correlation with two joining pixel of plain image.

**Differential analysis**- Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) measures the invulnerability of algorithm against the differential attacks on image.

**Section 2-**

**Image encryption using affine Transform and XOR operation**- Different techniques has been used by researchers regarding image encryption. Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Sushanta Biswas, D. Sarkar and Partha Pratim Sarkar have proposed image encryption based on affine transform and XOR operation. The techniques required 64 bits key for encryption. In the technique first, the affine transformation dispel the pixels by applying 4 sub keys of 8 bits. Then it decomposes 2\*2 pixel block size and applies XOR operation on each block with 4 sub keys of 8 bits. It modifies the pixel values.

Limitation- It has very short key space (64 bits only). It is less effective reducing correlation between pixel and cipher image. Simple XOR operation and key procedure do not provide adequate complexity to ensure security of the image.

**Section 3-**

**One dimensional random scrambling**- This technique of image encryption was proposed by Qiudong Sun, Ping Guan, Yongping and Yunfeng Xue. In this technique, the algorithm first transforms two dimensional images into one dimensional vector and then performs one dimensional random shuffling. Then it performs an anti-transformation on the dispersed vector. It generate an encipher image. The technique does not need iterative computation as one or two executions provide sufficient and best effect.

Limitation- In case of histogram, it shows that the scrambling process fail to break the similarities between original and cipher histogram. Although scrambling process reduce the correlation between pixels and cipher image but it fails to create completely different histogram for cipher and original image.

**Section 4-**

**Hybrid chaotic maps for image encryption**- Hikmat N. Abdullah and Hamsa A. Abdullah have proposed this technique. They have applied three chaotic maps such as Arnold cat map, Henon map and logistic map. The Arnold Cat chaotic map is described as follows-

Xn+1 = 1 p Xn mod N

Yn+1 q pq+1 Yn

Here, q are control parameters, N\*N is the size of image, (Xn,Yn) is the pixel location of original image and (Xn+1, Yn+1) is the new pixel location after applying Arnold transformation to shuffle the pixels. Arnold transformation serves as first secret key. Later more shuffling of pixels applied to add more randomness and increase effectiveness of encryption and it serves as second secret key. To increase more security the process then generate key by XOR the digital sequences resulting from Henon and logistic chaotic maps. Two different chaotic sequences increase the key space. Finally, the shuffled pixels modified by the XOR with encryption key to create cipher image. The Henon map described as-

Xn+1= 1 – aX^2n + Yn.

Yn+1= bXn.

a and b is the parameters which regarded as secret keys together with the initial values of X0 and Y0. And the logistic map described as Xn+1= µXn (1- Xn). Here initial value X0 and µ is regarded as secret key.

The proposed algorithm can be shown by following diagram-

Original image

image

Recover image

Arnold Map

Logistic Map

Encryption key

Cipher

Image

Henon map

Cipher

Image

Encryption Decryption

The algorithm satisfied the security parameters. The key space is larger as the two chaotic sequences increase the key space. In histogram analysis, sufficient difference occurs between original and cipher image. The correlation between two pixel and cipher image is very low because of confusion, multiple shuffling and diffusion. In case of information entropy, it is found that the entropies of cipher image after applying the algorithm is close to 8. It indicates the cipher image has sufficient randomness. Therefore the proposed algorithm based on chaotic maps is very effective in terms of encryption. It provides best security for image encryption.

**Conclusion-**

In this paper the image encryption has been described in terms of different techniques. Some of the techniques fail to provide best image encryption as they could not satisfy most of the security parameters. The use of chaotic maps with some XOR operation brings the best result. The use of Arnold, Henon and logistic chaotic maps provides less complex operation but most secured image encryption. Therefore, it can be determined that use of chaotic maps is the best technique for secured image encryption.

**References**

1. N. Abdullah, A. Abdullah. “Image Encryption Using Hybrid Chaotic Map.” *IEEE: 2017 International Conference on Current Research in Computer Science and Information.*
2. Kumar, Aggarwal, Grag. “A Review on Various Digital Encryption Techniques and Security Criteria.” 2015 *International Journal of Computer Applications (Vol-96).*
3. Nag, Singh, Khan, Biswas, D. Sarkar, P. Sarkar “Image Encryption Using Affine Transform and XOR Operation” *2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies*.
4. Sun, Guan, Yongping Qiu, Yunfeng Xue “A Novel Digital Image Encryption Method Based on One-dimensional Random Scrambling” 2012 *9th International Conference on Fuzzy Systems and Knowledge Discovery.*