Performance analysis of Encryption and Decryption Algorithms for Securing Images

[1]Ms.Pallawi R.Motghare , [2]Dr. Pankaj Agrawal

[1]M.Tech Scholar, G H Raisoni Academy of Engineering and Technology, Nagpur, Maharashtra, India
[2]Professor, G H Raisoni Academy of Engineering and Technology, Nagpur, Maharashtra, India

***Abstract*— This paper focuses mainly on the different image encryption algorithms and various parameters. As the use of digital techniques for transmitting and storing images are increasing, it becomes an important issue that how to protect the confidentiality, integrity and authenticity of images. There are various techniques to encrypt the images for making the images more secure.**

Therefore, along with security, factors like implementation cost and performance, speed of different encryption algorithms also needs to be considered for practical implementation. Parameters like Histogram, Information entropy, Correlation coefficient and Encryption Ratio need to be analyzed for comparative performance analysis of various encryption algorithms.

***Keywords*—: Encryption, Decryption, Block based transformation algorithm, Chaotic map algorithm, Region based selective image encryption algorithm**

I. INTRODUCTION

In recent days, image security has found a place in many applications like internet banking transactions, military image database and communication, document storage systems, and medical imaging systems. Image encryption has gained a lot of focus in the field of image processing. The very fact that the data has to be encrypted to maintain the secrecy involved in it makes it very attractive for a detailed study. Encryption was first being studied and applied for all kinds of information in the same way. This is no longer sufficient. Image encryption differs from data encryption. Different representations of information like text, images, audio, video, etc, have to be treated individually in a specific manner so that features specific to each of them are analyzed and appropriate techniques are applied. Application of text encryption techniques on images may not completely hide all the image features and hence, proper encryption of images cannot be achieved. The image features can be used to provide a greater level of security. Robust image encryption algorithms are required to make the images sturdy against possible attacks. Large amount of processing is involved in image encryption. This demands for an efficient algorithm that reduces the overhead involved in encrypting the image. This problem can be handled in many ways. One way is to look in to the image for the presence of information that is more sensitive which needs protection, and to encrypt only such parts. In many applications there is no need to encrypt the whole image, for e.g., in a bank draft only the signature, the amount and the seal of the bank need to be protected. The image encryption is to transmit the image securely over the network so that no unauthorized user can able to decrypt the image. Image encryption, video encryption, chaos based encryption have applications in many fields Including the internet communication, transmission, Medical imaging .Tele-medicine and military Communication, etc. The evolution of encryption is moving towards a future of endless possibilities. The image data have special properties such as bulk capability, high redundancy and high correlation among the pixels. Encryption techniques are very useful tools to protect secret information. Encryption will be defined as the conversion of plain message into a form called a cipher text that cannot be read by any people without decrypting the encrypted text Decryption is the reverse process of encryption which is the process of converting the encrypted text into its original plain text, so that it can be read Encryption of data has become an important way to protect data resources especially on the internet, intranets and extranets. Encryption is the process of applying special mathematical algorithms and keys to transform digital data into cipher code before they are transmitted and decryption involves the application of mathematical algorithms and keys to get back the original data from cipher code. The main goal of security management is to provide authentication of users, integrity, accuracy and safety of data resources.

II. THE PROPOSED TECHNIQUE

➢ Block based transformation algorithm:

Mohammad Ali Bani Younes and Aman introduce a block-based transformation algorithm based on the combination of image transformation and a well-known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm, and then the transformed image was encrypted using the Blowfish algorithm

Chaotic map algorithm: The Chaotic map algorithm presents several interesting features, such as selective encryption. The main goal of selective encryption is to reduce the amount of data to be encrypted. The chaotic function is sensitive to initial condition, is unpredictable, indecomposable and yet contains regularity. This algorithm uses Henon map for image encryption.

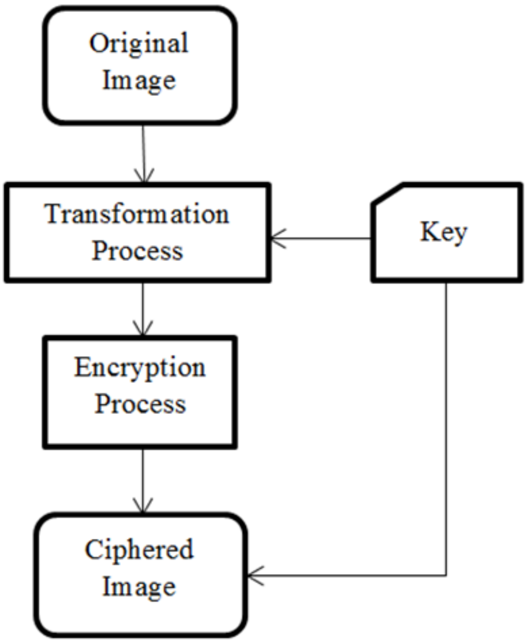
Region based selective image encryption algorithm:

The proposed Region Based Selective Image Encryption technique is a new approach to image Encryption .The main idea is to follow a selective approach for both encryption and decryption Region Based Selective Image Encryption is one of the concepts to provide security to the image and in the same time, some part of the image is visible. One of the uses of this algorithm is in Medical field

III. Related Work:

Block based transformation algorithm:

The proposed algorithm is divided the image in to it random number of blocks with predefined maximum and minimum number of pixels, resulting in a stronger encryption and a decreased correlation. Overview of the Transformation Algorithm The transformation technique works as follows: where the original image is divided into number of blocks which are shuffled within the image to build a newly transformed image. The generated (or transformed image) is then fed to the blowfish encryption algorithm and thus generated one can be viewed as an arrangement of blocks. This perceivable information can be reduced to decreasing the correlation among the image elements using certain transformation technique. The secret key of this approach is used to determine the seed. The seed plays as role in building the transformation table which is then used to generate the transformed image with different random number of block sizes. In this case, the transformation process refers to the operation of dividing and replacing an arrangement of the original image. Block based encryption and decryption algorithms based on the combination of image transformation followed by encrypted images and image measurements of correlation, entropy and histograms will be used to measure to the security of the original image, transformed images, encrypted images and decrypted image using the combination technique.



5

Fig1.General block diagram of the transformation Algorithm

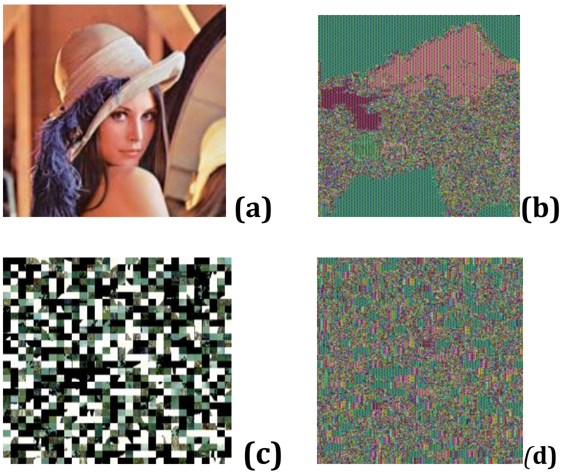


Fig2.Results of encryption by using 10 pixels × 10 pixels Blocks. (a) Original image. (b) Encrypted image using Blowfish. (c) Transformed image. (d) Encrypted image Using transformed followed by the Blowfish algorithm.

Region based selective image encryption algorithm*:*

The idea of selective encryption is being followed in various applications. This is used mainly to reduce the overhead involved in data transmission over secure channels. The image is first compressed. The algorithm only encrypts part of the bit-stream with a well proven ciphering technique; incidentally a message is added during this process. With the decryption key, the receiver decrypts the bit-stream, and decompresses the image. In principle, there should be no difference between the original image and the image that has been encrypted and decrypted. In encryption process the original image is first processed for feature extraction that involves identification of sensitive areas, which are marked. The image is then segmented into regions of a given block size. Then, all the regions that contain the sensitive area are encrypted and other regions are left as they are. The regions are permuted. Different block sizes are considered for region segmentation. Various algorithms are used for encryption and permutation. All these parameters form the encryption information. The encryption information is added to the cipher image.

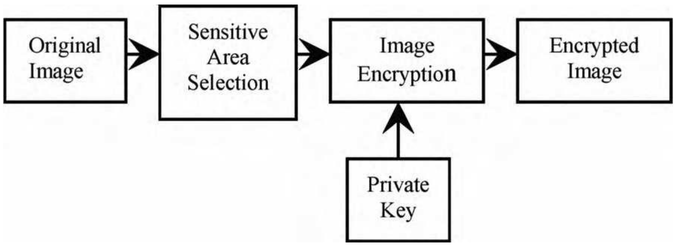


Fig3.Schematic of Region Based Selective Image Encryption

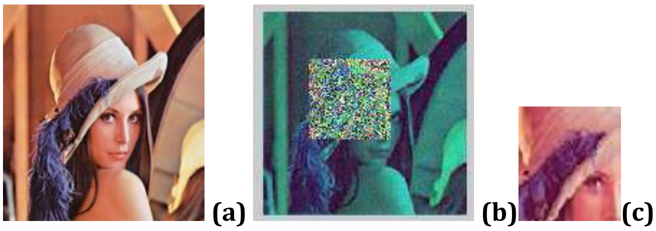


Fig4.Image encryption experimental result 1: (a) Plain-image, (b) Selective Encrypted image(c) Selective decrypted image

Chaotic map algorithm:

The chaos-based image cryptosystem mainly consists of two stages. The plain image is given at its input. The typical architecture of the chaos-based image cryptosystems is depicted in Figure. There are two stages in the chaos based image cryptosystem The confusion stage is the pixel permutation where the position of the pixels is scrambled over the entire image without disturbing the value of the pixels and the image becomes unrecognizable. Therefore these initial conditions and control parameters serve as the secret key. It is not very secure to have only the permutation stage since it may be broken by any attack. To improve the security, the second stage of the encryption process aims at changing the value of each pixel in the whole image. The process of diffusion is also carried out through a chaotic map which is mainly dependent on the initial conditions and control parameters. In the diffusion stage, the pixel values are modified sequentially by the sequence generated from one of the three chaotic systems selected by external key. The whole confusion- diffusion round repeats for a number of times to achieve a satisfactory level of security. The randomness property inherent in chaotic maps makes it more suitable for image encryption. The proposed scheme is shown in Figure. Different chaotic systems are employed in confusion and diffusion stages. Also complex chaotic maps are chosen rather than the simple ones to further enhance the complexity of the algorithm and thereby improving the security. The input to the cryptosystem is the plain image which is to be encrypted.

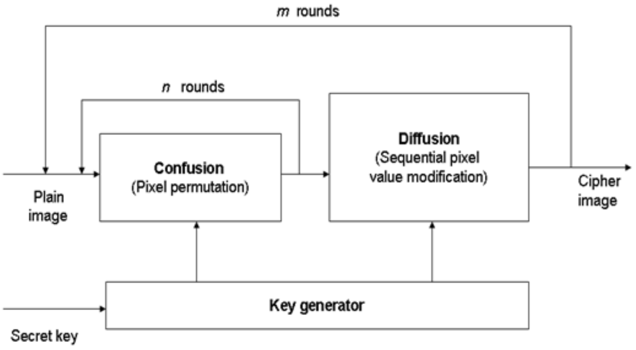


Fig5 Architecture of proposed Chaos-based image cryptosystem

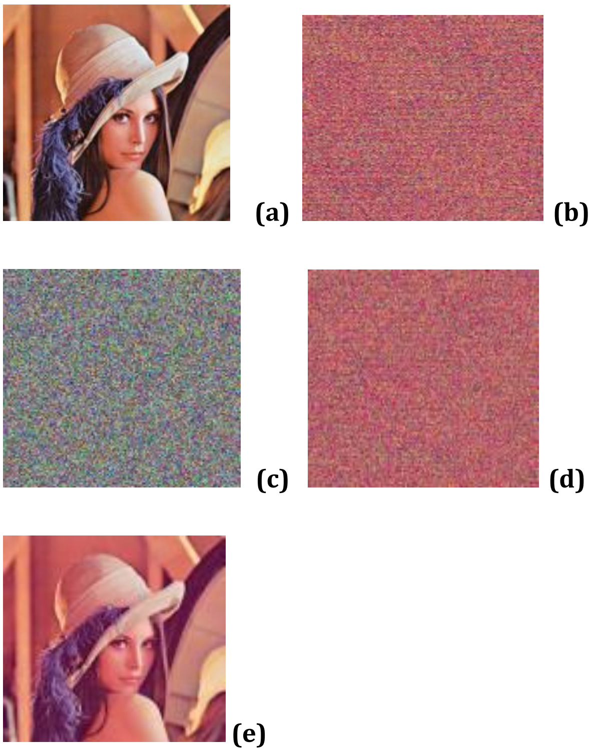


Fig6.Image encryption experimental result 1: (a) Plain- image, (b)The Pixel Permuted image **,(c)** Encrypted image,(d) Undiffused image,(e) decrypted image

V. **HISTOGRAM ANALYSIS:**

Fig 7 depicts histogram analysis. Fig 7 shows histogram of red, green and blue component of plain image and the histogram of red, green and blue component of cipher image. It is clearly visible that histogram of cipher image is fairly uniform and it does not leak any amount of information about the plain image.

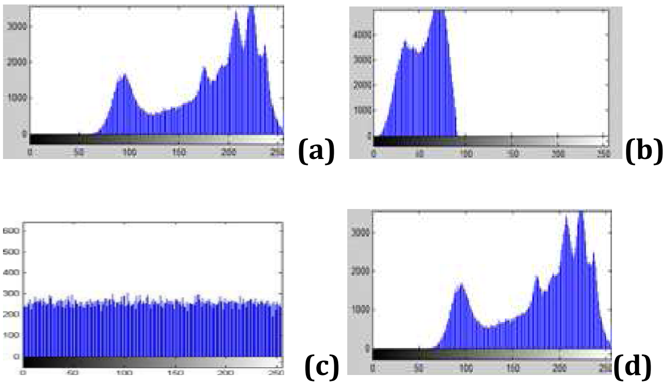


Fig7.Histogram of plain-image and partial encrypted image (a) Lena Plain-image histogram, (b)
Histogram of Lena partial Encrypted image, (c) Histogram of Lena Encrypted image (d) Histogram of Decrypted image

IV. **INFORMATION ENTROPY:**

Information theory is the mathematical theory of data communication and storage founded in 1949. Information entropy is defined to express the degree of uncertainties in the system. It is well known that the entropy $H(x)$ of a message source m can be calculated as:

$$h = -\Sigma(p_i log_2 p_i)$$

Sr.No.	Technique	No.of blocks	Entropy Value	
			Encrypted image	Original image
1	Region Based Selective image Encryption	100×100	7.6453	7.7335
		300×300	7.5357	7.7545
2	Chaotic Map	100×100	7.9874	7.7335
		300×300	7.9936	7.7545
3	Blocked based transformation algorithm	100×100	7.9939	7.7173
		300×300	7.9994	7.7565

Table 1 : Image Entropy

Where $P(xi)$represents the probability of symbol xi and the entropy is expressed in bits. Truly random source entropy is equal to 8. Actually, given that a practical information source seldom generates random messages, in general its entropy value is smaller than the ideal one. However, when the messages are encrypted, their entropy should ideally be 8. If the output of such a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security. The entropy is as follows: The value obtained is very close to the theoretical value of 8. This means that information leakage in the encryption process is negligible and the encryption system is secure upon the entropy attack

VI.CORRELATION COEFFICIENTS ANALYSIS:

There is a very good correlation between adjacent pixels in the image data. Equation is used to study thecorrelation between two adjacent pixels in horizontal, vertical and diagonal orientations. where *x* and *y* are intensity values of two neighboring pixels in the image and *N* is the number of adjacent pixels selected from the image to calculate the correlation. Correlation test image is depicted in shows the correlation distribution of two adjacent pixels in the plain image and cipher-image. It is observed that neighboring pixels in the plain-image are correlated too much, while there is a little correlation between neighboring pixels in the encrypted image. Results for correlation coefficients are shown in table 1.

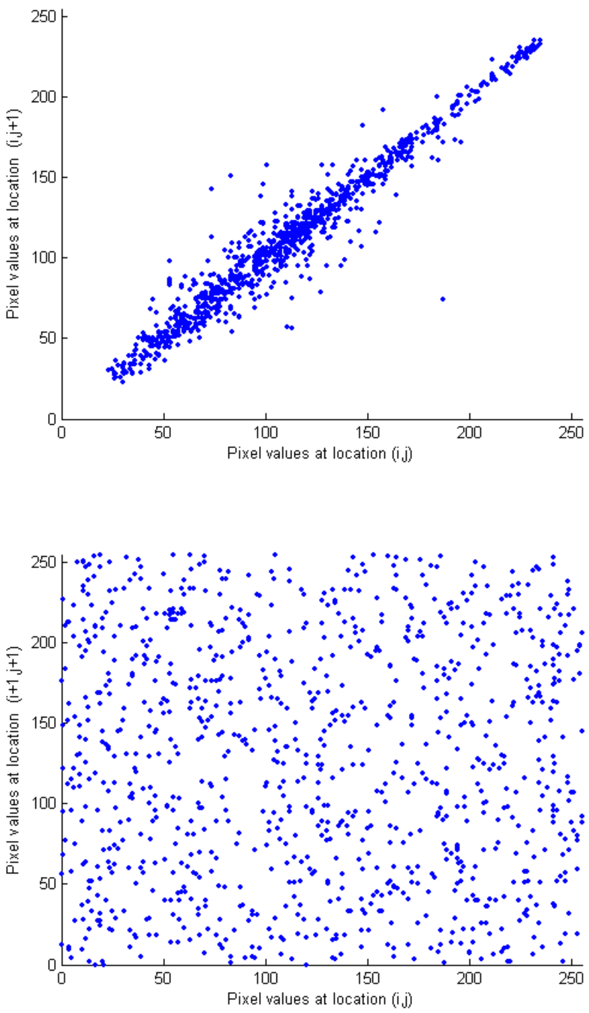


Fig.8.Correlation of two adjacent pixels: (a) Plain Image and (b) Cipher Image

VII. CONCLUSION

This paper describes the concept of selective encryption technique and full encryption Technique. Security analysis of a different image encryption algorithm has been presented. All parts of the encryption system were simulated using MATLAB. Security analysis covers histogram analysis, correlation analysis, and entropy analysis. Histogram analysis shows that histogram of cipher image is flat or uniformly distributed, so the algorithm is secure from frequency analysis attack. Entropy analysis shows that the algorithm has entropy that close to ideal entropy, so the algorithm is secure from leakage of information. The region based approach for encryption of the images is faster with appropriate block size. Selective encryption approach reduces the overhead of encrypting the non-sensitive areas. Loss of information is less, makes the decryption faster. Selective Image Encryption using Chaotic Map is reduced the encryption time and provides high level of security. Advantage of a New Image Encryption Approach Using Block Based Transformation Algorithm, is that it reproduce the original image with no loss of information for the encryption and decryption process we used a blowfish algorithm. The proposed algorithm will expect in the best performance; the lowest correlation and the highest entropy. Selective encryption is faster as compared to the full encryption of the data.

REFERENCES

[1] Mahmood Al-khassaweneh, Selin Aviyente,"Image Encryption Scheme Based on Using Least Square Approximation Techniques" IEEE Transactions, pp.108-111, 2008.

[2] DeWang, Yuan-Biao Zhang, "image encryption algorithm based on
s-boxes substitution and chaos random sequence", International Conference on Computer Modeling and Simulation, 2009 IEEE.

[3] H. T. Panduranga, and S. K. Naveen Kumar, "Selective image encryption for Medical and Satellite Images", International Journal of Engineering and Technology (IJET), vol. 5, no. 1, 2013, pp. 115–121.

[4] Ahmed Bashir Abugharsa, Abd Samad Bin HasanBasari and Hamida
Almangush "A New Image Encryption Approach using Block-Based
on Shifted Algorithm", IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.12, December 2011.

[5] Mohammad Ali Bani Younes and Aman Jantan Image Encryption
Using Block-Based Transformation Algorithm IAENG International Journal of Computer Science, 35, 2008

[6] Jui-Cheng Yen and Jiun-In Guo, "A New Chaotic Image Encryption Algorithm", *IEEE Int. Conf. Circuits and Systems*, 2000, Vol. 4, pp. 49-52.

[7] Marc Van Droogenbroeck and Raphael Benedett, "Techniques for a selective encryption of uncompressed and compressed image" , *ACIVS 2002 Proceedings*, September 9-11, 2002.

8] Marc Schneider and Shih-Fu Chang, "A Robust Content Based Digital Signature for Image Authentication", Columbia

University, Image and Advanced Television Laboratory, New York.

[9] J.C. Yen and J.I. Guo, "The Design and Realization of a Chaotic Neural Signal Security System", *Pattern Recognition and Image Analysis*, 2002, Vol. 12, No. 1, pp. 70-79.