Comparative Analysis and Implementation of Image Encryption Algorithms

Rajinder Kaur
University College Of Engineering Punjabi University,Patiala

Abstract: Due to the rapid growth of digital communication and multimedia application, security becomes an important issue of communication and storage of images.,Image security has found a great need in many applications where the information (in the form of image) is to be protected from unauthorized access.Encryption is one of the ways to ensure high security. In recent years, encryption technology has been developed and many image encryption methods have been used. These methods produce randomness in the image so that the content is not visible. Encryption and decryption consume a considerable amount of time. So there is a need for an efficient algorithm. This paper proposed three different image encryption techniques for color image. Simulation results are presented and a comparative analysis of the different methods is discussed.

Keywords: Cryptography, Correlation Coefficient, Encryption,Decryption,Histogram, Selective Image Encryption.

1. INTRODUCTION

With the ever-increasing growth of multimedia applications, security is an important issue in communication and storage of images, and Encryption is a common technique to uphold image security. Image encryption techniques try to convert original image to another image that is hard to understand; to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption. The process of encoding plain text messages into cipher text messages is called **encryption**.and the reverse process of transforming cipher text back to plain text is called as **decryption**. Image and video encryption have applications in various fields including internet communication, multimedia systems, medical imaging, Tele-medicine and military communication. Color images are being transmitted and stored in large amount over the Internet and wireless networks, which take advantage of rapid development in multimedia and network technologies. In recent years, plenty of color image encryption approaches have been proposed.Until now, various data encryption algorithms have been proposed and widely used, such as AES, RSA, or IDEA most of which are used in text or binary data.It is difficult to use them directly in multimedia data and inefficient for color image encryption because of high correlation among pixels. For multimedia data are often of high redundancy,of large volumes and require real-time interactions.

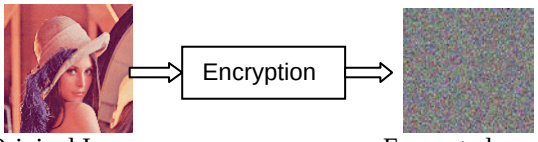

Figure 1**:** showing image encryption

This paper is organized as follows In Section 1; we present general guide line about cryptography. In Section 2, comparative analysis of the different methods is discussed. Finally, we conclude in section 3.

CRYPTOGRAPHY : The many schemes used for enciphering constitute the area of study known as cryptography.

There are three types of cryptography:

1.1 Secret Key Cryptography

This type of cryptography technique uses just a single key. The sender applies a key to encrypt a message while the receiver applies the same key to decrypt the message. Since only single key is used so we say that this is a symmetric encryption.The biggest problem with this technique is the distribution of key as this algorithm makes use of single key for encryption or decryption.

1.2 Public Key Cryptography

This type of cryptography technique involves two key crypto system in which a secure communication can take place between receiver and sender over insecure communication channel. Since a pair of keys is applied here so this technique is also known as asymmetric encryption.In this method, each party has a private key and a public key. The private is secret and is not revealed while the public key is shared with all those whom you want to communicate with. If Alice wants to send a message to bob, then Alice will encrypt it with Bob's

Manuscript received December 5, 2013
Manuscript revised December 20, 2013

public key and Bob can decrypt the message with its private key

1.3 Hash Functions

This technique does not involve any key. Rather it uses a fixed length hash value that is computed on the basis of the plain text message. Hash functions are used to check the integrity of the message to ensure that the message has not be altered,compromised or affected by virus.

Cryptography technique needs some algorithm for encryption of data. Nowadays when more and more sensitive information is stored on computers and transmitted over the Internet, we need to ensure information security and safety. Image is also an important part of our information Therefore it's very important to protect our image from unauthorized access.

2. Image Encryption Algorithms and Comparison analysis:

1. Region Based Selective Image Encryption

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.

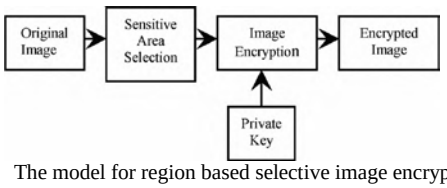

Figure 2: The model for region based selective image encryption

Region Based Selective Image Encryption is one of the concept to provide security to the image and in the same time, some part of the image is visible.One of the use of this algorithm is in Medical field, now a days the doctors are consulting the other doctors abroad, this algorithm can really help those.The medical image data is different from other visual data for multimedia applications. Since the lossy data may cause some negative misdiagnosis, it is constrained by the fact that a diagnosis should be based on a lossless compressed image which holds a much larger amount of data than the lossy compressed image. A possible solution to this problem is to use selective compression where parts of the image that contain crucial information are compressed in a lossless way whereas regions containing unimportant information are compressed in a lossy manner.

Selective Encryption

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 (if needed). The algorithm only encrypts part of the bit-stream with a well proven ciphering technique ; incidentally a message (a watermark) 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 (partly or fully) are encrypted and other regions are left as they are. The regions (both encrypted and nonencrypted) are permuted.

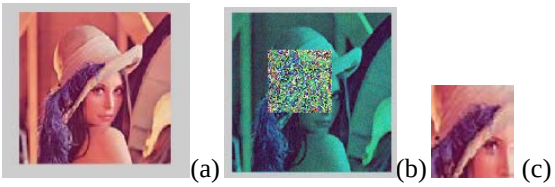

Figure 3. Image encryption experimental result 1: (a) Plain- image, (b) Selective Encrypted image (c) selective decrypted image

2. Selective Image Encryption using Chaotic Map

Chaos map technique is widely studied by many researchers, .we define a selective encryption technique for partial image encryption. Selective encryption is carried out with the help of chaos map. The encryption is carried out in two stages:

1. Chaos based key Generation

2. Selective Encryption

These two techniques are performed independently and at the end these technique are merged together.
In this algorithm, we proposed a technique for selective image encryption by confusion and diffusion using chaos map.

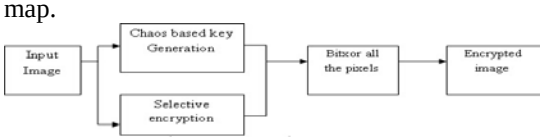

Figure.4 Selective Encryption Proposed Technique

Selective Image Encryption using Chaotic Map

Selective image encryption algorithm using chaotic map is a wonderful techniques for encrypting and

compressing the data(Images and Videos). It is specifically designed for the colored images, which are 3D arrays of data streams. Because of the explosion of networks and the huge amount of content transmitted along, securing video content is becoming more and more important. There are traditional approaches to encode the data, which perform encryption on bit stream of data. The proposed 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 general approach for selective encryption is separated in two parts, public part which is unprotected and private part i.e protected part. Chaos map is used for encrypting the input data, which provide security.

Chaos based key Generation: The chaotic function is sensitive to initial condition, is unpredictable, indecomposable and yet contains regularity. This algorithm uses Henon map for image encryption.

The Henon map: Like the logistic map the Hénon system is a system with a discrete time scale **n=1, 2, .**(i. e. it is a map). Whereas the logistic map maps a one-dimensional real interval **[0..1]** onto itself, the Hénon map is defined on the two-dimensional real plane. And whereas there is only one control

parameter **r** in the logistic map, there are two control parameters **a** and **b** in the Hénon map.

Henon map is defined by the function:

$$x_{n+1} = y_n + 1 - ax_n^2$$

$$y_{n+1} = bx_n$$

Where a, b and c are constant. This function generates the random value and these random values are bitXORed with the original pixel value of the image, i.e. X value will be bitXORed with the red channel pixel, Y with the green channel and Z with the blue channel respectively. Image encryption using chaos map include the input image, secret key for encrypting the plain image.

As we can see in figure 5(c), the encrypted image still has some details that are not desired, encrypting the key image first and encrypt the original image with the encrypted key image is the best solution.After getting the encrypted key image as shown in figure 5(c), then the original image in figure 5(a) will be encrypted using this key image to output the encrypted image as shown in figure 5(b). As can be seen in figure 5(b) the encrypted image is unknowable. In the decryption processes, if we use the same key that has been used in encryption, we get the same image as the original image, it can be seen in figure 5(d) that the decrypted image is clear and correct without any distortion of the image.

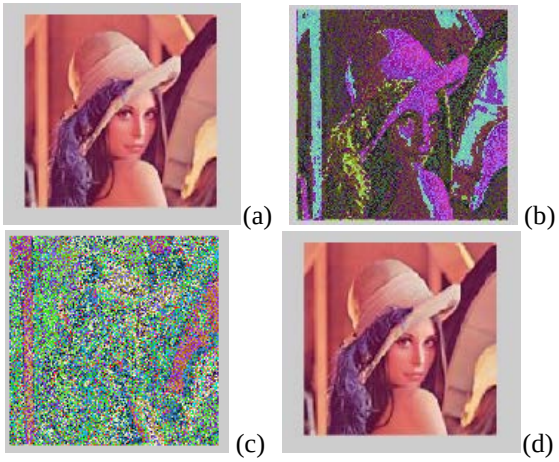

Figure 5:shows the experimental result for encrypting an image of size 256*256 with a key image of the same size. The image in figure 5(a) is the original image and the image in the figure 5(b) is the key image. The encrypted image is shown in figure 5(c).

3. A New Image Encryption Approach Using 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 algorithm is 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.

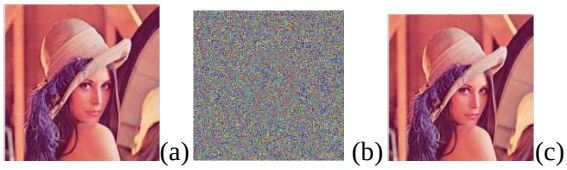

Figure 6:Image encryption experimental result 1: (a) Plain- image, (b) Encrypted image (c) Decrypted image

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.

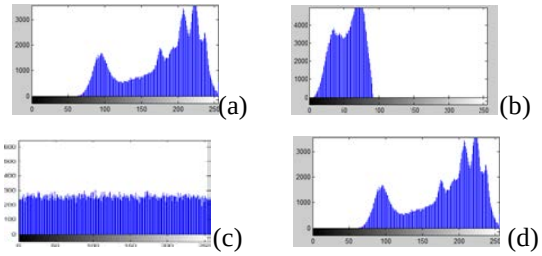

Figure 7: Histogram of plain-image and partial encrypted image (a) Lena Plain-image histogram, (b) Histogram of Lena partial Encrypted image, (c) Histogram of Lena Encrypted image (d) Histogram of Decrypted image

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:

Table 1 **:** Image Entropy

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	Selective Image Encryption Using Chaotic Map	100×100	7.9874	7.7335
		300×300	7.9936	7.7545
3	Image Encryption using Blocked based transformation algorithm	100×100	7.9939	7.7173
		300×300	7.9994	7.7565

$$H(X) = \sum_{i=1}^{n} P(x_i)\, I(x_i) = \sum_{i=1}^{n} P(x_i) \log_b \left(\frac{1}{P(x_i)}\right) = -\sum_{i=1}^{n} P(x_i) \log_b (P(x_i)),$$

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.

Correlation Coefficient Analysis

There is a very good correlation between adjacent pixels in the image data . Equation is used to study the correlation between two adjacent pixels in horizontal, vertical and diagonal orientations. where x and y are intensity values of two neighbouring pixels in the image and N is the number of adjacent pixels selected from the image to calculate the correlation.

$$r = \frac{\sum_{i=1}^{n}(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum_{i=1}^{n}(X_i - \bar{X})^2}\sqrt{\sum_{i=1}^{n}(Y_i - \bar{Y})^2}}$$

Correlation test image is depicted in Fig. 2(a). Fig.8 shows the correlation distribution of two adjacent pixels in the plain image and cipher-image. It is observed that neighbouring pixels in the plain-image are correlated too much, while there is a little correlation between neighbouring pixels in the encrypted image. Results for correlation coefficients are shown in table2.

Table 2. Correlation coefficients of two adjacent pixels

Correlation Coefficient Analysis				
Techique	image	No of blocks	Adjacent pixels orientation	
			Horizontal	Vertical
1.Region based Selective image encryption	Original image	100×100 300×300	0.8915 0..9795	0.9621 0.9621
	Encrypted image	100×100 300×300	0.5380 0.7940	0.5988 0.7917
2.Selective Image Encryption using chaotic map	Original image	100×100 300×300	0.8915 0.9795	0.9621 0.9621
	Encrypted image	100×100 300×300	-0.0486 -0.0495	0.0232 0.0697
3.Image Encryption using blocked based transformation algorithm	Original image	100×100 300×300	0.9661 0.9706	0.9518 0.9887
	Encrypted image	100×100 300×300	0.0548 0.0050	0.0433 -0.0619

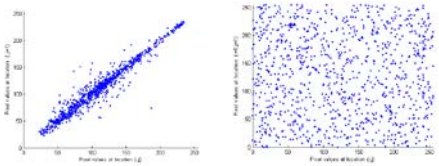

Figure 8. Correlation of two adjacent pixels: (a) Plain Image and (b) Cipher Image

Comparison charts

The graph clearly shows the dependence of encryption time over the block size. For comparison,
the behavior of chaotic algorithm,applied to whole image.

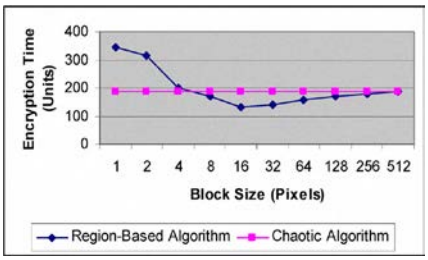

Figure 9: Behavior of Encryption time on Block Size

4. 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, entropy analysis. Histogram analysis shows that histogram of cipherimage is flat or uniformly distributed, so the algorithm is secure from frequency analysis attack.Entropy analysis show that the algorithm has entropy that close to ideal entropy (8), so the algorithm is secure from leakage of information.The region based approach for encryption ofthe images is faster with appropriate blocksize. 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 provide 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] Jui-Cheng Yen, Jiun-In Guo, “A new chaotic image encryption algorithm” Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China.

[2] M. A. Bani Younes and Aman Jantan, “Image Encryption Using Block-Based Transformation Algorithm”IAENG, 35:1, IJCS_35_1_03, February 2008.

[3] Ismet Ozturk and Abrahim Sogukpinar, “Analysis and Comparison of Image Encryption Algorithms”, World Academy of Science, Engineering and Technology 3 2005

[4] K.C. Ravishankar, M.G. Venkateshmurthy “Region Based Selective Image Encryption” 1-424-0220-4/06 ©2006 IEEE

[5] H.Gao,Y.Zhang, S. Liang, D.Li “A New Chaotic Image Encryption Algorithm “Chaos, Solitons and Fractals 29 (2006) 393–399.

[6] A.Gautam, M. Panwar, Dr.P.R Gupta “A New Image Encryption Approach Using Block Based Transformation Algorithm” 2011 (IJAEST) Vol No. 8, Issue No. 1, 090 - 096 .

[7] B.Furht and D.Socek,” A Survey Of Multimedia Security” Comprehensive Report on,2003

[8] Selectiveimageencryption.blogspot.com/.../selective-image-encryption

Bibliography

[1] c. Ratael, Gonzales, e. Richard, and woods, "Digital image processing," 2nd Ed, Prentice hall, 2002.

[2] W.Stallings,Cryptography and network security:Principles and Practice.Prentice hall,2010,vol.998