Partial Encryption Of Color Image By Edge Detection

Ali A.Yassin
Iraq-Basrah
Basrah University
Education College
Computer Science
AliAdel2005Alamre@Yahoo.com

Abstract

The research is aim to use some of image features which represent in edge detection method, color image analyses for main components (Red, Green and Blue) and then collected this features with main principles of partial encryption for obtain to modern algorithm can get exact results , high processing speed, in addition we use one bit from each byte that located in edge of each layer(Red, Green and Blue) of color image instead use all bits of byte, the operation of selected bit called "Bit-Plane" . The algorithm rely on two images , the first is representing the image that we want encryption it and the second key image is deriving from it. The high performing is very active of algorithm when we deal with pixels parts of both images , these parts are calling edge pixels that calculate in canny method. At last we are performed encryption operation by using "XOR" for each layers in input and key images for producing encrypted image. The strong of algorithm in expected difficult of key image and then discovered plane of bit for both images.

Key Word :- Encryption, Edge detection , partial encryption, Histogram, Correlation.

1- Introduction

The important characteristics of color image analysis is the possibility to their basic parts, a red, green and blue as well as at the expense of the edges of each layer in a manner "Canny", and then used in the partial encryption of the image by drawing on the way XOR "" and "Bit-Plane" of the input image and the key image stipulated that the Plane is the same for the key image, which added more power to the algorithm. The mechanics of the algorithm started with difficulty find a key and then selecting the plane located on the edges of the image as well as the possibility of the algorithm eventually work on the colorful image where you get the image color encrypted by grouping the three layers(Red, Green, Blue) and the production of the partial encrypted image will also be seen in the next sections.

Normally, The image have many features are different in how we can get image. These differences depend on type of image (Color ,Gray , Black white) therefore we focus on color image , in this research we increased effected of edge detection method because the previous method is deal just with gray level image and we work with color image to both images(Input, Key).

2- Literature Survey

This literature survey cover some related work reported in journals, thesis and conference proceedings as follows:

1. In 1997, Li X., Knipe J., Cheng H. [1] proposed two separate algorithms to compress and encrypt images. In the first, an quad tree-based algorithm is used to decompose the image in the spatial domain. In the second, a wavelet transform is used to decompose the image in the transform domain and a modification of the SPIHT algorithm. A partial encryption method in this work takes advantage of the image analysis and simplifies, or even eliminates, the need for broken secret-key encryption.

2. In 1998, Cheng H. [2] proposed an alternative solution, called *partial encryption*, in which a secure encryption algorithm is used to encrypt only part of the compressed data. Partial encryption is applied to several image and video compression algorithms in this work.

3. In 2000, Cheng H., Li X. [3] proposed a solution called *partial encryption*, in which a secure encryption algorithm is used to encrypt only part of the compressed data. Partial encryption is applied to still image. Only 13%-27% of the output from quad tree compression algorithms is encrypted for typical images, and less than 2% is encrypted for 512×512 images compressed by the SPIHT algorithm.

4. In 2002, Miaou S., Chen S., Lin C. [4] proposed a partially encrypting scheme combining SPIHT and AES. In this scheme, compressed SPIHT bit streams are

identified based on their importance to signal quality. Then, AES is used to encrypt only the important part that can be defined and chosen by a user.

5-In 2007, Hameed A.[5] proposed new partial encryption schemes are proposed, in which a secure encryption algorithm is used to encrypt only part of the compressed and uncompressed data. Partial encryption is applied using several image compression algorithms. Only 0.0244%-25% of the original data is encrypted for four different grayscale images and four color image images (256*256) pixels, resulting in a significant reduction in encryption and decryption time. **In this research**, we are rely on partial encryption by using XOR operation to encrypted edge detection of input image. The key extract from other image to support algorithm, during apply encryption method. The suggestion algorithm which depend on Bit-Plain Method and stream cipher for image encryption by using XOR away.

3- Color Images

Color images can be modelled as three-band monochrome image data, where each band of image corresponds to different color. The actual information stored in the brightness information in each spectral band. Typically, color images are represented as red, green, and blue; or RGB images. Figure (1.1c) shows color Lena's image [1, 11].

Graphics file formats store RGB images (True color image) as 24-bit images, whereas the red, green, and blue components are 8 bits each. RGB color information is transformed into a mathematical space that separates the image information better than RGB [1, 11]. This situation is shown in Figure (2).

a) Binary image

b) Gray-scale image

c) Color image

Figure (1.1): Lena image
a) Binary image
b) Grayscale image
c) Color image

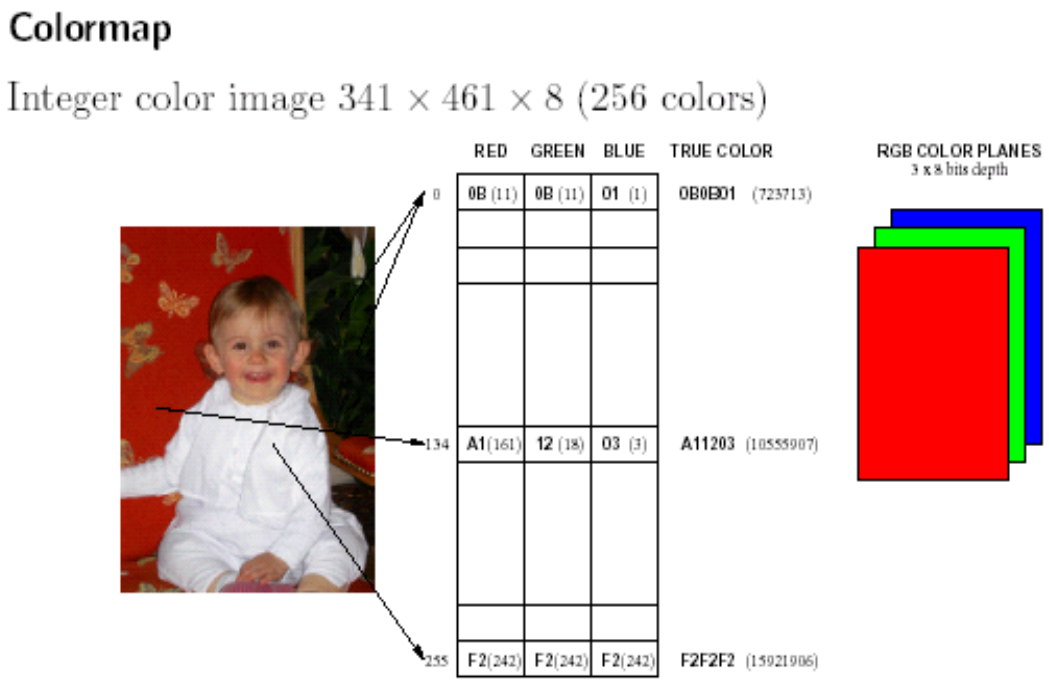


Figure (2): Color representation.

The colormap of a grayscale image has RED=GREEN=BLUE, which all maps to a luminance level. A True color image (depth=24) is equivalent to 3 images of depth 8, one per primary color [11].

4- Encryption

Encryption is the process of encoding a message/images such that its meaning becomes not obvious; *decryption* is the reverse process: transforming an encrypted message/image back into its normal form. A system of encryption and decryption is called *a cryptosystem*. This situation is shown in Figure (3)[6].

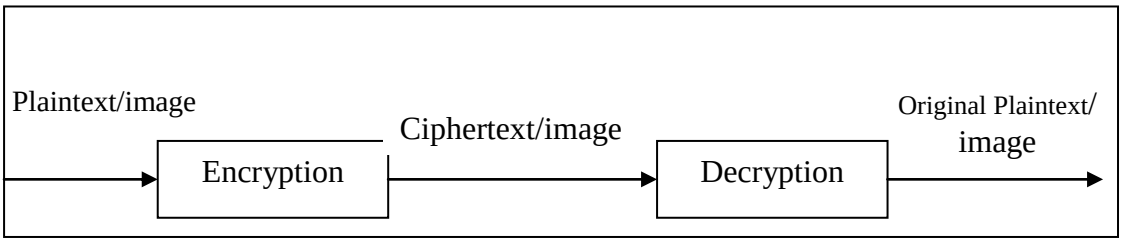


Figure (3): Cryptosystem

The art and science of keeping a message/image secure is *cryptography*, and it is practised by cryptographers. Cryptography deals with the design and analysis of systems that provide secure communications or resist cryptanalysis [6,7].

Cryptanalysts are practitioners of cryptanalysis; the art and science of breaking Cipher text/image; that is, seeing through disguise. The branch of mathematics encompassing both cryptography and cryptanalysis is *cryptology* and its practitioners are *cryptologists* [6,8].

A cryptographic algorithm, also called *a cipher*, is the mathematical function used for encryption and decryption. If the security of an algorithm is based on keeping the way that algorithm works a secret, it is a *restricted algorithm.*

The security of the modern cryptography is based on the key. The range of the possible values of the key is called *the key space* [8].

Cipher systems can be classified according to key into two types: secret key systems and public key systems [6,9].

4-1 Secret key systems (symmetric algorithms):

In most symmetric algorithms, the encryption key and the decryption key are the same as shown in Figure (4).

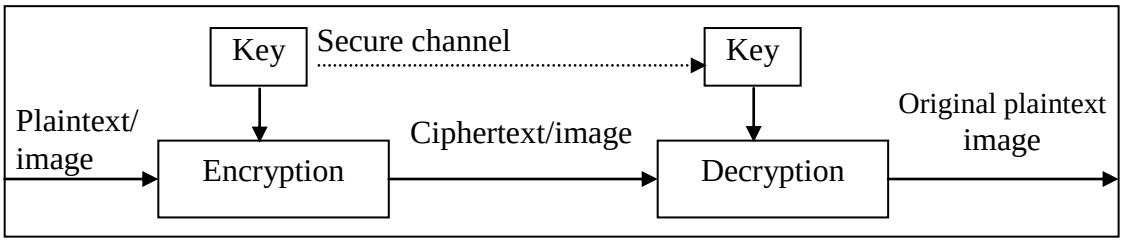


Figure (4): Secret key systems

4-2 Public key systems (asymmetric algorithms):

Asymmetric algorithms are designed so the key can used for encryption, which is different from the key used for decryption, see Figure (5).

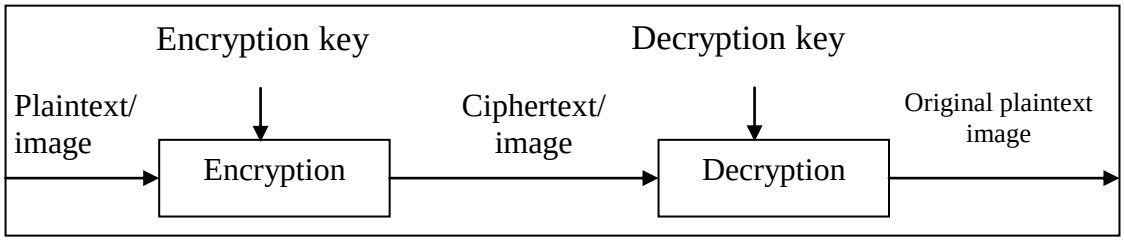


Figure (5): Public key systems

Figure (6) shows classification of cipher systems [6,10]. In this figure, we can see that symmetric modern cipher systems are also classified into block cipher systems, and stream cipher systems.

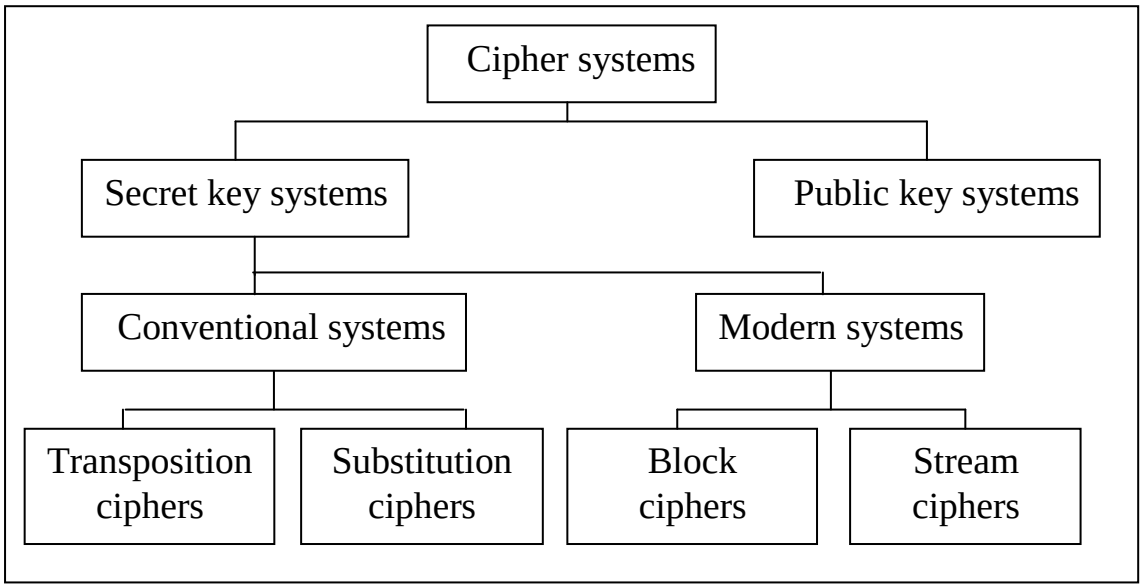


Figure (6): Classification of cipher systems based on key

4-3 Stream Cipher

Stream ciphers convert plaintext/image to ciphertext/image one bit a time. The simplest implementation of a stream cipher is shown in Figure (7) [6,9]. A keystream generator (sometimes called a *running-key generator*) outputs a stream of bits: K_1, K_2, K_3,……,K_i. This keystream is XORed with a stream of plaintext bits, P_1, P_2, P_3,….,P_i to produce the stream of ciphertext/image bits C_1, C_2,……C_i.

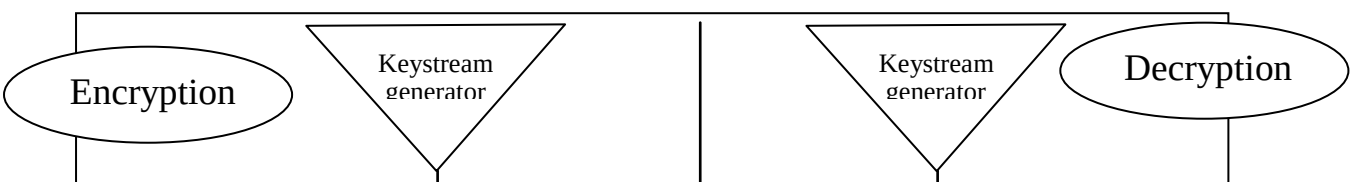
$$C_i = P_i \oplus K_i \qquad \ldots (1)$$

At the decryption end, the ciphertext bits are XORed with an identical keystream to recover the plaintext bits [10].

Since

$$P_i = C_i \oplus K_i \qquad \ldots (2)$$

$$P_i \oplus K_i \oplus K_i = P_i \qquad \ldots (3)$$



Stream cipher system consists of two main parts as shown in Figure (8) [9]:
1-Algorithm to generate keystream.
2- XOR gate.

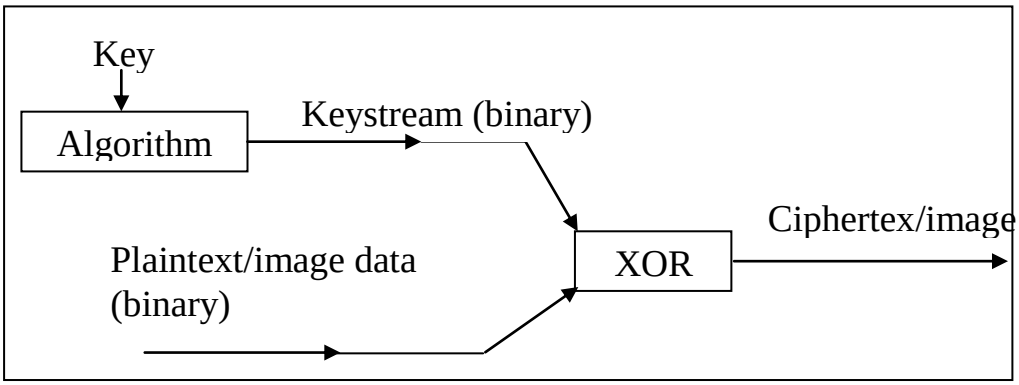


Figure (8): Stream cipher parts

Most algorithms which are used to generate keystreams are based on using shift register. Thus, the main component of the keystream generator is the shift register [5].

5- Partial Encryption

Partial encryption (also called *selective encryption* or *soft encryption*) is a secure encryption algorithm which is used to encrypt only part of the data. It is used to reduce encryption and decryption time [5]. Figure (9) illustrates the difference between the partial encryption approach and the traditional approach.

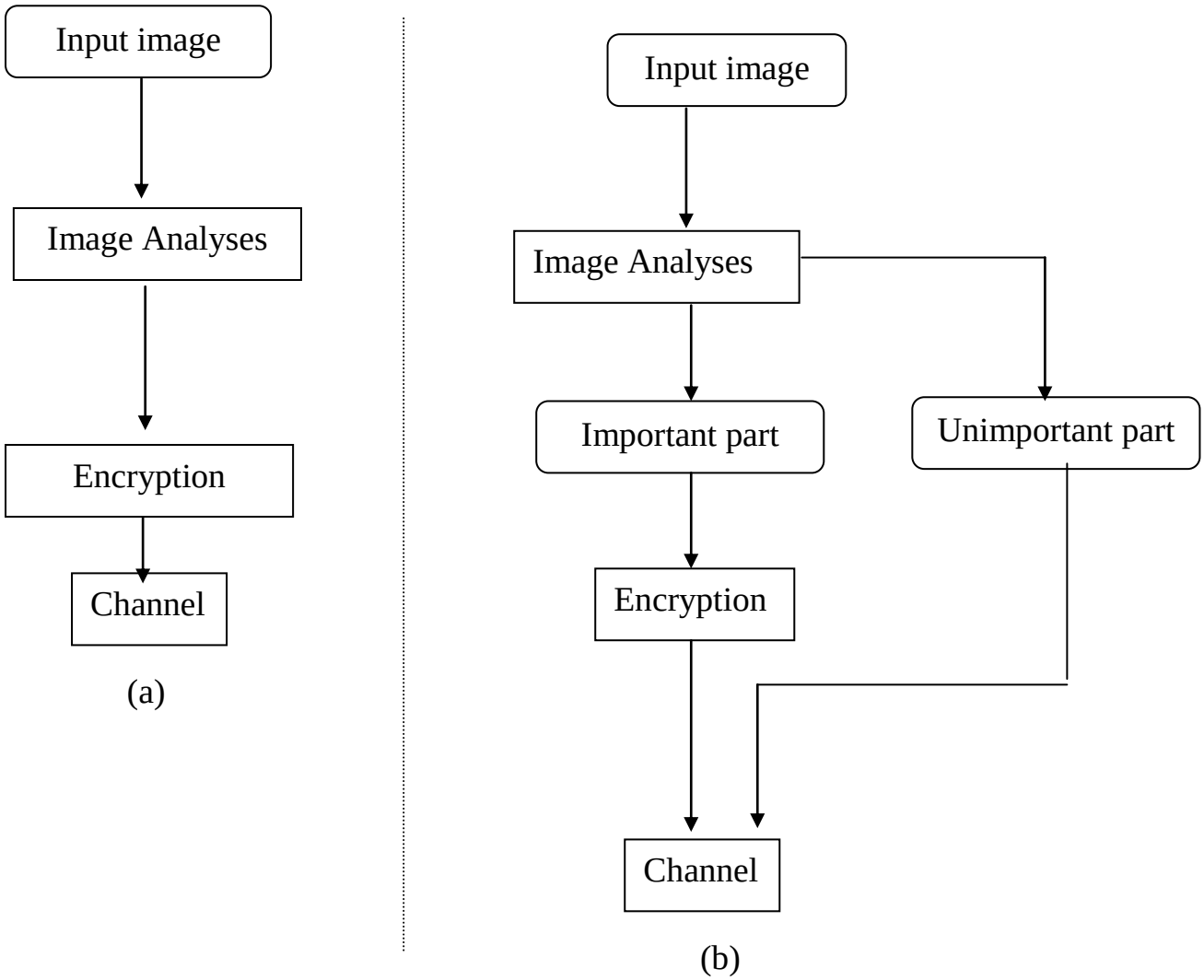


Figure (9): Encryption of (a) the traditional approach to secure image communication and (b) the partial encryption approach.

6-Edge detection by Canny method

We can use the edge method to detect edges, which are those places in an image that correspond to object boundaries. To find edges, this method looks for places in the image where the intensity changes rapidly, using one of these two criteria: Places where the first derivative of the intensity is larger in magnitude than some threshold Places where the second derivative of the intensity has a zero crossing edge provides a number of derivative estimators, each of which implements one of the definitions above. For some of these estimators, you can specify whether the operation should be sensitive to horizontal or vertical edges, or both. edge returns a binary image containing 1's where edges are found and 0's elsewhere. The most powerful edge-detection

method that edge provides is the Canny method. The Canny method differs from the other edge-detection methods in that it uses two different thresholds (to detect strong and weak edges), and includes the weak edges in the output only if they are connected to strong edges. This method is therefore less likely than the others to be "fooled" by noise, and more likely to detect true weak edges. The following figure(8) below illustrates the power of the Canny edge detector. It shows the results of applying the Canny edge detectors to lena image in the figure(9).

Figure (9)explain stages of Canny edge detection

7- Evaluation of Image Encryption Schemes

To evaluate each of the proposed image encryption schemes, five aspects are examined [5,6]:

1. **Security**. Security in this work means confidentiality and robustness against attacks to break the images. It is obvious that the goal is not 100% security, but many advanced algorithms are adopted, such as AES, Chaotic, and Stream ciphers that make them difficult to cryptanalyze.
2. **Speed**. Less data (important part) to encrypt means less CPU time required for encryption. So, in general partial encryption algorithms are used to reduce encryption and decryption time.
3. **Correlation**. Correlation (*Corr*) measures the similarity between the original image and the reconstructed image. The aim is to get a correlation value closed to 1.

The correlation can be defined as [1,5]:

$$Corr = \frac{\sum_{r=1}^{N}\sum_{c=1}^{M}(I_1(r,c)-\bar{I}_1)(I_2(r,c)-\bar{I}_2)}{\sqrt{[\sum_{r=1}^{N}\sum_{c=1}^{M}(I_1(r,c)-\bar{I}_1)^2][\sum_{r=1}^{N}\sum_{c=1}^{M}(I_2(r,c)-\bar{I}_2)^2]}} \quad \text{.....4}$$

Where:

: is the value of pixel at *(r,c)* of the original image. $I_1(r,c)$

: is the mean of the original image that: $\bar{I}_1$

$$\bar{I}_1 = \frac{1}{M \times N} \sum_{r=1}^{N} \sum_{c=1}^{M} I_1(r,c) \qquad \ldots\ldots\ldots 5$$

: is the value of pixel at *(r,c)* of the reconstructed image (or modified image). $I_2(r,c)$

: is the mean of the reconstructed image (or modified image) that: $\bar{I}_2$

$$\bar{I}_2 = \frac{1}{M \times N} \sum_{r=1}^{N} \sum_{c=1}^{M} I_2(r,c) \qquad \ldots\ldots\ldots 6$$

M: height of the image.

N: width of the image.

r and c: row and column numbers.

For color images, the reconstruction of the three color spaces must be considered in the correlation calculation. The correlation is calculated for the reconstruction of each color space. The average of these three correlations is used to generate the *Corr* of the reconstructed RGB image. The color correlation equation is as follow:

$$Corr_{RGB} = \frac{Corr_{red} + Corr_{green} + Corr_{blue}}{3} \qquad \ldots\ldots\ldots 7$$

where $Corr_{red}$, $Corr_{green}$ and $Corr_{blue}$ are the correlation for each space color and computed by equation (10).

4.Keyspace Analysis. A good image encryption algorithm should be sensitive to the cipher key, and the keyspace should be large enough to make brute-force attack infeasible. The keyspace of the algorithms in this research represent size(Rows * Columns) of one layers from three ,so that each pixel have 8bits.

5.Histograms of encrypted images. Select several 256 gray-level images with size of Row×Columns that have different contents, to calculate their histograms. One can see that the histogram of the cipher-image is significantly uniform and different from that of the original image.
In this work, several experiments will be presented.

8- Algorithms

We suggested in this research, algorithm of partial encryption for color image which are depending on edge detection operation of two images(input ,key) which previously were enter . But there are important question "How we can compute edge detection to color image?", well we know the edge detection rely on gray level image therefore we decomposed the color image into three layers Red(R) , Green (G) and Blue(B)and then compute edge detection for each one after this process will come role of separate operation for each pixel which is locate in edge zone for each image(input, key). The next step to perform encryption operation between each layer in input and key images so we will detected plain for each image. These plains refer for each bits which locate in edge zone and in end of this step ,we will get three layers (RGB) for

each image, which contains value of bit plain to the pixel located in edge detection. Finally we applied XOR operation between similar layers (such R of input with R of key image) and in the end we will get three layers are representing the result of XOR for each similar layers. The last layers will embedded in input image and we will get new image was encrypt partial as well as we will note strong of algorithm, through compute histogram and correlation. The following algorithm and figure(11)explain mechanism of algorithm work.

Encryption of Color ImageBy Using Edge Detection Algorithm

```
Input Im,Imk,PlainE,PlainK
[n m]=size(Im)
Iimresize(Imk,n,m)
Iim2RGB(Im,RI,GI,BI)
Iim2RGB(Imk,RK,GK,BK)
Edge(RI,GI,BI,RIE,GIE,BIE)
Edge(RK,GK,BK,RKE,GKE,BKE)
For k =1 To 3
  For i=1 To n
    For j=1 To m
      newR(i,,j,k)=Bitget(RIE(i,j,k),plainE) XOR Bitget(RKE(i,j,k),plainK)
      newG(i,,j,k)=Bitget(GIE(i,j,k),plainE) XOR Bitget(GKE(i,j,k),plainK)
      newB(i,,j,k)=Bitget(BIE(i,j,k),plainE) XOR Bitget(BKE(i,j,k),plainK)
    Next j
  Next i
Next k
For k =1 To 3
  For i=1 To n
    For j=1 To m
      Bitset(newR(i,,j,k),New,PlainE)
      Bitset(newG(i,,j,k),New,PlainE)
      Bitset(newB(i,,j,k),New,PlainE)
    Next j
  Next i
Next k
Correlation(New,Im)
```

End Encryption of Color ImageBy Using Edge Detection Algorithm

Where:

Im,ImK :The images which we needs in algorithm whears im(Input image that encrypted),ImK(Key image which extract key from it).

N,M,K,I,J : parameters are relate with image size.

Imresize : procedure is resize of key image in N,M.

Edge:- procedure for presented Canny method.

Iim2RGB : is procedure for image analyses to RGB layers.

PlainE : The number of bit which taken from any pixel in selected layer of input image.

PlainK : The number of bit which taken from any pixel in selected layer of Key image.

Layern new: The set of bits which get from one or more layers in input image by using bitget procedure .

Layern newKey : The set of bits which get from one or more layers in Key image using bitget procedure.

Layers:The set of bit which we obtain it from XOR operation.

Correlation: is one of scales image encryption.

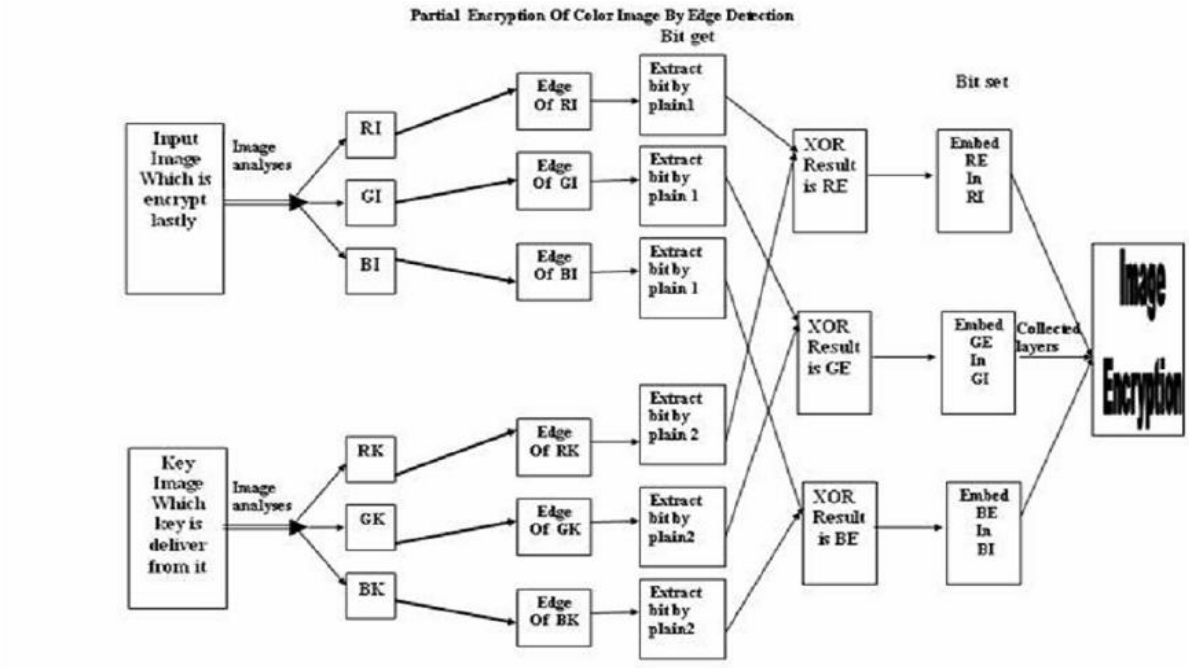


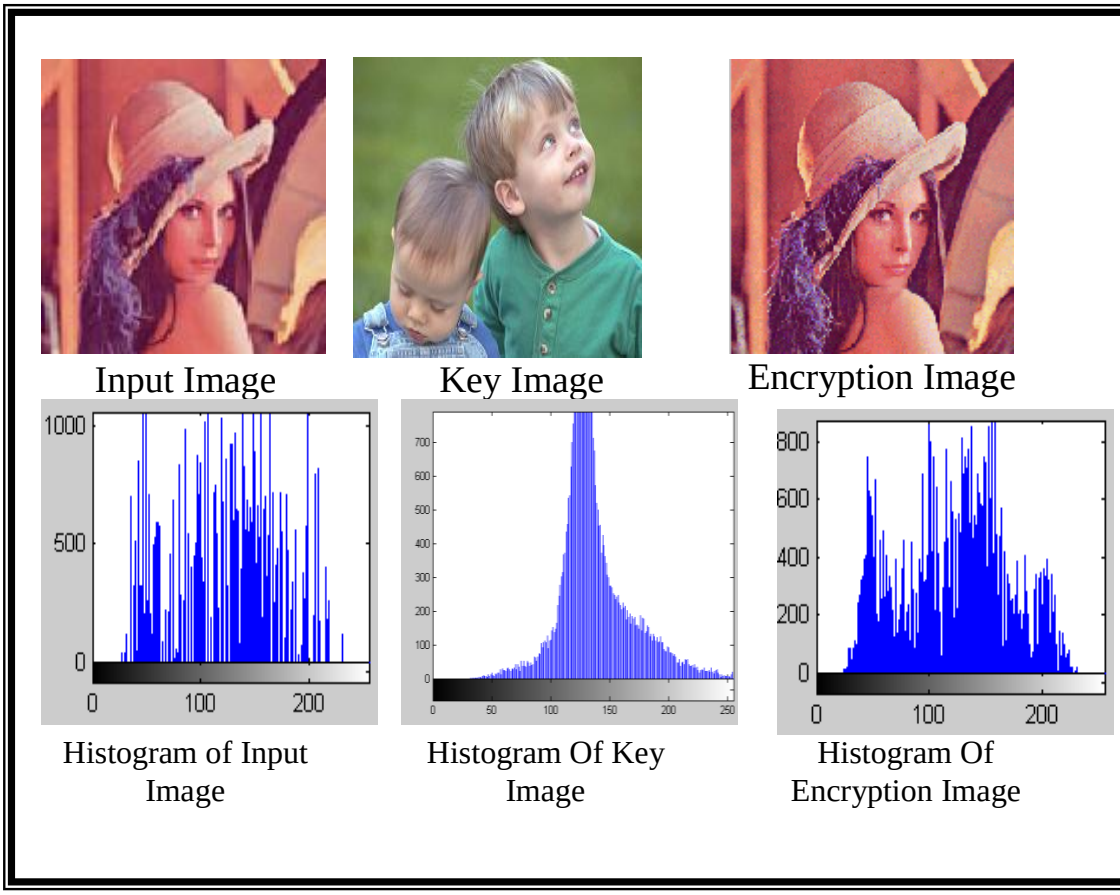
Figure (10)explain Propposed algorithim

9- Experimental Results

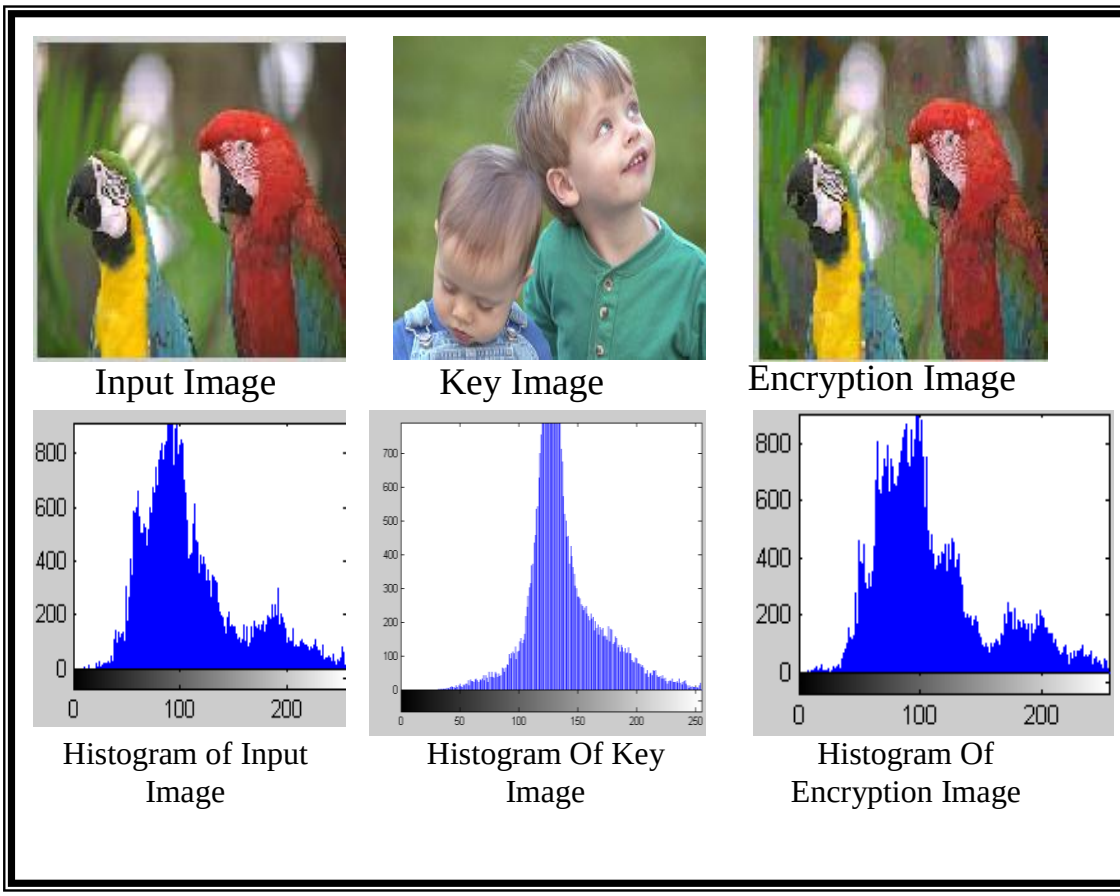
In this experiment, we will input two color image(Input/Key) the first represent image which encrypted by depending on key that derived from second image by using image analysis (RGB) and then applied edge detection for each layer. The figures(11,12,13,14) represent set of images before encryption and after perform it by using different plains as well as histogram of each image, as clear in the following table(1):-

Table(1) is explain the results experiential in Suggestion Algorithm

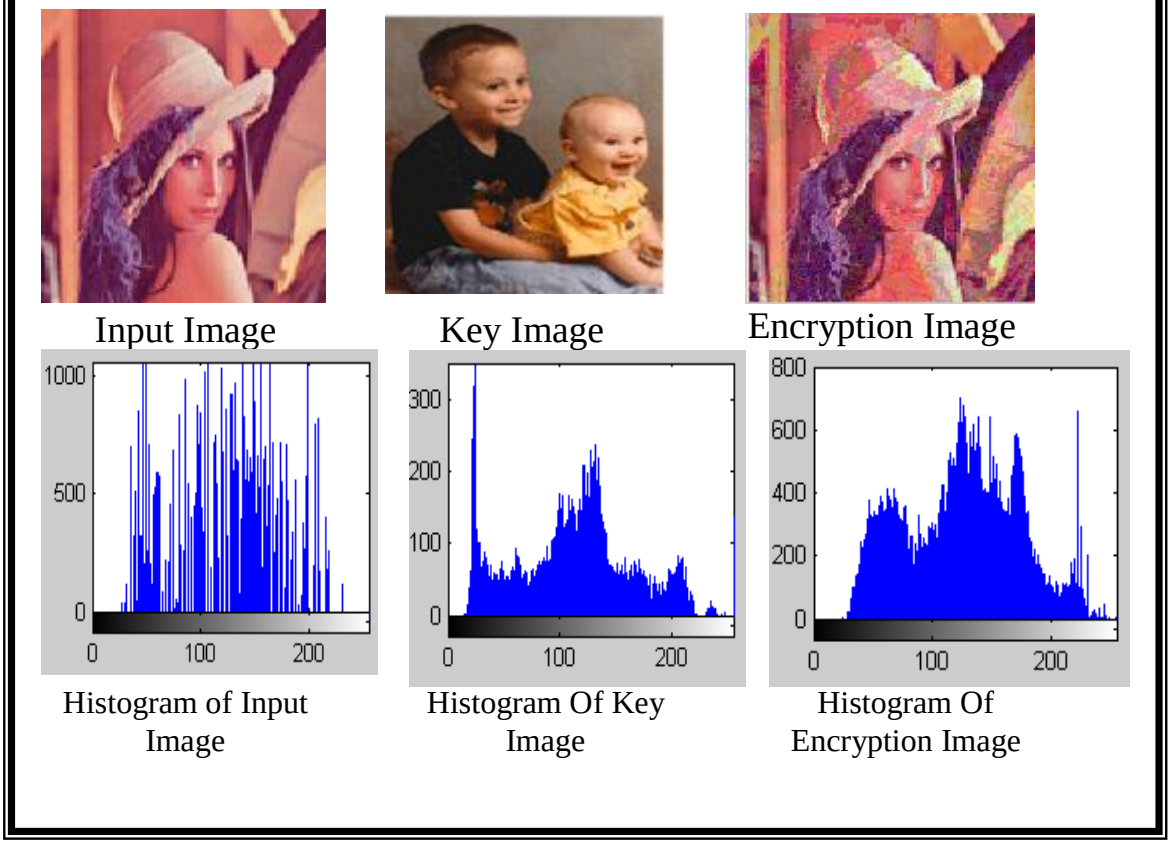
Plain Of Input Image	Plain Of Key Image	Correlation Ratio	State
4	**6**	**0.9934**	**1**
5	**7**	**0.9780**	**2**
6	**6**	**0.8910**	**3**
5	**4**	**0.9828**	**4**



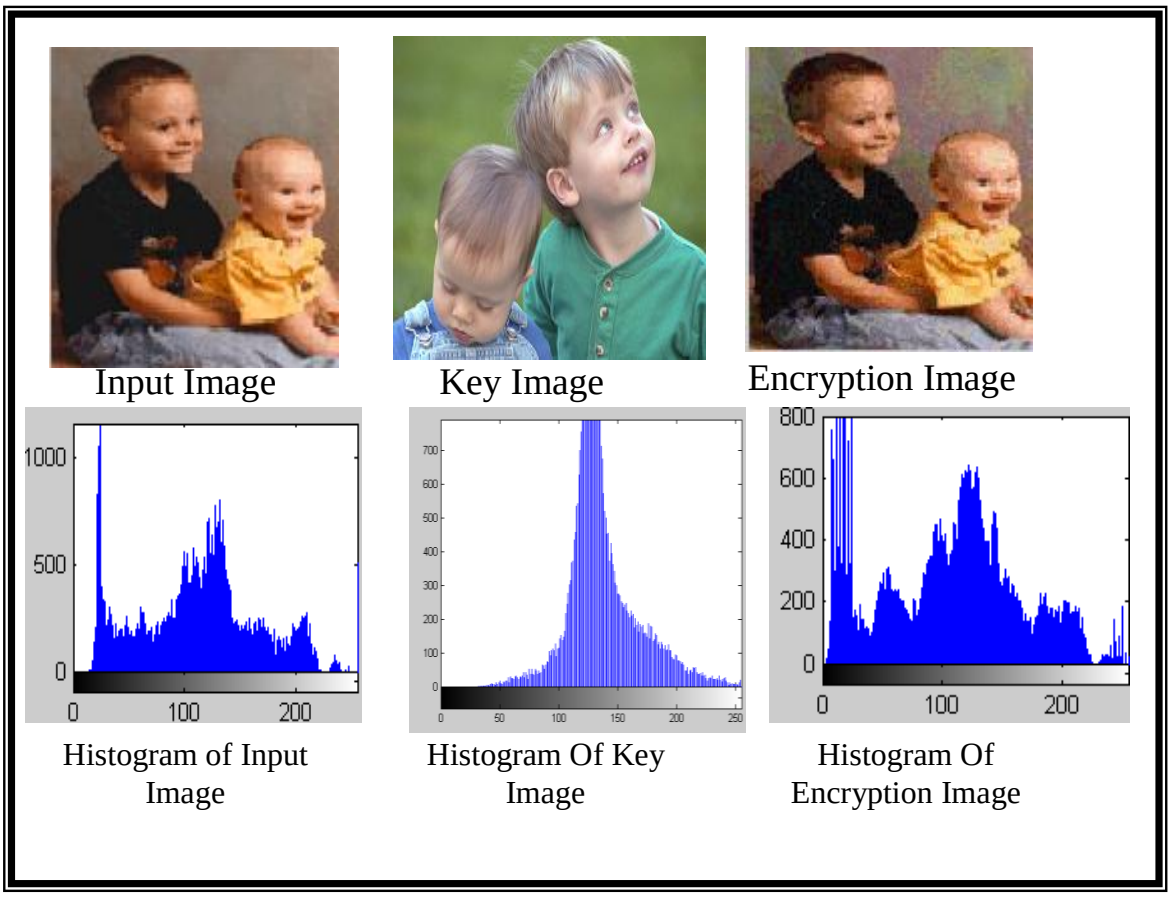
Figure(11) is explain first state1 in tabel1



Figure(12) is explain first state2 in tabel1



Figure(13) is explain first state3 in tabel1



Figure(14) is explain first state4in tabel1

10-Conclusion

During of experiments results of research ,we can conclude many important things from edge detection uses of color image in partial encryption through note exact results as well as, key image determining difficult from attackers and how can they detect the bit plain of pixels that located in edge of image. The algorithm depend on color image therefore we must convert image to basic colors (RGB) to make edge operation is very activity, the last step is representing development about edge detection so we know the edge detection work just on gray level image ,in this research the mechanism of edge detection develop to deal with color images and put new manner of partial encryption space and in the same time we note increase to processing speed.

References

[1] Blackledge J. M., Ptitsyn N., ***"Deterministic Chaos in Digital Cryptography",***
Institute of Mathematical and Simulation Sciences, Faculty of Computer Sciences and Engineering, De Montfort University,Leicester, England, 2000.

[2]Blelloch G. E.,*"Introduction to Data Compression",* Computer Science Department, Carnegie Mellon University, October 2001.

E-mail: blelloch@cs.cmu.edu.

[3] Cheng H., Li X., "Partial Encryption of Compressed Images and Videos", IEEE Transaction Signal Processing, Vol. 48, No. 8, pp. 2439-2451, August 2000.

[4] Miaou S., Chen S., Lin C., "An Integration Design of Compression and Encryption forBiomedical Signals",Journal of Medical and Biological Engineering, Vol. 22, No. 4, pp. 183-192, 2002.

[5] Hameed A.Younes "New Techniques for Partial Encryption of Wavelet-based Compressed and Uncompressed Images", PhD Thesis, Department of Computing Science, University of Basrah, November 2006.

[6] Baxes G. A., "Digital Image Processing: Principles and Applications", John Wiley & Sons, Inc., USA, 1994.

[7] Gonzalez R.C., Woods R. E., "Digital Image Processing", Addision-Wesley, Inc., USA, 1992.

[8] Stallings W.,"Cryptography and Network Security, Principles and Practice", third Edition, Pearson Education International, Inc., USA, 2003.

[9] Schneier B., "Applied Cryptography, Second Edition: Protocols, Algorithms and Source Code in C", John Wiley & Sons, Inc., USA, 1996.

[10] Umbaugh S. E., "Computer Vision and Image Processing", Prentice-Hall, Inc., USA, 1998.

[11] Lee D., *"Coding of Still Pictures",* In Proceedings of SPIE, Vol. 4115, of the 45th annual SPIE meeting, Applications of Digital Image Processing XXIII, July 2000.

الخلاصة

البحث يهدف الى استخدام بعض ميزات الصورة التي تتمثل بطريقة Canny لحساب حواف الصورة وتحليل الصورة الملونة الى اجزائها الاساسية (الاحمر والازرق والاخضر) ومن ثم جمع هذه الميزات مع المباديء الرئيسية للتشفير الجزئي للحصول على خوارزمية حديثة نستطيع من خلالها الحصول على نتائج جيدة و سرعة معالجة عالية فضلا عن كونها تستخدم ثنائية معينة من كل ثمانية تقع على حواف كل طبقة من طبقات الصورة الملونة بدلا من استخدام الثمانية باكملها وبطريقة " Bit-plane". الخوارزمية تعتمد على صورتين الاولى هي التي نريد تشفيرها و الثانية هي الصورة المفتاحية التي نشتق المفتاح من خلاللها والتي تحلل الى طبقات (الاحمر , الازرق،الاخضر) وتحسب حافة كل طبقة ثم نختار ثنائية معين من كل ثمانية لكي تشفر مع نظيرتها في الصورة المدخلة.
الانجازية العالية تكون جدا فعالة للخوارزمية عندما نتعامل مع جزء من نقاط الصورة بدلا من التعامل مع كافة بيانات الصورة وذلك من خلال طريقة " Canny" لحساب حواف الصورة. بالاخير سوف نقوم بعملية التشفير باستخدام طريقة "XOR" على كل طبقة من الصورة المدخلة و صورة المفتاح لينتج صورة مشفرة جزئيا . قوة الخوارزمية تتمثل بصعوبة توقع المفتاح لان الصورة غير محددة للشخص المهاجم ثم بعد معرفته الصورة عليه تحديد موقع كل ثنائية بين الصورة المدخلة والصورة المفتاحية.