Design New Algorithm For Partial Image Encryption Based colors Space

Ali A.Yassin
Basrah University, Education College, Computer Science

Abstract

This research aims to create two encryption algorithms and which have the ability to partial encryption of any image by using the key to be chosen from another image, both algorithms depend on techniques to analyze the image into three layers (RGB / YIQ) for both images entered and tagged. The next step is to determine the specific number for both images to select bit from each pixel of one of the three layers for both image tagged or the input image and then apply the XOR operation between the two bits opposing both classes of the input image and the image of the key. As a result of the last operation leads to encrypt three layers, both based on the RGB or YIQ and then they are incorporated into class's encoded leads to obtain the encrypted part. The strength of both algorithms how to find one key first and then specify the layer as second and then know the number of bit action chosen Third, where will be generated to have a space key is very much depends on image size, leading to difficult to break, but scales standards that are the similarities and the likelihood that the balance algorithm YIQ to RGB as well as processing speed, where we focused on the part of the image instead of dealing with all the data in addition to the difficulty in projecting the key through the very large key space.

Key words: Encryption, Correlation, Bit Plane, RGB, YIQ.

الخلاصة

يهدف هذا البحث إلى إنشاء خوارزميتي تشفير واللتان تمتلكان القابلية على التشفير الجزئي لأي صورة بواسطة استخدام مفتاح يتم اختياره من صورة أخرى، كلا الخوارزميتين تعتمدان على تقنيات تحليل الصورة إلى ثلاث طبقات (RGB/YIQ) لكلا الصورتين المدخلة والمفتاحية . الخطوة التالية هي تحديد رقم معين لكلا الصورتين لاختيار ثنائية من كل نقطة من واحدة من الطبقات الثلاث سواء للصورة المفتاحية أو الصورة المدخلة ثم بعد ذلك نطبق عملية XOR بين كلا الثنائيتين المتقابلتين لكلا الطبقتين من الصورة المدخلة وصورة المفتاح.نتيجة العملية الأخيرة تؤدي إلى تشفير الطبقات الثلاث سواء المعتمدة على RGB أو YIQ ثم بعد ذلك تدمج الطبقات المشفرة فتؤدي إلى حصول على صورة مشفرة جزئيا.تكمن قوة كلا الخوارزميتين في كيفية معرفة صورة المفتاح أولا ثم تحديد الطبقة ثانيا ثم معرفة رقم البت المختار ثالثا حيث سيتولد لدينا فضاء مفتاح جدا كبير يعتمد على حجم الصورة مما يؤدي لصعوبة كسره، أما المقاييس التي اعتمدنها هي التشابه والذي أرجح كفة خوارزمية YIQعلى RGB فضلا عن سرعة المعالجة حيث ركزنا على جزء من الصورة بدلا من التعامل مع كافة البيانات بالإضافة إلى صعوبة توقع المفتاح من خلال فضاء المفتاح الكبير جدا.

1- Introduction

The use of image processing has increased in recent years. When it is necessary to securely transmit data via networks in limited bandwidth, the encryption must be performed. Researchers have combined security and encryption together to reduce the overall processing time.

New partial encryption schemes are proposed, in which a secure encryption algorithm is used to encrypt only part of the image. Partial encryption is applied using several image encryption algorithms.

There are many encryption algorithms which are treat with encryption all or part of image, Whereas some of algorithms depending on create of key in random form or may be depending on equation to key generate it. The password of encryption field by key definition as image, whereas the last will be lead to reach broken key (decryption). The way that we suggested is difficult of knowing image that key derived from one layers (RGB/YIQ) of it.

Literature Survey

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

1. In 1997, Li X., Knipe J., Cheng H. (Li et .al., 1997) proposed two separate algorithms to compress and encrypt images. In the first, a 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(Set Partial in Hierarchical Trees) 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. (Cheng, 1998) 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. 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. (Miaou *et al.*, 2002) 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 2006, Hameed A. (Hameed A.Younes, 2006) 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. resulting in a significant reduction in encryption and decryption time. **Which approach**, we used some of image features by depending on color image analysis to the main elements of image by using color analysis in two algorithms the first using RGB and Second using YIQ image analysis. The key is derived from another image for encryption input image by using one layer of RGB or YIQ and different plants between image encrypted and image which derived key from it. The both algorithms which depend on Bit-Plan method and stream cipher for image encryption by using XOR away.

2- Image Representation

The human visual system receives an input image as a collection of spatially distributed light energy .This light energy will be represented in image as a ***pixel.*** Pixel is derived from image element and usually refers a single dot on a computer display. This energy will verify the types of images which will be explained here (Hameed Younes and 2006, Baxes, 1994):

2-1 Binary Images

In a binary image, each pixel assumes one of only two discrete values. Essentially, these two values correspond to on and off. A binary image is stored as a logical array of 0's (Off pixels) and 1's (On pixels). Lena’s binary image is shown in Figure (1.1a) as an example. These types of images are most frequently used in computer vision and other digital applications where the only information required for the task is general shape, or outline, information; for example, in facsimile (FAX) images (Hameed ,2006 and Baxes , 1994) .

2-2Grayscale Images

Gray-scale images are referred to one colour images. They contain brightness information only, i.e., no colour information. Lena's Gray scale image is shown in Figure (1.1b) as an example. Each pixel in these images is a single element. A digital greyscale image is typically represented by 8 bits per pixel (bpp) in its uncompressed form. Each pixel has a value ranging from 0 (black) to 255 (white), (Gonzalez and Woods , 1992).

2-3 Color Images

Colour images can be modelled as three-band monochrome image data, where each band of image corresponds to different colour. The actual information stored in the brightness information in each spectral band. Typically, colour images are represented as red, green, and blue; or RGB images. Figure (1.1c) shows colour Lena's image (Gonzalez R.C. and Woods R. E., 1992).

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 colour information is transformed into a mathematical space that separates the image information better than RGB(Li X. et .al.,1997 ,Gonzalez and Woods,1992 , and Stallings,2003). This situation is shown in Figure (1).

a) Binary image b) Gray-scale c) Color image

Figure (1): Color representation.

3- Color Space

There are other image representations, which are more effective in colour image processing. In this research, the **YIQ** color space of colour image representations is used. The type is described here.

In the case of a colour RGB picture, a point wise transform is made to the **YIQ** (luminance (Y), chrominance1 (I), and chrominance2 (Q)) color space. This space is more decors related than the RGB space and will allow for better processing later, as shown in Figure (2).

The transform is given by (Li X. et .al., 1997, Miaou S. et .al., 2002):

$Y = 0.299R + 0.587G + 0.114B$ . . . (1)

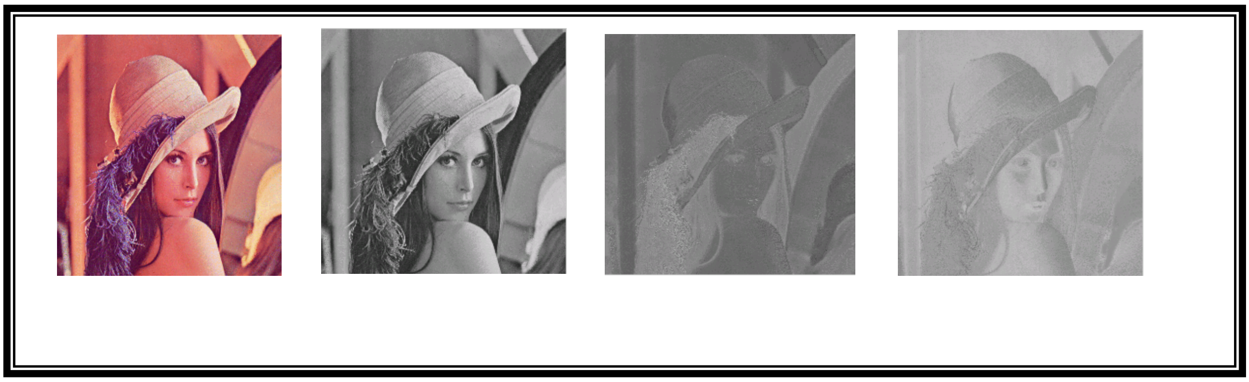
$I = 0.596R – 0.274G – 0.322B$ . . . (2)

$Q = 0.211R – 0.523G + 0.312B$ . . . (3), and the inverse transform is:

$R = Y + 0.956I + 0.621Q$ . . . (4)

$G = Y – 0.272I -0.647Q$ . . . (5)

$B = Y – 1.106I + 1.703Q$ . . . (6)



a) Lena image **b) Y** **c) I** **d) Q**

Figure (2): Lena image a) RGB image b) Y image c) I image d) Q image

4- Encryption

Encryption is the process of encoding message/images such that it's meaning becomes not obvious; *decryption* is the reverse process: transforming an encrypted text/sound/data/image back into its normal form. A system of encryption and decryption is called *a cryptosystem*. This situation is shown in Figure (3) (Schneier B., 1996).

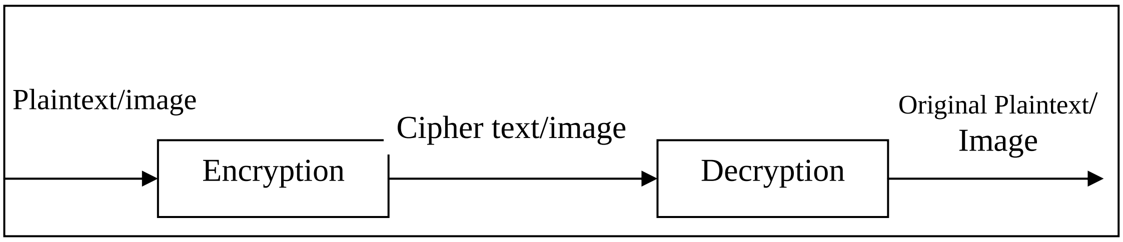


Figure (3): Cryptosystem

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 (Baxes G. A.1994, Umbaugh S. E., 1998).

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* (Schneier B., 1996).

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* (Stallings W., 2003).

Cipher systems can be classified according to key into two types: secret key systems and public key systems (Baxes G. A.1994 and Schneier B., 1996).

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).

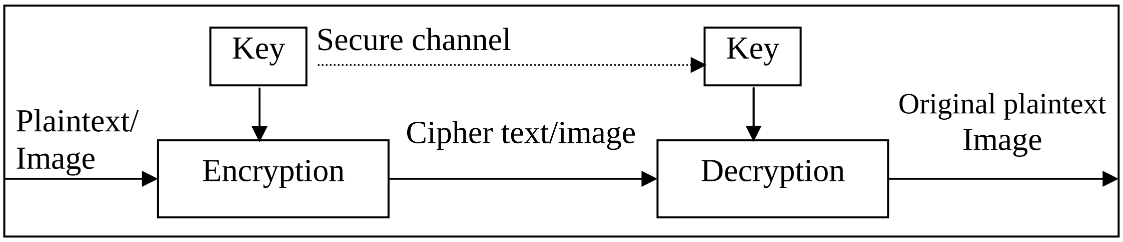


Figure (4): Secret key systems

4-2 Public key systems (asymmetric algorithms):

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

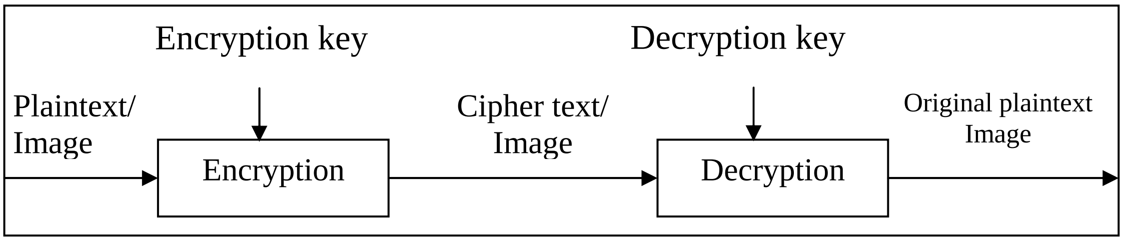


Figure (5): Public key systems

Figure (6) shows classification of cipher systems (Baxes G. A.1994 and Umbaugh S. E., 1998). In this figure, we can see that symmetric modern cipher systems are also classified into block cipher systems, and stream cipher systems.

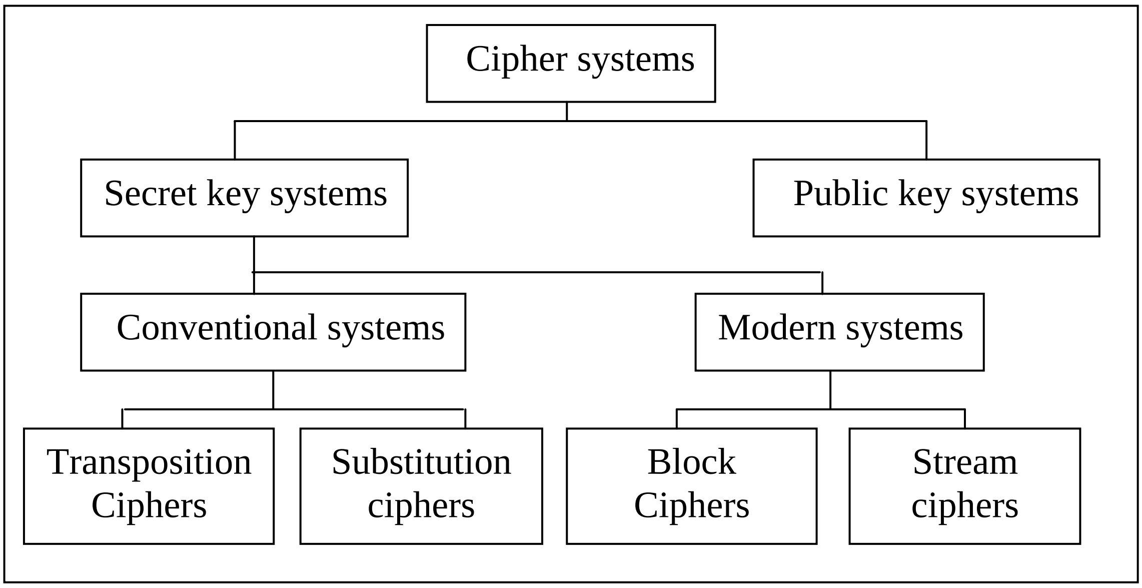


Figure (6): Classification of cipher systems based on key

4-3 Stream Cipher

Stream ciphers convert plaintext/image to cipher text/image one bit a time. The simplest implementation of a stream cipher is shown in Figure (7), (Schneier B., 1996). A key stream generator (sometimes called a *running-key generator*) outputs a stream of bits: K_1, K_2, K_3,……,K_i. This key stream is XORed with a stream of plaintext bits, P_1, P_2, P_3… Pi to produce the stream of cipher text/image bits C_1, C_2… Ci.

$$\boxed{C_i = P_i \oplus K_i} \qquad \ldots (7)$$

At the decryption end, the cipher text bits are XORed with an identical key stream to recover the plaintext bits (Stallings W., 2003).

Since

$$\boxed{P_i = C_i \oplus K_i} \qquad \ldots (8)$$

$$\boxed{P_i \oplus K_i \oplus K_i = P_i} \qquad \ldots (9)$$

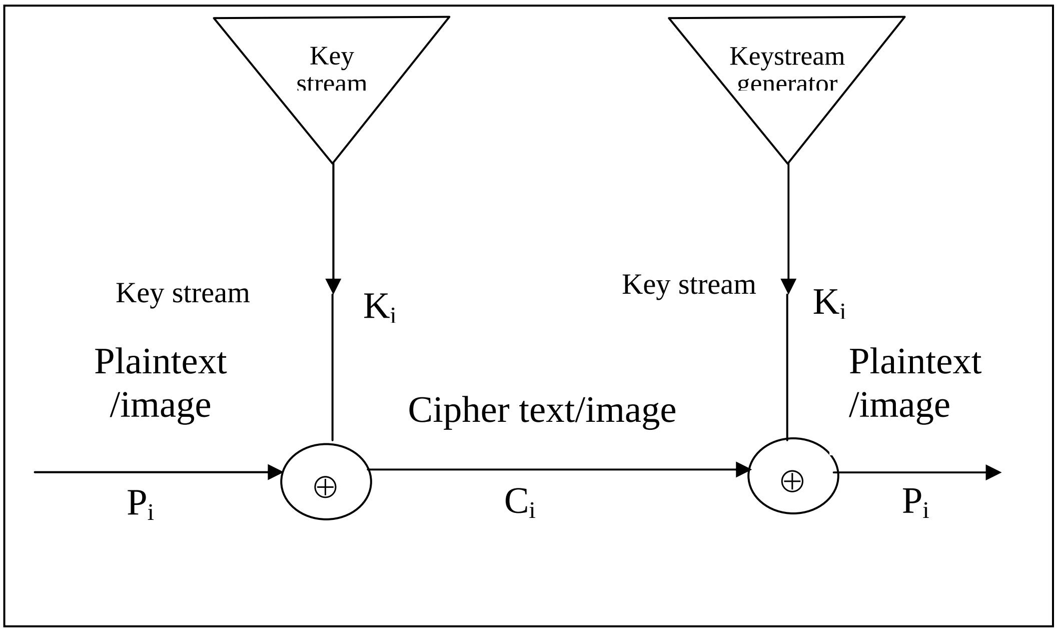


Figure (7): Stream cipher system

Stream cipher system consists of two main parts as shown in Figure (8), (Schneier B., 1996):

1-Algorithm for generate key stream.

2- XOR gate.

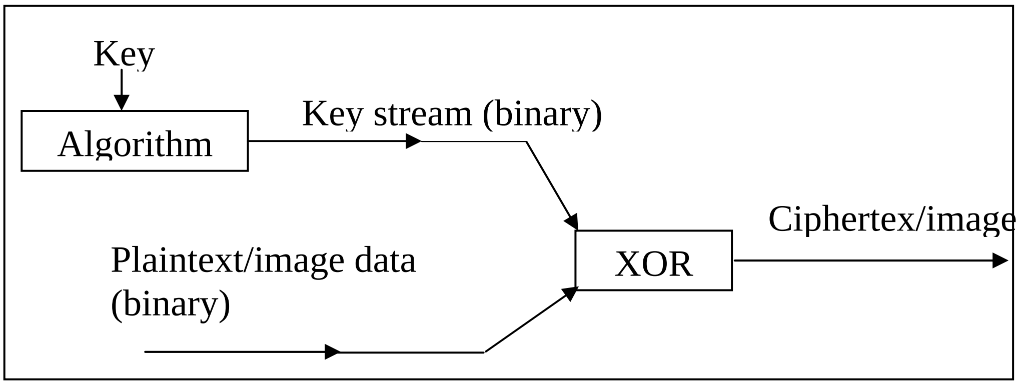


Figure (8): Stream cipher parts

Most algorithms which are used to generate key streams are based on using shift register. Thus, the main component of the key stream generator is the shift register (Hameed A.Younes, 2006).

4-4 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 (Hameed A.Younes, 2006).The following Figure (9) illustrates the difference between the partial encryption approach and the traditional approach.

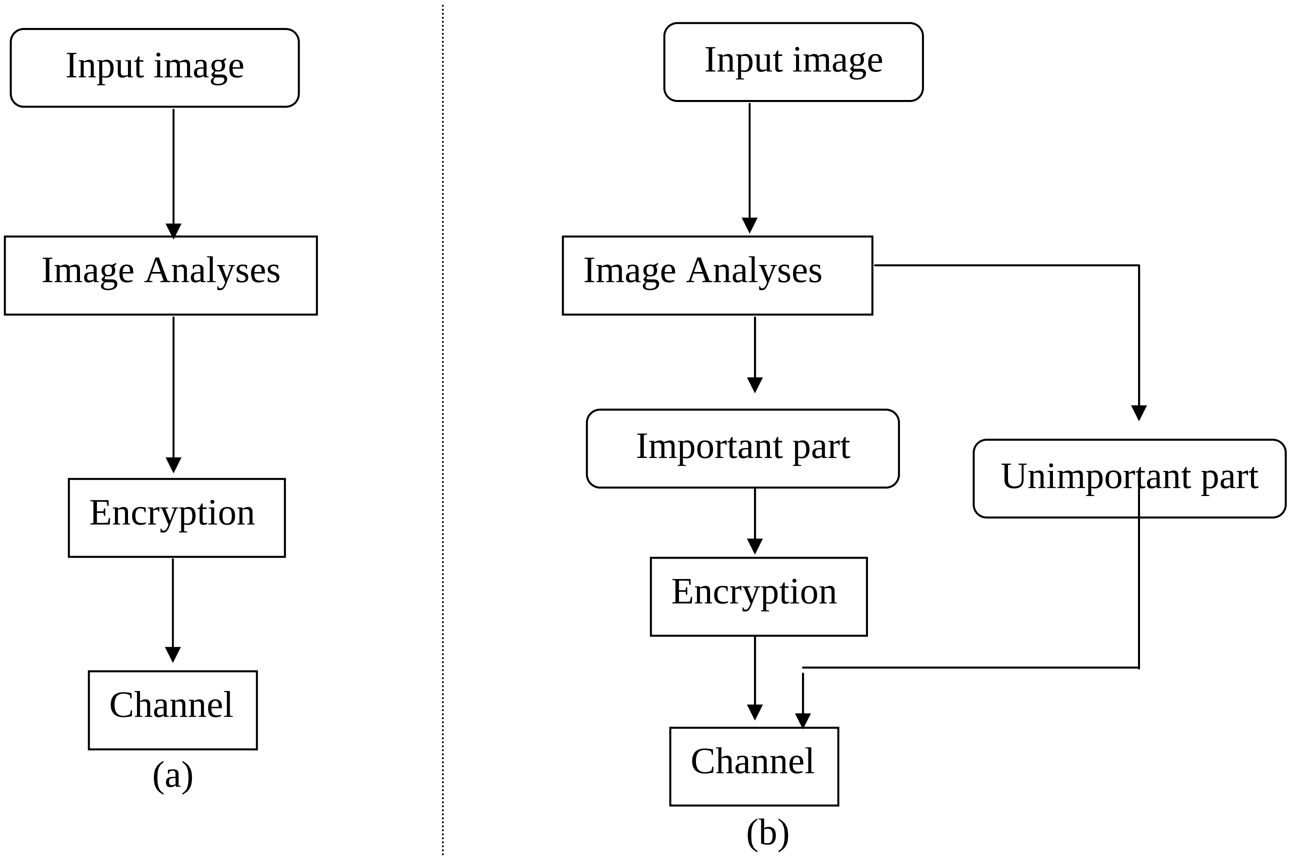


Figure (9): Encryption of (a) the traditional approach to secure image communication And (b) the partial encryption approach.

5- Evaluation of Image Encryption Schemes

To evaluate each of the proposed image encryption schemes, four aspects are examined (Hameed A.Younes, 2006, Baxes G. A.1994):

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 crypt analyze.
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 (Li X. et .al., 1997, Hameed A.Younes, 2006):

$$Corr = \frac{\sum_{r=1}^{N}\sum_{c=1}^{M}(I_1(r,c)-\bar{I}_1)(I_2(r,c)-\bar{I}_2)}{\sqrt{[\sum_{r=1}^{N}\sum_{c=1}^{M}(I_1(r,c)-\bar{I}_1)^2][\sum_{r=1}^{N}\sum_{c=1}^{M}(I_2(r,c)-\bar{I}_2)^2]}} \quad ....10$$

Where:

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

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

$$\bar{I}_1 = \frac{1}{M \times N}\sum_{r=1}^{N}\sum_{c=1}^{M} I_1(r,c) \quad ....11$$

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

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

$$\bar{I}_2 = \frac{1}{M \times N}\sum_{r=1}^{N}\sum_{c=1}^{M} I_2(r,c) \quad ....12$$

M: height of the image.
N: width of the image.
r and c: row and column numbers.

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

$$Corr_{RGB} = \frac{Corr_{red} + Corr_{green} + Corr_{blue}}{3} \quad ....13$$

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

4. Keyspace Analysis. A good image encryption algorithm should be sensitive to the cipher key, and the key space should be large enough to make brute-force attack infeasible. The key space of the algorithms in this research represent size (Rows * Columns) of each layers from three, so that each pixel have 8bits (Hameed A.Younes, 2006).

6- Algorithms

We suggested in this research two algorithms of partial encryption for color image which are depending on color image analysis to three layers (RGB/YIQ) as in the following form:-

6-1 RGB Encryption Algorithm

This algorithm is receive two input images, the first represent the image that will be encrypted ,and the second is represented key image throughout it. Both of them will be analysis into main components of image (RGB), after that we will detected one or more layers which ready for process and selected plane for each pixel of image. The plane represents the bit that will take from each pixel of image, and it isn't necessary the equal event of plane value in both of images, and also same state for layers.

This process will lead to difficult for obtain key or predict it and at the last will get strong algorithm for image partial encryption. Algorithm will be as the following:

```
RGB Encryption Image Algorithm
Input Im,Imk,PlaneE,PlaneK
[n m]=size(Im)
Iimresize(Imk,n,m)
Iim2RGB(Im,R,G,B)
Iim2RGB(Imk,R,G,B)
For k =1 To 3
   For i=1 To n
      For j=1 To m
          Layern new(i,,j,k)=Bitget(layers(i,j,k),planeE)
         Layern newKey(i,,j,k)=Bitget(layersKey(i,j,k),planeK)
     Next j
  Next i
Next k
New = XOR( Layern new, Layern newKey)
For k =1 To 3
   For i=1 To n
      For j=1 To m
          Bitset(layers,New,PlaneE)
     Next j
  Next i
Next k
Correlation(New,Im)
End RGB Encryption Image Algorithm
```

6-2 YIQ Encryption Algorithm

This algorithm works at the same style of previous algorithm but this different the first one because of using YIQ in analysis of both of images (Key/Input Image). Algorithm will be as the following :

```
YIQ Encryption Image Algorithm
Input Im,Imk,PlaneE,PlaneK
[n m]=size(Im)
Iimresize(Imk,n,m)
```

```
Iim2YIQ(Im,Y,I,Q)
Iim2YIQ(Imk,Y,I,Q)
For k =1 To 3
  For i=1 To n
    For j=1 To m
        Layern new(i,,j,k)=Bitget(layers(i,j,k),planeE)
       Layern newKey(i,,j,k)=Bitget(layersKey(i,j,k),planeK)
     Next j
  Next i
Next k
New = XOR( Layern new, Layern newKey)
For k =1 To 3
  For i=1 To n
    For j=1 To m
        Bitset(layers,New,PlaneE)
     Next j
  Next i
Next k
Correlation(New,Im)
End RGB Encryption Image Algorithm
```

Where:

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

N,M,K,I,J : parameters are related.

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

Iim2YIQ : is procedure for image analyses to YIQ layers.

Iim2RGB : is procedure for image analyses to RGB layers.

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

PlaneK : 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.

7- Experimental Results

In this term, a number of experiments which are used to investigate the effectiveness of our proposed algorithms will be performed.

7-1 Experiment

In this experiment, we will input two color images (Input/Key) the first represented image that encrypt by depend key which derived from second image. Experiment are used colors space (RGB) and then selected different layers , plans in both images. The figure (10) represent set of images encryption in many state layers and planes, that is cleared in the following table (1):-

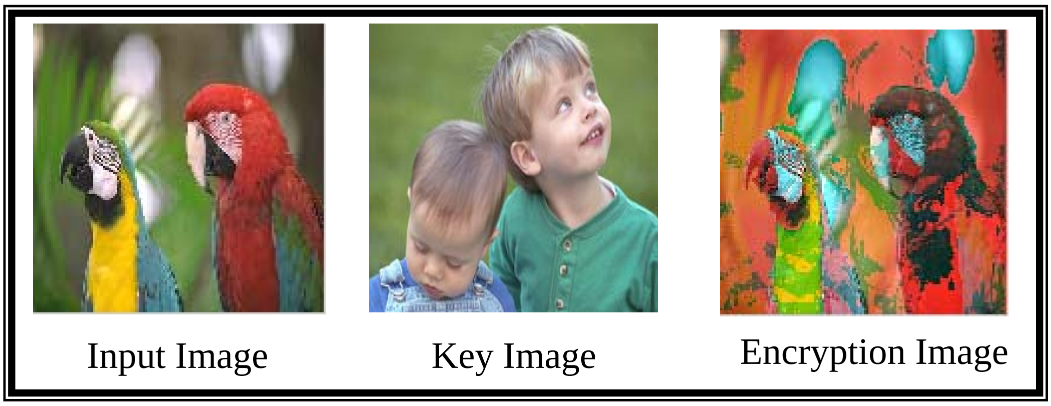


Figure (10-1) is explained first state in tabel1

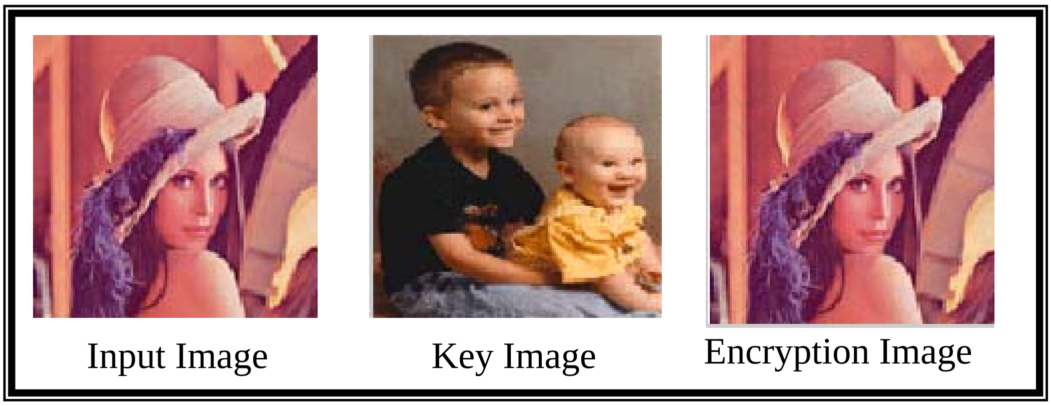


Figure (10-2) is explained second state in tabel1

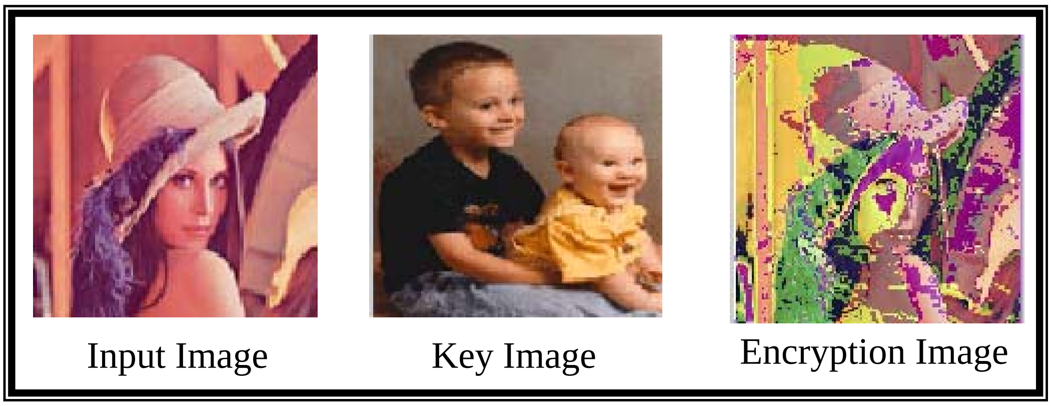


Figure (10-3) is explained third state in tabel1

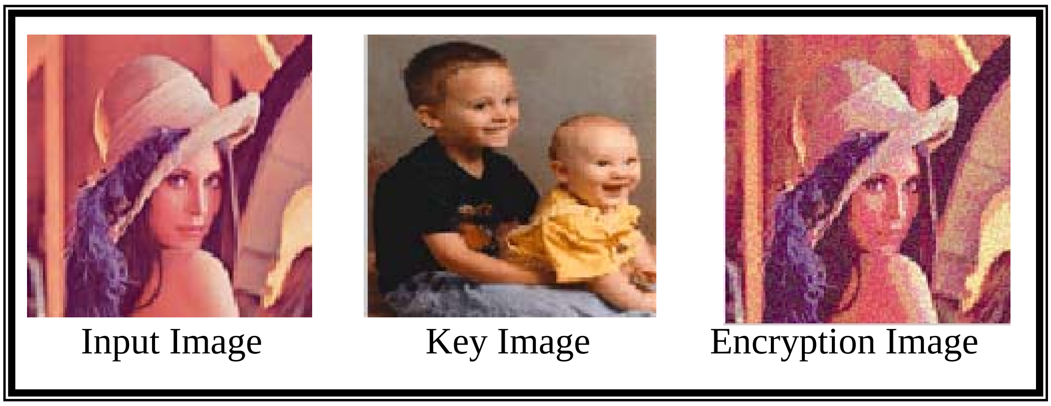


Figure (10-4) is explained fourth state in tabel1

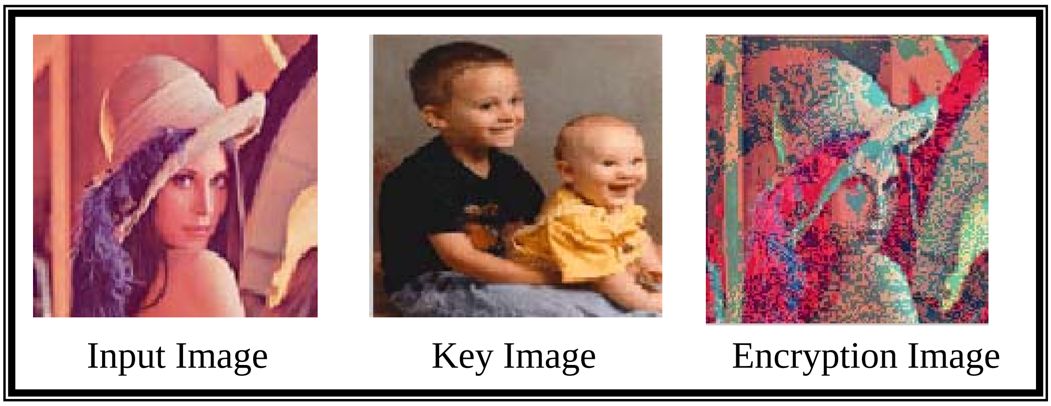


Figure (10-5) is explained fifth state in tabel1

7-2 Experiment

In this experiment, we will input two color image (Input/Key) the first represent image which encryption by depending on key that derived from second image by using image analysis (YIQ) and in different layers and plans in both image. The figure (11) represents set of image encryption in different state of layers and plane, as clear in the following table(2):

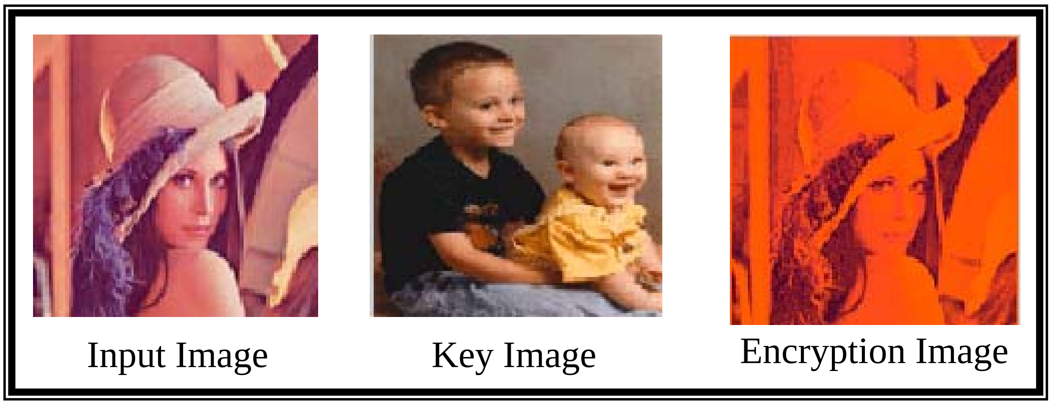


Figure (11-1) is explained third state in tabel2

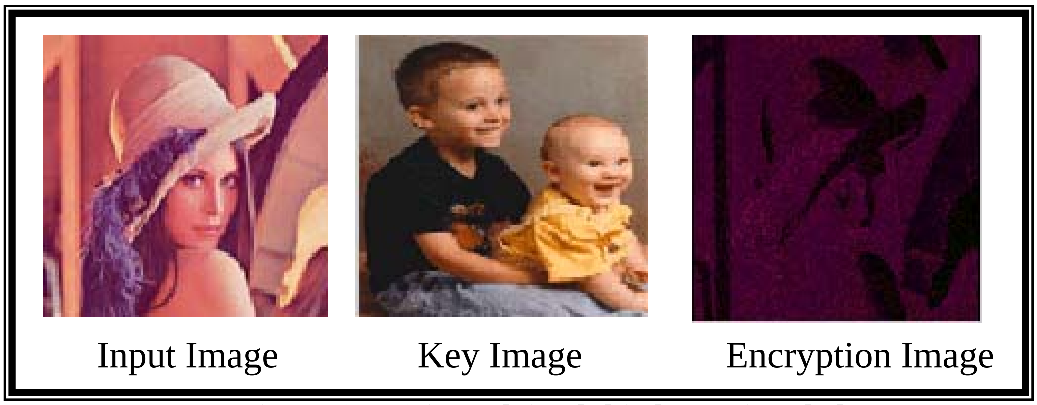

Input Image Key Image Encryption Image

Figure (11-2) is explained third state in tabel2

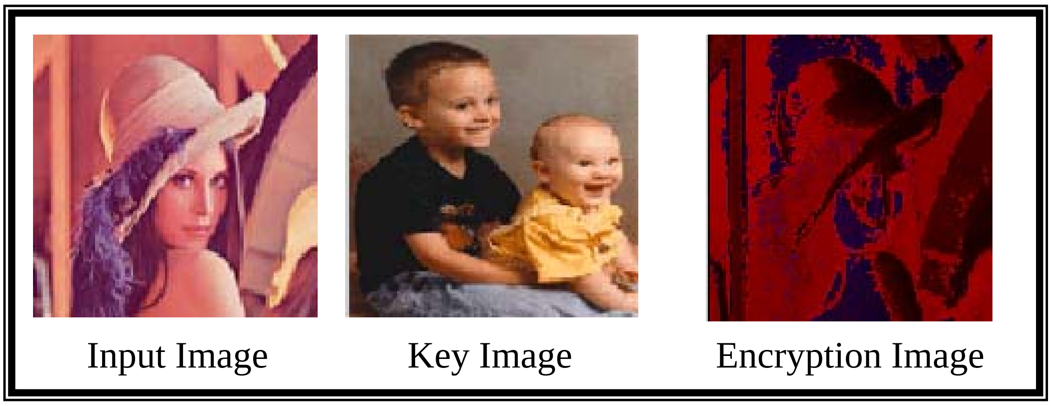

Input Image Key Image Encryption Image

Figure (11-3) is explained third state in tabel2

8- Conclusion

During of experimental results of research can conclude many important things and as in the following figure:-

1- Difficult of key broken, The attackers must be detected key image first and then predicate target layer and bit plan .
2- The technique of key chose from another image which is analysis to main layer (RGB or YIQ) and then applied algorithm.
3- YIQ algorithm is better than RGB during experimental results of correleation.

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

Input Image				Key Image				Correlation Ratio	State
R	G	B	Plane	R	G	B	Plane		
/			8		/		8	0.8924	١
/			٤			/	٢	0.9934	٢
		/	٧	/			٨	0.765	٣
		/	٢	/	/		٦	٠,٩٢٦٨	٤
/	/		٨		/	/	٥	٠,٧١٦٣	٥

Table (2) is explain the results experiential in YIQ Algorithm

Input Image				Key Image				Correlation Ratio	State
Y	I	Q	Plane	Y	I	Q	Plane		
/			٤		/		٥	٠,٥٣٧٧	١
/			٤			/	٢	٠,٤٨٢٣٦	٢
		/	٥	/	/		٧	٠,٣٥٤٥٤	3

References

Baxes G. A., 1994, “Digital Image Processing: Principles and Applications”, John Wiley & Sons, Inc., USA.

Cheng H., 1998, “Partial Encryption for Image and Video Communication”, M.Sc. Thesis, Department of Computing Science, University of Alberta.

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

Li X., Knipe J. and Cheng H., 1997, “Image Compression and Encryption Using Tree Structures”, Pattern Recognition Letters, Vol. 18, No. 11-13, pp. 1253-1259.

Gonzalez R.C. and Woods R. E., 1992, “Digital Image Processing”, Addision-Wesley, Inc., USA.

Hameed A.Younes, November2006,"New Techniques for Partial Encryption of Wavelet-based Compressed and Uncompressed Images", PhD Thesis, Department of Computing Science, University of Basrah.

Miaou S., Chen S. and Lin C., 2002, “An Integration Design of Compression and Encryption for Biomedical Signals”, Journal of Medical and Biological Engineering, Vol. 22, No. 4, pp. 183-192.

Stallings W., 2003,“Cryptography and Network Security, Principles and Practice”, third Edition, Pearson Education International, Inc., USA.

Schneier B., 1996, “Applied Cryptography, Second Edition: Protocols, Algorithms and Source Code in C”, John Wiley & Sons, Inc., USA.

Umbaugh S. E., 1998, “Computer Vision and Image Processing”,Prentice-Hall, Inc., USA.