Applying Encryption Method to Color FlC

Nevart Alias Yousif
Faten Hassan Al-Qadhee

Technical Institute of Kirkuk - Iraq

Abstract

In this paper a simple and fast algorithm that used XOR function to encrypt color images compressed with a fast fractal image compression (FFIC)was used. The algorithm first included converting the image from the RGB color space into the YIQ color space and each band was treated separately. Main difficulty with fractal coding method is that it takes long time to compress single image. The FIC is speeded up by filtration of the domain pool blocks using the centralized moments coefficients which are applied to each of range and domain blocks. Another speeding is applied by using these descriptors to determine the suitable symmetry case reducing the eight isometric trails to one trail. After finding the fractal coefficients for the best matching, two of the fractal coefficient are encrypted using XOR operation. The first key encryption is used to generate an array of sequenced numbers with an increase depending on the key, and length of the array is equal to the number of the range blocks, this key is used to encrypt the average coefficients. The symmetry coefficients are encrypted by another key. Then quantization, deferential pulse code modulation(DPCM) process are applied to each of the fractal coefficient. The decryption procedure is similar to that of the encryption but in the reversed order. The proposed method provided fast, good compression ratio (CR), secure image and good quality for the reconstructed image after decompression and decryption process.

Keywords: **I**mage Encryption, cryptography, Fractal Image Compression, XOR, FIC, IFS, Moment**s.**

تطبيق طريقة لتشفير الصور المضغوطة باستخدم الكسور

م.نفارت الياس يوسف ا.م.د فاتن حسن القاضي

الجامعة التقنية الشمالية-المعهد التقني/كركوك

المستخلص

في هذا البحث تم استخدام خوارزمية سريعة باستخدام الدالة الحصرية XOR لتشفير الصور الملونة المضغوطة بالطريقة السريعة لضغط الصور الكسوري (FFIC). تضمنت الخوارزمية اولا تحويل الصورة من فضاء الالوان RGB الى فضاء الالوان YIQ ، حيث تم معالجة كل حزمة بشكل منفصل.ان الصعوبة الرئيسية بالتشفير بطريقة الكسور هي انها تاخذ وقتاً أطول لضغط صورة واحدة لهذا تم تسريع ضغط الصور الكسوري FIC بفلترة كتل مجموعة المجال باستخدام معاملات العزم المركزي التي تم تطبيقها على بلوكات المجال والمدى ،كما تم اجراء تسريع اخر لضغط الصور باستخدام معاملات العزم المركزي لتحديد حالة التناظر المناسب لتقليل محاولات التدوير الثمان الى محاولة واحدة ، وذلك بعد ايجاد معاملات الضغط الكسوري للتطابق الافضل. اثنان من معاملات الكسور تم تشفيرها باستخدام عملية ال XOR. حيث ان المفتاح السري المستخدم للتشفير استخدم لتوليد مصفوفة من الارقام المتسلسلة بزيادة تعتمد على المفتاح وطول المصفوفة مساو لعدد بلوكات المدى واستخدمت المصفوفة لتشفيرمعاملات المعدل. اما معامل التدوير تم تشفيره باستخدام مفتاح اخر. تم تطبيق عملية التكميم، اي تمثيل شفرة النبضة التفاضلي (DPCM) على كل من معاملات الكسور. الاجراء المستخدم لعكس التشفير يشبه الروتين المستخدم لعملية التشفير لكن بترتيب عكسي. الخوارزمية المقترحة اعطت للصورة المرجعة السرعة ،نسبة ضغط جيد (CR)، امنية جيدة اضف الى الكفاءة الجيدة للصورة بعد عملية اعادة الضغط واعادة التشفير.

1. INTRODUCTION

Security is an important issue in communication and storage of images, and encryption is one of the ways to ensure 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 words, it is essential that nobody could get to know the content without a key for decryption[1].

Encryption is one of the ways to ensure high security images and is used in many fields such as medical science,

military. Modern cryptography provides essential techniques for securing information and protecting multimedia data. In recent years, encryption technology has been developed quickly and many image encryption methods have been used to protect confidential image data from unauthorized access[2].

Fractal image coding is a mathematical process used to encode bitmaps containing a real-world image as a set of mathematical data that describes the fractal properties of the image. Most data contains amount of redundancy, which can be removed from storage and replaced for recovery. Based on this fact and on Bernsley's assumption[3], many objects can be closely approximated by self-similarity objects which might be generated by use of Iterated Function System(IFS), where the IFS can be seen as a transformation between the whole and its parts, the fractal image coding evolved. Hence, the main problem that arises is how to find these IFS transformation. It was Jacquin[4] who solved this problem by developing an algorithm to automate the way to find this transformation based on the fact that different parts of the image at different scales are similar and on the assumption that the image parts do not need to resemble the whole image, but it is sufficient for them to be similar to some other bigger parts in it. Using these advantages, the FIC became an inspiration for solving several techniques whose main characteristic is the use of the similarity property in image block[5]. In this work, a symmetric key encryption is applied using XOR operation to the fractal compressed images that speeded by using moment descriptors on color images.

2. PREVIOUS WORK

Many algorithms are available to protect image from unauthorized access. Gao H., Zhang Y., Liang S. and Li D., have proposed a new image encryption scheme based on a chaotic system and on power and tangent function instead of linear function. It uses chaotic sequence generated by NCA map to encrypt image data with different keys for different images by using XOR operation with the integer sequence[6]. Seyedzade S., Atani R. and Mirzakuchaki S., proposed a novel algorithm for image encryption based on SHA-512 hash function. The algorithm consists of two main sections: the first does preprocessing operation to shuffle one half of image,and the second uses hash function to generate a random number mask. The mask is then XORed with the other part of the image which is going to be encrypted[7].

Amitava N. has proposed an algorithms using affine transform and encrypted the image using XOR operation. They redistribute the pixel values to different location using affine transform technique. The transformed image is then divided into (2x2) pixels blocks that encrypted by four 8-bit keys (64 bit) [8]. Emad S. O. presents a secured image compression system for satellite communication based on the fractal theory of iterated contractive image transformation combined with the EHMC algorithm[9]. Rad R. M. et al, exploits the scan patterns and function XOR in three stand alone steps. The simulation results for gray-level images show that the proposed algorithm has great performance in terms of sensitivity, speed, and security[10].

3. IMAGE ENCRYPTION

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 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 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.

The many schemes used for enciphering constitute the area of study known as cryptography. There are three main types of cryptography:

i. **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.

ii. **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.

iii. **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.

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[11].

Decreasing the level of encryption (using, for example, partial encryption) does not yield much improvement in compression efficiency. Hence, if complexity permits, full encryption should be employed to maximize security of the transmitted images[12].

4. FRACTAL CODING

The main idea is to decompose the image into segments by using standard image processing techniques such as color separation, edge detection, and spectrum and texture analysis. Then each segment is looked up in a library of fractals. The library really contains codes called iterated function system (IFS) codes, which are compact sets of numbers. A set of codes for a given image are determined, such that when the IFS codes are applied to a suitable set of image blocks yield an image that is a very close approximation of the original. This scheme is highly effective for compressing images that have good regularity and self-similarity [13]. Barnsley's collage theorem[3] provides the basis for converting natural images into IFS code, and a random iteration algorithm could be used to "decode" the data back to images.

The IFS code is actually a set of affine transformations. An affine transformation maps a point back into the same set of points it came from. General form for an affine transformation[14]:

$$w\begin{pmatrix}x\\y\end{pmatrix}=\begin{pmatrix}a & b\\c & d\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}+\begin{pmatrix}e\\f\end{pmatrix}=\begin{pmatrix}ax+by+e\\cx+dy+f\end{pmatrix} \qquad (1)$$

If the translations, rotations, and scaling that make up W are known in advance, then the coefficients may be calculated by:

$$a = r\cos\theta\ ,\ b = -\sin\phi\ ,\ c = r\sin\theta,\ d = s\cos\phi$$

Where,

r = scaling factor on x, s = scaling factor on y.

θ= angle of rotation on x, ϕ = angle of rotation on y.

e = translation on x, f = translation on y.

For a range block with pixel values (r_o, $r_1,\ldots,r_{n-1}$), and the domain block ($d_o,d_1,\ldots,d_{n-1}$) the contractive affine approximation is [2]:

$$r_i^{'} = sd_i + o \qquad (2)$$

Where, r_i' is the optimally approximated i^{th} pixel value in the range block. d_i is the corresponding pixel value in the domain block. The symbols s and o represent the scaling and offset coefficients, respectively. Taking the average of both sides in equation (2) the following equation is obtained:

$$\bar{r} = s\bar{d} + o \qquad (3)$$

So, this contractive affine transform could be rewritten to become in the form:

$$r_i^{'} = s(d_i - \bar{d}) + \bar{r} \qquad (4)$$

Where,

$$\bar{r} = \frac{1}{m}\sum_{i=0}^{m-1} r_i \quad , \qquad (5)$$

$$\bar{d} = \frac{1}{m}\sum_{i=0}^{m-1} d_i \qquad (6)$$

Where, *m* is the block size.

From equation (4), the fractal parameters become {*s, r* } instead of the of the conventional {*s, o*} coefficients in traditional IFS mapping equation (2).

The scale (*s*) parameter could be determined by applying the least mean square difference (χ^2) criteria between the approximated (r_i') and actual (r_i) values; that is:

$$x^2 = \frac{1}{m}\sum_{i=0}^{m-1}(r_i' - r_i) \qquad (7)$$

Before the determination of (χ^2) values, the values of the scale (s) and range average ($\bar{r}$) values coefficients should be bounded and quantized[2].

Moments describe the shape's layout (i.e., the arrangement of its pixels), a bit like area. Compactness and irregularity order descriptions. The calculation of moment invariants for any shape requires knowledge about both the shape boundary and its interior region[14]. Given a function *f(x,y)*, the regular moments are defined as[14]:

$$\mu_{pq} = \sum_x \sum_y x^p y^q f(x, y) \qquad (8)$$

μ_{pq} is a two-dimensional moment of the function *f(x,y)*, the order of the moment is (*p*+*q*), where *p* and *q* are both integer numbers. To translation invariance, in the image plane, the image centrism is used to define the central moments. The coordinates of the center of gravity of the image are calculated using the following equations[14]:

$$x = \frac{M_{10}}{M_{00}} \quad , \quad y = \frac{M_{01}}{M_{00}} \qquad (9)$$

For an image block f(x,y) the central moment of order (p+q), around the block's central point (x_c,y_c), is defined as:

$$M(p, q) = \sum_x \sum_y (x - x_c)^p (y - y_c)^q f(x, y) \qquad (10)$$

From the pair of n^{th} moments {i.e., M(n,0)& M(0, n) } the following moments blocks descriptors could defined:

$$R_n = \frac{M^2(0,n) - M^2(n,0)}{M^2(0,n) + M^2(n,0)} \qquad (11)$$

The values of the factors (R) are rotation and reflection invariant. This result implies that "if the two blocks (range and domain) satisfy the contractive affine transform (equation 7), then their moments ratio factors (R_d and R_r) should have similar values. This doesn't means that any two blocks have similar R factors are necessarily similar to each other". This derived conclusion was utilized, to speed up the domain blocks search. Instead of matching all domain blocks listed in domain pool with each tested range block; it is enough to test the domain blocks whose R factors are close to the R-value of tested range block[15]. The moments (M_x ,M_y) of each block are determined, and then the blocks are indexed, also its symmetry (or isometric states) are indexed using the following three Boolean criteria:

1) is $|M_x| \geq |M_y|$ or not?
2) is $M_x \geq 0$ or not?
3) is $M_y \geq 0$ or not?

The required isometric process is assessed using a predefined lookup table whose indices depends on the isometric indexes of the two matched blocks[14].

The values of adjacent pixels in an image are often similar, i.e., they are highly correlated. This property is exploited in predictive coding techniques where the value of a given pixel is predicted based on the values of the surrounding pixels. Differential pulse code modulation (DPCM) is procedure of converting analog to digital signal in which analog signal is sampled and then difference between actual sample value and

its predicted value is quantized and then encoded forming digital value[16].

5. SECURE FRACTAL SCHEME

In the proposed secure fractal coding scheme, some sensitive parameters in fractal image coding will be selected and encrypted. Only some parameters of image data are encrypted while the others are left unchanged. To keep secure, some principles are required to select the suitable parameters:

i. The parameter with the properties of large space and random distribution is preferred to be encrypted. because it will be more difficult to be broken. If the parameter is in random distribution, then the difficulty of statistical attack will be increased.

ii. The parameter with high sensitivity is preferred to be encrypted. If the quality degradation is big, the parameter is regarded as of high sensitivity.

iii. For parameter encryption, the cipher with high security is preferred. The parameter should be encrypted with the cipher that has high key sensitivity. It can confirm that a slight difference in the key will lead to great differences in the parameter [17] .

The security of image can be achieved by various types of encryption schemes.

- **Number of pixel change rate (NPCR) :**It is a common measure used to check the effect of one pixel change on the entire image. This will indicate the percentage of different pixels between two images. Let $I_o(i, j)$ and $I_{ENC}(i, j)$ be the pixels values of original and encrypted images, I_o and I_{ENC},

at the ith pixel row and jth pixel column, respectively. Equation (12) gives the mathematical expression:

$$NPCR = \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times \frac{100\%}{MxN} \quad (12)$$

Where, $D(i, j) = 0$ if $I_o(i, j) = I_{ENC}(i, j)$, if not then $D(i, j) = 1$

- **Unified average changing intensity (UACI):** A small change in plaintext image must cause some significant change in ciphertext image. UACI is helpful to identify the average intensity of difference in pixels between the two images. For the plaintext image $I_o(i, j)$ and encrypted image $I_{ENC}(i,j)$ the equation (13) gives the mathematical expression for UACI.

$$UACI = \left[\sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|I_o(i,j) - I_{ENC}(i,j)|}{255}\right] \times \frac{100\%}{MxN} \quad (13)$$

Higher NPCR values are desired for ideal encryption schemes. The UACI values must be in the range of 33%. Two images are taken for comparison[18].

The paper also carried out a comparisons between the histograms of the original and encrypted images to see the data range changing after encryption.

6. PROPOSED ENCRYPTION METHOD

The main objective of this paper is to encrypt the compressed color image with FFIC. The range image first is transformed from the RGB color space to YIQ color space where Y is the luminance component, and the other components (I and Q) are the chromatic components. Each

band (Y, I and Q) is down sampled to create the domain image. The range image is partitioned into array of non-overlapped fixed size blocks (4x4) and the domain image is partitioned into an overlapped fixed size blocks (4x4). FFIC is applied to find the best matching domain block for each range block using IFS coding. The result of the fractal compression are the coefficients: average, scale, domain position and symmetry state.

Two of these fractal coefficients (average and symmetry) are encrypted using XOR operation using symmetric key algorithm. The average coefficients for all range blocks are encrypted by 8 bit secret key (K) that is used to generate an array of keys of length equal to the number of image blocks, the array values start from (0) with an increase of K. As an example, if the key is 5, the array will have the values (0, 5, 10,....) which are used to encrypt the averages of the blocks with XOR function. Other 3 bit key is used to encrypt the symmetry coefficients (which takes 3 bits to be represented). The scale and domain index coefficients are left without encryption because they are sensitive parameters and affected to the reconstructed image.

To obtain good compression ratio, the resulted FIC parameters for all blocks are quantized and coded with DPCM as further entropy coding, this saves low values which represent the differences instead of the coefficients.

The encryption and encoding steps are summarized by the following algorithm steps:

Input: The original color bitmap image.

Output: Fractal parameters for the compressed and encrypted image file.

step 1: Load the original bitmap image with RGB form.

step 2: Convert (R,G,B) arrays to (Y,I,Q) arrays.

step 3: For each color component (Y, I and Q) do:

step 4: Down sample the range image to produce the domain array of quarter size of range that represents the domain image.

step 5: partition the range image into a non-overlapping fixed blocks.

step 6: partition the domain image into an overlapping blocks of size: 2x2 or 4x4.

step 7: Generate the array of encryption keys of size equal to the number of image blocks.

step 8: Find the moment descriptor for all domain blocks and sort them according it.

step 9: For each range block do the IFS mapping:

1) Find The range average parameter ($\bar{r}$) and scale (s) using affine mapping for the corresponding range block (d).
2) Find the moment descriptor for the range block.
3) Pick up a domain block from the domain pool with the defined jump step.
4) Match the range with only domain blocks that have the same moment descriptor.
5) Perform one of the isometric mappings depending on the moment descriptor.
6) Find the minimum error of the matching.
7) if the minimum error is less than the threshold, consider the block as best match block, else goto step 3.
8) Encrypt the range average parameter with one of the previously generated keys.
9) Encrypt the symmetry parameter with another external 3 bits key.

10) Encode the fractal parameters of the best matching block obtained from the previous steps (encrypted average, scale, encrypted symmetry and domain position) with DPCM and quantize them.
11) Save the fractal parameters into the encryption file.
12) End for loop (take next range block)

step 10: End for loop (take next color component)

step 11: End.

The decoding stage will take the inverse steps. The image must be decoded with DPCM, de-quantized, decrypted with the same keys used by the encryption process, perform inverse IFS, and at last the image will be retransformed from YIQ to RGB color space.

The proposed encryption method was applied to three bitmap images (Lena, Pepper and Parrot), the encryption coefficients (NPCR and UACI) are tested for the system. Also the compression performance is evaluated using the peak signal-to-noise ratio (PSNR) to measure the quality, and the compression ratio(CR) for the reconstructed images. The jump step used for the compression was 2 to accelerate the search process, and different block sizes (2x2 or 4x4) are tested to find the best performance for the system. Another comparison using histogram is made between the original and the encrypted images with each block size.

8. RESULTS AND DISCUSSION

The proposed method performance for the resulted images was tested. The PSNR and CR were used to evaluate the compression performance for reconstructed images. The security tests against differential attack are used by

calculation of the NPCR, UACI, and the image histogram which is an important feature in image analysis.

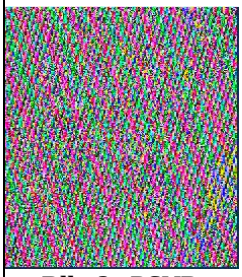
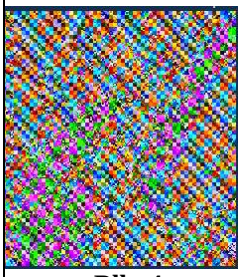
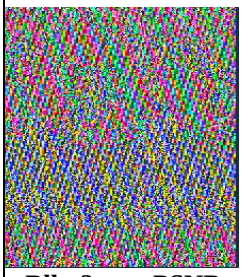
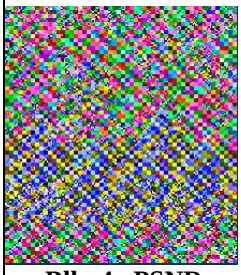
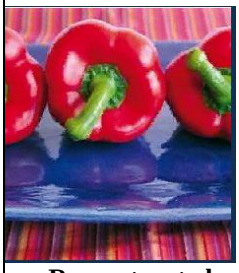
From figure 1, for the three tested images (Lena, Pepper and Parrot), if the block length is small (blk=2) the PSNR is best than it with (blk=4), but the CR is very low, and also the block length effected only on the vision of the images but the encryption parameters has not changed, so the preferred block length is 4 that gave higher CR and secure encryption. Because of the use of moment features in the compression stage, the encryption with the encoding time was lowe than (2 sec), unlike the traditional FIC that suffers from high encoding time.

The encryption algorithm tested results proved that it obeys the secure encryption principles, it gave a high NPCR (about 98%), and UACI with the acceptable range about (33-37)% and the histograms shown in figure 2 proved that the histograms of the encrypted images are nearly uniform and different from the histograms of the original images (whatever the block length was). The histograms shows the data range of the encrypted image. The data range is the range of intensity values actually used in the image.

9. CONCLUSION

The paper proposed a secure algorithm to encrypt images after compressing them using FFIC with a good compression and encryption properties. The decoding process is composed of iterated contract transforms. That is, the initial image range block is transformed by the iterated fractal transform, which makes the initial image contracted to the original image. The uses of FIC offer the advantage of increaing the security because of the use of the fractal codes instead of original

image. When some of the fractal coefficient changed using the encryption process, the image cannot be transformed correctly to the original image. The hacker must guess the encrypted parameters, also the use of two keys and long key array has increased the security of the algorithm. Another possibility for future research is to encrypt other fractal parameters using different keys for each of the three color components of the image.

 **Original Lena 256x256**	 **Blk=2 PSNR= 7.29 CR=2.11 NPCR = 98% UACI=34 %**	 **Blk=4 PSNR=7.48 CR=8.59 NPCR=98 % UACI=32 %**	 **Reconstructed lena Blk=4 PSNR= 30.91 CR=8.59**
 **Original Pepper 256x256**	 **Blk=2 PSNR= 6.57 CR=2.31**	 **Blk=4 PSNR= 6.63 CR=9.33 NPCR =**	 **Reconstructed Pepper Blk=4 PSNR= 27.93**

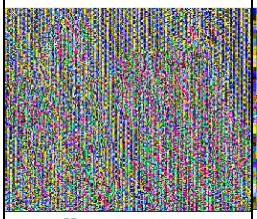
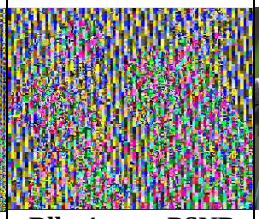
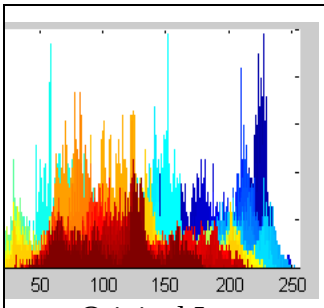
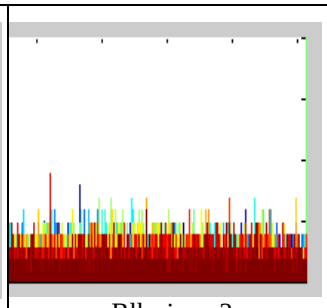
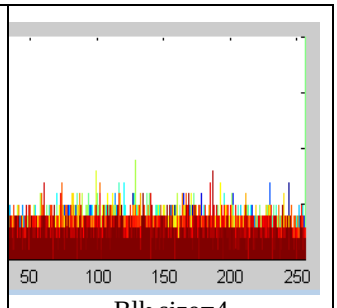
	NPCR = 98% UACI=37 %	98% UACI=37 %	CR=9.33
			
Original Parrot 384x256	Blk=2 PSNR= 7.00 CR=1.00 NPCR = 98% UACI=36%	Blk=4 PSNR= 7.14 CR=8.98 NPCR = 98% UACI=35%	Reconstructed Parrot Blk=4 PSNR= 89.87 CR=8.98

Figure 1: The results of the encryption, compression parameters and reconstructed images for (Lena, Pepper and Parrot) with different block sizes.



Original Lena


Blk size =2



Blk size=4

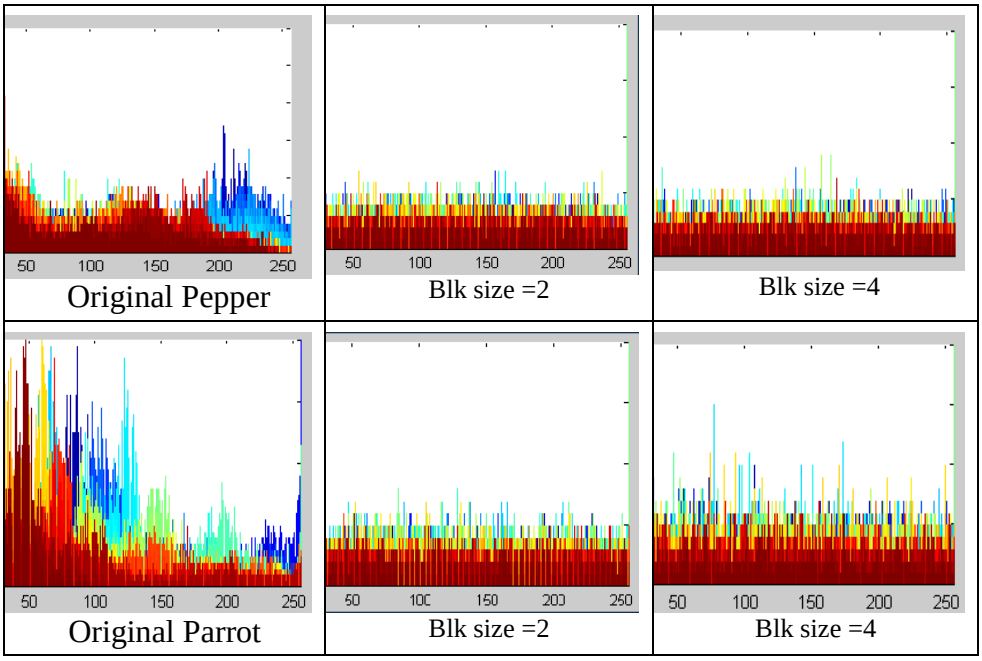


Figure 2: Histograms for the original and encrypted images(Lena, Pepper and Parrot)
with different block sizes.

REFERENCES:

[1] Patel K. D. & Belani S., **"Image Encryption Using Different Techniques: A Review",** International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, Volume 1, Issue 1, November 2011.

[2] George L. E. and Al-Hilo A., **"Color FIC by Adaptive Zero-Mean Method",** Symposium on Computing, Communication, and Control (ISCCC 2009) Proc .of CSIT vol.1, 2011.

[3] Barnsley M. F. and Hurd L. P., **"Fractal Image Compression"**, A K Peters, Wellesley, Mass, USA, 1993.

[4] A. Jacquin, "**A Fractal Theory of Iterated Markov Operators With Application to Digital Image Coding**", Doctoral thesis, Georgia Institute of Technology, 1989.

[5] Al-Saidi N. M. G., Said M. M., " **Password Authentication Based on Fractal Coding Scheme",** Hindawi Publishing Corporation, Journal of Applied Mathematics, Volume, Article ID 340861, 16 pages, 2012.

[6] Gao H., Zhang Y., Liang S. and Li D., **"A New Chaotic Image Encryption Algorithm"**, Chaos Solutions and Fractals 29, 393–399, 2006.

[7] Seyedzade S. M., Atani R. E. and Mirzakuchaki S., **"A Novel Image Encryption Algorithm Based on Hash Function"**, 6th Iranian Conference on Machine Vision and Image Processing, 2010.

[8] Nag A., Singh J. P., Khan S., Ghosh S., Biswas S., Pratim S. P., **"Image Encryption Using Affine Transform and XOR Operation"**, International Conference on Signal Processing, Communication, Computing and Networking Technologies(ICSCCN), 2011.

[9] Emad S. O. and Sakre M., " **Compression and Encryption Algorithms for Image Satellite Communication**", International Journal of Scientific & Engineering Research, Volume 3, Issue 9, ISSN 2229-5518, September 2012.

[10] Rad R. M., Attar A., and Atani R. E., **"A New Fast and Simple Image Encryption Algorithm Using Scan Patterns and XOR"**, International Journal of Signal Processing, Image Processing and Pattern Recognition, pp.275-290, Vol.6, No.5, 2013.

[11] Kaur R., Singh Er. K., **"Image Encryption Techniques: A Selected Review",** Journal of Computer Engineering, (IOSR-JCE) ISSN: 2278-8727, Vol 9, Issue 6, 2013.

[12] Gurijala A., Khayam S. A. **"The impact of encryption on compression efficiency of still images"**, 10.100/123456, November 2005.

[13] Kuppusamy K. and Ilackiya R., **"Fractal Image Compression & Algorithmic Techniques",** International Journal of Computer & Organization Trends, Vol 3 Issue4, ISSN: 2249-2593, May 2013.

[14] George L. E., Suad K. A., **"Hiding Image in Image Using Iterated Function System (IFS)"**, European Conference of Computer Science (ECCS '10), 68-74, ISBN: 978-960-474-250-9 , 2010. **[15]** George L. E**., "Fast IFS Coding for Zero-Mean Image Blocks Using Moments Indexing Method", Iraqi Journal of Science, Vol 6, No 1,pp 8-14, 2006.**

[16] Rabbani M. and Jones P. W., **"Image Compression Techniques for Medical Diagnostic Imaging Systems"**, Journal of Digital Imaging, Digital Imaging Basics, Vol 4, No 2 May 1991.

[17] Lian S., Chen X., and Ye. D., **"Secure Fractal Image Coding"**, Fractals 17:02, 149-160. Online publication, Jun, 2009.

[18] Abraham L., Daniel N., **"Secure Image Encryption Algorithms: A Review",** International Journal of Scientific & Technology Research, ISSN 2277-8616 186 , Vol 2, Issue 4, April 2013.