DOI: 10.24996/ijs.2020.61.4.25

ISSN: 0067-2904

Selective Image Encryption Based on DCT, Hybrid Shift Coding and Randomly Generated Secret Key

Loay E. George[1], Enas Kh. Hassan[*2], Sajaa G. Mohammed[3], Faisel G. Mohammed[1]

[1] Department of Remote Sensing and Geographic Information's, college of science, University of Baghdad, Baghdad, Iraq

[2]Department of computer science, College of science, University of Baghdad, Baghdad, Iraq

[3]Department of Mathematics, College of science, University of Baghdad, Baghdad, Iraq

Received: 13/7/ 2019 Accepted: 21/1/2020

Abstract

Most of today's techniques encrypt all of the image data, which consumes a tremendous amount of time and computational payload. This work introduces a selective image encryption technique that encrypts predetermined bulks of the original image data in order to reduce the encryption/decryption time and the computational complexity of processing the huge image data. This technique is applying a compression algorithm based on Discrete Cosine Transform (DCT). Two approaches are implemented based on color space conversion as a preprocessing for the compression phases YC_bC_r and RGB, where the resultant compressed sequence is selectively encrypted using randomly generated combined secret key.

The results showed a significant reduction in image quality degradation when applying the system based on YC_bC_r over RGB, where the compression ratio was raised in some of the tested images to 50% for the same Peak Signal to Noise Ratio (PSNR). The usage of 1-D DCT reduced the transform time by 47:1 times compared to the same transform using 2-D DCT. The values of the adaptive scalar quantization parameters were reduced to the half for the luminance (Y band) to preserve the visual quality, while the chrominance (C_b and C_r bands) were quantized by the predetermined quantization parameters. In the hybrid encoder horizontal zigzag, block scanning was applied to scan the image. The Detailed Coefficient (DC) coefficients are highly correlated in this arrangement- where DC are losslessly compressed by Differential Pulse Coding Modulation (DPCM) and the Accumulative Coefficients (AC) are compressed using Run Length Encoding (RLE). As a consequence, for the compression algorithm, the compression gain obtained was up to 95%. Three arrays are resulted from each band (DC coefficients, AC values, and AC runs), where the cipher is applied to some or all of those bulks selectively. This reduces the encryption decryption time significantly, where encrypting the DC coefficients provided the second best randomness and the least encryption/decryption time recorded (3×10^{-3} sec.) for the entire image. Although the compression algorithm consumes time but it is more efficient than the saved encryption time.

Keywords: Selective Image Encryption, Random Number Generators, Symmetric Key Encryption

*Email: Enas.mkhazal@gmail.com

تشفير الصور انتقائياً بالاعتماد على تحويل الجيب تمام والتحويل الهجين ومفتاح سري مولد تلقائياُ

. لؤي ادور جورج[1] , ايناس خزعل حسن*[2], سجا غازي محمد[3] , فيصل غازي محمد[1]

[1]قسم التحسس النائي والمعلومات الجغرافية كلية العلوم جامعة بغداد، بغداد، العراق

[2]قسم علوم الحاسبات كلية العلوم جامعة بغداد، بغداد، العراق

[3]قسم الرياضيات كلية العلوم جامعة بغداد، بغداد، العراق

الخلاصه

التشفير المرئي هو تقنية تشفير خاصة لتشفير المعلومات المحتواة في الصور ,بطريقة لايمكن فتحها باستخدام خوارزميات تحليل الشفرات او ادراك محتواها بواسطة الجهاز البصري البشري التشفير الانتقائي اصبح منتشرا بشكل كبير نتيجة للتطور السريع في تقنيات المعلومات و الاتصالات المرئية عبر الشبكات المفتوحة حول العالم ,ويعتبر مهم جدا في تطبيقات الوقت الحقيقي والتي يجب ان تكون سريعة ومؤمنة بشكل تام ,بحيث تكون البيانات الرقمية سليمة من الوصول غير المرغوب فيه والمتنصتين .اغلب التقنيات الحالية تشفر الصورة بشكل كامل والتي تتطلب وقت معالجة وحسابات هائلة ,هذا البحث يقدم تقنية تشفير انتقائي للصور حيث يتم تشفير اجزاء محددة مسبقا من بيانات الصورة في سبيل تقليل وقت التشفير وفك الشفرة وتعقيد الحسابات التي تتطلبها بيانات الصور التي تعتبر كبيرة جدا .هذه التقنية تطبق خوارزمية ضغط تعتمد على تحويلات الجيب تمام المتقطعة وتم حيث يتم YCC و RGB اعتماد مسارين كخطوة ما قبل المعالجة بتحويل المجال اللوني الى تشفير ناتج الضغط انتقائيا بواسطة مفتاح سري مركب مولد عشوائيا .نتائج الاختبارات اوضحت وجود تحسن كبير في نوعية الصور عند تطبيق النظام اللوني حيث ارتفعت نسبة الضغط الى 50 %عند نفس درجة RGB, مقارنة بالنظام اللوني YCbCr بينما استخدام تحويلات الجيب تمام احادية البعد قد قلل وقت التحويل PSNR, وضوح الصورة بنسبة 1:47 لنفس نوع التحويلات ثنائية البعد لنفس الصورة ,في تقليل القيم العددي التكيفي تم تقليل المعاملات الى النصف لحزمة الانارة بينما استخدمت نفس قيم المعاملات لحزمتي الانارة ,في التشفير الهجين تم استخدام المسح المتعرج للمقاطع لكل الصورة(حيث يعتبر هذا الترتيب هو على معاملات التفاصيل لكل مقطع في الصورة)وفي نفس الوقت تم DPCM الافضل لتنفيذ على المعاملات التراكمية لكل الصورة ,وكنتيجة لتطبيق خوارزمية الضغط فقد RLE تنفيذ وصل ربح الضغط الى 95 %, ولتنتج ثلاث مصفوفات احادية من كل قناة لونية(مصفوفة معاملات التفاصيل و مصفوفة قيم المعاملات التراكمية و مصفوفة عدد تكرار كل قيمة من المعاملات التراكمية .)حيث تم تطبيق الشفرة انتقائيا على بعض او كل المصفوفات الناتجة مما ادى الى تقليل وقت التشفير وفك الشفرة بشكل كبير على سبيل المثال تشفير مصفوفة المعاملات) لتشفير صورة كاملة10*3− . التراكمية سجل ثاني اعلى عشوائية مسجلة على الرغم من كون خوارزميات الضغط تستغرق وقت لكن مقارنة بالوقت الذي تم تقليله في التشفير فان المقايضة تستحق .في هذا العمل تم تعديل خوارزمية الضغط لتقليل الوقت المستغرق في ضغط المعلومات وتشفيرها انتقائيا.

I. Introduction

Nowadays, internet is considered a major source for information gathering and transmission. Electronic-financing, military and medical applications involve extensive use of digital media [1]. In such scenarios, security plays an important role [2]. One way to achieve security goals is by encrypting the digital media. Visual cryptography is the conversion of image data from their original form to another form that basically hides the content of images and preserves privacy from unauthorized access [3]. Image data have different features than text data, such as high correlation against pixels, bulk capacity, and high redundancy, in addition to their huge size that makes them slow to process and difficult to apply [4] [5].

There are many information hiding techniques such as steganography, watermarking, and cryptography [6]. Traditional encryption techniques provide a good security level but they are not suitable for multimedia data [1]. Another approach that is considered to preserve the security and privacy of images is known as "*Selective Encryption of Images*", which is obtained by applying cipher to part of the image to produce an obvious reduction in processing time and computational payload [7]. The resultant data are much easier to manipulate and dominate after applying compression algorithms that partition the data according to different aspects and reduces their volume. Then the result is selectively encrypted to provide security [2], [8].

Some of the articles relevant to this work were previously published. Belazi *et al*. [1] introduced a partial encryption scheme utilizing lifting wavelet transform to compress the image and extract the requisite information to be encrypted. The substitution boxes (S-boxes) generated by linear fractional transform chaotic system are used to encrypt the image components. The confusion and diffusion characteristics are achieved by three phases, namely substitution, block permutation, and diffusion, using dynamic keys in encryption process to produce scrambled image. Kekre *et al*. [3] introduced a scheme for partial image encryption that the input image is partitioned into four components (LL, HL, LH, HH) using sinusoidal wavelet transform. LL, LH and HH are then scrambled using Walsh sequence and the result is a partially encrypted image, while the HL sub-band is neglected. A Selective encryption technique was proposed by Paraveenkumar *et al*. [9], where the confusion and diffusion are applied to the input image, producing new values using pseudo-random number generator. Then the result is XORed with the original pixel values, while the modified image is then transformed using Discrete Cosine Transform (DCT) and quantized. Finally, the compressed image is encrypted using Arnold Shuffling to produce a scrambled image. Wen *et al*. [10] introduced a selective image encryption infrared target-based scheme by using logistic-sine system and block cross encryption. First, the infrared beam targets specific regions of the image that can be effectively detected using geometric active counter model based on partial differential equation (PDE). The detected regions of interest are encrypted using block cross encryption mode based on logistic-sine system to produce scrambled images. Zhou *et al*. [6] designed a novel scheme for partial encryption by combining discrete fractional random transform with compressive sensing. A measurement matrix and two random circular matrices employed in compressive sensing are generated by using two dimensional logistic modulation maps. The modified image is then encrypted using Arnold Transform and discrete fractional random transform. Choudhary *et al*. [7] presented a partial encryption scheme where the input image is partitioned into blocks, using block wise shuffling, and permuted by utilizing Arnold map. The permuted blocks are then combined to form the final presentation of the scrambled image. Rehman *et al*. [11] proposed a selective image encryption approach based on DNA complementary rules and block cipher, where the input image is partitioned into blocks. The most significant bit (MSB) in each block is added, under DNA algebraic addition operation, to the least significant bit (LSB) that is already encrypted by selecting chaotically different DNA rules for each pixel.

The image blocks are permuted using piecewise linear chaotic map (PWLCM) while the selection of encoding and decoding rules is done by logistic sequence for each pixel. Hazarika *et al*. [12] proposed a partial encryption scheme in which the input image is transformed using Discrete Wavelets Transform (DWT) to four components while only the (LL approximation) is quantized. The bit positions are permuted using two dimensional chaotic logistic maps then the result is XORed with third chaotic logistic map. Finally, the whole image is retransformed using Inverse Discrete Wavelet Transform (IDWT) to generate the encrypted image. Som *et al*. [13] proposed a non-adaptive scheme based on chaos. They first decomposed the gray scale images to their equivalent 8-bit planes, then encrypted the bit planes using couple tent map binary number generator (PRBNG). The four significant bit planes are determined by the level of significance for each pixel value and encrypted using a key obtained by using the recurrence relation of tent map based on couple tent map binary number generator (PRBNG). The significant bit planes are then combined to produce the cipher image. Parameshachari *et al*. [14] presented a novel algorithm for partial image encryption using combined phase modulation and sign encryption. First Fourier Transform (FT) is applied to the input image to obtain the phase and magnitude, then the image phase is scrambled using sign encryption that extracts sign bits to obtain partially encrypted image. Bahrami *et al*. [15] presented a scheme for partial encryption of images using an orthogonal transform known as Discrete Cosine Transform (DCT) that provides good compaction for multimedia data. The DCT coefficients are then quantized and the entropy coding is calculated to produce compressed image. The compressed image is then encrypted using stream cipher with an encryption key generated similarly to the AES key generation process. Then each coefficient is encoded using different stream cipher algorithm. Panduranga *et al*. [16] proposed a scheme for selective image encryption in which only the region of interest is detected, either manually or automatically, to be encrypted using a morphological operation. The block encryption process has two inputs, namely the selected block and the map image, to encrypt the blocks partially. Complete encryption for the selected blocks can be achieved by using separate map image for each block. Lian *et al*. [17] introduced two aspects for partial image encryption (sub-band and bit-plane). Sub-band layers are dependent on each other, which provides a vulnerable security that the encrypted layers can be recovered from the unencrypted ones, while, bit- planes are independent. The most significant 8-bits of the low frequency blocks are encrypted with AES cipher, while the middle and high frequency blocks are all encrypted with AES cipher to form the scrambled image. Panduranga *et al*. [18] introduced a scheme for image partial encryption in which the input image is divided into several blocks; i.e., the image is divided each time into different block sizes. Bits in each block are permuted using a chaotic map to generate new sequences and, subsequently, to generate the cipher image. Zang *et al*. [19] proposed an embedded partial image encryption for compressed colored images based on chaos. The color images is decomposed to RGB components that are going to be transformed to YC_bC_r. The channels are then transformed using DWT. The coefficients matrix is then encoded by CSPIHT that maintains three sets of data, which are the list of insignificant sets (LIS), list of insignificant pixels (LIP), and list of significant pixels (LSP). The Pricewise Linear Chaotic Map (PWLCM), that is then XORed with the LIP bit stream to produce partially encrypted image, performs the generation of the secret key stream.

II. The proposed method

As mentioned earlier, the main problem of image encryption strategy is the magnitude of the images to be encrypted (or scrambled). Hence, before applying the cipher, a lossy-compression algorithm is used.

The Selective Image Encryption starts with color space conversion to the basic three color bands of red, green and blue for RGB color model, or to luminance Y band, chrominance C_b, and C_r bands for YC_bC_r color model. Then, DCT is used to transform the data to frequency domain [20]. Quantization is used to reduce the statistical redundancy, while the resultant DCT quantized coefficients are scanned using Zigzag to reorder each block in one dimensional array. This prepares the blocks to be coded and encrypted in the hybrid shift encoder, that processes the DC coefficient of each block with DPCM for the entire image and RLE for AC coefficients. Horizontal block scanning was used in this step. The resultant three 1D arrays from each band of a specific color model were then selectively encrypted by XORing the selected bulks with the randomly generated combined secret key. The same seed is simultaneously fed to two random generators; First, the Linear Feedback Shift Register, where the seed was converted to its binary representation, then the bits comprising the seed were shifted circularly to form the new seed) and, second, the Linear Congruential Generator. The randomly generated sequence of each of the generators is then combined to produce the final secret key) [21]. Finally, the stream is passed through an insecure channel to be transmitted. The Image Reconstruction Unit implies the modules that are functioning in reverse order to the modules of a selective image encryption unit. Figure 1 shows the entire operation of the selective encryption.

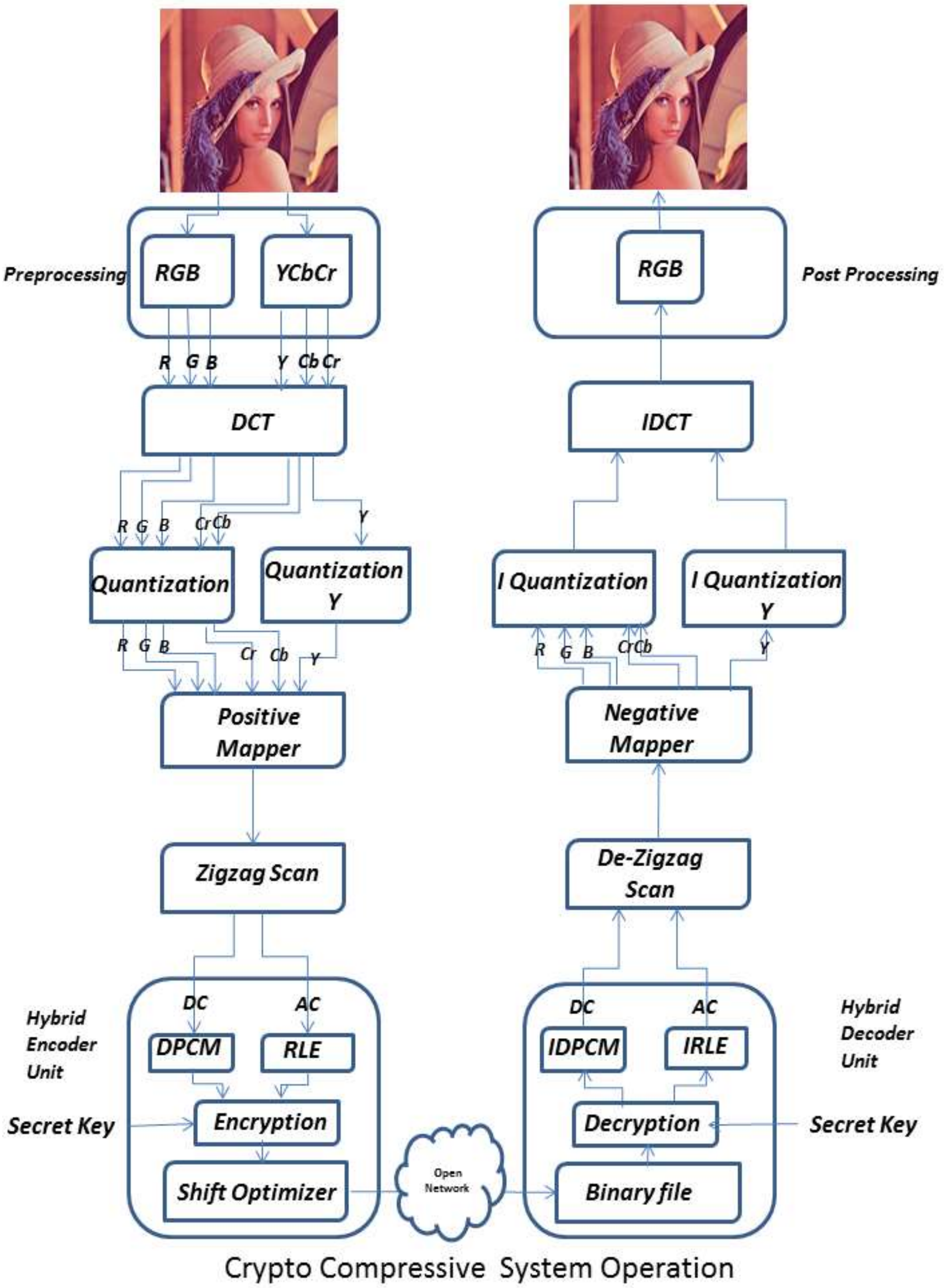


Figure 1-The selective image encryption process

III. Evaluation metrics

A. First Order Entropy

A digital image entropy is described as a statistical measure that states the randomness of colors, and it is defined by the following equation:

$$\boldsymbol{E1} = -\sum_{i=0}^{2^Q-1} \boldsymbol{Pi} * \log_2(\boldsymbol{Pi}) \qquad (1)$$

where Q represents the total amount of bits of the digital image according the agreement $\log_2(0) = 0$, while $\text{Pi} = \frac{\text{Ki}}{\text{M}*\text{N}}$ represents the probability of occurrence of color i, Ki represents the frequency of occurrence of color i in the digital image, and M and N represent the numbers of rows and columns of the image, respectively [22].

B. Second Order Entropy

The second order entropy E2 is calculated as in equation 2 [23]:

$$E2 = -\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} Pi(i,j) * lo\, g\big(pi(i,j)\big) \qquad (2)$$

where N and M represent the dimensions of the digital image according the agreement $\log_2(0) = 0$, while $\text{Pi} = \frac{\text{Ki}}{\text{M}*\text{N}}, \frac{\text{Kj}}{\text{M}*\text{N}}$ represents the probability of occurrence of colors i and j, respectively, since the color j= i+1, and Ki represents the frequency of occurrence of color i and j in the digital image [24].

C. Run Test for Randomness

A statistical check that was employed to recognize the randomness in data. The run test for randomness is occasionally described as the Geary test, and it is a nonparametric test. This test is a substitute test to check auto-association in the data. Auto-association means that the data has association with its lingered value. To authenticate whether or not the data has association with the lingered value, the run test for randomness is smeared.

The following equation was used to calculate the run test value [23]:

$$\boldsymbol{Z} = \frac{r-\mu r}{Ơr} \qquad (3)$$

where:

r is the number of runs,

µ*r* is the expected number of runs,

Ơ*r* is the standard deviation of the number of runs.

IV. Image Test Materials and Results

The developed compression/encryption method was tested using different BMP image files; each image file has different characteristics. Several smooth image files "[Lena.bmp (true color), Lena.bmp (gray), Peppers.bmp] and sharp edge image files [Barbara.bmp (true color), Barbara.bmp (gray), Baboon.bmp], (with a size of 256×256 were used as image test samples in order to evaluate the compression method performance. Figure-2 presents these images.

a. Color Lena.bmp **b. Gray Lena.bmp** **c. Color Peppers.bmp**

d. Color Barbara.bmp **e. Gray Barbara.bmp** **f. Color Baboon.bmp**

Figure 2-Image test materials.

Table 1-The optimal values obtained from the underlying compression algorithm for the tested images.

Image	Color Model	PSNR	Compression Ratio	Compression Gain	Time in Sec.	
					Compression	Decompression
Color Lena	YC_bC_r	29.14	21.33	95%	0.712	0.657
	RGB	29.50	7.68	86%	0.732	0.653
Gray Lena	YC_bC_r	29.17	5.81	82%	0.795	0.670
	RGB	25.69	2.56	60%	0.755	0.664
Color Peppers	YC_bC_r	29.22	12	91%	0.726	0.698
	RGB	22.02	8.72	88%	0.819	0.666
Color Barbara	YC_bC_r	29.21	13.71	92%	0.787	0.629
	RGB	26.98	6.4	84%	0.810	0.662
Gray Barbara	YC_bC_r	29.20	5.81	82%	0.736	0.620
	RGB	28.10	1.88	46%	0.799	0.618
Color Baboon	YC_bC_r	26.25	7.86	86%	0.783	0.673
	RGB	26.09	2.25	55%	0.830	0.674

The compressed stream was then scrambled by XORing a randomly generated combined secret key with selected bulks of the compressed image data. The compressed data bulks tested are shown in table 1, along with two metrics for measuring randomness caused in the image data (1st order entropy and 2nd order entropy) as well as the encryption and decryption time.

Table 2-The effects of encryption on images randomization using 1st order entropy and 2nd order entropy

Image	Encrypted Bulks	First Order Entropy	Second Order Entropy	Run Test	Time (in seconds)	
					Encrypt	Decrypt
Color Lena (with YCC color model)	All Coefficients	6.84	10.93	0.48	0.014	0.009
	DC Coefficients Only	7.24	11.50	0.73	0.0007	0.0005
	AC Coefficients Only	6.86	10.96	0.47	0.0042	0.0032
	AC Runs Only	7.27	11.60	0.79	0.0074	0.0006
	DC+ AC Coefficients	6.83	10.93	0.47	0.0054	0.0005
	DC Coefficients+ AC Runs	7.26	11.61	0.76	0.0075	0.0005
	AC Coefficients+ AC Runs	6.99	11.09	0.62	0.016	0.010
Color Lena (with RGB color model)	All Coefficients	6.87	11.53	0.58	0.031	0.026
	DC Coefficients Only	6.79	11.33	0.51	0.001	0.031
	AC Coefficients Only	6.72	11.27	0.48	0.018	0.015
	AC Runs Only	7.01	11.68	0.63	0.016	0.019
	DC+ AC Coefficients	6.71	11.30	0.47	0.015	0.016
	DC Coefficients+ AC Runs	7.01	11.72	0.67	0.020	0.017

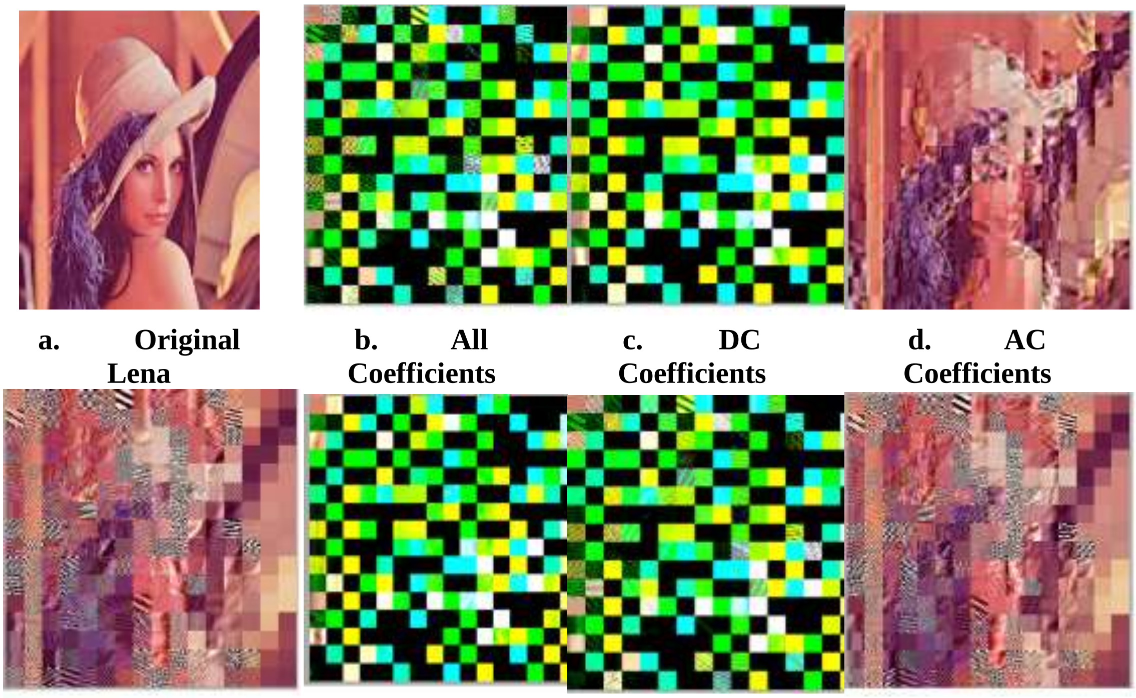
	AC Coefficients+ AC Runs	6.96	11.63	0.62	0.029	0.032
Color Peppers (with YCC color model)	All Coefficients	7.21	11.85	0.75	0.019	0.014
	DC Coefficients Only	7.21	11.78	0.77	0.0009	0.001
	AC Coefficients Only	7.18	11.81	0.73	0.0122	0.0101
	AC Runs Only	7.19	11.79	0.76	0.0085	0.0011
	DC+ AC Coefficients	7.19	11.81	0.78	0.0094	0.0010
	DC Coefficients+ AC Runs	7.21	11.79	0.79	0.010	0.0008
	AC Coefficients+ AC Runs	7.16	11.81	0.76	0.017	0.019
Color Peppers (with RGB color model)	All Coefficients	7.18	11.69	0.74	0.014	0.010
	DC Coefficients Only	7.30	11.79	0.83	0.0007	0.017
	AC Coefficients Only	7.21	11.72	0.77	0.0067	0.0078
	AC Runs Only	7.29	11.77	0.80	0.0068	0.0069
	DC+ AC Coefficients	7.22	11.71	0.74	0.0069	0.0083
	DC Coefficients+ AC Runs	7.29	11.80	0.81	0.0080	0.0090
	AC Coefficients+ AC Runs	7.21	11.72	0.78	0.013	0.014
Gray Lena(with YCC color model)	All Coefficients	7.20	11.71	0.76	0.012	0.013
	DC Coefficients Only	7.15	11.86	0.75	0.0008	0.0008
	AC Coefficients Only	7.15	11.60	0.74	0.0052	0.0068
	AC Runs Only	7.18	11.67	0.72	0.0059	0.0007
	DC+ AC Coefficients	7.17	11.56	0.75	0.0056	0.0005
	DC Coefficients+ AC Runs	7.20	11.68	0.78	0.0061	0.0009
	AC Coefficients+ AC Runs	7.19	11.71	0.77	0.010	0.012
Gray Lena(with RGB color model)	All Coefficients	6.89	12.92	0.49	0.080	0.064
	DC Coefficients Only	6.95	11.90	0.58	0.0009	0.074
	AC Coefficients Only	6.99	12.17	0.63	0.058	0.034
	AC Runs Only	6.95	11.90	0.61	0.040	0.038
	DC+ AC Coefficients	6.99	12.17	0.65	0.043	0.035
	DC Coefficients+ AC Runs	6.95	11.90	0.62	0.044	0.037
	AC Coefficients+ AC Runs	7.00	12.17	0.69	0.085	0.072
Color Barbara	All Coefficients	6.86	11.36	0.58	0.017	0.020

(with YCC color model)	DC Coefficients Only	7.00	11.53	0.67	0.0007	0.0007
	AC Coefficients Only	6.96	11.54	0.65	0.010	0.007
	AC Runs Only	6.86	11.31	0.58	0.0088	0.0007
	DC+ AC Coefficients	6.96	11.55	0.66	0.0094	0.0005
	DC Coefficients+ AC Runs	6.88	11.32	0.57	0.0097	0.0008
	AC Coefficients+ AC Runs	6.85	11.38	0.54	0.020	0.019
Color Barbara (with RGB color model)	All Coefficients	6.79	11.60	0.53	0.47	0.043
	DC Coefficients Only	6.97	11.87	0.64	0.0007	0.0006
	AC Coefficients Only	6.82	11.63	0.58	0.024	0.022
	AC Runs Only	6.75	11.36	0.54	0.029	0.026
	DC+ AC Coefficients	6.98	11.88	0.60	0.0308	0.0306
	DC Coefficients+ AC Runs	7.00	12.81	0.73	0.0007	0.0007
	AC Coefficients+ AC Runs	6.83	11.63	0.58	0.047	0.034
Color Baboon (with YCC color model)	All Coefficients	6.83	11.54	0.58	0.041	0.033
	DC Coefficients Only	6.78	11.42	0.53	0.0008	0.0011
	AC Coefficients Only	6.78	11.52	0.54	0.018	0.013
	AC Runs Only	6.88	11.49	0.58	0.023	0.0007
	DC+ AC Coefficients	6.80	11.53	0.57	0.016	0.0010
	DC Coefficients+ AC Runs	6.84	11.44	0.58	0.039	0.0011
	AC Coefficients+ AC Runs	6.93	11.76		0.056	0.039
Color Baboon (with RGB color model)	All Coefficients	6.54	11.36	0.48	0.341	0.104
	DC Coefficients Only	6.71	11.51	0.52	0.0009	0.122
	AC Coefficients Only	6.58	11.49	0.47	0.194	0.041
	AC Runs Only	6.71	11.51	0.53	0.065	0.066
	DC+ AC Coefficients	6.57	11.48	0.46	0.204	0.055
	DC Coefficients+ AC Runs	6.73	11.52	0.51	0.194	0.058
	AC Coefficients+ AC Runs	6.58	11.49	0.48	0.189	0.084
Gray Barbara (with YCC color model)	All Coefficients	6.70	10.97	0.54	0.016	0.013
	DC Coefficients Only	6.71	10.92	0.56	0.0004	0.0006
	AC Coefficients	6.68	10.93	0.50	0.0090	0.0097

	Only					
	AC Runs Only	6.74	10.97	0.57	0.0087	0.0018
	DC+ AC Coefficients	6.68	10.93	0.53	0.009	0.004
	DC Coefficients+ AC Runs	6.78	10.94	0.56	0.0082	0.004
	AC Coefficients+ AC Runs	6.70	10.98	0.53	0.017	0.019
Gray Barbara (with RGB color model)	All Coefficients	6.69	11.48	0.51	0.053	0.052
	DC Coefficients Only	6.73	11.12	0.54	0.001	0.065
	AC Coefficients Only	6.74	11.12	0.53	0.031	0.032
	AC Runs Only	6.74	11.12	0.58	0.025	0.030
	DC+ AC Coefficients	6.75	11.13	0.59	0.026	0.033
	DC Coefficients+ AC Runs	6.74	11.12	0.57	0.029	0.028
	AC Coefficients+ AC Runs	6.75	11.12	0.54	0.062	0.046

Table-1 shows the randomness caused in the image when encrypting different bulks of data under the default quantization parameters. Changing the quantization parameters showed a behavior that the measures of the encrypted image varied regarding the compression gain; the lower the compression gain was, the higher randomness was caused in the image, which is consistent with the randomness in data rule which states that the bigger the data is the higher the caused randomness.

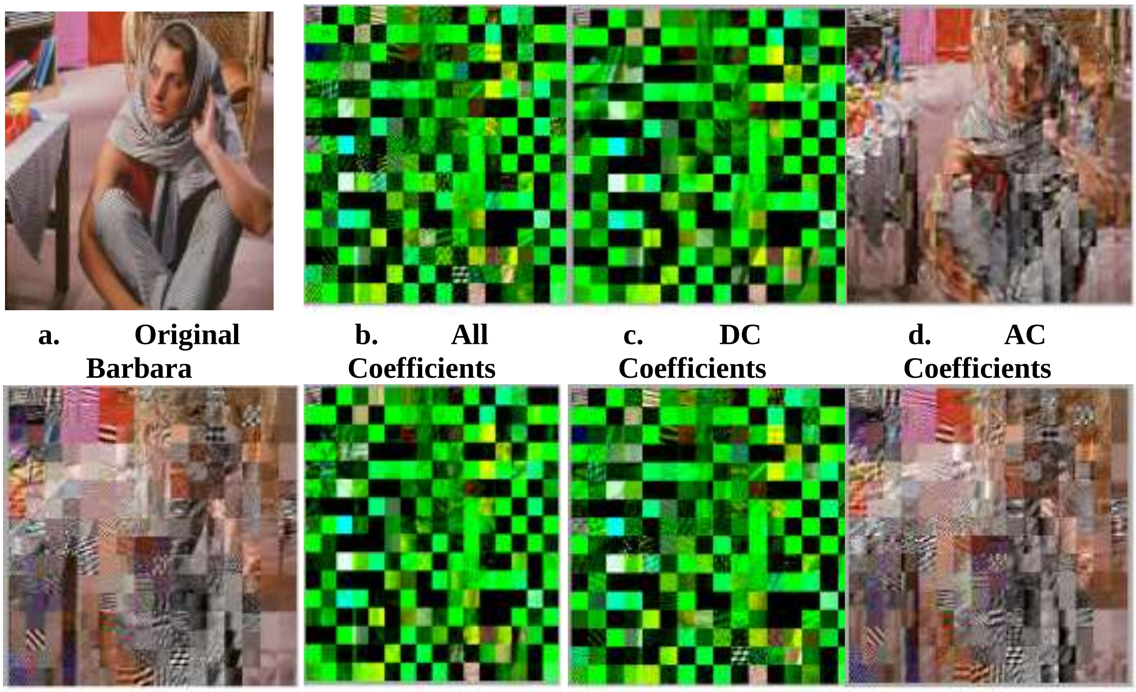
Different results were obtained by encrypting each of the bulks mentioned above (Table-1). The effects of applying the cipher are shown in figures 3 and 4 for two test images (Lena.bmp and Barbara.bmp).



a. Original Lena **b. All Coefficients** **c. DC Coefficients** **d. AC Coefficients**

e. AC Runs **f. DC+ AC Coefficients** **g. DC Coef.+ AC Runs** **h. AC Coeff.+ AC Runs**

Figure 3-Encrypting different bulks using randomly generated secret key for standard Lena image.

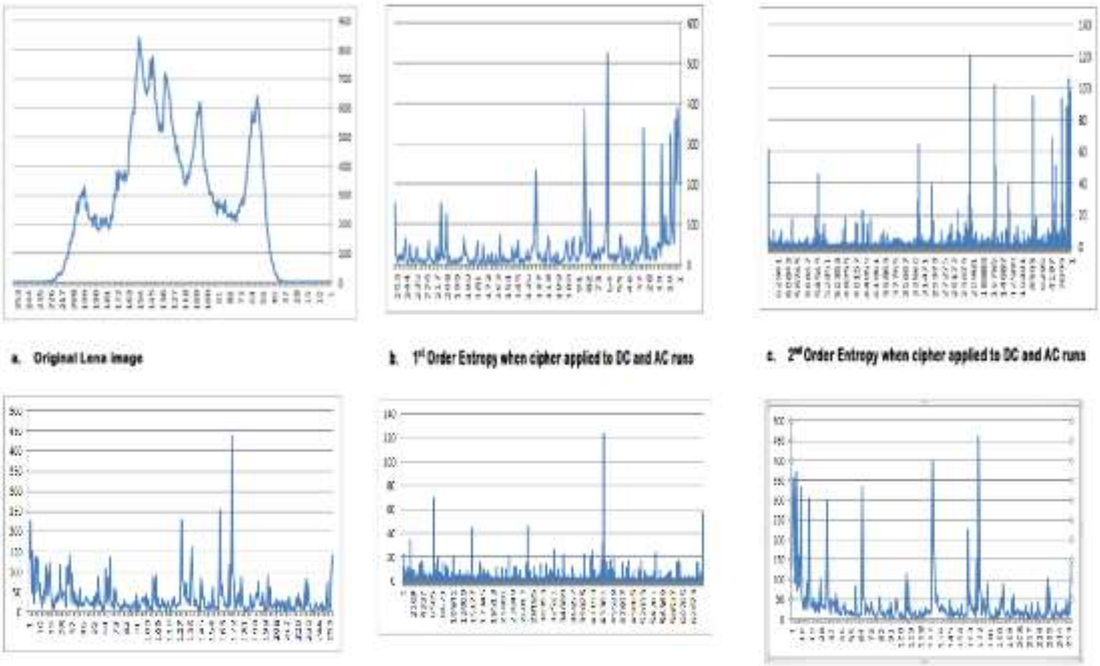


a. Original Barbara **b. All Coefficients** **c. DC Coefficients** **d. AC Coefficients**

e. AC Runs **f. DC+ AC Coef.** **g. DC Coef.+ AC Runs** **h. AC Coef.+ AC Runs**

Figure 4-Encrypting different bulks using randomly generated secret key for standard Barbara image.

Also, a histogram evaluation was calculated to illustrate the randomization caused in image data after applying the cipher, where the metrics used to measure the randomization were 1st order entropy and 2nd order entropy. Figures 5 and 6 show the histogram of the cipher images, Lena Bmp Barbara Bmp, respectively, when different bulks were encrypted.



a. Original Lena image

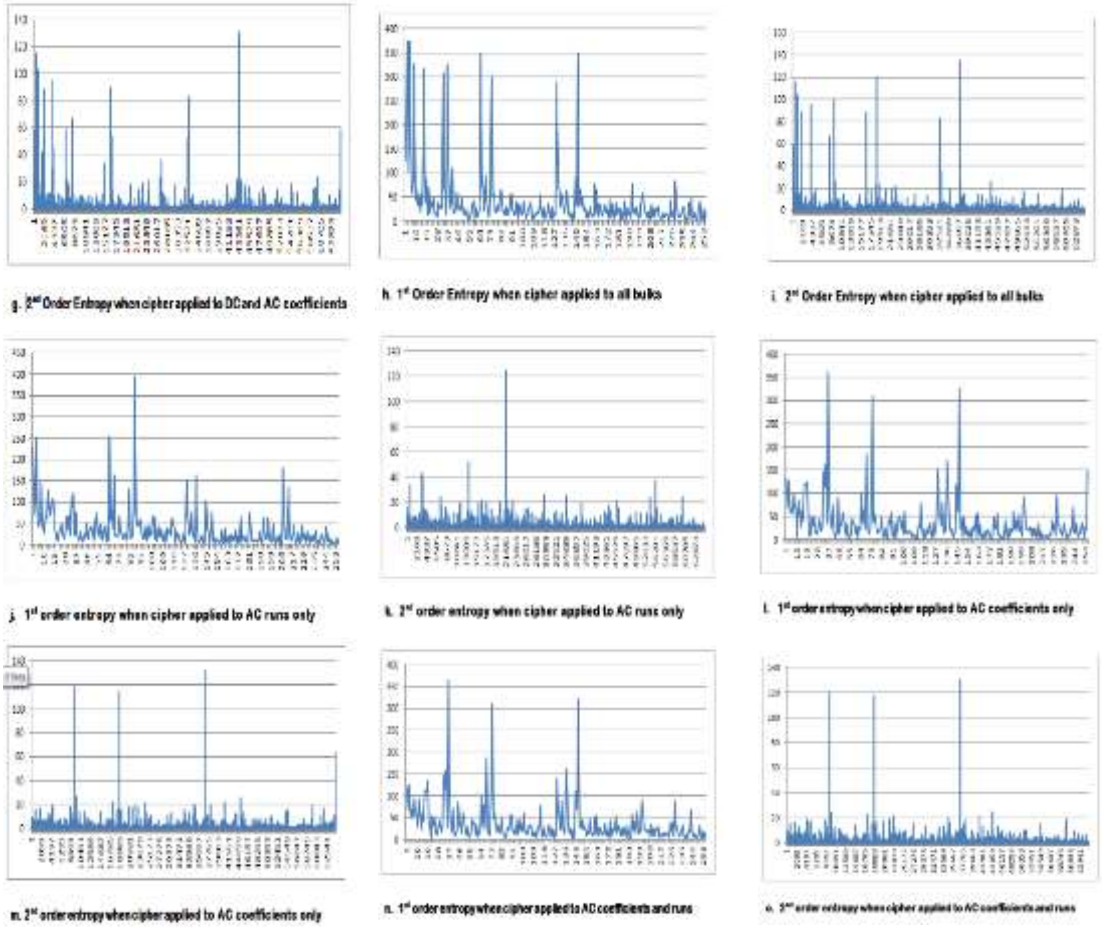
b. 1st Order Entropy when cipher applied to DC and AC runs

c. 2nd Order Entropy when cipher applied to DC and AC runs

d. 1st Order Entropy when cipher applied to DC coefficients only

e. 2nd Order Entropy when cipher applied to DC coefficients only

f. 1st Order Entropy when cipher applied to DC and AC coefficients



g. 2nd Order Entropy when cipher applied to DC and AC coefficients

h. 1st Order Entropy when cipher applied to all bulks

i. 2nd Order Entropy when cipher applied to all bulks

j. 1st order entropy when cipher applied to AC runs only

k. 2nd order entropy when cipher applied to AC runs only

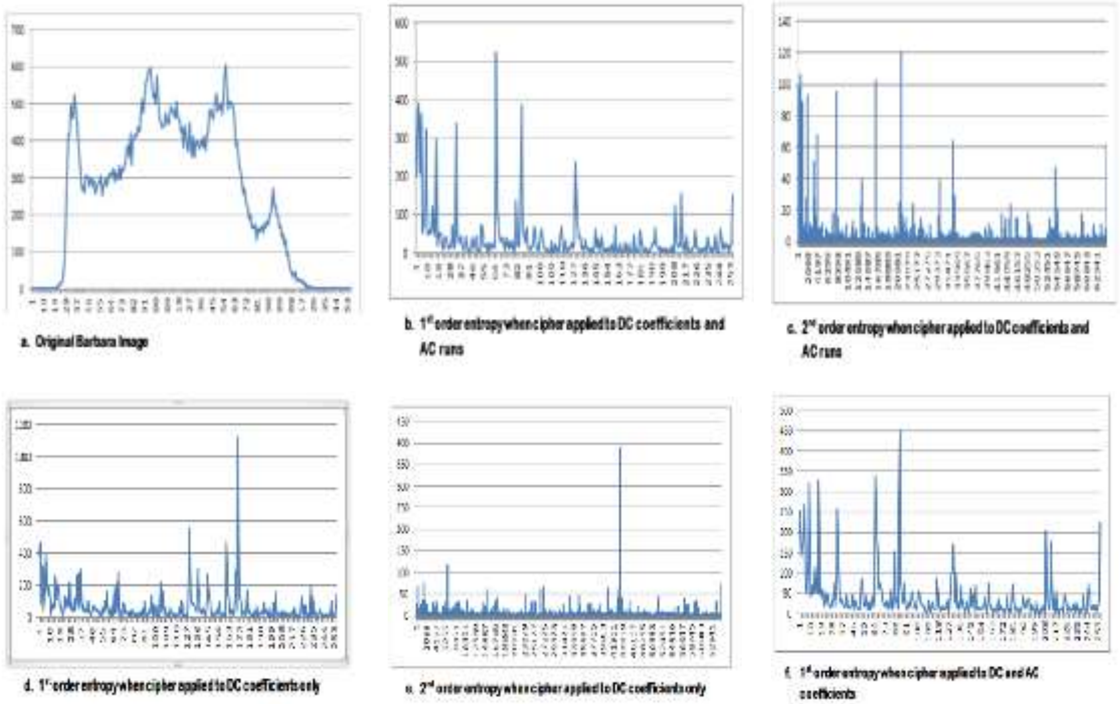
l. 1st order entropy when cipher applied to AC coefficients only

m. 2nd order entropy when cipher applied to AC coefficients only

n. 1st order entropy when cipher applied to AC coefficients and runs

o. 2nd order entropy when cipher applied to AC coefficients and runs

Figure 5-Histogram of the cipher Lena image when the cipher applied to different bulks of image data.



a. Original Barbara Image

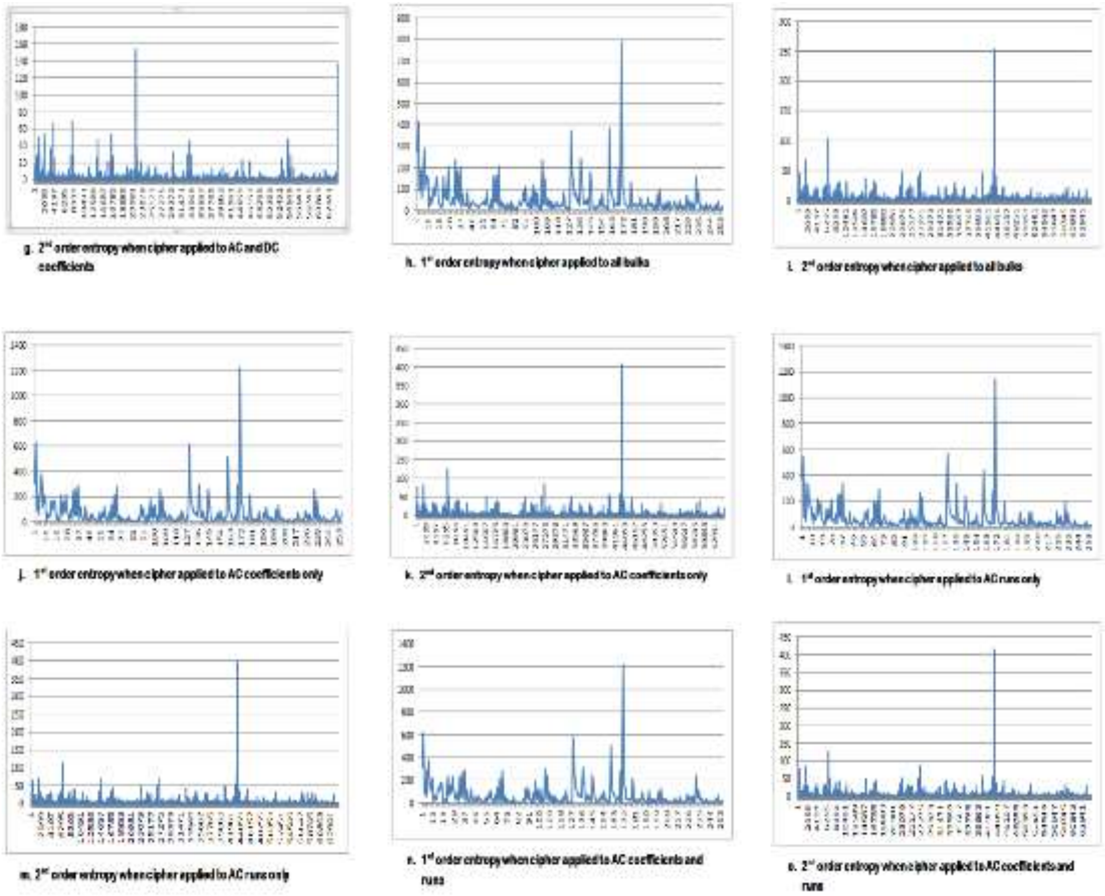
b. 1st order entropy when cipher applied to DC coefficients and AC runs

c. 2nd order entropy when cipher applied to DC coefficients and AC runs

d. 1st order entropy when cipher applied to DC coefficients only

e. 2nd order entropy when cipher applied to DC coefficients only

f. 1st order entropy when cipher applied to DC and AC coefficients



g. 2nd order entropy when cipher applied to AC and DC coefficients

h. 1st order entropy when cipher applied to all bulks

i. 2nd order entropy when cipher applied to all bulks

j. 1st order entropy when cipher applied to AC coefficients only

k. 2nd order entropy when cipher applied to AC coefficients only

l. 1st order entropy when cipher applied to AC runs only

m. 2nd order entropy when cipher applied to AC runs only

n. 1st order entropy when cipher applied to AC coefficients and runs

o. 2nd order entropy when cipher applied to AC coefficients and runs

Figure 6-Histogram of the cipher Barbara image when the cipher applied to different bulks of image data,

V. Comparisons with Previous Studies

Many methods for selective image encryption were developed in the past few years. In this section, the results of our proposed method (CCSC)) are compared with some previously published methods.
Table 3 lists the encryption and decryption time attained by our proposed CCSC method with those given in previous studies, taking into consideration that in these studies the same images with different or same sizes were used. The results shown in the table demonstrate that our proposed scheme outperforms the other methods.

Table 3-Comparison between the encryption/decryption time results of some related works and the proposed CCSC scheme used to encode different standard images.

Image	**Reference**	**size**	**Time (in seconds)**	
			Encrypt	**Decrypt**
~~Elaine~~	[13]	**---------**	**0.923**	**0.634**
	CCSC	**200∗200**	**0.569**	**0.421**
Baboon	[13]	**256∗256**	**0.398**	**0.296**
	CCSC	**256∗256**	**0.907**	**0.873**
	[8]	**512*512**	**1.113**	**---------**
	[17]	**512*512**	**9.9**	**---------**
	CCSC	**512*512**	**4.518**	**3.795**
Airplane	[8]	**512*512**	**1.099**	**---------**
	CCSC	**512*512**	**4.483**	**3.634**
Lena	[8]	**256*256**	**0.272**	**---------**

	[6]	**256*256**	**0.606061**	**---------**
	[17]	**256*256**	**7.9**	**---------**
	[4]	**256*256**	**0.0538**	**---------**
	[1]	**256*256**	**0.155**	**---------**
	[15]	**256*256**	**1.75**	**---------**
	[6]	**256*256**	**0.606061**	**---------**
	CCSC	**256*256**	**0.762**	**0.620**
	[6]	**512*512**	**2.6354**	**---------**
	[4]	**512*512**	**0.2338**	**---------**
	CCSC	**512*512**	**4.368**	**3.596**
~~Barbara~~	[8]	**512*512**	**1.113**	**---------**
	~~CCSC~~	**256*256**	**0.715**	**0.677**
~~Couple~~	[8]	**256*256**	**0.273**	**---------**
	[15]	**256*256**	**1.74**	**---------**
	~~CCSC~~	**512*512**	**4.176**	**3.394**
~~Jelly beans~~	[8]	**256*256**	**0.273**	**---------**
	~~CCSC~~	**200*200**	**0.575**	**0.494**
Peppers	[8]	**512*512**	**1.092**	**---------**
	CCSC	**512*512**	**0.0018**	**0.0025**
	[17]	**256*256**	**9.5**	**---------**
	CCSC	**256*256**	**0.714**	**0.606**
Tiffany	[8]	**512*512**	**1.100**	**---------**
	CCSC	**512**512**	**4.120**	**3.296**
~~Child~~	[8]	**256*197**	**0.211**	**---------**
	CCSC	**256*256**	**0.768**	**0.609**
Camera man	[17]	**256*256**	**8.0**	**---------**
	CCSC	**256*256**	**0.782**	**0.682**
~~Chemical plant~~	[15]	**256*256**	**1.67**	**---------**
	CCSC	**200*200**	**0.574**	**0.423**
~~Aerial~~	[15]	**256*256**	**1.65**	**---------**
	CCSC	**200*200**	**0.583**	**0.467**
~~Stream and bridge~~	[15]	**256*256**	**1.66**	**---------**
	CCSC	**512*512**	**4.585**	**3.504**
~~Man~~	[15]	**256*256**	**1.69**	**---------**
	CCSC	**200*200**	**0.538**	**0.452**
~~Airport~~	[15]	**256*256**	**1.68**	**---------**
	CCSC	**200*200**	**0.586**	**0.446**

VI. Conclusions and Future Work

VII. In this paper, a selective image encryption scheme was developed for YCC and RGB color models. The conclusions from or results assessment are abridged in the following remarks:

1. For the compression phase that was based on discrete cosine transform (DCT), the test results indicated that the performance of the developed scheme are encouraging regarding the size reduction that reached up to 95% for the compressed image files.
2. Converting the test image subjects to YCC color model improves both compression ratio and PSNR for the reconstructed images, and gives better results than the RGB color model does.
3. Using 1D discrete cosine transform (1D DCT) decreases the transformation time down to 1:47 sec. as compared to 2D discrete cosine transform that is usually applied for images.
4. Including the encryption process in the hybrid encoder reduces the processing time sufficiently than reading and rewriting the compressed/encrypted binary file.
5. The higher the compression gain is the higher the value of the first order entropy, but the lower the value of the second order entropy for all types of images tested.

VIII. Suggestions for Future Work

1. Using quad trees in the compression phase as a scanning tool (instead of Zigzag scanning). The latest published researches proved the usefulness of using quad trees for JPEG 2000.
2. Using the same affection mechanism to connect the diffusion and compression modules with video crypto compressive scheme to establish fast and robust encryption scheme for video streaming over transmission channels.
3. Encrypting different bulks using sinks in the compressed binary file.
4. For the process of combined secret key generation, it is possible to combine the bit sequence generated from LFSR with variable indexed of the bit sequence generated by LCG for further robustness (i.e. the combining index does not necessarily start from zero regarding the LCG generated bit sequence).

References

1. Belazi, A. **2017**. "chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transform," *optics and laser in engineering, Elsevier* , pp. 37-50.
2. Chaudhari, P. and Sonali, A. **2015**. "Review on Secret Data Hiding in Encrypted Compressed Video Bit Streams," *International Journal of Computer Science Trends and Technology (IJCST)* , **3**(2): 94-96.
3. Kekre H.B., Sarode T. and Halarnkar P.N. **2016**. Partial Image Scrambling Using Walsh Sequency in Sinusoidal Wavelet Transform Domain. In: Berretti S., Thampi S., Srivastava P. (eds) Intelligent Systems Technologies and Applications. Advances in Intelligent Systems and Computing, vol 384.
4. Springer, Cham y. z. c.-m. p. C. p. c. zhongyun hua, **2015**. "2D sine logistic modulation map for image encryption," *Information Sciences, Elsevier,* pp. 80-94.
5. Gbashi E. K., "Text Compression & Encryption Method Based on RNA and MTF," *Iraqi Journal of Science*, pp. 1149-1158, 2017.
6. Zhoua, M. **2015**. "double image encryption scheme combining DWT-based compressive sensing with discrete fractional random transform," *optics communications, Elsevier.*
7. Choudhary **2014**. "Partial Image Encryption based on Block wise Shuffling using Arnold Map," *International Journal of Computer Applications,* **97**(10).
8. KHASHAN et al, **2014**. "Performance study of selective encryption in comparison to full encryption for still visual images," *Journal of Zhejiang University-SCIENCE , springer,* pp. 435-444.
9. Praveenkumar et al, **2016**. "Chaotic & Partial Encrypted Image on XOR Bus - Unidentified Carrier Approach," in *2016 International Conference on Computer Communication and Informatics (ICCCI -2016), ©2016 IEEE,* Coimbatore, INDIA.
10. Wen, A. **2015**. "infrared target based selective encryption by chaotic map," *optics communications, Elsevier,* pp. 131-139.
11. Rehman et al, **2014**. "Selective encryption for gray images based on chaos and DNA complementary rules," *Multimed Tools Appl, # Springer Science+Business Media New York*.
12. Hazarika et al, **2014**. "A Wavelet Based Partial Image Encryption using Chaotic Logistic Map," in *2014 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT).*
13. Som et al, **2013**. "A Non-adaptive PartialEncryption of Grayscale Images Based on Chaos," in *First International Conference on Computational Intelligence: Modelling, Techniques and Applications(CIMTA-2013), Elsevier*.
14. Parameshachari et al, **2013**. "Secure Transmission of an Image using Partial Encryption based Algorithm," *International Journal of Computer Applications,* **63**(16): 33-36.
15. Bahrami et al, **2013**. "encryption of multimedia content in partial encryption scheme of DCT transform coeffiecent using a light weight stream algorithm," *optik, Elsevier,* pp. 3693-3700.
16. Panduranga et al, **2013**. "Selective image encryption for Medical and Satellite Images," *International Journal of Engineering and Technology (IJET),* **5**(1).
17. Lian et al, **2013**. "On the design of partial encryption scheme for multimedia content," *MathematicalandComputerModelling, Elsevier,* pp. 2613-2624.

18. Panduranga et al, **2013**. "Partial Image Encryption using block wise shuffling and chaotic map," in *Proceedings of International Conference on Optical Imaging Sensor and Security, Coimbatore, Tamil Nadu, India, July 2-3, 2013* , Coimbatore, Tamil Nadu, India.

19. Zhang N. **2013**. "Chaos-based partial encryption of SPIHT coded color images," *signal processing, Elsevier,* pp. 2422-431.

20. Ahmed et al, **2017**. "The Use of Wavelet, DCT & Quadtree for Images Color Compression," *Iraqi Journal of Science,* **58**: 550-561.

21. Hassan, H. **2018**. "Color Image Compression Based on Dct, Differential Pulse Coding Modulation, and Adaptive Shift Coding," *Journal of Theoretical and Applied Information Technology* , **96**(11): 3160-3171.

22. Torres et al, **2015**. "Behavior Study of Entropy in A Digital Image Through an Iterative Algorithm of the Mean Shift Filtering," *International Journal of Soft Computing, Mathematics and Control (IJSCMC),* **4**(3): 1-21.

23. Bujang et al, **2018**. "An Application of the Runs Test to Test for Randomness of Observations Obtained from a Clinical Survey in an Ordered Population," *The Malaysian Journal of Medical Sciences*.

24. Chang et al, **1994**. "A Relative Entropy-Based Approach to Image Thresholding," *Pattern Recognition Society ,Elsevier Science Lid,* **27**(9): 1275- 1289.