Modification of RC5 Algorithm for Image Encryption

[1]Ashwaq T. Hashim, [2]Dr. Rasha Fahim Nathim, and [3]Gaidaa Saeed Mahdi

[1]Control and Systems Engineering Dep., University of Technology

[2]Electromechanical Engineering Dep.. University of Technology

[3]Chemical Engineering Dep. , University of Technology

e-mail: ashwaqtalib@yahoo.com , rasha.mushtaq@yahoo.com

Received: 1/10 /2013

Accepted: 4/6 /2014

Abstract – Encryption is mainly used to transmit the data over networks. There are so many techniques introduced which are used to protect the confidential image data from any unauthorized access. Multimedia data contains different types of data that includes text, audio, video, graphic, and images with the increasing use of multimedia data over internet; here comes a demand of secure multimedia data. Most of the encryption algorithm available is generally used for text data and not suitable for multimedia data. In this paper 256-bit RC5 in quadrate design has been proposed. It is a secret-key block cipher that uses good features of RC5 algorithm using another overall structure design. In RC5 quadrate design of F-functions will be used instead of rounds. To ensure improving the encryption performance; mainly for images characterized by reduced entropy, the implementation of both techniques has been realized for experimental purposes. Comparative study with traditional encryption algorithms shows the superiority of the modified algorithm.

.

Keywords – ***Cryptography, Image Encryption, RC5, Quadrate Design,***

1. Introduction

With the ever-increasing growth of multimedia applications, security is an important issue in communication and storage of images, and Encryption is a common technique to uphold image security. Image encryption techniques try to convert original image to another image that is hard to understand; to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption. The process of encoding plain text messages into cipher text messages is called encryption and the reverse process of transforming cipher text back to plain text is called as decryption. Image and video encryption have applications in various fields including internet communication, multimedia systems, medical imaging, Tele-medicine and military communication. Color images are being transmitted and stored in large amount over the Internet and wireless networks, which take advantage of rapid development in multimedia and network technologies. In recent years, many of color image encryption approaches have been proposed. Until now, various data encryption algorithms have been proposed and widely used, such as AES, RC5, 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. Multimedia data are often of high redundancy, of large volumes and require real-time interactions [1].

In most of the natural images, the values of the neighboring pixels are strongly correlated (i.e. the value of any given pixel can be reasonably predicted from the values of its neighbors). In order to dissipate the high correlation among pixels and increase the entropy value, a transformation algorithm has been proposed that divides the image into blocks and then pass them to the quadrate design of RC5 encryption algorithm and then shuffle their positions. By using the correlation and entropy as a measure of security, this process results in a lower correlation and a higher entropy value when compared to using the RC5 algorithm alone, and thus improving the security level of the encrypted images.

2. Literature Review

The security of digital images has become more and more important due to the rapid evolution of the Internet in the digital world today. The security of digital images has attracted more attention recently, and many different image encryption methods have been proposed to enhance the security of these images. Hai Yu and Zhiliang Zhu in 2009 [2]. An efficient image encryption algorithm has been proposed, based on image reconstruction using some adjacent pixel characteristics**.** According to the different characteristics of different bit level binary images, the proposed encryption scheme reconstructs the image at the bit level. Two parts of information, the significant one and the unimportant one, are treated differently and processed separately. Simulations and cryptanalysis both show that the proposed image encryption scheme is more efficient and yields better level of security. Zhang Yun-peng , and Zhai Zheng in 2009 [3], suggested the chaotic encryption and improved DES encryption and a combination of image encryption algorithm was used to find the gaps. In this paper new encryption logistic Map which produced pseudo random sequence on RGB image and make double times encryption with improved DES. Combination of Chaos and the improvement DES make the final

algorithm more secure, faster and more suitable for digital image encryption. Seyed Hossein Kamali and Reza Shakerian [4] in 2010, proposed a new encryption scheme as a modification of AES algorithm based on both Shift Row Transformations. If the value in the first row and first column is even, the first and fourth rows are unchanged and each bytes in the second and third rows of the state are cyclically shifted right over different number, else the first and third rows are unchanged and each byte of the second and fourth rows of the state are cyclically shifted left over different number of bytes. Experimental results show that MAES gives better encryption results in terms of security against statistical attacks and increased performance. In 2011 Paul A.J P. Mythili and K. Paulose Jacob [5] proposed a fast symmetric key encryption procedure, Matrix Array symmetric Key Encryption (MASK) based on matrix manipulation is presented**.** This provides fast conversion of plaintext and images into cipher text and cipher images**.** The encryption scheme presented here is a block cipher with a block size of 128 bits and key size of 128 bits. Mask result is also compared with AES. The performance test results indicate the suitability of MASK for fast image encryption. Aditee Gautam et. al. [6] in 2011, reported a block based transformation algorithm has been used in which image is divided into number of blocks. These blocks are transformed before going through an encryption process. At the receiver side, these blocks are retransformed in to their original position and decryption process is performed. Advantage of this approach, is that it reproduces the original image with no loss of information for the encryption and decryption process, where a blowfish algorithm is used. In [7], Nithin N. el al in 2013, proposed Fast Encryption Algorithm (FEAL), an encryption/ decryption strategy for gray scale images. FEAL works almost similar to Data Encryption Standard (DES) algorithm, but it is faster than DES. To encrypt the images, the input image is split into 16x16 blocks of information. Encryption/ Decryption which is carried out using 12 keys, each of length 16-bits. In 2013, Narendra K. Paree el. al. [8] proposed an encryption algorithm for gray images using a secret key of 128-bits size. Initially, visual quality of image is degraded by the mixing process. Resultant image is partitioned into key dependent dynamic blocks and, further, these blocks are passed through key dependent diffusion and substitution processes. Total sixteen rounds are used in the encryption algorithm

3. RC5 Algorithm

RC5 has a variable word size, a variable number of rounds and a variable length secret key. RC5 is exactly designated as RC5-w/r/b, where w denotes word size in bits, the standard value is 16, 32 and 64 bits; r denotes number of rounds and allowable value ranges from 0 to 255; b denotes length of user's secret key in bytes and the allowable value ranges from 0 to 255. The parameters we have used is RC5-32/12/16. RC5 consists of three components: key expansion, encryption and decryption algorithm. This uses three primitive operations and their inverse.

1. Addition of words "+". This is modulo-2w addition and the inverse operation subtraction of words"-".

2. Bit wise exclusive OR (XOR) of words

3. The rotation of word x left by y bits is denoted x<<<y. The inverse operation is the rotation of word x right by y bits is denoted x>>>y .

In the key expansion module, the password key K is expanded to a much larger size in a key table S. The size of table S is 2(r+1), where r is the number of rounds.

The encryption process takes a plaintext input and produces a cipher-text as the output. The key-expansion process must have already been performed before this process. The decryption process takes a cipher-text as the input and produces a plaintext as the output.

In general, the same plaintext block will always encrypt to the same cipher-text when using the same key in a block cipher whereas the same plaintext will encrypt to different cipher-text in a stream cipher. The conventional architecture of RC5, shown in Figure (1) [9].

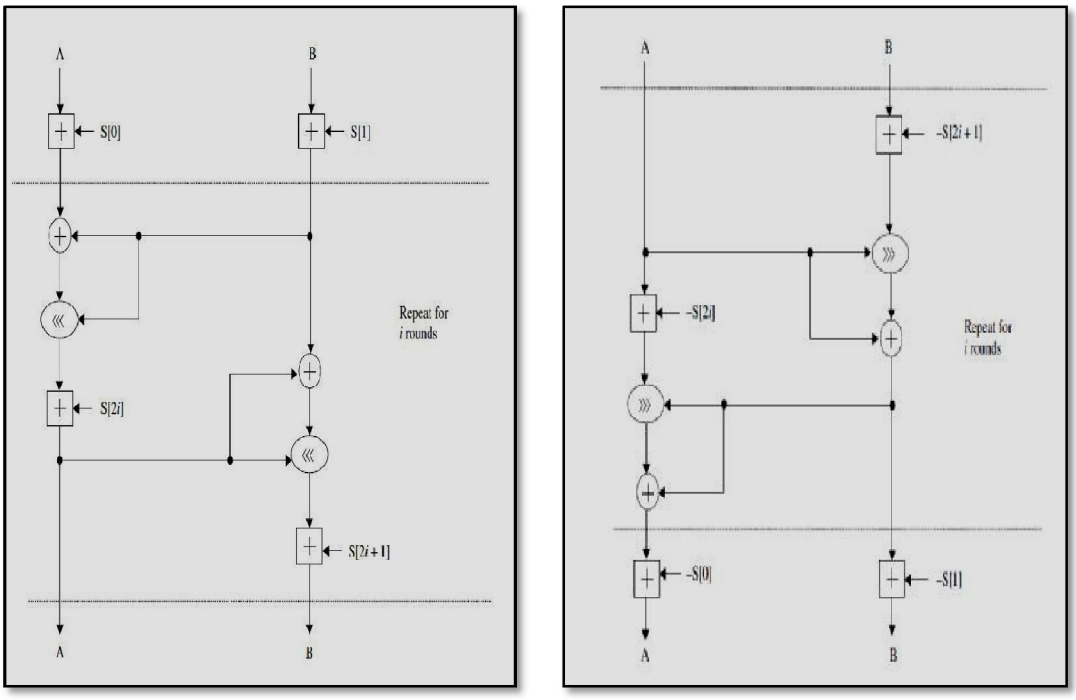


Figure1 RC5 Encryption and Decryption

4. Proposed Image Encryption System

The original image is divided into 4 × 8 pixels blocks, which are rearranged into a permuted image using a permutation process of previous RC5 in quadrate design. A block diagram of the proposed system is shown Figure (2):

4.1 The Quadrate RC5 algorithm

RC5 Quadrate design is 256-bit RC6-like block cipher. The plaintext is 256 bit which is divided into four parts p1, p2, p3 and p4 each of which is 64 bit. The F-function in modified RC5 has used quadrate design instead of rounds as it is shown in Figure (3). The output is 256 bit c1, c2, c3 and c4. Where each of is 64bit

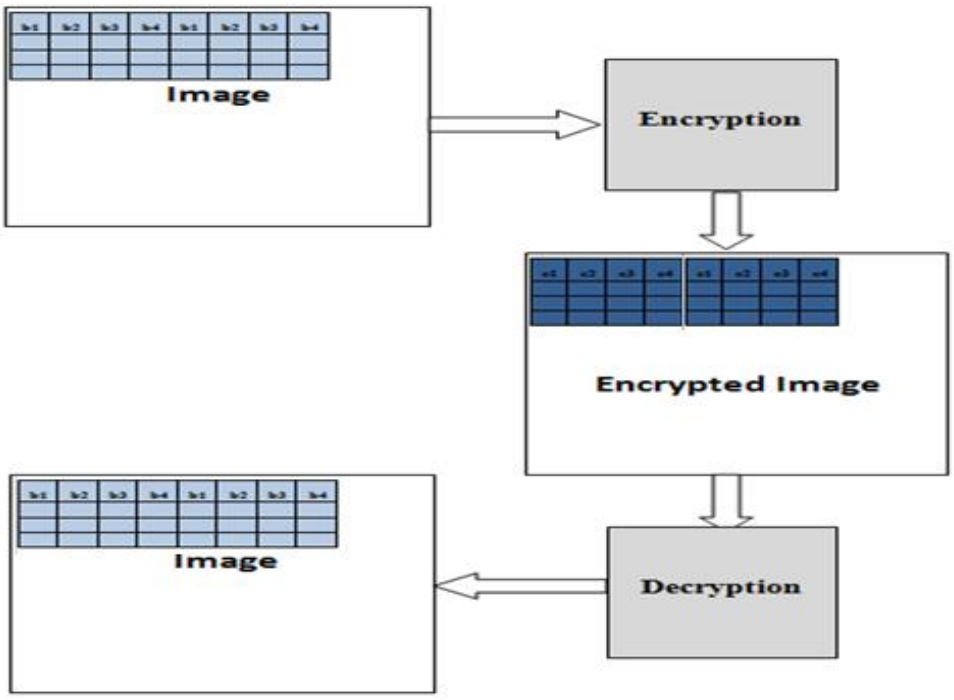


Figure 2 Block Diagram of proposed Algorithm

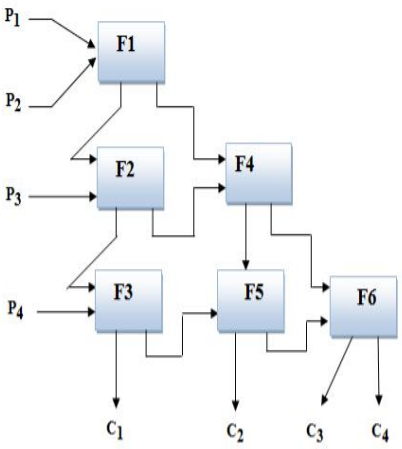


Figure3 Proposed Quadrate Function

4.2 F-function of Proposed Algorithm:

The function, F of proposed algorithm uses two rounds of pervious RC5 algorithm in a Feistel network. The input of each function is two plaintexts of 64 bits and four sub key Si, Si+1, Si+2, and Si+3 as shown in Figure (4). The Feistel network consists of dividing the input into two halves, and applying a non-linear function only to the right half. The result is added into the left half and subsequently left and right half are swapped. Ciphers following this approach are called Feistel ciphers. The output of one nonlinear function is input directly to the next one, which increases the propagation of local changes. The non-linear function of proposed algorithm is the pervious RC5 algorithm.

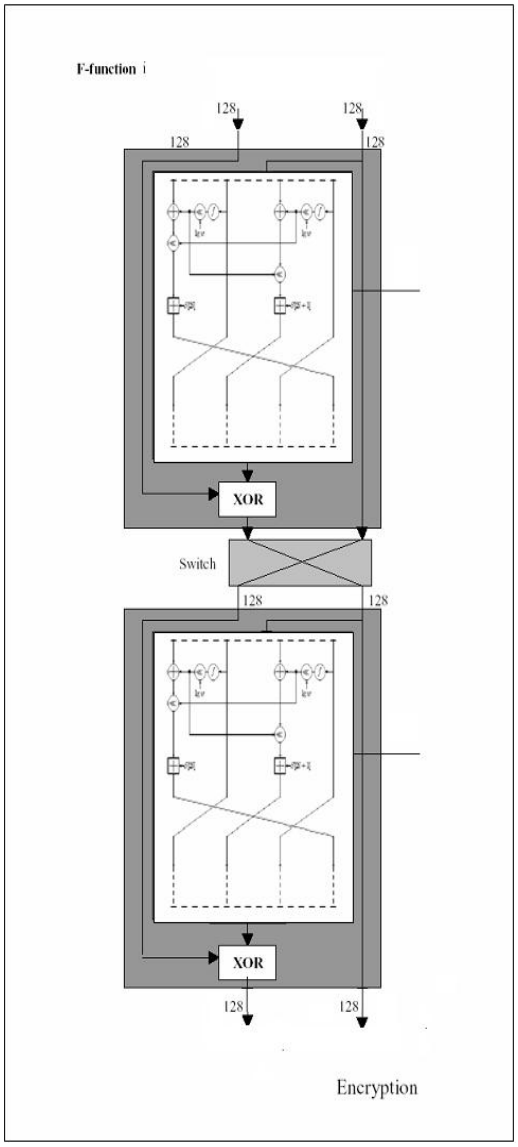


Figure 4 The F-function Proposed Algorithm

5. Statistical Security Analysis

In this section, we present the tests that were conducted to assess the efficiency and security of the proposed image encryption algorithm. These tests involve visual testing. For visual testing, four color images of size 300 × 300 pixels were used. Figure (5) depicts these test images-A, Duck, Nike, Lena and Baboon, as well as the images encrypted using the proposed RC5 quadrate design and previous RC5 encryption algorithm. From this figure, one can see that there is no perceptual similarity between original images and their encrypted counterparts with proposed algorithm while with previous RC5 encryption algorithm still some information can be inferred from the cipher image so as draw a conclusion about the appearance of the original image. The encrypted image should greatly differ from its original form. In general, two different measurements are used to quantify this requirement. The first measurement is the number Correlation Coefficient and the second is Entropy measurement.

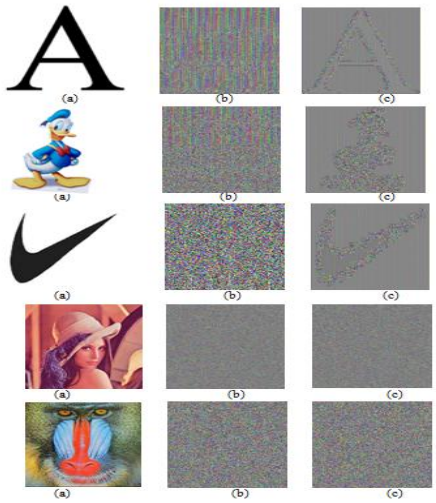


Figure 5 (a) Original image. (b) Encrypted image with proposed algorithm. (c) Encrypted image with RC5 algorithm.

5.1. The Correlation Coefficient Measuring Factor

Correlation is a measure of the relationship between two variables. If the two variables are the image and its encryption, then they are in perfect correlation (i.e. the correlation coefficient equals one) if they are highly dependent (identical). In this case the encrypted

image is the same as the original image and the encryption process failed in hiding the details of the original image. If the correlation coefficient equals zero, then the original image and its encryption are totally different, i.e., the encrypted image has no features and highly independent on the original image. If the correlation coefficient (C.C) equals -1, this means the encrypted image is the negative of the original image. So, success of the encryption process means smaller values of the C.C. The C.C is measured by the following equation:

$$The\_Correlation\_Coefficient = \frac{cov(x,y)}{\sigma_x \sigma_y} = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}(x_i - E(x))^2}\sqrt{\sum_{i=1}^{N}(y_i - E(y))^2}}, \quad \text{.....(1)}$$

where $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$, and x and y are gray-scale pixel values of the original and encrypted images. Measuring the C.C is done through running the C.C built in function in the used MATLAB 6.0 software (Corr2).

An extensive study of the correlation between pairs of plain image and their corresponding cipher image produced using the proposed encryption scheme by computing correlation coefficient (CR) between RGB components of the plain images and corresponding cipher images have been done. Results for a few images are shown in Table 3. Since the correlation coefficients shown in the Table 1 are very small (C»0), it indicates that the plain images and their corresponding cipher images are completely independent of each other.

Table 1 CR between Original images and their corresponding Encrypted images with proposed Algorithm

Image	C_{RR}	C_{GG}	C_{BB}
A	-0.0188	-0.0024	0.0061
Duck	0.0061	-0.0041	0.0044
Nike	0.0031	-0.0017	0.0051
Lena	3.4122e-004	0.0025	-0.0020
Baboon	-0.0040	-0.0042	-0.0045

5.2 Entropy

It is well known that entropy measures the uncertainty association with random variable. A secure cryptosystem should fulfil a condition on the information entropy that is the ciphered image should not provide any information about the plain image. The information entropy is calculated using equation (2) [10].

$$He = -\sum_{K=0}^{G-1} P(K) \log 2(P(K)) \quad \text{..... (2)}$$

Where:
He: entropy.
G: gray value of input image (0.. 255).
P(K): is the probability of the occurrence of symbol *K*.

Table 1 shows the entropy of image, entropy of encrypted image with proposed algorithm and entropy of encrypted image with RC5 algorithm.

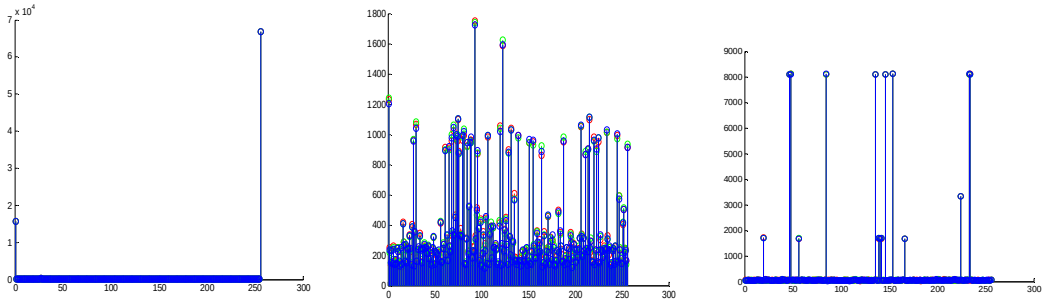
Table 2 Entropy for different images

Images	Plain Image	Cipher Image with proposed algorithm	Cipher Image with RC5
A	1.6501	7.3736	4.7337
Duck	3.5675	7.8647	5.7243
Nike	1.2321	7.8647	4.4549
Lena	7.7431	7.8647	7.9921
Baboon	7.7533	7.9916	7.9914

5.3 Histogram analysis

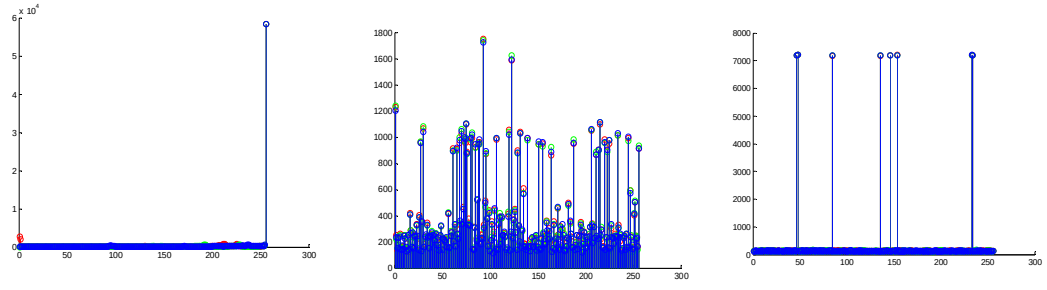
In an image, neighboring pixels will be having statistical similarity with respect to color and intensity levels. A good encryption strategy should lead to secure encrypted image. Image histograms help in understanding the similarity measure among the pixels. If there is no or negligible similarity among the pixels then cipher image is secured from adversary attacks. Figure (6) represents the histograms of the original and the encrypted images. One can see those histograms of the encrypted images are almost uniform and are significantly different from that of the four original images. Therefore, the proposed image encryption algorithm responds well to the diffusion properties: it does not provide information that can be exploited for attacks based on statistical analysis of the encrypted image. It is clear from the histogram plot shown in figure (6) that adversary may infer least information from the ciphered image as neighboring images are least related one another. Thus the proposed that can be performed on encryption strategy avoids any statistical attacks encrypted image.

A Image



(a) (b) (c)

Duck Image



(a) (b) (c)

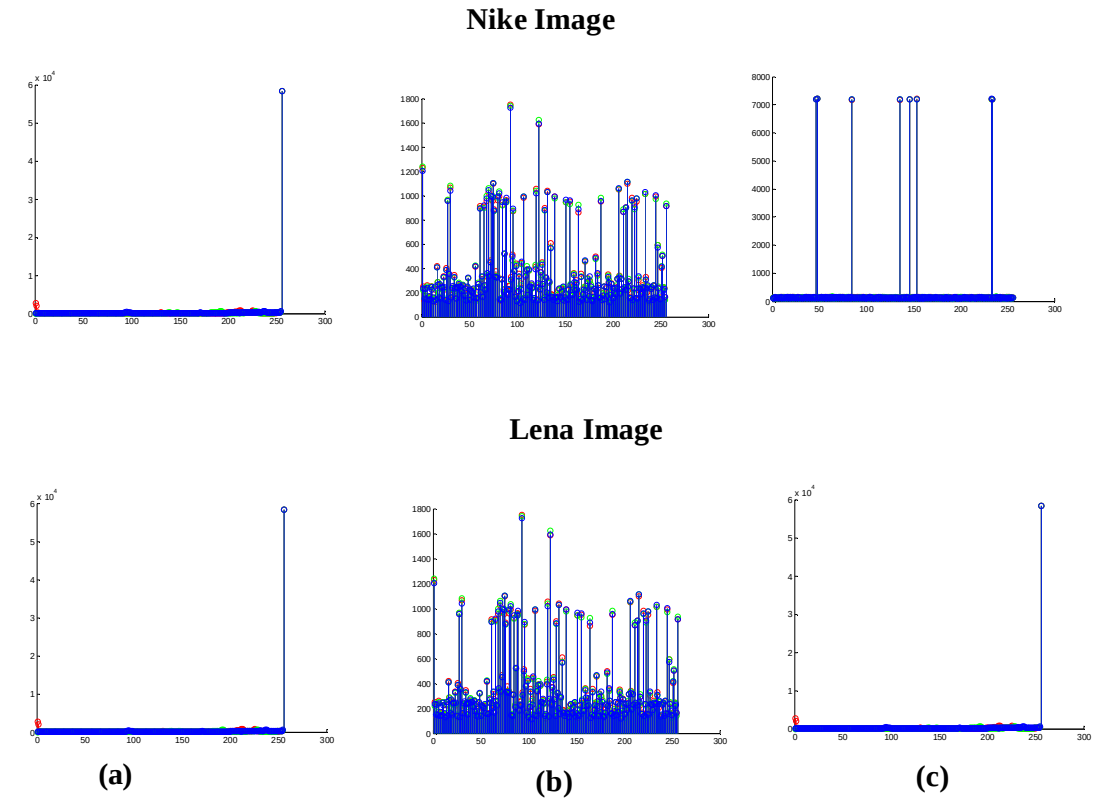


Figure 6 (a) Histogram of Original.
(b) Histogram of Encrypted images with Proposed Algorithm.
(c) Histogram of Encrypted images with RC5 Algorithm.

6. Speed performance

Apart from the security consideration, encryption/decryption rate of the algorithm is also an important aspect for a good image cipher. Time taken by the proposed cipher to encrypt/decrypt various with different sized color images has been measured. The results are summarized in Table 3.

Table 3 Encryption Time Using RC5 before and after Modification for different image sizes

Image	Size	Time in Sec. using Modified RC5	Time in Sec. using Previous RC5
A	300×300	0.015	0.093
Duck	600×600	0.047	0.374
Nike	520×520	0.031	0.249
Lena	900×900	0.140	1.138
Baboon	1200×600	0.110	1.010

7. Conclusion

In this paper an image encryption and decryption strategy based on RC5 algorithm is proposed. The proposed system is a fast and secure symmetric-key block cipher with a quadrate structure. It offers much improved security/ performance over existing ciphers by taking advantage of the powerful operations supported in today's computers. As a result, the modified RC5 algorithm showed that, by using the correlation, entropy, and histogram as a measurement of security, This technique enhances the security level of the encrypted images by reducing the correlation among image elements, which increasing its entropy value by decreasing the mutual information among the encrypted image variable. It is concluded that the proposed image encryption technique is perfectly suitable for the secure image storing and transmission.

Reference

[1] Rajinder Kaurand Er.Kanwalprit Singh, "Image Encryption Techniques:A Selected Review", IOSR Journal of Computer Engineering Vol. 9, No. 6, pp. 80-83, 2013.

[2] H. Yu, Z. Zhu "An Efficient Encryption Algorithm Based on Image Reconstruction" 2009 International Workshop on Chaos-Fractals Theories and Applications.

[3] Z.Yun-peng , Z. Zheng-jun " Digital Image Encryption Algorithm Based on Chaos and Improved DES "Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics San Antonio, TX, USA - October 2009.

[4] S.H. Kamali, R. Shakerian "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption" 2010 International Conference on Electronics and Information Engineering (ICEIE 2010).

[5] Paul A.J P. M. K. Paulose Jacob "Matrix based Cryptographic Procedure for Efficient Image Encryption" 978-1-4244-9477-4/11 ©2011 IEEE.

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

[7] Nithin N, Anupkumar M Bongale, G. P. Hegde, "Image Encryption based on FEAL algorithm", International Journal of Advances in Computer Science and Technology, Vol. 2, No.3, 2013.

[8] Narendra K. Paree, Vinod Patida and Krishan K. Sud, "**Diffusion-substitution based gray image encryption scheme**", Journal of Digital Signal Processing, Vol. 23 No.3, pp. 894-901, 2013.

[9] Man Young Rhee "Internet Security Cryptographic, principles, algorithms and protocols",John Wiley & Sons Ltd, Englang,2003.

[10] M. Sonka, V. Hlavac. and R. Boyle, "Digital image processing," in: image Processing, Analysis, and Machine Vision, 2nd ed, 1998. http://www.pws.com