Digital Image Confidentiality Depends upon Arnold Transformation and RC4 Algorithms

Khalid Hamdnaalla[1,2], Abubaker Wahaballa[1, 3], Osman Wahballa[1,2]
University of Electronic Science and Technology of China[1], Karay University[2] , National Council of Technical and Technological Education, Mihareeba Technical College[3]

mahs135@yahoo.com , wahaballah@hotmail.com , wahballa_77@hotmail.com

***Abstract*— with the development of digital image production and applications, digital image security has become very important in today's world. This paper proposes image confidentiality relying on one spatial domain transformation (Arnold transformation) and one stream cipher algorithm (RC4). The paper has three phases; the first phase is the design and implementation of digital image scrambling using Arnold transformation based on best iteration. The second phase is the design and implementation of digital image encryption using RC4 stream cipher and the third phase makes use of both Arnold transform and RC4 algorithm based on best iteration which applies Arnold transform to scramble a digital image and then encrypt it using RC4. The input key to RC4 is generated using Blum Blum Shub (BBS) pseudo random bit generator algorithm. All phases are implemented using Matlab. Each phase is followed by some security evaluations. The security evaluations are presented by calculating a correlation coefficient and a security quality factor. The results show that for the same digital gray image, a correlation coefficient produced by Arnold transform based on best iteration is better than that produced by RC4; however an Arnold transform based on best iteration has a security quality factor of zero. Applying Arnold transform in scrambling before encrypting using RC4 gives a correlation coefficient as well as the Arnold transform in addition to the security quality factor better than encryption using RC4.**

***Index Term*— algorithm, Arnold transformation, BBS, confidential, digital image, encryption, RC4 stream cipher and scrambling.**

I. INTRODUCTION

Computer security related to system and network security has been widely studied. With the development of multimedia processing and applications, several types of media security have been taken in consideration. **The digital media include**: digital images, digital audio, digital video and Computer documents (texts, web pages, computer graphics, etc.).

Media security defined as: one of the information security family which includes the following research areas [2]: Stenography, watermarking digital scrambling and video surveillance.

A. Digital image

The digital image composed of many image points. This image points also namely pixels, are of spatial coordinates that indicate the position in the image, and intensity (gray level value) [12]. An image as described above, refers to a grayscale image (2 D image).

A colored image accompanies high dimension information than gray image (3D, 4D), as red, green and blue values are typically used in different combination (color systems) to reproduce the colors of an image in the real world. An image defines as two dimensional function $f(x, y)$, where x and y are coordinates and f is amplitude, or gray level value at the point(x, y). When x, y and f are all discrete finite values, we call the image a digital image.

B. Digital scrambling

Scrambling a digital signal in the spatial or the frequency domain corresponds to modify that signal in such a way that the original semantic media loses it's meaning and become hard to be viewed (the inverse of scrambling is descrambling).

C. Digital image scramble

Refer to transforming the digital image into another completely different digital image. The users only know the algorithm and keys; this allows them to restore the original image [2].

Also image scrambling can be seen as encryption. The plain text is the original image and the cipher text is meaningless noises for unauthorized users.

Some digital positions scrambling methods "according to pixel positions" are:

Chessboard based scrambling.

1) Digital image based on Hilbert space-filling curve.
2) Caesar/ affine based coding scrambling
3) Digital image scrambling based on Arnold transformation.
4) DES based scrambling
5) Digital image scrambling based on the magic square matrix.
6) Digital image scrambling based on gray code transformation.

D. The cryptography

The area of study of encryption constitutes is known as cryptography. In the other words, the cryptography is the area of study the encryption schemes (crypto-systems or enciphers). The crypto-systems are characterized alone three independent dimensions [1], these dimensions are:

1) The operation will be used to convert the plain text to cipher text (substitution cipher, transposition cipher and product cipher)
2) The number of the keys will be used (symmetric cipher and asymmetric cipher)

3) The way which the plain text process (block cipher and stream cipher)

E. Symmetric cipher

A symmetric cipher is a form of the crypto system in which encryption and decryption processes are performed using the same key. It is also called a single key encryption [3].

F. Stream cipher

A stream cipher is cryptography approach which encrypted a digital data one bit or one byte at the time. With optimum design of pseudo number generator a stream cipher can be secured as the block cipher of comparable key length. A main advantages of stream cipher "that don't use block ciphers as building block" are typically faster and they use far less code than does block cipher.

Our paper is aiming to provide the confidentiality for the most important digital media "digital images" using one of digital scrambling techniques to break the digital image semantic and provide the kind of confidentiality, mixed with one stream cipher algorithms to ensure the confidentiality. On the other hand we can say that, the paper is combining the two operations, which convert the plain text "original image" to cipher text "encrypted\scrambled image". These operations are substitution which presented by RC4, and transposition technique which presented by Arnold transformation. As we know the information security is a wide field, which has several purposes to be achieved. The **confidentiality** is one of information security concepts, which provides a protection against the passive attacks [3].

II. Motivation and Objectives

The confidentiality can be applied in several ways. The paper is seeding to provide the confidential for digital image, which makes uses for Arnold transformation and RC4 stream cipher. The main function of the Arnold transformation is breaking the image semantic, which become unintelligible "provide the confidentiality as permutation cipher". The purpose of the RC4 stream cipher is to achieve the confidentiality as substitution cipher. Although the RC4 algorithms have several weaknesses, but still many applications make use for it, especially the applications need fast encryption schemes. On the other hand adding Arnold transformation to the RC4 cipher will improve the security performance of the combination. The paper suggests a new form of Arnold transformation, which based on best iteration. Besides Arnold transformation and RC4 stream cipher based on best iteration. This work is a new idea, which no one before was combining the RC4 algorithm and Arnold transformation for digital image confidentiality and evaluate the performance.

III. Literature Survey

The previous researches [13,14] suggest and propose combine digital images scrambling with one of cryptography algorithms. The following are some remarks.

A. *Image Scrambling Based on Chaos Theory and Vigenere [13], the weakness of this method is that, this algorithm is a Vigenere cipher with key length equal N which is the total numbers of image pixels. In other words, the key is a permutation of the sequence from 0 to N, which means the key space is N!. Nowadays, with existing of high performance software and hardware, it's easy to apply brute force attack.*

B. *Image scrambling algorithm using parameter based on M sequence [14]. from this technique we observe the following:*

1) If one of the parameters was missing-chosen, then one or both of the coefficient matrices may not be invertible.

2) If brute force attack is applied to one of the coefficient matrices, then a good recognition of an image is achieved. That makes it easier to get the other matrix.

IV. Design Tools

This section provides explanations for each algorithm or technique will be used.

A. Arnold transformation

We can define Arnold transformation as follows. Let (x, y) is pointing in the unit square. Its move to (x', y') by the following equation.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 11 \\ 12 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} mod\ l \quad (1)$$

L is length of the unit square. This transformation called 2-D Arnold transformation. For digital image we can define Arnold transformation as follows. Let (i, j) be pixel for square digital image $I = [I_{i,j}]_{NXN}$ its move to another pixel using the following transform [4].

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{bmatrix} 11 \\ 12 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} mod\ N \quad (2)$$

Arnold transformation is a periodic and invertible mapping. Besides, the Arnold transformation is valid for square images only. The Arnold transformation is used to scramble the digital images and has many applications, especially in digital watermarking [2]. Many papers estimate the Arnold transformation period as $< N^2$ .But one paper gives a linear approximation for an Arnold period as the following equation(3) as in [4].

$$\hat{T} = 1.4938N + 40.8689 \quad 2 \le N \le 2000 \quad (3)$$

B. RC4 stream cipher algorithm

The RC4 was designed by Ron Rivest of RSA Security in 1987. The RC4 is an abbreviation of "Rivest Cipher 4" or "Ron's Code 4"[6]. RC4 is variable key length stream cipher algorithm. The output of RC4 is one byte at a time which will use with "xor" operation to encrypt the stream of the plain

text. The decryption operation just inverse of the encryption operation implies it uses the same key stream "or" with the cipher text stream. RC4 stream cipher algorithm can be divided into [5]:

1) KSA (key scheduling algorithm)

The key-scheduling algorithm is used to initialize the permutation in the array "S". Key length is defined as the number of bytes in the key and can be in the following range 1 B≤ key length ≤ 256B. First, the array "S" is initialized to the identity permutation and then processed for 256 iterations which will mix with the key. An "algorithm1" shows the KSA procedures.

Algorithm 1: KSA Algorithm

$for\ i\ from\ 0\ to\ 255$
$S[i] := i$
$endfor$
$j := 0$
$for\ i\ from\ 0\ to\ 255$
$j := (j + S[i] + key[i\ mod\ keylength])\ mod\ 256$
$swap\ values\ of\ S[i]\ and\ S[j]$
$endfor$

2) Pseudo random generator algorithm(PRGA)

For as many iterations as are needed (in our case the number of total pixels), the PRGA modifies the state and outputs a byte of the key stream. For alliterations, the PRGA increments i , looks to the ith element of S $\left(S[i]\right)$, and adds that to j. Then swap $S[i]$ and $S[j]$. then uses the sum $S[i] + S[j]$ (modulo 256) as an index to bring a third element of S, which will *xor* it with the next byte of the message to produce the next byte of either cipher text or plaintext. Each element of S is swapped with another element at least one time each "256" iterations. An "algorithm2" shows the steps of PRGA.

Algorithm 2: PRGA Algorithm

$i := 0$
$j := 0$
$while\ GeneratingOutput:$
$i := (i + 1)\ mod\ 256$
$j := (j + S[i])\ mod\ 256$
$swap\ values\ of\ S[i]\ and\ S[j]$
$K := S[(S[i] + S[j])\ mod\ 256]$
$output\ K$
$endwhile$

C. BBS algorithm (Blum Blum Shub)

BBS is cryptographically secure pseudo random bit generator (GSPRBG). The pseudo random bit generator is "GSPRBG" if and only if can pass the next bit test. In other words, if there is no polynomial time algorithm that, by known first k bit of output sequence can estimate k+1 bit by probability significantly greater than 0.5 [1].

The procedures of BBS are as follows. First choose two big prime numbers p and q which satisfy the following condition. $pmod4 = 3, qmod4 = 3$, then get the compost number n which $n = pxq$ then selecting seed number which satisfies the following condition $\gcd(s, n) = 1$ in other words s and n are relative prime. The following is the algorithm steps.

Algorithm 3: Blum Blum Shub pseudo random bit generator algorithm

$x_0 = s^2 mod\ n$
$for\ i = 1\ to\ le\ ngth\_wanted$
$x_i = {x_{i-1}}^2 mod\ n$
$b_i = x_i mod\ n$
$endfor$

V. EVALUATION TOOLS

A. Correlation coefficient

In general, for two random variables X and Y the correlation coefficient is given by the following equation(4) as in [7].

$$\sigma = \frac{cov(X,Y)}{\sqrt{var(X).var(Y)}} \tag{4}$$

σ is the correlation coefficient for X and Y, where cov and var are vthe varianceand covariance respectively.

$$cov(X,Y) = E\left(\left(X - E(X)\right)\left(Y - E(Y)\right)\right) \tag{5}$$

E is statistical expectation.

$$var(X) = E^2(X) - E\left(X^2\right) \tag{6}$$

In our case we consider each of an original image and scrambled (encrypted) image as discrete random variables. So one has to give a definition of the correlation coefficient for discrete random variables [8,9] as follow:

$$\sigma = \frac{cov(I, I')}{\sqrt{var(I).var(I')}} \tag{7}$$

Where *I* is original image and I' is scrambled (encrypt).

$$cov\left(I, I'\right) = \sum_{i,j}^{M,N}\left(I(i,j) - E(I)\right) \times \left(I'(i,j) - E\left(I'\right)\right) \tag{8}$$

$I(i,j)$ Is the intensity of the pixel in ith row and jth column respectively. N and M are total the numbers of pixel in each column and row respectively. The multiply of N and M called image resolution [9].

$$E(I) = \frac{1}{M \times N}\sum_{i,j}^{M,N} I(i,j) \tag{9}$$

The correlation coefficient between any two random variables is a statistical measurement for how much these two random variables are similar. In our case if the correlation coefficient is equal one that's means an original image and scrambled\encrypted image are the same. In other side if the correlation coefficient is equal to zero, that means the original image and scrambled\encrypted image are totally different.

Else if the correlation coefficient between the original digital image and scrambled/encrypted image is equal minus one that's mean the two images are negative to each other [8].

B. Security quality factor

The paper uses the average difference between the gray level digital image histogram and it is scrambled\encrypted histogram as security quality factor [10,11]. The encryption quality factor represents the average number of changes to each gray level.

$$SQ = \frac{\sum_{i=0}^{255} h(i) - h'(i)}{256}, \quad (10)$$

h Is the original image histogram and h' is scrambled/encrypted image histogram.

To make it clear must define what an image histogram is. The gray level digital image histogram is the intensity distribution in the gray level digital image [12], mathematically define as:

A histogram of digital images with gray level in the range $[0, L-1]$ is a discrete function given by the equation (11).

$$h(r_i) = n_i, \quad (11)$$

Where r_i is ith gray level and n_i is the number of pixels in the image has r_i gray level.

Large security quality factor means more difference between an original image and scrambled image histograms. In other works the intensity distribution of the two images (original, scrambled) is more different when the security quality is large.

C. Average execution time

This metric absolutely depends on the working environment, this environment is present by the computer itself "hardware". Besides, the platform" the operation system (OS)", in additional to the software was used in the simulation and digital image size. The paper calculates the average execution time for thousand iterations of each technique we will describe later.

VI. Design and Implementation Procedures

This section discusses design and implementation of digital image scrambling and descrambling (digital image encryption and decryption), which the design tools mentioned previously will be used. There are three independent phases, which they are showing the designs and implementation procedures. Follow each phase security and performance evaluations, which make use of the evaluation tools were introduced before. All the simulations was done using Matlab.

Definition1: **the best iteration**: as mentioned before Arnold transformation is periodic. The best iteration is an iteration which gives a minimum correlation coefficient between the original image and it's scrambled/encrypted within the Arnold transformation period.

A. Phase 1: image scrambling/descrambling using Arnold transformation based on best iteration.

The procedures of a digital image scrambling using Arnold transformation based on best iteration are:

1) Calculate Arnold transform period for digital image using an equation(3) .
2) Scramble a digital image using alliteration within the period
3) Calculate the correlation coefficient between the original digital image and its scrambled using equation (7).
4) Get the best scrambling iteration, which has a minimum correlation coefficient
5) Construct the scrambled digital image according to the best iteration.

The descrambling process is applying Arnold transformation to the scrambled digital image, which uses the best iteration as descrambling key.

The algorithm 4 shows Arnold transformation based on best iteration technique in algorithmic form.

Algorithm 4: Arnold transformation based on best iteration algorithm

$t = 0, T = ceil(T_{Arnold}), c[T], \quad I_{scram} = I$
$while(t < T)$
  $for\ i\ form\ 0\ to\ N-1$
  $for\ j\ form\ 0\ to\ N-1$
$I_{scram}(i,j) = I_{scram}[i + jmodN, i + 2jmodN]$
  $end\ for$
  $end\ for$
  $c[t] = \sigma(I_{scram}, I)$
  $t = t + 1$
 $end\ while$
  $c = abs(c)$
  $for\ j\ from\ 0\ to\ T-1$
  $count = 0$
  $for\ i\ from\ 0\ to\ T-1$
 $if[c[j] < c[i])$
  $count = count + 1$
 $else$
 $count = count$
$end\ if$
$end\ for$
$if(count == T-1)$
$break$
$iteration_{best} = j$
$end\ if$
$end\ for$

B. Phase 2: digital image encryption/decryption using RC4 stream cipher

The following procedures show a digital image encryption using RC4 stream cipher:

1) Implement BBS.
2) Implement RC4 stream cipher.
3) Get the output of BBS into the RC4 input (512 bit key).
4) Change a digital image to binary stream.
5) Encrypted an image binary stream using RC4 key stream (byte each time).
6) Construct an encrypted image.

The decryption process is as same as the encryption process; the only difference is it will be applied to the encrypted digital image instead of the original digital image.

C. Phase 3: digital image security relying on Arnold transformation and RC4 stream cipher.

This phase makes use for both Arnold transformation and RC4 stream cipher algorithm, to scramble and then encrypt the digital image.

The following steps show the design and implementation procedures.

1) Calculate Arnold transform period of the input digital image, using equation (3).
2) Scramble a digital image using alliteration within the Arnold transformation period, then encrypt each iteration output using the RC4 key stream.
3) Calculate the correlation coefficient between original image and encrypted image each time using equation (7).
4) Get the best iteration depend on the absolute minimum correlation coefficient.
5) Depends on the best iteration construct a secure digital image.

The algorithm 5 shows the digital image security relying on both Arnold transformation and RC4 encryption scheme.

Algorithm 5: digital image security relying on Arnold transformation and RC4 stream cipher

$$t = 0, T = ceil(T_{Arnold}), \quad c[T],$$
$$while(t < T)$$
$$I_{scram} = I$$
$$for\ k\ from\ 0\ to\ t$$
$$for\ i\ form\ 0\ to\ N-1$$
$$for\ j\ form\ 0\ to\ N-1$$
$$I_{scram}(i,j) = I_{scram}[i + jmodN, i + 2jmodN]$$
$$end\ for$$
$$end\ for$$
$$end\ for$$
$$I_{sram} = E_{RC}(I_{sram})$$
$$c[t] = \sigma(I_{scram}, I)$$
$$t = t + 1$$
$$end\ while$$
$$c = abs(c)$$
$$for\ j\ from\ 0\ to\ T-1$$
$$count = 0$$
$$for\ i\ from\ 0\ to\ T-1$$
$$if[c[j] < c[i])$$
$$count = count + 1$$
$$else$$
$$count = count$$
$$end\ if$$
$$end\ for$$
$$if(count == T-1)$$
$$break$$
$$iteration_{best} = j$$
$$end\ if$$
$$end\ for$$

VII. RESULTS AND DISCUSSION

A. General

In order to compare and evaluate the three phases" which each phase consider as independent image security technique", the same digital gray level images will be used. The table I shows these images.

Table I
all images used in this paper

Image name	Image format	Image size(KB)	pixels
Lena	JPEG	8.15	225x225
Beauty	JPEG	4.22	153x153
Beijing	JPEG	5.23	183x183

B. Phase 1 results and discussions

This section shows the results of applying Arnold transformation based on best iteration on the digital gray images in table I.

1) The following images and figures shows the results of applying Arnold transformation based on best iteration for Lena image.

Image 1: Lena original image.

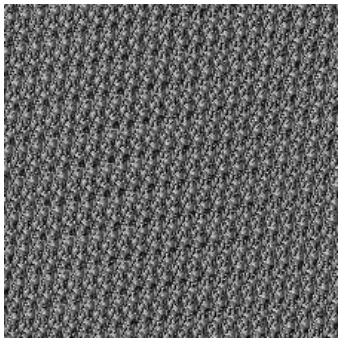

Image 2: Lena scrambled image.

Image 3: Lena descrambled image

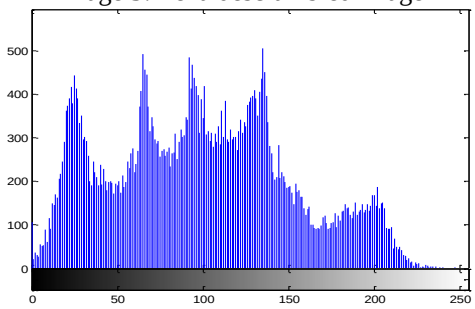

Fig. 1. Lena original image histogram

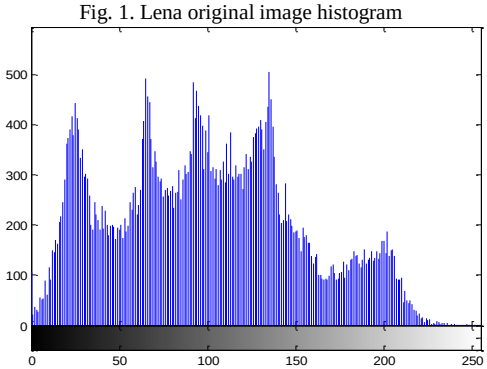

Fig. 2. Lean scrambled image histogram.

2) The following images and figures shows the results of applying Arnold transformation based on best iteration on beauty image.

Image 4: Beauty original image

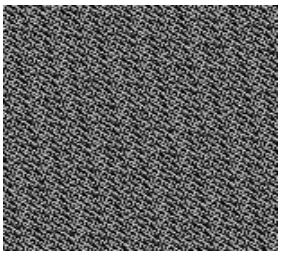

Image 5: Beauty scrambled image

Image 6: beauty descrambling image

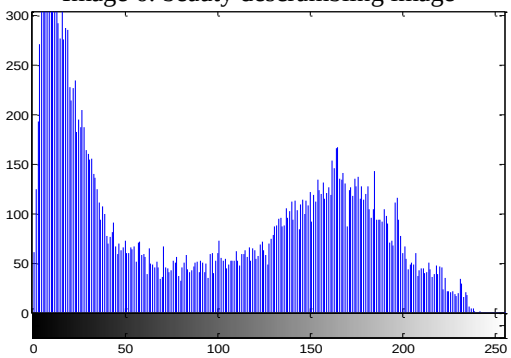

Fig. 3. beauty original image histogram

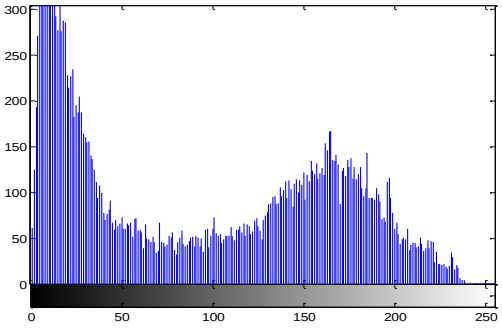

Fig. 4. beauty scrambled image histogram.

3) The following images and figures shows the results of applying Arnold transformation based on best iteration on Beijing image.

Image 7: Beijing original image

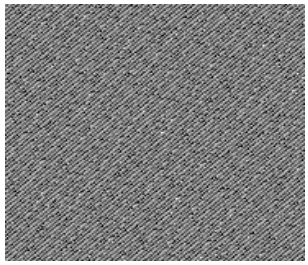

Image 8: Beijing scrambled image

Image 9: Beijing descrambled image.

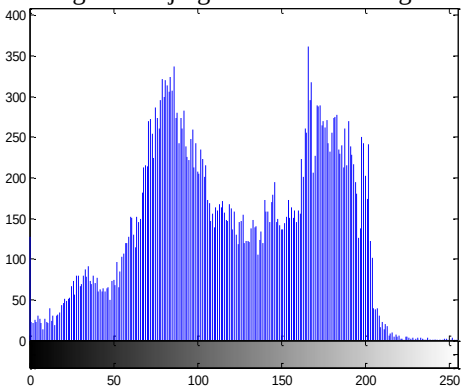

Fig. 5. Beijing original image histogram.

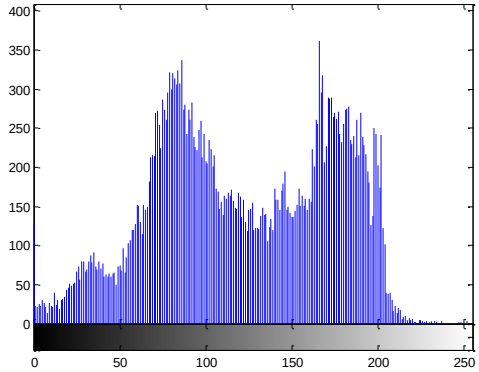

Fig. 6. Beijing scrambled image histogram.

4) Discussion

From the previous results, clearly the Arnold transformation based on best iteration doesn't affect an intensity distribution, implies a scrambled image histogram remain as same as an original image histogram. In other words, every gray level has a same number of pixels in both an original image and it's scrambling. Table II shows the absolute minimum correlation coefficients, security quality factors, the average execution times of the images on table I, when Arnold transformation based on best iteration will be applied.

Table I
Arnold transformation based on best iteration evaluation results

Image name	Min correlation coefficient	Security quality	Best iteration
Lena	$3.8158e^{-006}$	0	248
Beijing	$1.6022e^{-004}$	0	33
Beauty	$9.5859e^{-006}$	0	13

From this table we observe that, the Arnold transformation based on best iteration has a security quality factor of zero. That means an Arnold transformation based on best iteration doesn't change an original image intensity distribution. Besides, Arnold transformation based on best iteration has very good correlation coefficient, which close to zero. That implies an original image and its scrambled are significant differences according to the pixel position.

C. Phase 2 results

This section shows the results of applying the RC4 stream cipher scheme on the digital gray images in table I.

1) The following images and figures show the encryption and decryption process of using RC4 to encrypt and decrypted Lena image.

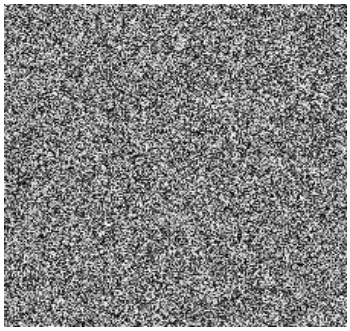

Image 4: Lena encrypted image using RC4 stream cipher.

Image 5: lean decrypted image using RC4 stream cipher

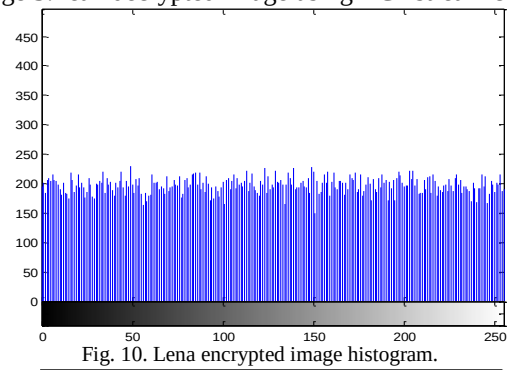

Fig. 10. Lena encrypted image histogram.

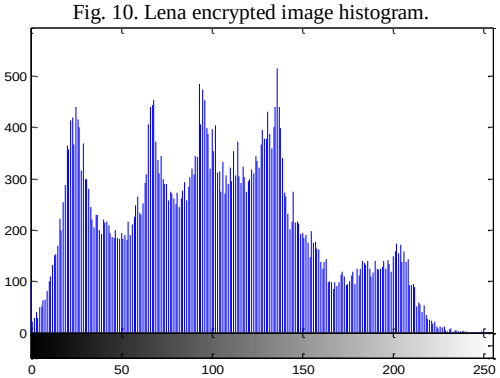

Fig. 11. Lena decrypted image histogram

2) The following images and figures show the encryption and decryption process of using RC4 to encrypt and decrypted beauty image.

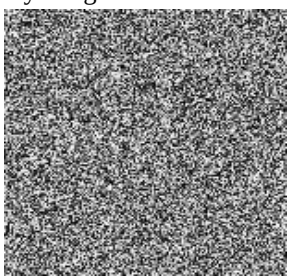

Image 6: beauty encrypted image using RC4 stream cipher

Image 7: beauty decrypted image using RC4 stream cipher

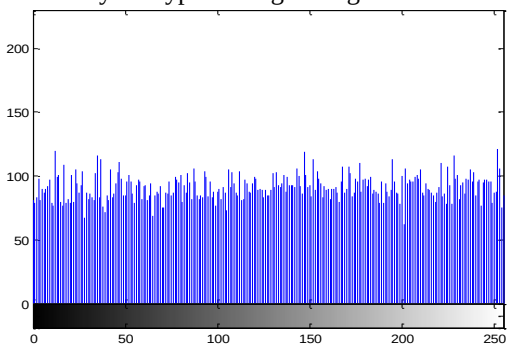

Fig. 12. beauty encrypted image histogram

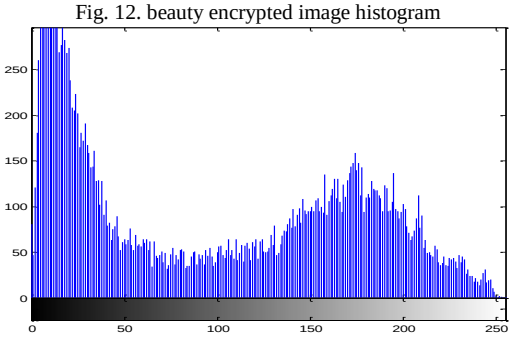

Fig. 13. beauty decrypted image histogram

3) The following images and figures show the encryption and decryption process of using RC4 to encrypted and decrypted Beijing image

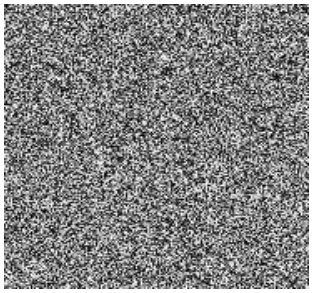

Image 8: Beijing encrypted image using RC4 stream cipher

Image 9: Beijing decrypted image using RC4 stream cipher

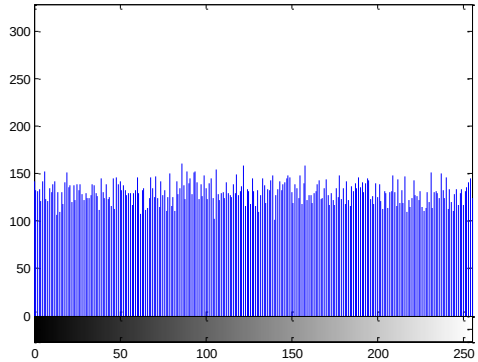

Fig. 14. Beijing encrypted image histogram

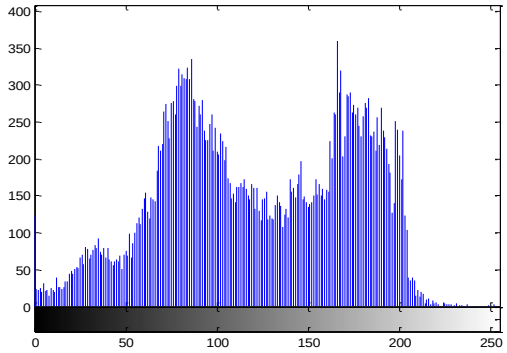

Fig. 15. Beijing decrypted image histogram

4) Discussion

The pervious results illustrate that, an encrypted image histograms have uniform distribution, that implies whatever the original image histogram is, the encrypted image will have uniform intensity distribution. That's given significant security quality factor.

Table III shows the correlation coefficients, the security quality factors, the average execution times of the images on table I, when RC4 stream cipher scheme will be applied.

Table III
RC4 image encryption technique

Image name	Correlation coefficient	Security quality
Lena	-.0019	112.9219
Beijing	-.0130	82.6953
Beauty	.0090	55.6563

Unlike Arnold transformation based on best iteration the RC4 stream cipher gives significant security quality factor. Beside, the good correlation coefficient but is not better than the Arnold transformation based on best iteration.

D. Phase 3 results

This section shows the results of applying image security relying on Arnold transformation and RC4 stream cipher based on best iteration. The following images and figures are showing the results on this technique on the images on table I.

1) The following images and histograms are showing the result of applying Arnold transformation and RC4 based on best iteration on lean image.

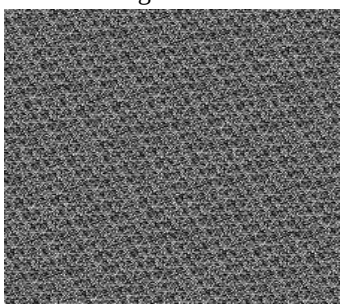

Image 10: Lena scrambled image using Arnold and RC4 based on best iteration

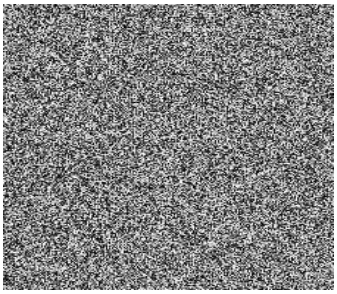

Image 11: Lena encrypted image using Arnold and RC4 based on best iteration

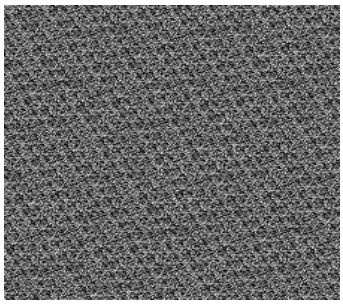

Image 12: Lena decrypted image using RC4

Image 13: Lena descrambled image using Arnold transformation

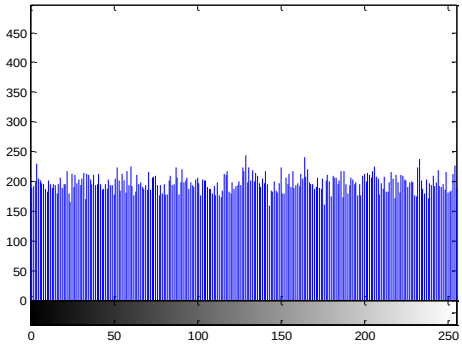

Fig. 16. Lena secure image histogram

2) The following images and histograms are showing the result of applying Arnold transformation and RC4 based on best iteration on beauty image.

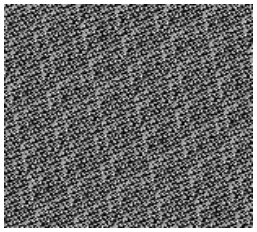

Image 13: beauty scrambled image using Arnold and RC4 based on best iteration

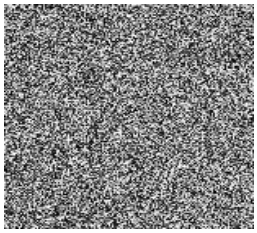

Image 14: beauty encrypted image using Arnold and RC4 based on best iteration

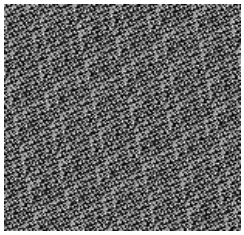

Image 15: beauty decrypted image using RC4

Image 16: beauty descrambled image

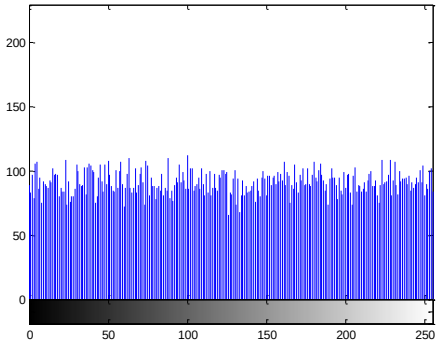

Fig. 17. beauty secure image histogram

3) The following images and histograms are showing the result of applying Arnold transformation and RC4 based on best iteration on Beijing image.

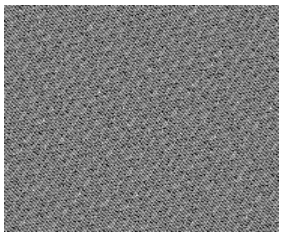

Image 17: Beijing scrambled image using Arnold and RC4 based on best iteration

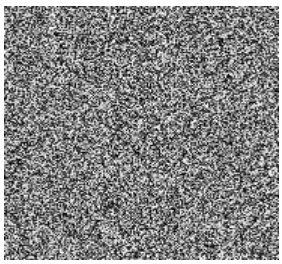

Image 18: Beijing encrypted image using Arnold and RC4 based on best iteration

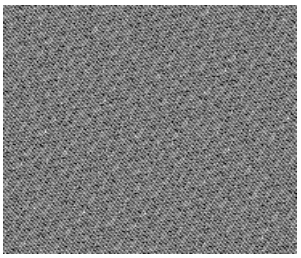

Image 19: Beijing decrypted image using RC4

Image 20: Beijing descrambled image using Arnold transformation

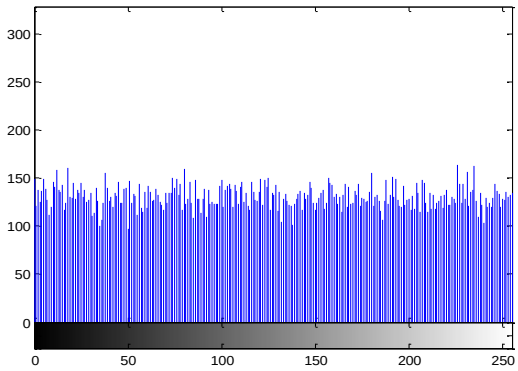

Fig. 18. Beijing secure image histogram

4) Table IV shows the correlation coefficient, the security quality factor, the average execution time of the images on the table I, when Arnold transformation and RC4 cipher based on best iteration will be applied.

Table IV
Arnold transformation and RC4 based on best iteration evaluation results

Image name	Min correlation coefficient	Security quality	Best iteration
Lena	$1.8307e^{-005}$	112.9844	171
Beijing	$5.7217e^{-005}$	84.2109	18
Beauty	$9.3014e^{-004}$	55.6797	26

From table IV we realize that, using Arnold transformation and RC4 stream cipher together is providing significant correlation coefficient as well as R4 stream cipher does. Besides, security quality factor as well as Arnold transformation based on best iteration.

VIII. Conclusion

According to the experimental results, we can conclude the following:

1) For both image scrambling using Arnold transformation based on best iteration and image encryption using RC4 stream cipher we got good correlation coefficient(close to zero), but the correlation coefficient of image scrambling using Arnold transform based on best iteration is better than the correlation coefficient of an image encryption using RC4. That implies an Arnold based on best iteration has a better pixel passion scrambling than encryption using RC4.
2) Arnold transform has security quality factor of zero. That means the intensity distribution remains same in scrambled images.
3) Image encryption using RC4 has a significant security quality factor which implies the intensity distributions for the original images and scrambled image are different. When we look at the encrypted image histogram we realize that they have a uniform distribution. This implies whatever an original image histogram is; the encrypted image has a uniform image histogram.
4) For Arnold transform and RC4 together the correlation coefficient is almost same as the correlation coefficient achieved by the Arnold transform. Besides, the security quality factor is better than either that of Arnold transformation or RC4.
5) Using Arnold transform to scramble digital images and then encrypt using RC4 improves the security performance of both Arnold transform and RC4.

References

[1] G William, Stallings. Cryptography and Network Security, 4/E. Pearson Education India, 2006.
[2] Yan, WeiQi, and Jonathan Weir. *Fundamentals of Media Security*. Bookboon, 2010.
[3] William, Stallings. "Network security essentials." (2003).
[4] Xiaoqiang Zhang, Guiliang Zhu, Weiping Wang, Mengmeng Wang and Shilong Ma" Period Law of Discrete Two-dimensional Arnold Transformation" 2010 Fifth International Conference on Frontier of Computer Science and Technology.
[5] Paul, Goutam, and Subhamoy Maitra. "RC4 state information at any stage reveals the secret key." *IACR Eprint Server, eprint. iacr. org* 2007/208 (2007): 16-17.
[6] http://en.wikipedia.org/wiki/RC4 accessed at 25 Jan 2013.
[7] Ross, Sheldon M. "Introduction to probability models". Academic press, 2006.
[8] Marwa Abd El-Wahed, Saleh Mesbah, and Amin Shoukry" Efficiency and Security of Some Image Encryption Algorithms" Proceedings of the World Congress on Engineering 2008 Vol I WCE 2008, July 2 - 4, 2008, London, U.K.
[9] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps", Chaos, Solitons and Fractals, vol. 21, pp. 749-761, 2004.
[10] H.E.H. Ahmed, H.M. Kalash2 and O.S. Farag Allah" Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images" Electrical Engineering, 2007. ICEE 07. International Conference on Date of Conference: 11-12 April 2007.
[11] H.H. Ahmed, H.M. Kalash, and O.S. Farag Allah, "Encryption Quality Analysis of RC5 Block Cipher Algorithm for Digital Images." Journal of Optical Engineering, vol. 45, 2006.

[12]] huiyu zhou, jaihua wu & jianguo zhang, “digital image processing part1”, ventus publishing aps from internet www.bookboon.com, accessed at 10.Dec.2012.
[13] Shanshan Li and Yinghai Zhao, “Image Scrambling Based on Chaos Theory and Vigen`ereCipher”, Computational Intelligence and Security (CIS), Seventh International Conference, 2011
[14] Zhou, Yicong, K. A. R. E. N. Panetta, and Sos Agaian. "An image scrambling algorithm using parameter bases M-sequences." Machine Learning and Cybernetics, 2008 International