IOSR Journal of Engineering (IOSRJEN)
e-ISSN: 2250-3021, **p**-ISSN: 2278-8719
Vol. 3, Issue 10 (October. 2013), ||V1|| PP 16-27

Design and implementation proposed system for encryption true images

Asst. Prof. Dr.Baheja K.Shukur[1], Ala aldeen abbas Abdulhassan
[1, 2] Computer Technology /network department, Babylon University, Iraq

Abstract: - Image encryption method prepared information unreadable. Therefore, no hacker or eavesdropper, including server administrators and others, have access to original message or any other type of transmitted information through public networks such as internet.

This paper presented a secure encryption method for true image encryption, which gets the benefits of both methods (symmetric and asymmetric encryption methods); a hybrid technique is usually used. In this technique, asymmetric encryption (RSA) is used to encrypt the security message the resulting cipher text is converted to binary form then symmetric encryption designed to encrypt the resulted cipher bits by making XOR operation with it. The design of symmetric key provides good confusion and diffusion properties that ensures high security. The easiest way to do this is through the design of the strong threshold linear feedback shift register, where the R,G,B bytes is ciphered with a single distinct bit generated from making XOR operation between key generator and resulting binary cipher bits ,which made the ciphers are more complex, the key is said to be well designed and its size provides an upper bound of an algorithm's cryptographic strength ,which consist of four shift registers the length them are 12,10,7,5 respectively, three of them are linear and the other are non-linear,also the design of the linear feedback function very strong ,which provided maximum length period. The opposite operation is performed to reconstructed the original image and the original secure message .in addition to that different measured have been used to explain the range of the difference between the regional and cipher images and to show the power of the encryption methods, such as histogram, Calibrated area, Mean, Standard deviation, Median, Calibrated center of mass , Calibrated perimeter, and Calibrated ferret diameter.

Keyword: *linear feedback shift register, RSA, symmetric cipher, asymmetric cipher*.

I. INTRODUCTION

Information security is a description of each process that prevent unauthorized access or use of the data transmitted, that access or use may be takes the form of distortion, use, disclosure, modification, or disruption. The main use of cryptography is to provide the following criteria such as the confidentiality; integrity and availability of the information ignoring data form for protecting the interconnected and share the common services.

Encryption changes the shape or location information so that does not allow unauthorized access or use of content. The strength of the encryption and decryption code system depends on the length and strength of the encryption key to prevent unauthorized person from access to the content of the text [1].

In the encryption and decryption process of a symmetric cipher both, must use the same key. Thus any messages can be decrypted the encryption key must be shared between the two persons. For this reason symmetric systems are known as shared secret systems or private key systems. Compared to asymmetric ciphers the Symmetric ciphers are significantly faster than asymmetric ciphers, but the requirements for key exchange make them difficult to use.

In an asymmetric cipher, there are two kinds of functions and two different keys. As a result each person has two keys. One of them is, the public key, is shared publicly [2], while the other is the private key, should never be shared with anyone. The recipient's public key using to encrypt the message when you send a message using asymmetric cryptography. The recipient then decrypts the message using his private key. For this reason the system is called asymmetric.

In this work the security massage for long length encrypted using RSA system, the resulted cipher text converted to the binary form then making XOR operation with the sequences bits resulted from threshold key generator for long 12,10,7,5 bits and strong feedback function.

.Because the security of image data from unauthorized uses is important therefore; images are widely used in different-different processes. To protect confidential image data from unauthorized access so many image encryption techniques are available to be used [3].

For suitable access to and sharing a large number of digital images now transmitted over Internet and wireless networks through the developments of multimedia and networks technologies, [4], therefore the content of the Multimedia must be protected from an authorized by using method or a set of methods of security, which based on cryptography and they allow each communication security, or security against piracy or both. The security of this multimedia can be accomplished by using hybrid methods between the symmetric and asymmetric algorithm and the (R, G, and B) bytes of the images after converting them to the binary value exploiting the properties of the XOR operation between the results of the encryption and bytes of image. The using of these methods for encryption to this multimedia attempt to transform an image to another one that is hard to recognize. To recovers the original image from the encrypted one image decryption used [5].

In addition to that two main parts involves in stream cipher which are they a key generator, and a mixing function. The first one is a mixing function which is usually just an XOR function; the second one is a key stream generator which is the main unit in stream cipher encryption method. Stream ciphers encrypt plaintext bits individually. Each bit x_i is encrypted by adding a secret key stream bit s_i modulo 2 .

i.e., $x_i, y_i, s_i \in \{0, 1\}$.

Encryption: $y_i = e_{si}(xi) \equiv x_i + s_i \bmod 2$.

Decryption: $x_i = d_{si}(y_i) \equiv y_i + s_i \bmod 2$.

II. THE STRUCTURE OF THE PROPOSED SYSTEM

The structure of the proposal system can be shown in the figure (1) as shown below:

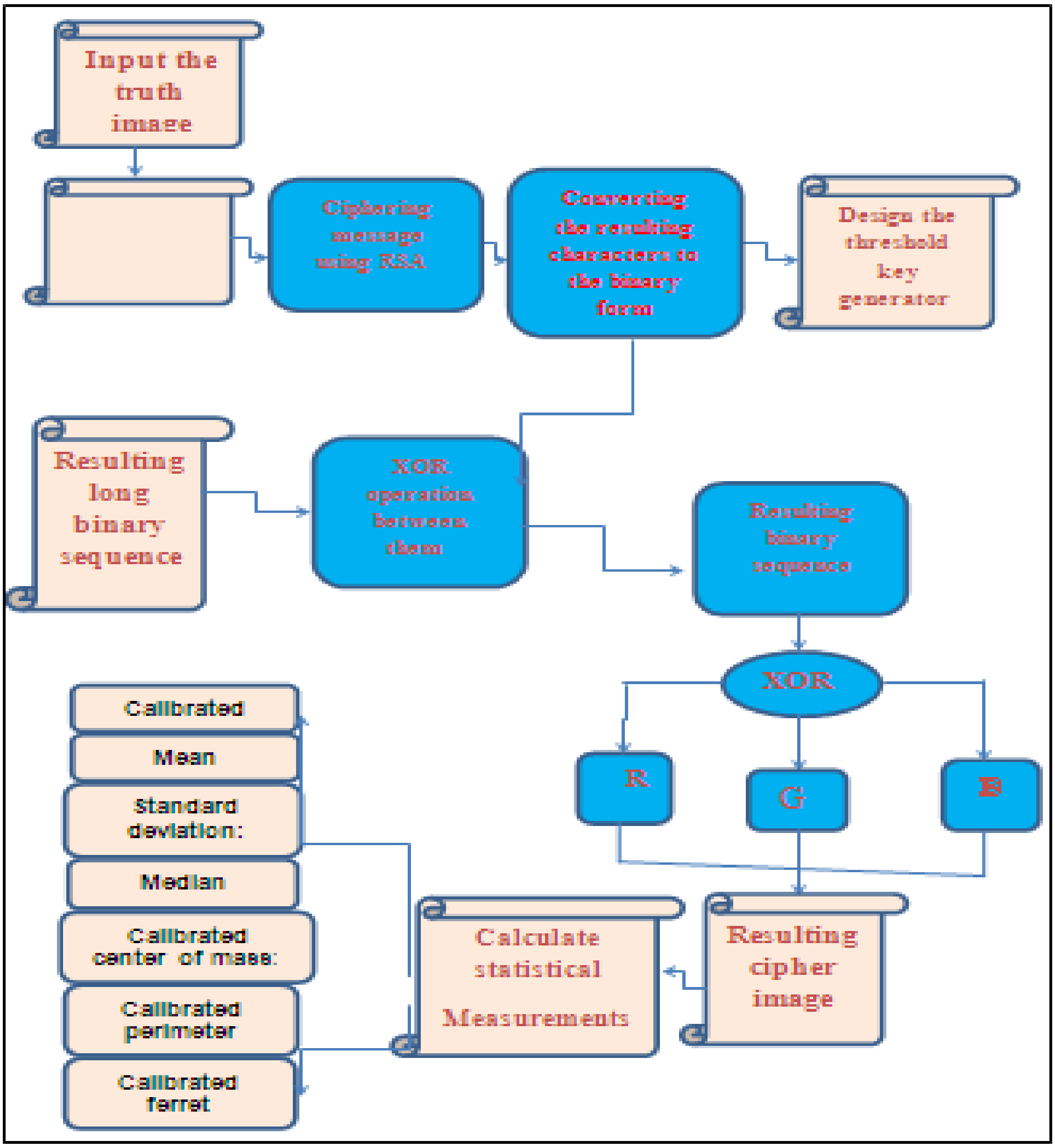

Input the truth image
Ciphering message using RSA
Converting the resulting characters to the binary form
Design the threshold key generator
Resulting long binary sequence
XOR operation between them
Resulting binary sequence
XOR
R
G
B
Calibrated
Mean
Standard deviation:
Median
Calibrated center of mass:
Calibrated perimeter
Calibrated ferret
Calculate statistical Measurements
Resulting cipher image

Figure (1) the structure of the suggested system

III.THE ALGORITHMS USED IN THIS SYSTEM

III.1RSA Algorithm

Public-key cryptography called asymmetric cryptography, where the keys used to encrypt and decrypt are different [6].

One type of the public key system is RSA which involves a public and private key. Anyone who wants to be sender need to publish an encryption key, which is known as the public key, but anyone who want to be receiver needs a unique decryption key which is known as private key [7]. Each letter in the message is converted to a decimal number by ASCII code, and encrypted by using the public key.

This algorithm is the most widely public-key encryption algorithm used, that provides confidentially and digital signature.

The keys for the RSA algorithm are generated in the following way [8].

Each entity A creates public key and corresponding private by doing the following:

- Generate three distinct large random prime numbers p, q, and e
- Compute n=p*q
- A’s public key (e, n) // to be published
- Who is capable of computing d?

$$d = \frac{\gcd(\Phi(n))*\Phi(n)+1}{e}$$

- Ψ (n) = (p-1)(q-1)

To verification d: we must [e*d mod Φ (n) =1]

A’s private key :(d, n)//to be kept secretly by A

e is released as the public key exponent [9].

Encryption: $C= m^e$ (mod *n*), **Decryption:** $m= c^d$ (mod *n*)

The decoder can recover m from by using her private key exponent d by the following computation:

m Ξ c^d (mod n) ,Given *m*., the decoder can recover the original message *w*here

m: The plain-text message, *c* : the encrypted message expressed as an integer number.

n: the product of two randomly selected, large primes *p* and *q* .

e : a large, random integer relatively prime to (*p* -1) *(*q* -1) .

d: the multiplicative inverse of *e*.

III.2 The suggested threshold key generator

This generator is one type of the stream cipher ,in this work this key consist of four linear feedback shift registers of length 12,10,7,5 , three of them are linear and the other are non-linear, where each one have maximum length period according to the primitive feedback function used.

The dynamic of this generator are:

If more than half the output 1, then the output of the generator 1 Otherwise 0.

The structure of this generator can be shown in figure (2):

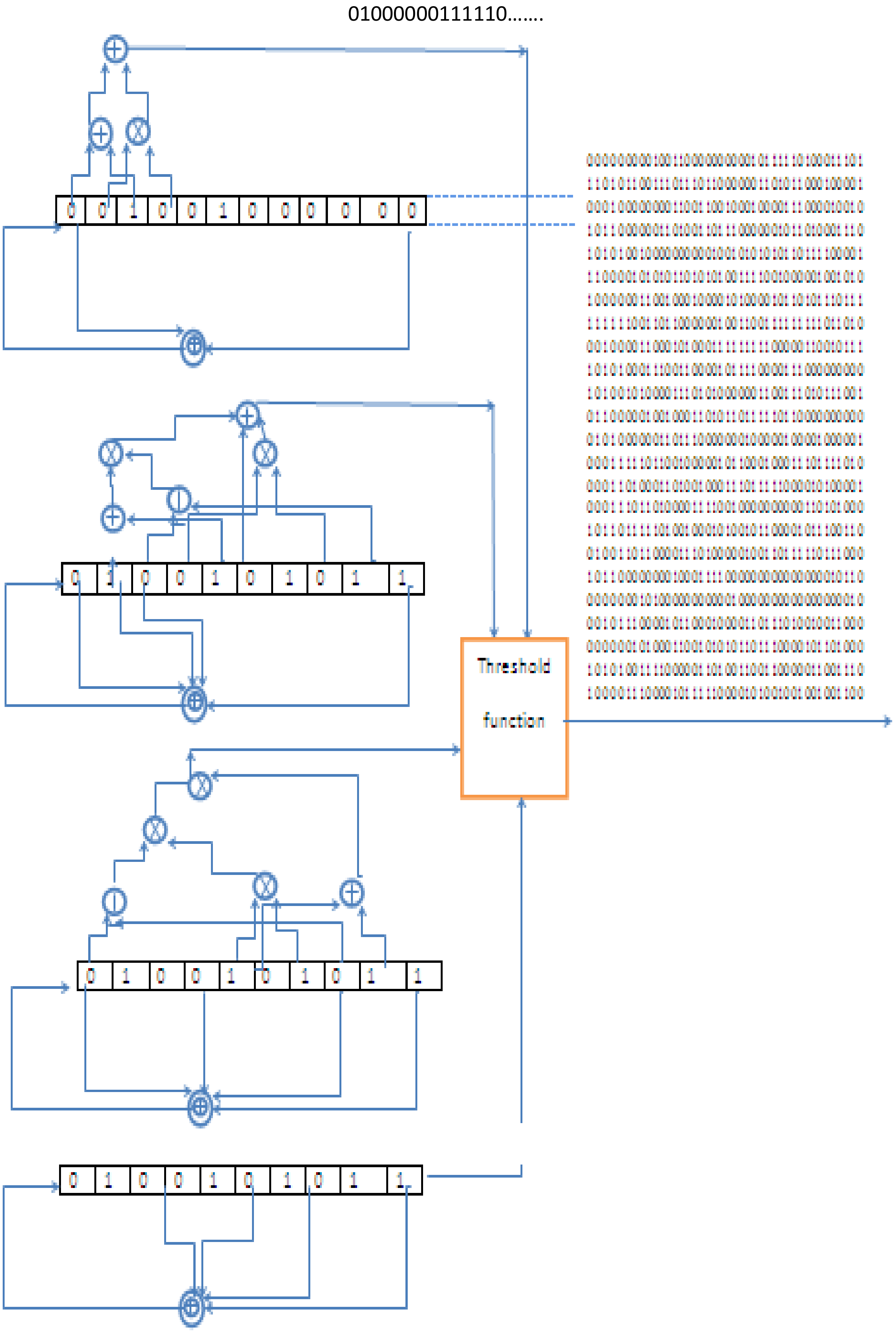
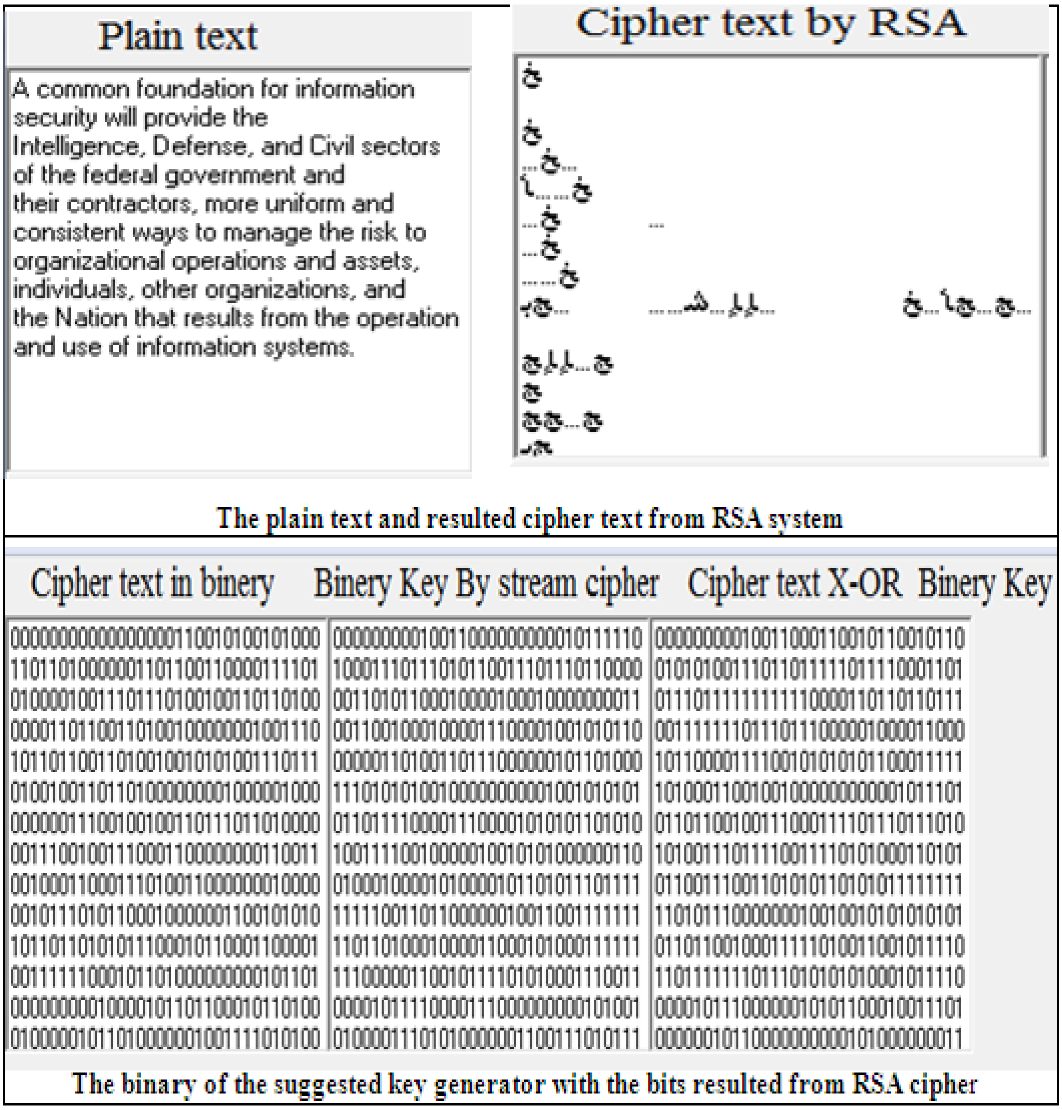


Figure (2) the suggested structure of the key generator

III.3 The plain and cipher text used in this system

For example the secure message supposed to be protected from the malicious passed in all steps before encrypted with the image bytes as below in table (1):

Table (1) contain the plain and cipher text and suggested key generator used in the encryption processes



Plain text	Cipher text by RSA
A common foundation for information security will provide the Intelligence, Defense, and Civil sectors of the federal government and their contractors, more uniform and consistent ways to manage the risk to organizational operations and assets, individuals, other organizations, and the Nation that results from the operation and use of information systems.	ځ ځ ...ځ... ٵ.....ځ ...ځ ... ...ځ ......ځ ـځ... ......ڜ...ﻟﻟ... ځ...ٵځ...ځ... ځﻟﻟ...ځ ځ ځځ...ځ ـځ

The plain text and resulted cipher text from RSA system

Cipher text in binery	Binery Key By stream cipher	Cipher text X-OR Binery Key
00000000000000000110010100101000	00000000010011000000000010111110	00000000010011000110010110010110
11011010000001101100110000111101	10001110111010110011101110110000	01010100111011011111011110001101
01000010011101110100100110110100	00110101100010000100010000000011	01110111111111110000110110110111
00001101100110100100000001001110	00110010001000011100001001010110	00111111101110111000001000011000
10110110011010010010101001110111	00000110100110111000000101101000	10110000111100101010101100011111
01001001101101000000001000001000	11101010100100000000001001010101	10100011001001000000000001011101
00000011100100100110111011010000	01101111000011100001010101101010	01101100100111000111101110111010
00111001001110001100000000110011	10011110010000010010101000000110	10100111011110011110101000110101
00100011000111010011000000010000	01000100001010000101101011101111	01100111001101010110101011111111
00101110101100010000001100101010	11111001101100000010011001111111	11010111000000010010010101010101
10110110101011100010110001100001	11011010001000011000101000111111	01101100100011111010011001011110
00111111000101101000000000101101	11100000110010111101010001110011	11011111110111010101010001011110
00000000010000101101100010110100	00001011110000111000000000101001	00001011100000010101100010011101
01000001011010000001001111010100	01000011101010000001100111010111	00000010110000000000101000000011

The binary of the suggested key generator with the bits resulted from RSA cipher

III. THE SECURITY OF THE PROPOSED SYSTEM

Below table (2) show the implementation of the proposed system using hybrid methods for text security and encrypted different images which reflect the security of this system.

Table (2) the implementation of the security system

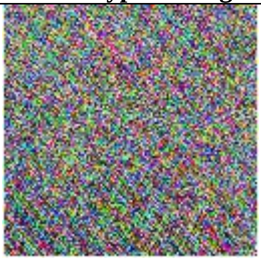
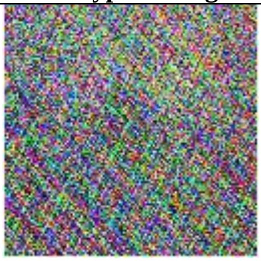
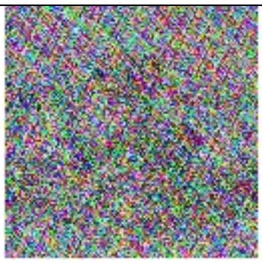
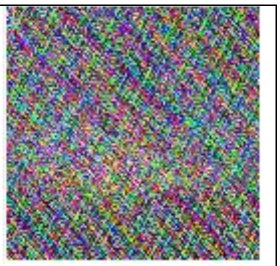
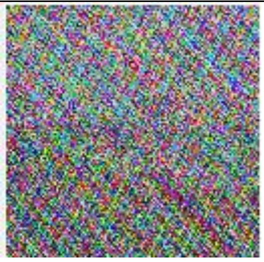
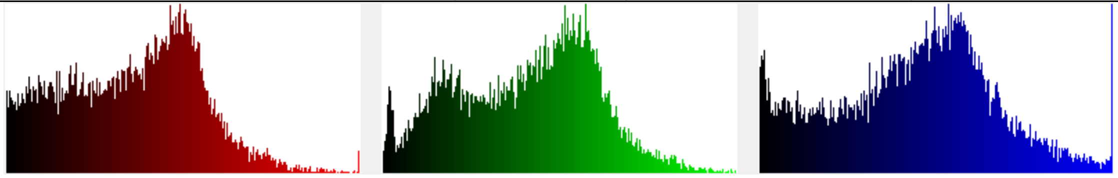
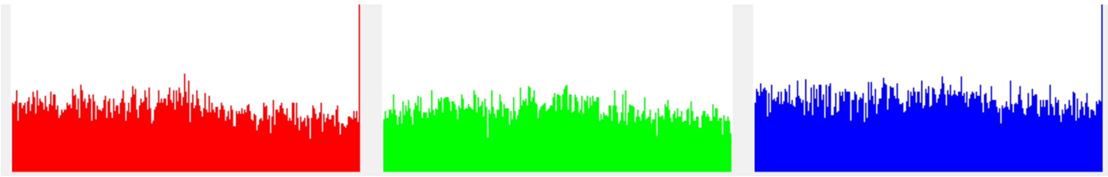
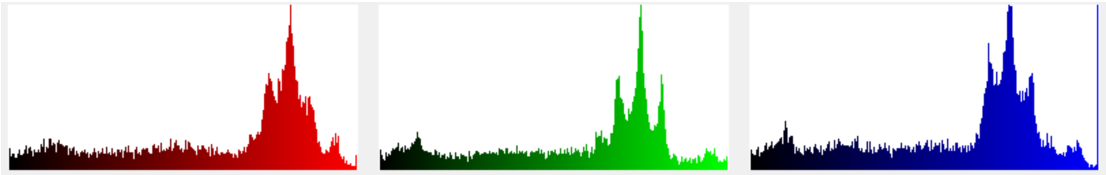
Original image	Encrypted image	Original image	Encrypted image
 Image1		 **Image4**	

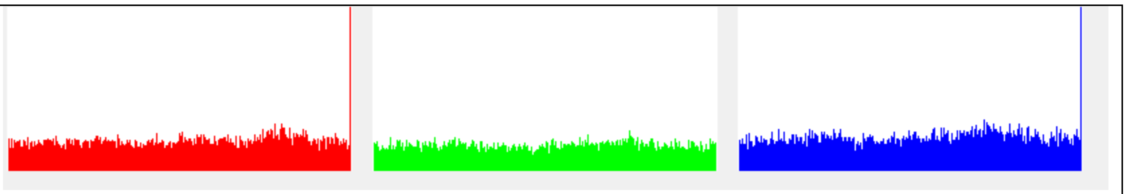
 Image2		 **Image5**	
 Image3		 **Image6**	

IV. THE HISTOGRAM OF THE ORIGINAL AND ENCRYPTED IMAGES

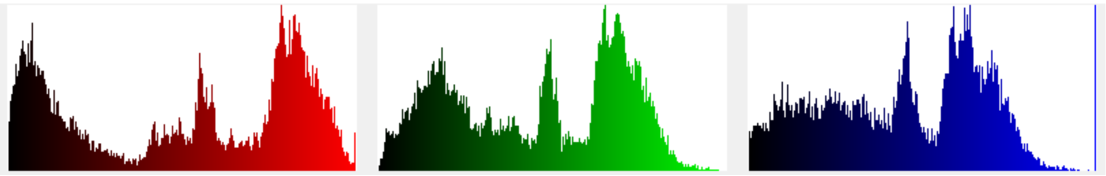
The histogram of the original and encrypted images used to show the difference between them, which reflects the strength of the encryption methods usedin this system, that combining the behavior for the symmetric and a symmetric encryption methods using with bytes of these images for different types of image. As shown in table (3) below.

Table (3) the histogram of the original and encryption images

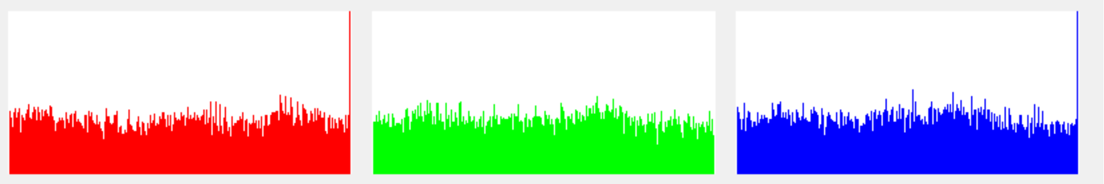
 **The histogram of the original image1**
 **The histogram of the encrypted image1**
 **The histogram of the original image2**



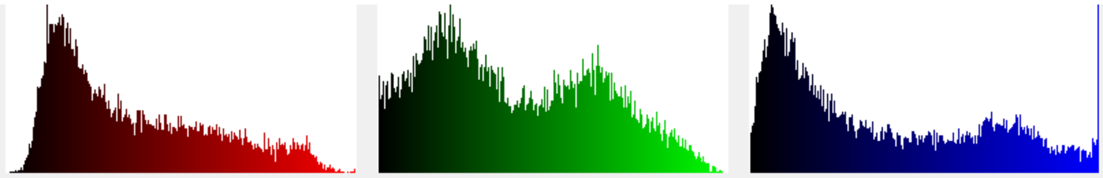
The histogram of the encrypted image2



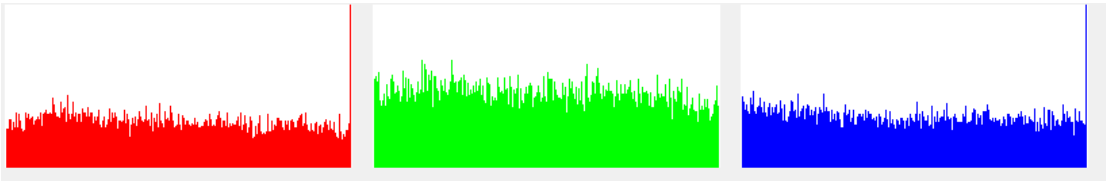
The histogram of the original image3



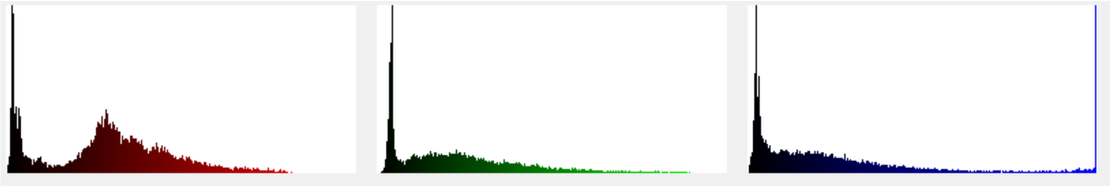
The histogram of the encrypted image3



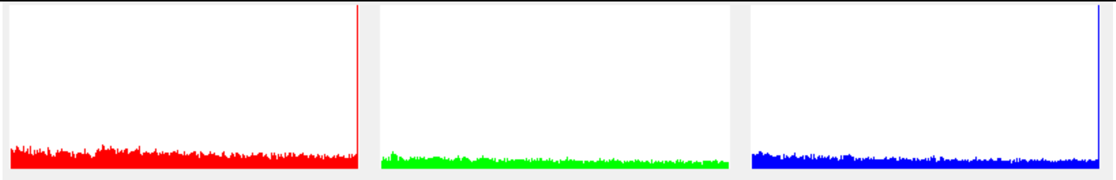
The histogram of the original image4



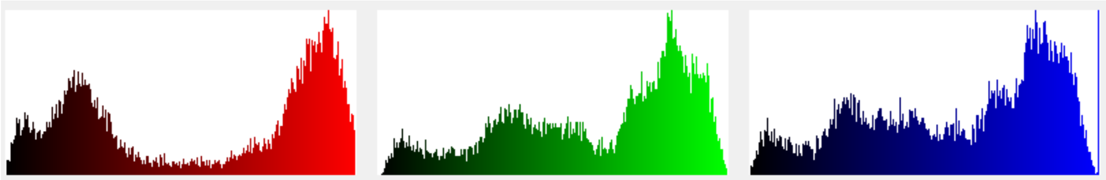
The histogram of the encrypted image4



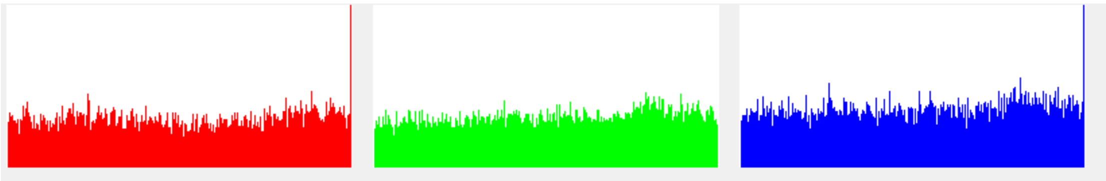
The histogram of the original image5



The histogram of the encrypted image5



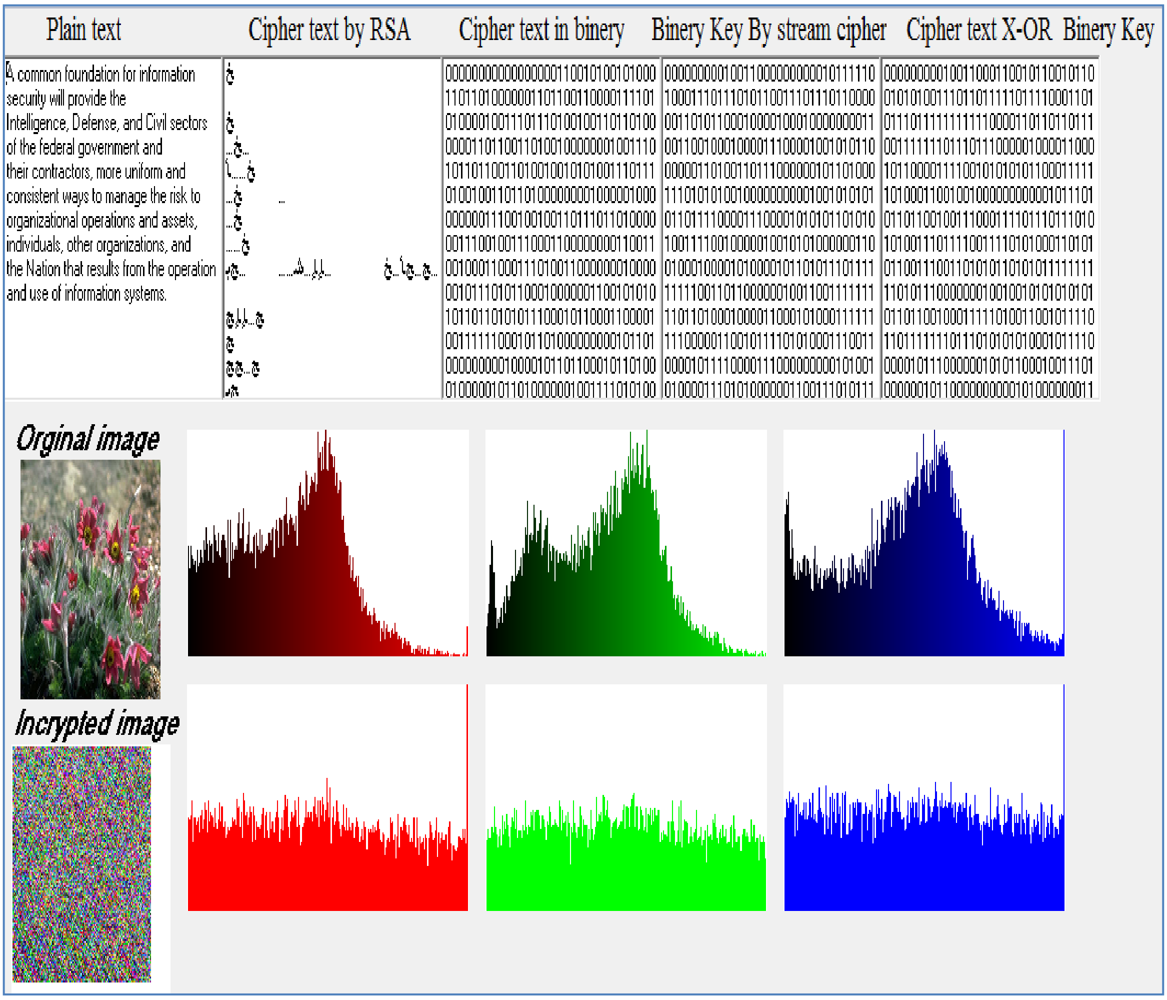
The histogram of the original image6



The histogram of the encrypted image6

V. THE IMPLEMENTATION OF THE PROPOSED SYSTEM AND RESULTS

This system is tested for different types of image, figure (3) show the this system, which implemented for image1, That's where the RSA method used to encryption chosen plain-text, which in turn converts to binary bits These bits combine with bits resulting from the proposed generator key and then encrypts each byte of the image with the bytes of the resulting binaries of encryption.



Plain text	Cipher text by RSA	Cipher text in binery	Binery Key By stream cipher	Cipher text X-OR Binery Key
A common foundation for information	ڂ	00000000000000000110010100101000	00000000010011000000000010111110	00000000010011000110010110010110
security will provide the		11011010000001101100110000111101	10001110111010110011101110110000	01010100111011011111011110001101
Intelligence, Defense, and Civil sectors	ڂ	01000010011101110100100110110100	00110101100010000100010000000011	01110111111111110000110110110111
of the federal government and	...ڂ...	00001101100110100100000001001110	00110010001000011100001001010110	00111111101110111000001000011000
their contractors, more uniform and	ا.....ڂ	10110110011010010010101001110111	00000110100110111000000101101000	10110000111100101010101100011111
consistent ways to manage the risk to	...ڂ ...	01001001101101000000001000001000	11101010100100000000001001010101	10100011001001000000000001011101
organizational operations and assets,	...ڂ	00000011100100100110111011010000	01101111000011100001010101101010	01101100100111000111101110111010
individuals, other organizations, and	.....ڂ	00111001001110001100000000110011	10011110010000010010101000000110	10100111011110011110101000110101
the Nation that results from the operation	ڂ... ......ﻫ...ﻟﻠ... ڂ...ڂا...ڂ...	00100011000111010011000000010000	01000100001010000101101011101111	01100111001101010110101011111111
and use of information systems.		00101110101100010000001100101010	11111001101100000010011001111111	11010111000000010010010101010101
	ڂ...ﻟﻠﻟڂ	10110110101011100010110001100001	11011010001000011000101000111111	01101100100011111010011001011110
	ڂ	00111111000101101000000000101101	11100000110010111101010001110011	11011111110111010101010001011110
	ڂ...ڂڂ	00000000010000101101100010110100	00001011110000111000000000101001	00001011100000010101100010011101
	ﻫ	01000001011010000001001111010100	01000011101010000001100111010111	00000010110000000000101000000011

Figure (3) show the implemented of proposed system for image1

VI. THE STATISTICAL MEASUREMENTS USED

Table (4) show the statistical measurements for encrypted image1 and original image1

measurements	encrypted image2	measurements	original image2
Calibrated area:	3.160 sq. in	Calibrated area:	0.182 sq. in
Mean:		Mean:	
- Luminosity	131.163	- Luminosity	143.17
- Red	131.405	- Red	144.035
- Green	131.593	- Green	142.055
- Blue	132.636	- Blue	151.266
Standard deviation:		Standard deviation:	
- Luminosity	52.048	- Luminosity	68.499
- Red	75.284	- Red	68.208
- Green	74.339	- Green	69.054
- Blue	75.065	- Blue	71.724
Median:		Median:	
- Luminosity	131	- Luminosity	173
- Red	135	- Red	174
- Green	135	- Green	171
- Blue	136	- Blue	186
Calibrated center of mass:		Calibrated center of mass:	
- x	0.889 in	- x	0.213 in
- y	0.889 in	- y	0.213 in
Calibrated perimeter:	7.111 in	Calibrated perimeter:	1.707 in
Calibrated feret diameter:	2.006 in	Calibrated feret diameter:	0.481 in

Number of statistical measurements applied to six different images before and after the suggested system implemented to show the difference between them, as tables (4) for image1, also the measurements of the other images can be shown in appendix(1) :

VII. CONCLUSIONS

1. The mixing of the symmetric and asymmetric encryption methods strength the proposed system.
2. The suggested key generator produced long maximum length period sequence, which provides a strong encryption method for images**.**
3. Increasing the structure complexity of the suggested key generator strength the cipher complexity.
4. Encryption of each byte of true image with different byte of cipher sequence making image more secure.
5. This system is more flexible for any type of images and for any size.
6. The using of the long text increasing the complexity system.

REFERENCES

[1] P.Shanmugam & C.Loganathan," Involuntary matrix in visual cryptography ", IJRRAS 6 (4) , March 2011.

[2] Varsha Bhatt, "Implementation of new advanced image encryption algorithm to enhance security of multimedia component ",IJATER, ISSN No: 2250-3536, Volume 2, Issue 4, July 2012.

[3] Fauzan Saeed and Mustafa Rashid, ”Integrating Classical Encryption with Modern Technique” IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.5, May 2010.

[4] Kahate A., “Cryptography and network security”, Tata-McGraw-Hill, 2nd edition , 2008.

[5] Mohammed Abbas Fadhil Al-Husainy, "A Novel Encryption Method for Image Security", International Journal of Security and Its Applications, Vol. 6, No. 1, January, 2012.

[6] Nada Abdul Aziz Mustafa," Design and Implementation proposed Encoding and Hiding Text in an Image", University of Sulaimani, M.Sc. Thesis, 2010.

[7] Mohammad Ahmad A. Alia," A New Approach to Public-Key Cryptosystem based on Mandelbrot and Julia Fractal sets", University Sains Malaysia, 2008.

[8] Mohammad Ahmad Alia and Azman Bin Samsudin," A New Digital Signature Scheme Based on Mandelbrot and Julia Fractal Sets", American Journal of Applied Sciences 4 (11): 848-856, 2007.

[9] Fadhil Salman Abed, "A proposed encoding and hiding text in an image by using fractal image compression", IJCSE, Vol. 4 No. 01 January 2012.

Appendix (1)

The experiments of statistical measurements for other images types can display the tables (5-9):

Table (5) Show the statistical measurements for encrypted image2 and original image2

measurements	encrypted image1	measurements	original image1
Calibrated area:	3.160 sq. in	Calibrated area:	1.778 sq. in
Mean:		Mean:	
- Luminosity	125.394	- Luminosity	104.017
- Red	126.621	- Red	111.105
- Green	126.027	- Green	103.7
- Blue	123.127	- Blue	90.754
Standard deviation:		Standard deviation:	
- Luminosity	50.926	- Luminosity	50.891
- Red	73.843	- Red	59.854
- Green	73.132	- Green	50.933
- Blue	74.001	- Blue	49.882
Median:		Median:	
- Luminosity	124	- Luminosity	110
- Red	126	- Red	117
- Green	125	- Green	111
- Blue	119	- Blue	96
Calibrated center of mass:		Calibrated center of mass:	
- x	0.889 in	- x	0.667 in
- y	0.889 in	- y	0.667 in
Calibrated perimeter:	7.111 in	Calibrated perimeter:	5.333 in
Calibrated feret diameter:	2.006 in	Calibrated feret diameter:	1.504 in

Table (6) show the statistical measurements for encrypted image3 and original image3

measurements	encrypted image3	measurements	original image3
Calibrated area:	3.160 sq. in	Calibrated area:	1.778 sq. in
Mean:		Mean:	
- Luminosity	127.027	- Luminosity	116.318
- Red	126.734	- Red	111.849
- Green	127.481	- Green	116.879
- Blue	129.876	- Blue	130.377
Standard deviation:		Standard deviation:	
- Luminosity	51.644	- Luminosity	62.905
- Red	74.021	- Red	58.378

- Green	74.25	- Green	62.472
- Blue	75.949	- Blue	83.148
Median:		Median:	
- Luminosity	126	- Luminosity	124`
- Red	128	- Red	117
- Green	129	- Green	125
- Blue	132	- Blue	146
Calibrated center of mass:		Calibrated center of mass:	
- x	0.889 in	- x	0.667 in
- y	0.889 in	- y	0.667 in
Calibrated perimeter:	7.111 in	Calibrated perimeter:	5.333 in
Calibrated feret diameter:	2.006 in	Calibrated feret diameter:	1.504 in

Table (7) show the statistical measurements for encrypted image4 and original image4

measurements	encrypted image4	measurements	original image4
Calibrated area:	3.160 sq. in	Calibrated area:	0.046 sq. in
Mean:		Mean:	
- Luminosity	124.422	- Luminosity	96.259
- Red	124.1	- Red	93.911
- Green	125.697	- Green	98.884
- Blue	122.93	- Blue	93.181
Standard deviation:		Standard deviation:	
- Luminosity	52.254	- Luminosity	63.175
- Red	75.602	- Red	73.756
- Green	74.884	- Green	62.421
- Blue	73.922	- Blue	57.943
Median:		Median:	
- Luminosity	123	- Luminosity	80
- Red	122	- Red	70
- Green	124	- Green	89
- Blue	119	- Blue	76
Calibrated center of mass:		Calibrated center of mass:	
- x	0.889 in	- x	0.107 in
- y	0.889 in	- y	0.107 in
Calibrated perimeter:	7.111 in	Calibrated perimeter:	0.853 in
Calibrated feret diameter:	2.006 in	Calibrated feret diameter:	0.241 in

Table (8) show the statistical measurements for encrypted image5 and original image5

measurements	encrypted omage5	measurements	original image5
Calibrated area:	3.160 sq. in	Calibrated area:	1.778 sq. in
Mean:		Mean:	
- Luminosity	118.378	- Luminosity	60.214
- Red	118.308	- Red	59.557
- Green	118.814	- Green	59
- Blue	120.664	- Blue	73.69
Standard deviation:		Standard deviation:	
- Luminosity	52.951	- Luminosity	50.396
- Red	75.964	- Red	59.607
- Green	76.05	- Green	48.133
- Blue	74.619	- Blue	47.285
Median:		Median:	
- Luminosity	115	- Luminosity	50
- Red	112	- Red	42
- Green	113	- Green	49
- Blue	114	- Blue	75
Calibrated center of mass:		Calibrated center of mass:	
- x	0.889 in	- x	0.667 in
- y	0.889 in	- y	0.667 in
Calibrated perimeter:	7.111 in	Calibrated perimeter:	5.333 in
Calibrated feret diameter:	2.006 in	Calibrated feret diameter:	1.504 in

Table (9) show the statistical measurements for encrypted image6 and original image6

measurements	encrypted image6	measurements	original image6
Calibrated area:	3.160 sq. in	Calibrated area:	1.778 sq. in
Mean:		Mean:	
- Luminosity	133.588	- Luminosity	154.06
- Red	132.911	- Red	150.454
- Green	134.847	- Green	158.561
- Blue	133.195	- Blue	144.416
Standard deviation:		Standard deviation:	
- Luminosity	52.022	- Luminosity	69.083
- Red	74.75	- Red	68.999
- Green	74.471	- Green	66.806
- Blue	76.678	- Blue	86.157
Median:		Median:	
- Luminosity	134	- Luminosity	177
- Red	134	- Red	169
- Green	138	- Green	181
- Blue	134	- Blue	178
Calibrated center of mass:		Calibrated center of mass:	
- x	0.889 in	- x	0.667 in

- y	**0.889 in**	**- y**	**0.667 in**
Calibrated perimeter:	**7.111 in**	**Calibrated perimeter:**	**5.333 in**
Calibrated feret diameter:	**2.006 in**	**Calibrated feret diameter:**	**1.504 in**