ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 2, August 2015

Design And Implement Rabin Crypto Code as Guider for Stego-system

Ismael Abdul Sattar, Reham Ayham Raheem, Maryam Hussein Hamad
Al Mustansiriyah University, Collage of science, Department of computer science

***Abstract*— Information Security one of the important field in human live in all aspect and there are many way (techniques) to achieved it like using cryptography steganography or a combination of them. In our proposed system, a benefit of the illusions messages has been took where was consider as a weakness point in Rabin crypto algorithm due to size problem, and we turned to advantages in steganography field which will used not only constructing hiding map but also authenticated mechanism which guide the hiding process..**

***Index Terms*— Rabin code, Information hiding, Illusion messages, Rabin cryptosystem, map constructing.**

I. INTRODUCTION

Information security become one of the human need in all of human life issues, if he live a civil life (protecting personal information) or military one (protecting government, agency information). The demand on the security software raise over and over with network connection due to many kinds of attack that could appear during the connections and exchanging vast of information through network, obviously not all the information have same security level that will depend on the user demand and his criteria.

Steganography is the art and science of concealing communication [4]. The goal of steganography is to hide the very existence of information exchange by embedding messages into unsuspicious digital media covers. Cryptography, or secret writing, is the study of the methods of encryption, decryption, and their use in communications protocols. Both techniques manipulate data to ensure the security of information, but the concept of steganography differs from cryptography [5]. Cryptography obscures the meaning of a message, but it does not conceal the fact that there is a message. The goal of cryptography is to make data unreadable by a third party, whereas the goal of steganography is to hide the data from a third party. Both techniques have an ancient origin, but the modern field is relatively young [2]. Cryptography and steganography are fundamental components of computer security [3]. The focus of the current work is on the integration of cryptography and steganography concepts in such a way to handle the output that come from Rabin crypto system and take advantage of the illusion messages which consider a useful from crypto view and useless from communicator view, well finally we make these illusion messages useful not only as map for guiding stego system but also for authenticating purpose.

II. RABIN CRYPTOSYSTEM

The Rabin cryptosystem is an asymmetric system, that is why requires two different keys, a public key and a private key, one to encrypt the text and the other one to decrypt it. The first step is to choose the key which is defined by:

$$k = \{n, p, q\}$$

Where p and q are primes such that $p, q \equiv 3 \bmod 4$ which are the private key. The public key is $n = p * q$. Then, to encrypt the message m, the encryption function is applied:

$$E_k(m) = m^2 \bmod n = c$$

The result is the cipher text, c. Now the encoded message can be sent. Once the message reaches the destination, it must be decrypted. For that, the decryption function is applied:

$$D_k(c) = \sqrt{c} \bmod n$$

Since the encryption function E_k is not an injection function, the decryption is not ambiguous. There exist four square roots of c mod n $(c = m^2 \bmod n)$, so there are four possible messages, m.

The decryption try to determine m such that:

$$(c = m^2 \bmod n)$$

And this is equivalent to solving the two congruence:

$$z^2 = c \bmod p$$
$$z^2 = c \bmod q$$

Then:

$$m_p = p^{\frac{p+1}{4}}$$
$$m_q = p^{\frac{q+1}{4}}$$

Finally, the four square roots of c mod n can be computed applying the Chinese remainder theorem to the system of congruencies:

$$+m_p \bmod p$$
$$-m_p \bmod p$$
$$+m_q \bmod q$$
$$-m_q \bmod q$$

Rabin cryptosystem is secure against a chosen plaintext attack because $n = pq$ cannot be factored, however, is insecure against a chosen cipher text attack [1].

III. PROPOSED SYSTEM

In our proposed system the text secret message converted to ASCII values and then feed it to Rabin Encryption algorithm which gives the system encrypted message c which will represent the input to Decryption algorithm that will give four messages $\{m_0, m_1, m_2, m_3\}$ one of them secret message and the rest are illusion messages with a different length will

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 2, August 2015

construct the map as shown below:

Pseudo code for determining Map

I=0

While $(m_i <> c)do$

$hiding_{map} = m_i$

End

Now, prepare color cover image for hiding *c* as shown in below algorithm

Hiding Algorithm

Input:

Cipher Message (Text)
Cover Image (Image)
Map (binary format)

Output

Stego-object

Process

1. Read secret message
2. Convert secret to binary format.
3. Read cover color image and get three bands (RGB).
4. Convert all band of RGB to binary format.
5. Get k_1, k_2, k_3 based on Map (Output of Decryption)
6. For each byte band do the following steps.
   6.1) prepare a Target Address through the following equation
   $T_{address} = (1 * k_1 + 2 * k_2 + 4 * k_3)\ Mod\ 3$
   6.2) Replacing the Target Address Bit with the secret bit message
7. Go to step 6 until hide all the secret.
8. Gather all the bands to form stego-object.

Both of the map and stego-object will transmit through channel from sender to receiver as shown in the figure (1) , when the receiver get both of them will start extract *c* the encrypted message and start decrypted to get four messages $\{m_0, m_1, m_2, m_3\}$ one of them is a secret message and rest are map and this cane easy to filter now because we have the map already if the extracted map matched the received one that is authenticated otherwise it's not, and that will raise suspicion it is unsecure channel.

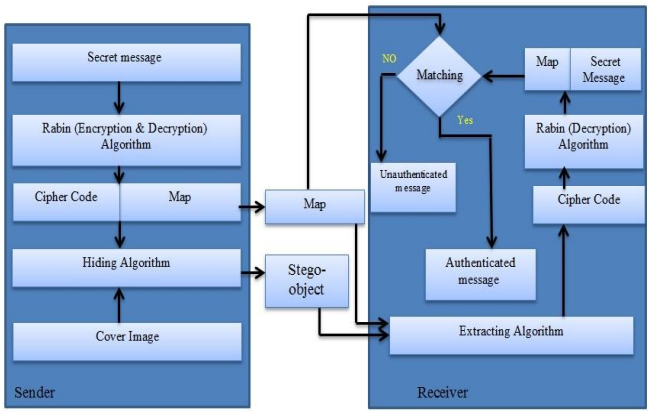

Fig (1) Block diagram of the proposed system

V. EXPERIMENTAL RESULT

One of the best decisions to turn out weakness point (drawbacks) of the data security algorithm to advantage in another security algorithm and form a system that would be more secure for handling more security criterion, that's what we have done by use the extra messages (illusion) as output of the Rabin cryptosystem for constructing a map that will work as a guide for hiding mechanism. The output of implemented proposed system shown in the following table:

Cover image size	Secret message size	Illusion messages size	PSNR	Public key	Private keys	
					P	Q
100*100	1 KB	23 KB	63.5469	11924687581	113027	105503
128*128	2 KB	32 KB	67.7708	11954596421	106019	112759
256*256	3 KB	66 KB	84.4392	29671133	124147	239
300*300	4 KB	82 KB	78.8271	20186981	105691	191
512*512	5 KB	150 KB	77.4637	124055547157	1127911	109987

Table (1) show the secret message of the different size and its effect over objective measure analysis

Cover image size	Secret message size	Illusion messages size	PSNR	Public key	Private keys	
					p	q
100*100	1 KB	23 KB	42.33708	11182379609	105527	105967
128*128	1 KB	25 KB	44.97809	12395042713	109583	113111
256*256	1 KB	17 KB	51.48815	26734333	211	126703
300*300	1 KB	31 KB	49.40507	74141650570513	74142911	999983
512*512	1 KB	26 KB	56.05091	558951861761	4883083	114467

Table (2) show the secret message of the same size and its effect with different private keys

VI. CONCLUSION

It is a big challenge to handle the output of the size problem in a cryptographic algorithm especially where there is a limitation problem with channel transfer (due to rise suspicion problem), it make a good decision to implement such size and make it useful in the other mechanism as we implemented in our proposed system it show a good result not only for guiding hiding mechanism but also authentication mechanism the things that can be slow down our system is using the decryption algorithm in the sender side this is one of the drawbacks of time consuming.

REFERENCES

[1] Rabin, N.s., 2014.Rabin cryptosystem. University of Paderborn

[2] Stinson, Cryptography: Theory and Practice, 2nd ed. Campman & Hall, 2001.

[3] Katz and Lindell, Introduction to Modern Cryptography, Ed. Campman & Hall, 2007.

[4] Kessler, G. (2004), Overview of Steganography for the computer forensics examiner, Forensics Science Communication, 6(3).

[5] Provos, N. & Honeyman, P. (2003). Hide and seek: An Introduction to Steganography, IEEE Security and Privacy Magazine.

AUTHOR BIOGRAPHY

ISMAEL ABDULSATTAR JABBAR is M.Sc. Member of staff (Assistant Lecturer) in the Computer Science Department at Al-Mustansiriyah University and Chairman of the Training and development Committee in The Iraqi Association for Information Technology and He is Member of Iraqi

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 2, August 2015

Programmer Union and Member of Iraqi association of information technology. He has published more than 12 Research Papers in National or International Journals and conferences.

Reham Ayham Raheem is a B.Sc. graduated from Computer Science Department collage of science at Al-Mustansiriyah University.

Maryam Hussein Hamad is a B.Sc. graduated from Computer Science Department collage of science at Al-Mustansiriyah University.