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 unsuspicous digital media covers. Cryptography, or secret writing, is the study of the methods of encryption, decryption, and 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 CRYPTO SYSTEM

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 \( p, q \equiv 3 \mod 4 \) which are the private key. The public key is \( n = p \times q \). Then, to encrypt the message \( m \), the encryption function is applied:

\[ E_k(m) = m^2 \mod n = c \]

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:

\[ D_k(c) = \sqrt{c} \mod n \]

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

The decryption try to determine \( m \) such that:

\[ (c = m^2 \mod n) \]

And this is equivalent to solving the two congruence:

\[ z^2 = c \mod p \]
\[ z^2 = c \mod q \]

Then:

\[ m_p = p^{\frac{p-1}{2}} \]
\[ m_q = q^{\frac{q-1}{2}} \]

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

\[ +m_p \mod p \]
\[ -m_p \mod p \]
\[ +m_q \mod q \]
\[ -m_q \mod q \]

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 \( \{m^1, m^2, m^3, m^4\} \) one of them secret message and the rest are illusion messages with a different length will
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
       \[ T_{address} = (k_1 \times 2 + k_2 + 4 \times k_3) \mod 3 \]
   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 can ease 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.

**REFERENCES**


**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
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 college of science at Al-Mustansiriyah University.

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