Journal of Engineering and Applied Sciences 14 (7): 2240-2243, 2019
ISSN: 1816-949X

Steganography Algorithm Based RSA Cryptosystem

Najlae Falah Hameed Al Saffar
Department of Mathematics, Faculty of Computer Science and Mathematics,
University of Kufa, 54001 Najaf, Iraq

Abstract: Now a days, it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret, this is why we present in this study a combination of cryptosystem algorithm and steganography. The proposed algorithm encrypts the information using RSA algorithm before hiding it in image file to increase the complexity of encryption and decryption process.

Key words: Steganography, cryptosystem, RSA, cryptosystem, decryption, encryption

INTRODUCTION

Steganography is a technique in which the secret data is hidden behind the carrier file within an image, text, audio or even video files and then the transformation will done from sender to receiver (Manjunath and Hiremath, 2015). The Cryptosystem is another technique in which the secret data is protecting within algorithms such as RSA (Rivest *et al*., 1978), Elgamal encryption (El-Gamal, 1985), ECC (Miller, 1986; Koblitz, 1987), etc. Hybrid the steganography and one of the cryptosystem algorithm will provide more security to the transferring data.

The process of steganography technique can be defined into four types: text, image, audio and video steganography. In text steganography text files are used to hide data, in image steganography the image file with extension png, gif, bmp, etc., will be a tool to hide a secret message, it is allows for two parties to communicate secretly and covertly. For the third type (audio steganography) the secret data embedded using a key in a digital cover file to produce a stego file, using some algorithms in which an observer cannot detect the hidden message. The video steganography is a combination of image and audio steganography (Eltahir *et al*., 2009).

Security of information is one of the most important factors of information technology and communication. A technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret, this technique is a cryptography.

In this study, a combination of cryptosystem algorithm (RSA algorithm) and steganography has been introduced. This combination encrypts the information using RSA algorithm, the processing of steganography will be done by using image of encrypted message and covered image. The encrypted message will be with little bit noise is such way it is noticeable to the human eye. All simulations in this work is implemented in MATLAB (R2014a).

Many researchers were interested in the topic of hybrid steganography techniques and some of algorithms of cryptosystem such as Yadav *et al*. (2014), Saleh *et al*. (2016), Roy and Venkateswaran (2014) and Islam *et al*. (2014).

Steganography: Steganography means "covered writing" is the art and science of hiding information such that its presence. The main purpose of steganography is to communicate securely in a completely undetectable manner to preclude drawing uncertainty to the transmission of a hidden message. The first recorded uses of steganography can be traced back to around 440 BC in many method such as: wax tablets, shove heads, invisible ink or morse code (Sheth and Tank, 2015).

Nowadays, steganography is being used all over the world on computer systems. Many tools and technologies have been interduced that take advantage of old steganographic techniques. Since, the steganographic techniques are covered, so, so according to this idea the there are four types of steganographic techniques: encoding secret messages in text, encoding secret messages in images, encoding secret messages in audio and encoding secret messages in video (Dunbar, 2002) (Fig. 1).

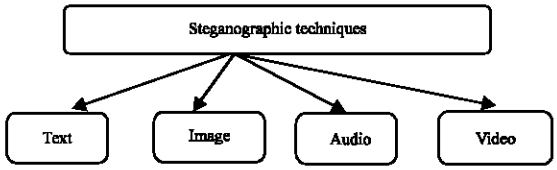

Fig. 1: Types of steganographic techniques

RSA cryptosystems: The RSA cryptosystem has been introduced in 1977 by Rivest *et al.* (1978). It is the most widely-used public key cryptography algorithm in the world, also it can be used to encrypt a message without the need to exchange a secret key separately. RSA is used in many commercial systems. It is used by Web servers and browsers to secure web traffic, it is used to ensure privacy and authenticity of Email, also it is used to secure remote login sessions and many others applications (Boneh, 1999).

RSA derives its security from the hypothesis which is said that: when pand q are two large prime, it is computationally intractable to factor n = pq. In practice, p and q should both be 1024 bits long.

The public key of RSA cryptosystem consists of the moduluo n and the value e which is act as public key exponent. The private key consists of the modulus n and the d which is act as private key exponent. In the following we will illustrate this algorithm the situation Alice wants to send to Bob a message:

- Bob chooses secret primes p and q of approximately equal size and computes n = pq
- Bob chooses an exponent e, $1<e<\varphi(n)$ with gcd $(e, \varphi(n)) = 1$
- Bob computes d, $1<d<\varphi(n)$ with $de \equiv 1 \bmod \varphi(n)$
- Bob makes (n, e) public and keeps (p, q, d) secret
- Alice encrypts m as $c \equiv m^e \pmod n$ and sends c to Bob
- Bob decrypts by computing $m \equiv c^d \pmod n$

MATERIALS AND METHODS

Proposed algorithm: Hybrid steganography technique and RSA cryptosystem is approach to encrypt the plain text with image file. The proposed algorithm will be divided into two main class, steganography and cryptosystem. We will follow the following steps to implement this proposed algorithm. During the steps, we will need to create a binary image with extension png using MATLAB code and save it as a covered image with the same size of the saving image in step 2, this action will be done exactly after step 2 together with algebra properties. This covered image will be the public key for the proposed algorithm as well as the RSA public key.

Assume that there are two users (Bob and Alice) want to communicate using the proposed algorithm. So, the situation is: Bob want send message say (M) to Alice.

Algorithm 1; Proposed algorithm:

Step 1: The RSA cryptosystem will adopt to encrypt M
Step 2: Bob will save the C (encrypted of M) as an image with extension png. Say (C_I). Then, compute its size
Step 3: Image algebra properties will involve in step 3, where (C_I) will add to the covered image, the result will denoted by $C_{C_{I_m}}$
Step 4: Send $C_{C_{I_m}}$ with public keys to Alice

The next situation is: Alice want recover the message M from $C_{C_{I_m}}$ as decryption process.

Step 1: Alice will subtract $C_{C_{I_m}}$ from the covered image to get C_{I_m}'. This image had a little bit noise but it is readable
Step 2: She will use the RSA decryption steps to get M

RESULTS AND DISCUSSION

Implementation of proposed algorithm: In this subsection, we will introduce an example to illustrate the processing on the proposed algorithm to encrypt and decrypt a message using hybrid steganography technique and RSA cryptosystem.

Assume that there are two users (Bob and Alice) want to communicate using the proposed algorithm. So, the situation is: Bob want send message say (M: steganography and crptosystem) to Alice.

Step 1: The RSA cryptosystem will adopt to encrypt M. (p = 13, q = 11, so, n = 143 and $\varphi(n) = 120$. The exponent e = 7 and d = 103).

So, the first action is convert the M to decimal form using the Ascii to s as:

$$s = \begin{pmatrix} 83\,1\,16\,101\,103\,97 \\ 110\,111\,103\,114\,97 \\ 112\,104\,121\,32\,97 \\ 110\,100\,32\,67\,114 \\ 121\,112\,116\,111\,115 \\ 121\,115\,116\,101\,109 \end{pmatrix}$$

Now, implement the RAS algorithm to calculate the Ciphertext C as follows:

$$83^7 \bmod 143 = 8, 116^7 \bmod 143 = 129, 101^7 \bmod 143 = 62, 103^7 \bmod 143 = 103, 97^7 \bmod 143 = 59$$
$$110^7 \bmod 143 = 33, 111^7 \bmod 143 = 45, 103^7 \bmod 143 = 38, 114^7 \bmod 143 = 49, 97^7 \bmod 143 = 59$$
$$112^7 \bmod 143 = 18, 104^7 \bmod 143 = 91, 121^7 \bmod 143 = 121, 32^7 \bmod 143 = 98, 97^7 \bmod 143 = 59$$
$$110^7 \bmod 143 = 33, 100^7 \bmod 143 = 100, 32^7 \bmod 143 = 98, 67^7 \bmod 143 = 89, 114^7 \bmod 143 = 49$$
$$121^7 \bmod 143 = 121, 112^7 \bmod 143 = 18, 116^7 \bmod 143 = 129, 111^7 \bmod 143 = 45, 115^7 \bmod 143 = 80$$
$$121^7 \bmod 143 = 121, 115^7 \bmod 143 = 80, 116^7 \bmod 143 = 129, 101^7 \bmod 143 = 62, 109^7 \bmod 143 = 21$$

So, the cipher text is:

$$C = \begin{pmatrix} 8\,129\,62\,103\,59 \\ 33\,45\,38\,49\,59 \\ 18\,91\,121\,98\,59 \\ 33\,100\,98\,89\,49 \\ 121\,18\,129\,45\,80 \\ 121\,80\,129\,62\,21 \end{pmatrix}$$

Step 2: Bob will save the C as an image with extension png. say (C_{I_m}). Then, compute its size. That is the C_{I_m} as follows (Fig. 2):

Step 3: Image algebra properties will involve in step 3, where C_{I_m} will add to the covered image, the result will denoted by $C_{C_{I_m}}$. The covered image with size 200×200 is as follows (Fig. 3): So, the $C_{C_{I_m}}$ is as follows:

Step 4: Send $C_{C_{I_m}}$ with public keys of RAS cryptosystem to Alice (Fig. 4).

The next situation is: Alice want recover the message M from $C_{C_{I_m}}$ as decryption process.

Step 1: Alice will subtract $C_{C_{I_m}}$ from the covered image to get C_{I_m}'. This image had a little bit noise but it is readable as follows:

Step 2: She will use the RSA decryption steps to get M as follows (Fig. 5).

$$8^{103} \bmod 143 = 83, 129^{103} \bmod 143 = 116, 62^{103} \bmod 143 = 101, 103^{103} \bmod 143 = 103, 59^{103} \bmod 143 = 97$$
$$33^{103} \bmod 143 = 110, 45^{103} \bmod 143 = 111, 38^{103} \bmod 143 = 103, 49^{103} \bmod 143 = 114, 59^{103} \bmod 143 = 97$$
$$18^{103} \bmod 143 = 112, 91^{103} \bmod 143 = 104, 121^{103} \bmod 143 = 121, 98^{107} \bmod 143 = 32, 59^{103} \bmod 143 = 97$$
$$33^{103} \bmod 143 = 110, 100^{103} \bmod 143 = 100, 98^{103} \bmod 143 = 32, 89^{103} \bmod 143 = 32$$
$$121^{103} \bmod 143 = 121, 18^{103} \bmod 143 = 112, 129^{103} \bmod 143 = 116, 45^{103} \bmod 143 = 111, 80^{103} \bmod 143 = 115$$
$$121^{103} \bmod 143 = 121, 80^{103} \bmod 143 = 115, 129^{103} \bmod 143 = 116, 62^{103} \bmod 143 = 101, 21^{103} \bmod 143 = 109$$

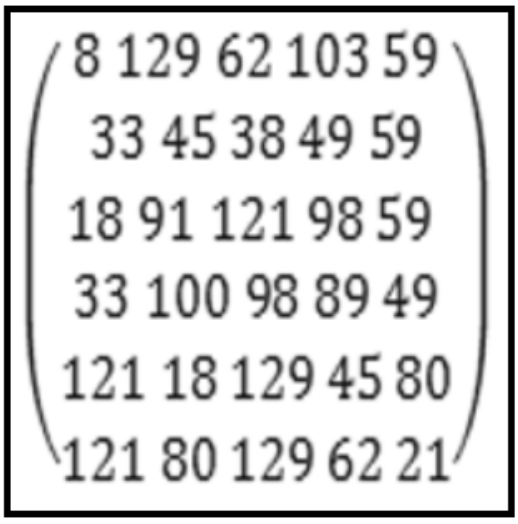

Fig. 2: With size 200×200

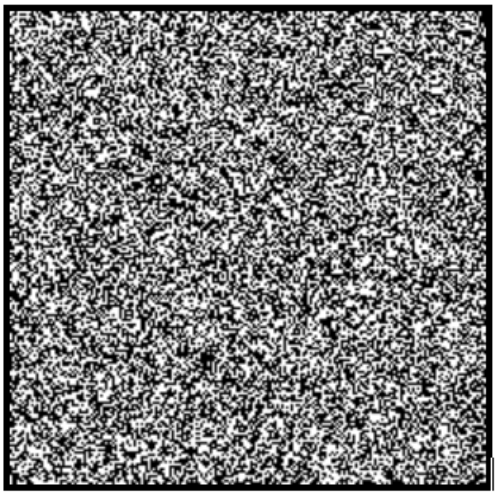

Fig. 3: The covered image with size 200×200

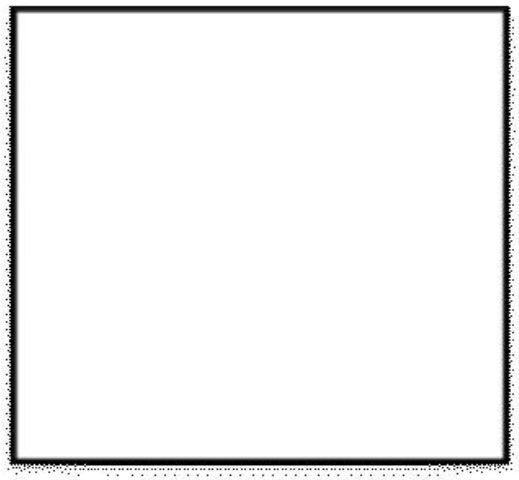

Fig. 4: Keys of RAS cryptosystem to Alice

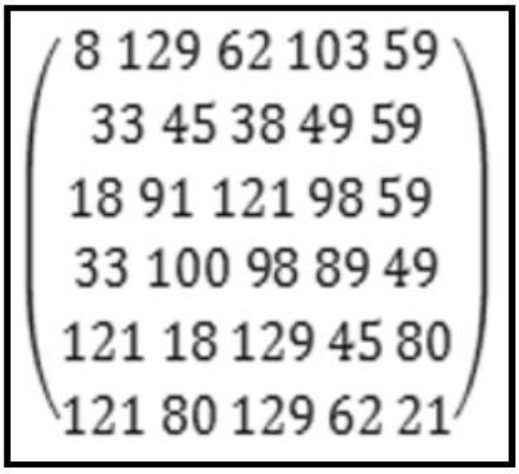

Fig. 5: RSA decryption steps

CONCLUSION

In this study, we introduce an algorithm to encrypt text information by RSA then hide it within image file and do the decryption process through public channels using some properties of algebra which is deal with matrix that construct from features of image. This algorithm use the concepts of public key cryptosystem (RSA) that is it is based in the most widely hard mathematical problem which is integer factorization problem.

RECOMMENDATIONS

There are many improvements that can be done as future researchs such as using another hard mathematical problem such as discrete logarithm problem or Computational Diffie-Hellman problem. These problems may be effect on the difficulty of the proposed algorithm.

REFERENCES

Boneh, D., 1999. Twenty years of attacks on the RSA cryptosystem. Notes Am. Math. Soc., 46: 203-213.

Dunbar, B., 2002. A detailed look at steganographic techniques and their use in an open-systems environment. Sans Institute, New Orleans, USA.

El-Gamal, T., 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inform. Theory, 31: 469-472.

Eltahir, M.E., M.L.M. Kiah, B.B. Zaidan and A.A. Zaidan, 2009. High rate video streaming steganography. Proceedings of the 2009 International Conference on Future Computer and Communication, April 03-05, IEEE Computer Society, Kuala Lumpur, Malaysia, pp: 550-553.

Islam, R., A. Siddiqa, P. Uddin, A. Kumar and M.D. Hossain, 2014. An Efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography. Proceedings of the 2014 3rd International Conference on Informatics, Electronics and Vision (ICIEV), May 23-24, 2014, IEEE, Dhaka, Bangladesh, ISBN:978-1-4799-5179-6, pp: 1-6.

Koblitz, N., 1987. Elliptic curve cryptosystems. Math. Comput., 48: 203-209.

Manjunath, N. and S.G. Hiremath, 2015. Image and text steganography based on RSA and chaos cryptography algorithm with hash-LSB technique. Intl. J. Electr. Electron. Comput. Syst., 3: 5-9.

Miller, V.S., 1986. Use of Elliptic Curves in Cryptography. In: Advances in Cryptology, Williams, H.C. (Ed.). Springer, Berlin, Germany, ISBN:978-3-540-16463-0, pp: 417-426.

Rivest, R.L., A. Shamir and L. Adleman, 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM., 21: 120-126.

Roy, S. and P. Venkateswaran, 2014. Online payment system using steganography and visual cryptography. Proceedings of the 2014 International Conference on IEEE Students Electrical, Electronics and Computer Science (SCEECS), March 1-2, 2014, IEEE, Bhopal, India, ISBN:978-1-4799-2525-4, pp: 1-5.

Saleh, M.E., A.A. Aly and F.A. Omara, 2016. Data security using cryptography and steganography techniques. Intl. J. Adv. Comput. Sci. Appl., 7: 390-397.

Sheth, R.K. and R.M. Tank, 2015. Image steganography techniques. Intl. J. Comput. Eng. Sci., 1: 10-15.

Yadav, V., V. Ingale, A. Sapkal and G. Patil, 2014. Cryptographic steganography. Comput. Sci. Inf. Technol., 2014: 17-23.