ISSN: 1304-7981 Number:**12**, Year: **2016**, Pages:**170-177** **http://jnrs.gop.edu.tr**

Gaziosmanpasa University
Graduate School of
Natural and Applied Sciences
Journal of New Results in Science

Received: 15.05.2016
Accepted: 10.09.2016

Invited Editor: Mahmut Hekim
Area Editor: Cem Emeksiz

Information Encryption and Hiding into an Image by Steganography Methods to Improve Data Security

Sefa TUNÇER[a,1] (sefa.tuncer@bilecik.edu.tr)
Cihan KARAKUZU[a] (cihan.karakuzu@bilecik.edu.tr)

[a]*Bilecik Şeyh Edebali University, Faculty of Engineering, Computer Engineering, 11000 Bilecik*

Abstract – Nowadays, data security has become very important. A data can be hidden with a steganography technique into text, image, audio and video files. Steganography is used widely data security applications. But there are stegoanalysis methods that provide obtaining hidden data. To prevent this, steganography can be used with cryptography or different methods. Cryptography is not enough alone for data security sometimes. In this study, the information is encrypted and hidden because of it is important to prevent capture of information by undesirable persons. Firstly, plain text is encrypted with RSA encryption algorithm and then encrypted data is hidden into an image for data security in this study. Stego image consist of text and an image which is data hidden into an image. We show that how is hidden information and besides how visual difference is become on example images.

Keywords -
Image steganography, RSA encryption, Asymmetric encryption algorithm, Cryptography and steganography.

1. Introduction

Since ancient times, people have tried to ensure security of information by various methods. In information transfer, states and nations have played an important role in relation to each other. Information security is one of the most important factors in the world of computer sciences, too. Steganography enables safely transmission of secret information. It plays an important role in data communication because protecting information is difficult in the public network.

Steganography is a combination word of steganos (secret) and graph (writing) in Greek. It provides storage an information into other data such as text, video, audio, image [1]. This

[1]***Corresponding Author***

method aims to confidentiality of information existence. This means that, although existence of information is known, it is not simple find out the hidden message. The main requirement of steganography is that existence of information should not be realized. It can be achieved by a good steganography technique [2].

Cryptography is a mathematical method to provide information security. Thus, message can be easily encrypted. Information is encrypted using a key, then sent to the receiver. Learning of the key by any third person, it will greatly affect the security of data. Though the key is known, there are some methods that require a second key [3]. RSA is an asymmetric encryption method that used very large prime numbers. The size of currently used prime number is selected more than 100 digit for secure RSA encryption [4]. Generated the secret key corresponding to the public key is the most damaging attack to RSA algorithm [5]. Steganography and cryptography are different from each other. Firstly the existence of information must detect in steganography. The second problem is to obtain existing information [6]. We have an encrypted data in cryptography. The secret key is sufficient to decryption.

In this study, image steganography and RSA encryption algorithm are used together to make very difficult obtaining the hidden information. To do this, firstly data will be encrypted with RSA encryption algorithm, then cipher text will be hidden into an image. Thus, hidden data will obtain extremely difficult. Also encryption and data hiding are used to take measures against steganalysis methods. Improved implementations are available for capturing confidential data [7]. Embedding operation of encrypted text into an image is performed in two different ways. These methods are explained in the following section.

2. Information Encryption and Hiding into an Image

Plain text is information to be transmitted. It is encrypted by RSA cipher. Stego image is obtained after cipher text is hidden into an image. Encryption and hiding steps are shown in Figure 1.

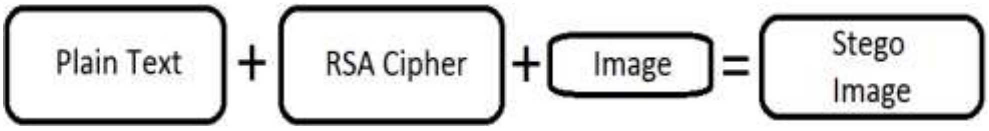

Figure 1. Information encryption and hiding steps.

2.1. RSA Cipher

RSA is the most popular asymmetric encryption method, it bases on algorithmic difficulty of factoring integers separation. Algorithm has become more difficult by choosing large prime numbers in the key generation process [5]. RSA algorithm consists of the following steps; key generation, encryption, decryption [5,8].

Two keys, public and secret; are generated in RSA. The public key is used to encrypt messages. If public key is learned without the secret key, any problem does not occur. Because messages can only be decrypted with the private key [9]. RSA transactions can be summarized as follow:

- The two prime numbers p and q are selected. Data security increases if these numbers are very large.
- Mode value is calculated for public and secret keys ($n = p.q$).
- $\vartheta(n) = (p-1)(q-1)$ totient is calculated.
- Produce an e integer in the interval of $1 < e < \vartheta(n)$. e and $\vartheta(n)$ numbers should be coprime [5,9].

e public key is disclosed after these transactions.

- $d.e = 1\, mod(\vartheta(n))$ number d is determined. d is the private key exponent and it is obtained with the extended Euclidean algorithm.
- Message is calculated as an reversible integer m. $(0 < m < n)$
- Encrypted message is calculated as $c = m^e mod(n)$. It is sent to the target point.
- After $m = c^d\, mod(n)$ is calculated to solve encrypted message, the inverse of m is the decrypted message [5,9].

The performance result of RSA algorithm is given according to p and q values and file size in Table 1 as an example.

Table 1. The RSA algorithm results.

Numeric values	Plain text (byte)	Encrypted text (byte)	Encryption time (second)

p = 439
q = 487
	10178	50217	0.244

	20356	100432	1.018
	40712	200862	5.401

p = 4327
q = 4567
	10178	57869	0.888

	20356	115736	2.144
	40712	230510	5.783

p = 9973
q = 9967
	10178	58745	1.614

	20356	120500	2.991
	40712	234862	8.172

2.2. Image Steganography

Information does not change during data communication and data integrity is provided in steganography [10]. Image steganography is method which hiding information into an image. On the other hand, RGB (Red, Green, Blue) values of pixels are change in image. Stego image includes both image and plain text (or cipher text) which is hidden data into. In this study, information is hidden into an image with two different methods. These methods are least significant bit and last significant 3 bits.

- The least significant bit method (LSB)

LSB method is the simplest approach to hiding information into an image. This method is done only by changing least significant bit of pixel values. Detection of changes by human eyes is almost impossible in the image, because of very small change occur in color tone

[11]. ASCII value of ‘A’ character is 01000001 in binary and other alphabetic characters have similar binary values, too. Because of this, we need 8 byte if we want to hide a character [12]. In this study, hiding operation is made for 24 bit (RGB) true color. Information hiding steps are as follows:

- ASCII values of encrypted text are obtained. Every letter of the text is translated from decimal to 8-bits binary system.
- RGB values of each pixel are determined in the image.
- 3 bits data is hidden into RGB value of each pixel. In this process, last bit of RGB values is changed.

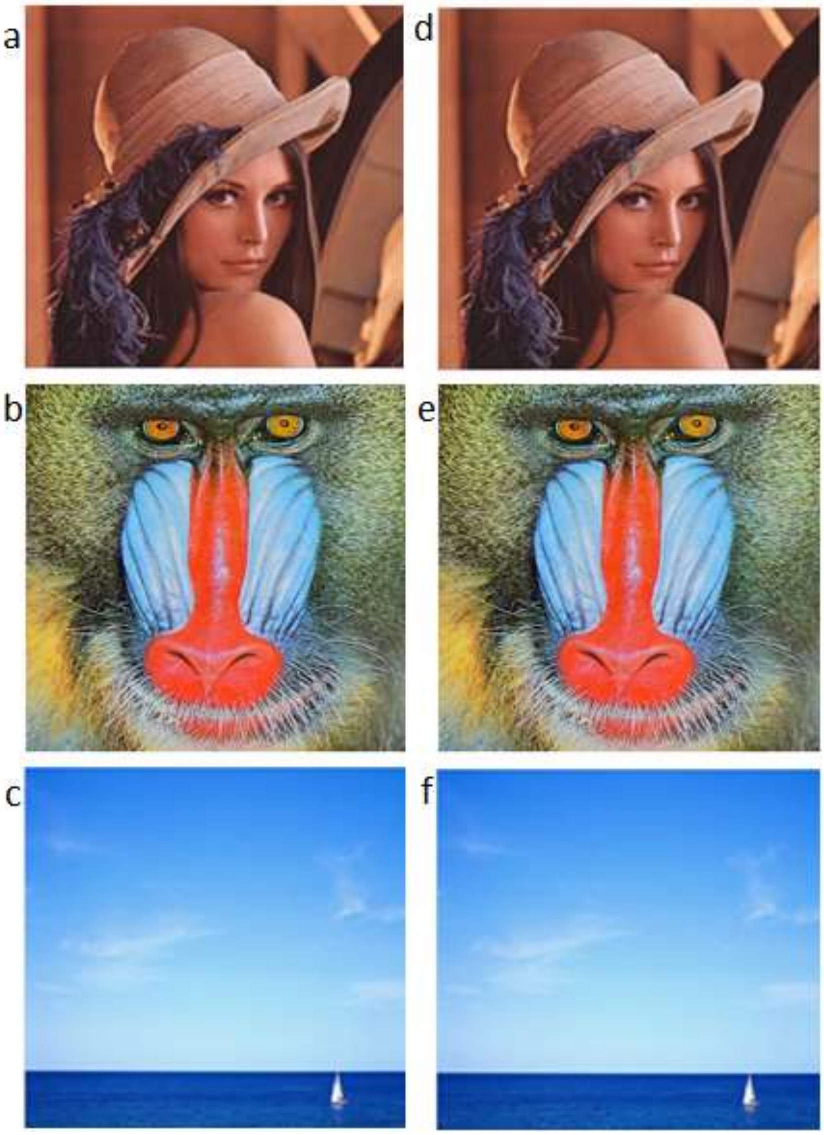

Figure 2. Lena, baboon, sky (a), (b), (c) Original images, (d), (e), (f) Stego images with LSB method.

Original images of Lena, baboon and sky are shown a, b, c and stego images of the mentioned images are shown d, e, f in Figure 2, respectively. The difference between original and stego images can not be seen by human eyes, it is almost impossible. Image color tone has not changed so much after the data hide by LSB method.

The following example can explain LSB data hiding. Red binary value of the first eight pixels and final status are shown in Table 2 after the hiding process, if data is selected as “01001001”.

Table 2. 8-bits data hiding in red value of pixels.

Pixel	Original image (Red value)	Stego image (Red value)
1	1111001**1**	1111001**0**
2	1001011**1**	1001011**1**
3	1001000**1**	1001000**0**
4	1001000**0**	1001000**0**
5	0001101**1**	0001101**1**
6	1001010**0**	1001010**0**
7	0001111**1**	0001111**0**
8	0001000**0**	0001000**1**

Last bits of *Stego image* column are bits of the data to be hide in Table 2, respectively. Data is also hidden to green and blue values of pixels respectively, after data hid to red values of all pixels. 512x512x3 bits data can be hidden inside of an image if you have an image size of 512x512. This means that approximately 98304 characters can be hidden.

- *The last significant 3 bits method (L3B)*

Aim of 3-bits data hiding is protection of data against attacks. Improved some attacks are available in order to obtain the data hidden on the LSB method. It will be more difficult obtaining data when we hide three bits. Information hiding steps are as follows:

- ASCII values of encrypted text are obtained. Every letter of the text translated from decimal to 8-bits binary system.
- RGB values of each pixel in the image are determined and it is converted from decimal to 8-bits binary. (The difference of LSB hiding)
- 9 bits data is hidden into RGB value of each pixel (3 bits data is hidden into each of red, green, blue values). In this process, last three bits of RGB values are changed.

The following example can explain L3B data hiding. Red binary value of first eight pixels and final status are shown in Table 3 after the hiding process, if data is selected as “000 110 010 100 101 001 000 111”.

Table 3. 24-bits data hiding in red value of pixels.

Pixel	Original image (Red value)	Stego image (Red value)
1	11110**011**	11110**000**
2	10010**111**	10010**110**
3	10010**001**	10010**010**
4	10010**000**	10010**100**
5	00011**011**	00011**101**
6	10010**100**	10010**001**
7	00011**111**	00011**000**
8	00010**000**	00010**111**

24-bits divided into three parts. Last three bits of *Stego image* column are the bits of hiding data in Table 3, respectively. Bit changes can be seen comparing *Original image* and *Stego* *image* columns in Table 3. Like LSB, data is hidden into green and blue values of pixels respectively, after the data is hidden to the red values of all pixels. 512x512x9 bits data can be hidden inside of an image if you have an image size of 512x512. This means that approximately 294912 characters can be hidden into the image.

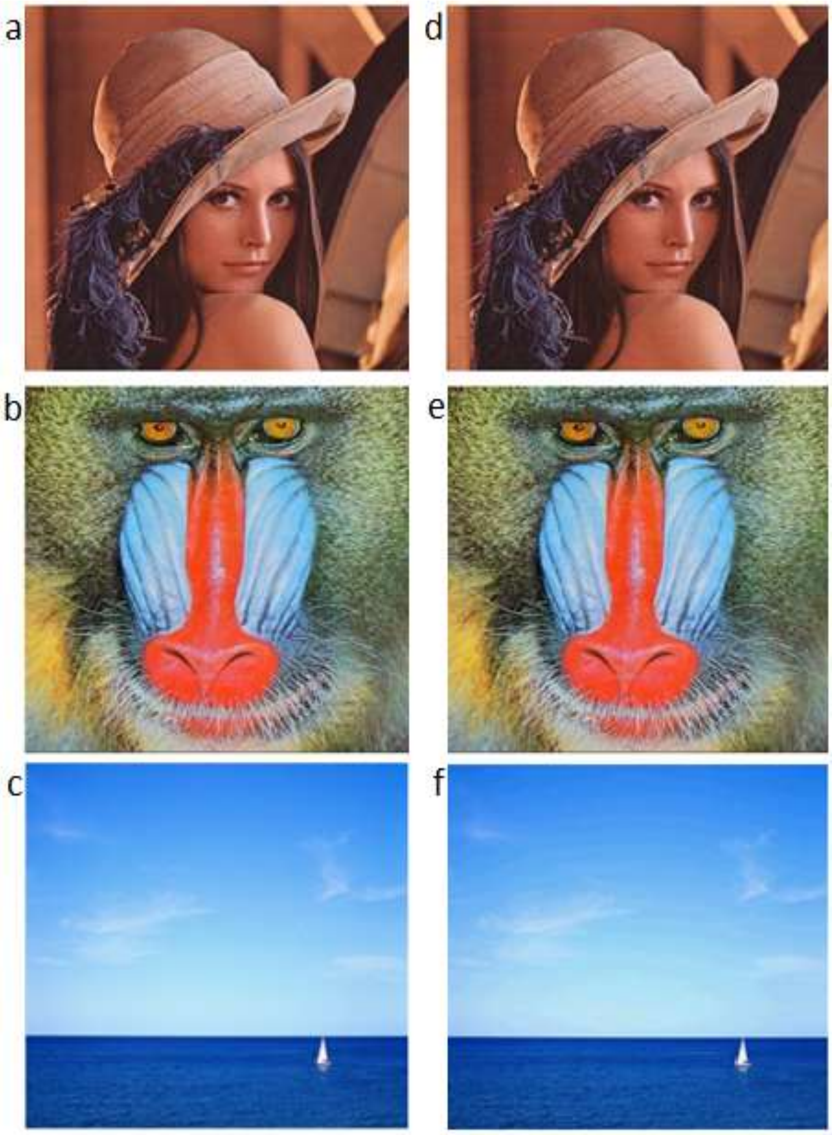

Figure 3. Lena, baboon, sky (a), (b), (c) Original images, (d), (e), (f) Stego images with L3B method.

Original images of Lena, baboon and sky are shown a, b, c and stego images of the mentioned images are shown d, e, f in Figure 3, respectively. Unlike LSB method, changes of image can see with human eye in L3B method. Compared to other images, change of color tone of the sky images (f) are seen conspicuously because of color intensity of sky the images (c) are less in Figure 3. In addition, the difference of color tone between original (b) and stego (e) baboon images cannot be easily felt.

3. Conclusions

Two different steganography methods are used and encrypted information with RSA is hidden into an image. In this way, data is transmitted and stored more safely. Information can be captured easily, if it is hidden directly into an image. In order to prevent this handicap, encrypted information is hidden into image after it is encrypted.

In the LSB method, the difference between original and stego image is too little because there is less increasing and decreasing or there is no changing (between 0-1) in pixel RGB decimal values varying between 0-255. Two images (original and stego) are almost identical to each other. Image pixel values are between 0-7 in L3B hiding method. For the given application of LSB and L3B hiding method, changing the decimal red values of the image are summarized in Table 4.

Table 4. Decimal values changing of RGB for the proposed LSB and L3B hiding methods.

Pixels	Original image (Red value)	LSB method		L3B method	
		Stego image (Red value)	Difference	Stego image (Red value)	Difference
1	243	242	1	240	3
2	151	151	0	150	1
3	145	144	1	146	1
4	144	144	0	148	4
5	25	25	0	27	2
6	148	148	0	145	3
7	31	30	1	24	7
8	16	17	1	23	7

As can be seen from the Table 4, decimal value changing of the related pixels is greater than the other in L3B method. Color tone difference of an image can be detected by human eyes if change of pixel value is greater than four. If it is four or less than four, changes are not able to realized. In addition, color tone difference occurs clearly if the change of pixels is more than seven.

As a result, we can say that it is difficult to know the existence of hidden data in LSB stego image but it is simpler to understand the existence of hidden data in L3B stego image, if we examine in appearance. Low color intensity must not be selected in the second method because we can simply realize in color change. Also known and widely used images should not be preferred. Important information can be protected with cryptography and steganography using the like presented methods here.

References

[1] M.R. Islam, A. Siddiqa, M.P. Uddin, A.K. Mandal, M.D. Hossain, *An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography*, Informatics, Electronics & Vision (ICIEV), DOI: 10.1109/ICIEV.2014.6850714.

[2] Q. Huang, W. Ouyang, *Protect fragile regions in steganography LSB embedding*, Knowledge Acquisition and Modelling (2010) 175-178.

[3] G. Singh, Supriya, *Modified vigenere encryption algorithm and its hybrid implementation with Base64 and AES*, Advanced Computing, Networking and Security (ADCONS) (2013) 232-237.

[4] J.M. Ahmed, Z.M. Ali, *The enhancement of computation technique by combining RSA and El-Gamal cryptosystems*, Electrical Engineering and Informatics, DOI: 10.1109/ICEEI.2011.6021779.

[5] T. Yerlikaya, E. Buluş, H.N. Buluş, *RSA şifreleme algoritmasının pollard RHO yöntemi ile kriptanalizi*, Kütahya Akademik Bilişim Konferansı, 2007.

[6] G.K. Selvi, L. Mariadhasan, K.L. Shunmuganathan, *Steganography using edge adaptive image*, Computing, Electronics and Electrical Technologies (ICCEET) (2012) 1023-1027.

[7] J. Guo, Y. Guo, L. Li, M. Li, *A universal JPEG image steganalysis method based on collaborative representation*, security, pattern analysis, and cybernetics (SPAC) (2014) 285-289.

[8] V. Nabiyev, A. Günay, *Şifreleme yönteminin tespiti amacıyla çeşitli şifreleme algoritmalarının araştırılması*, ISCTurkey Bilgi Güvenliği ve Kriptoloji Konferansı, 2006.

[9] E. Akyıldız, A. Doğanaksoy, E. Keyman, M. Uğuz, *Kriptolojiye giriş ders notları*, ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi Bölümü, 2004.

[10] K.T. Durai, G.S. Devi, *An analysis of LSB based image steganography techniques*, Computer Communications and Informatics International Conference, DOI: 10.1109/ICCCI.2014.6921751

[11] S.M. Masud Karim, M.S. Rahman, M.I. Hossain, *A new approach for LSB based image steganography using secret key*, Computer and Information Technology (ICCIT) (2011) 286-291.

[12] S. Dagar, *RGB based dual key image steganography*, Confluence 2013: The Next Generation Information Technology Summit (2013) 316-320.