International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-4, February 2019

FPGA Based RSA Authenticated Data Hiding in Image through Steganography

Sk. Sadiya Shireen, B. Murali Krishna, K. Naga Lakshmi Prasanna, A. Poorna Chander Reddy

Abstract*: Now-a-days, information security has a vital role in different applications of digital communications like medical, military, commerce etc., to conceal the secret data from unauthorized access. Steganography is the most eminent technique for providing information security with the help of a carrier file. The communication carrier can be of various formats like text, image, video etc. Among all these, digital images are the most common format due to high capacity and frequency of availability. In image steganography, the secret data is embedded into an inconspicuous carrier i.e., digital image is used as cover image to conceal the secret message which is known as stego image. Cryptography techniques are used to strengthen the security for the stego image. In this paper, a zigzag method has proposed for concealing patient's secret information with RSA cryptography algorithm in a RGB medical cover image. The medical cover image is implemented on Nexys 2 1200E FPGA (Field Programmable Gate Array).

***Index Terms*: Cryptography, RSA Algorithm, Steganography, RGB medical cover image, Stego image, FPGA**

I. INTRODUCTION

Now-a-days various medical systems are drifting in mobile and cloud environments. In telemedicine, the doctor examines the patient's data and medical images which are transmitted from remote places to promote immediate treatment [1], [2]. For secure transmission of information and medical images, certain parameters like authentication, integrity, confidentiality and availability are to be considered.

Encryption technology protects electronic patient records while they are being transferred and ensures that only intended recipients are able to view them. RSA (Ron Rivest, Adi Shamir & Leonard Adleman, 1996) algorithm is one of the asymmetric cryptography technique. It provides two keys known as public key and private key. Public key is distributed to all the users who are taking part in communication where as private key is known only to a particular user [3].

Steganography is a method of concealing information within another cover medium. The word steganography is originated from the two Greek words which are "steganos" means covered or protected and "graphie" means writing. Simply the equation for steganography can be given as 'Stego medium = Cover medium + Secret message'. Based on cover medium, there are various steganography techniques such as image steganography, text steganography, audio steganography, video steganography [4].

In this paper, a novel security system has been proposed by using RSA algorithm and steganography method. This approach can be understood from the following sections. In section III, a brief description of cryptography and RSA algorithm is discussed. In section IV, steganography and its types are discussed. In section V, the proposed methodology is discussed. The results are discussed in section VI and finally, the work is concluded in section VII.

II. LITERATURE REVIEW

Kamaldeep Joshi [5] proposed a new method for image steganography in spatial domain which extracts two LSBs and two MSBs of the selected pixel value. Then the XOR operation is performed on the first and last bit and second bit and seventh bit. Based on the result of these two XOR operations every bit of secret data is embedded one by one on LSB of selected pixel value. The experimental results show that this method can achieve maximum PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error) rate.

Ki-Hyun Jung and Kee-Young Yoo [6] proposed a new semi-reversible data hiding method that utilizes interpolation and the least significant substitution. Interpolation methods are used before hiding the secret data for a cover image. Later, the LSB substitution method is used to embed a large amount of secret data with very high visual quality.

Weiqi Luo, Fangjun Huang and Jiwu Huang [7] proposed an edge adaptive scheme and expanded the LSB matching revisited image steganography which can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image. When embedding rate increases, huge data can be concealed at the edges. From the experimental results, it is evaluated that visual quality and security of stego images are improved significantly when compared to typical LSB-based approaches.

Ammad Ul Islam, Faiza Khalid [8] proposed a novel image stegnography method which concentrates on MSB of image pixel. Bit no.5 is used to store the secret bits based on the difference of bit no. 5 and bit no.6 of cover image. MSB method is used to hide data rather than LSB due to two reasons i.e., the LSB method is the oldest method used for the embedding secret data into an image where the data is kept in the least significant bit of every pixel so that a little change in the image is observed and also the hackers mostly focus on LSB bits.

Manuscript published on 28 February 2019.
*Correspondence Author(s)
Sk. Sadiya Shireen, P.G Scholar, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P, India.
B. Murali Krishna, Assistant Professor, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P, India.
K. Naga Lakshmi Prasanna, P.G Scholar, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P, India.
A. Poorna Chander Reddy, P.G Scholar, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P, India.

The proposed technique is analyzed on factor like PSNR and found that it was efficient. Jarno, Mielikainen [9] proposed a steganographic method which allows embedding of the same amount of information into the stego image as LSB matching. In the LSB matching, the choice of addition or deletion of one from the cover image pixel is random and it can set a binary function of two cover pixels to the desired value. The embedding is performed using a pair of pixels as a unit, where the LSB of the first pixel carries one bit of information, and a function of the two pixel values carries another bit of information. The proposed method shows better performance than traditional LSB matching in terms of distortion and resistance against existing steganalysis.

V. M. Potdar and E. Chang [10] proposed a new grey level modification (GLM) steganography technique for secure information transmission. The principle behind this technique is to embed information by modifying the grey level values of the grey scale image pixels. Grey scale is a calibrated sequence of grey shades ranging from black to white with intermediate shades of grey. GLM steganography uses the concept of odd and even numbers to map data within an image. It is one-to-one mapping between the binary data and the selected pixels in an image. The grey level values of the pixels are examined and compared with the bit stream that is mapped in the image.

III. CRYPTOGRAPHY

Cryptography has a crucial role in existing technology because the communication is transmitted securely to the end users. It is especially very important in communicating personal information that is vulnerable to distortion. Cryptography word is derived from ancient Greek where “krypto” means hidden and “graphene” means writing. The plain text is encrypted into the cipher text in turn is decrypted back as shown in Fig. 1. This encryption & decryption is based on type of scheme used by a key. Two types of keys are involved in cryptography for encryption: Public key used for encryption and Private key used for decryption. Public key is distributed to all the users who are taking part in communication whereas the private key is known to only particular users. Depending on the usage of key, cryptography is mainly classified into

1. Symmetric key cryptography
2. Asymmetric key cryptography

Symmetric key cryptography is also known as secret key or private key. Secret key is a method where a single key is used for both encryption and decryption. Sender uses the key to convert the plain text to cipher text. Receiver applies the same key to recover the original message. Popular symmetric key techniques include AES, DES, blowfish etc.

Asymmetric key cryptography is also known as public key. In general Public Key Cryptography (PKC) has two keys that are mathematically related to each other. One key is used to convert plaintext to cipher text, and the inverse of the key is used to recover the data from cipher text. Popular asymmetric key techniques include RSA, ECC, Diffie-Hellman key exchange.

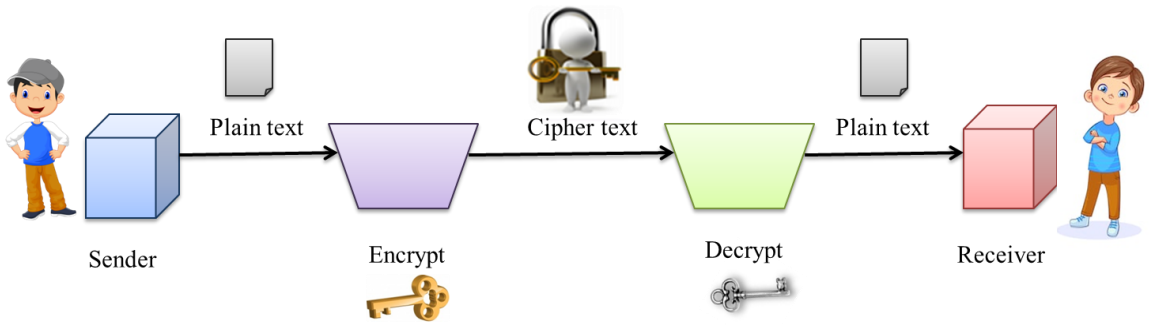

Fig. 1: Overview of Cryptography

A. *RSA Algorithm*

RSA algorithm is named after Ron Rivest, Adi Shamir and Len Adlemann, which was invented in the year 1977. It is also known as asymmetric cryptography. RSA algorithm is based on finding the factors of an integer (prime factors must be kept secret) [11]. Messages can be encrypted without the need of exchanging a secret key separately. Both sender and receiver must know the value of ‘N’. The public key ‘E’ is known to everyone and the value of private key ‘D’ is known only to the receiver. Thus, this is a public key encryption algorithm with a public key of $KU = \{E, N\}$ and a private key of $KR = \{D, N\}$. The RSA algorithm is classified into three components as Key generation, Encryption and Decryption which is explained below.

Key Generation:

i. Choose two different random prime numbers ‘P’ & ‘Q’.
ii. Compute modulus (N) for the public and private keys.
$$N = P * Q$$
iii. Calculate the totient function $\emptyset(N)$ as
$$\emptyset(N) = (P-1) * (Q-1)$$
iv. Choose an integer for public key ‘E’ such that $1<E<\emptyset(N)$ and ‘E’ is co-prime to $\emptyset(N)$ i.e., $GCD(E, \emptyset(N)) = 1$.
v. Compute private key ‘D’ which should satisfy congruence relation.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

$E*D\ mod\ \emptyset\ (N)$ =1(or)

$E*D = K*\emptyset\ (N)$ +1; K is an integer.

Encryption: Encryption is a process of converting the plain text into cipher text. The cipher 'C' can be obtained as $C = M^E\ mod\ N$ where 'M' is the message (Plain text), 'E' is the public key, 'N' is the modulus for both public and private key.

***Decryption*:** Decryption is a process of converting the cipher text into plain text. The message 'M' can be obtained as $M = C^D\ mod\ N$ where 'C' is the cipher, 'D' is the private key, 'N' is the product of two different prime numbers.

To avoid repeated binary multiplications for encryption and decryption it can be easily computed using XOR operation as discussed in section V.

IV. STEGANOGRAPHY

In olden days, various attempts are done to hide the secret message within a reliable media to deliver across the enemy territory. Herodotus sent secret messages using the concept of steganography. Greeks wrote their secret messages on wood and covered them with wax. Invisible ink was used during World War II period and the messages were written on the bald scalp of slaves and when the hair is grown on their head, they were sent as messengers. Steganography is a method of concealing information within another cover medium [12]. The word steganography is originated from the two Greek words which are "steganos" means covered or protected and "graphie" means writing.

Simply the equation for steganography can be given as 'Stego medium = Cover medium + Secret message' [13].

Steganography techniques can be applied to images, a video file or an audio file. At any rate, steganography protects from pirating copyrighted materials as well as aiding in unauthorized viewing.

V.PROPOSED METHOD

Image steganography is the most eminent method for concealing the information inside an image file known as cover image [14]. There are many types of images like gray scale images, RGB images etc. In RGB images, each pixel consists of three components like R, G, B and each component has the intensity levels ranging from 0 to 255. The proposed method considers a RGB image with 'R', 'G' as 3 bit component and 'B' as 2 bit component and embedded the patient's secret information into the cover image in zigzag manner (as shown in Fig. 2 and 3) which can be illustrated from the following steps.

Step-1: Consider a RGB medical cover image and convert it into binary text file by using MATLAB R2016a tool.

Step-2: The patient's secret information is encrypted with the help of an asymmetric cryptography technique i.e., RSA algorithm which is described below.

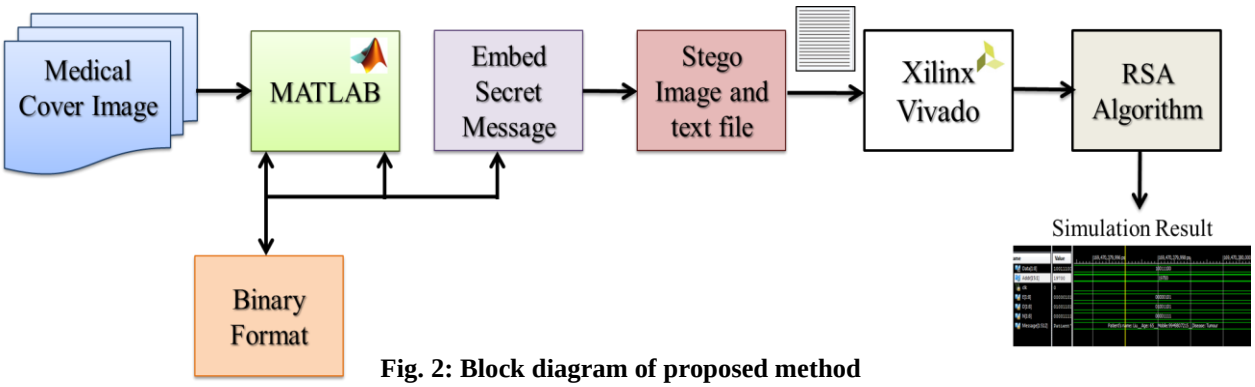

Fig. 2: Block diagram of proposed method

(a) Compute modulus (N) for the public and private keys.

$N = P * Q$; N= 3 * 5 = 15

(b) Calculate the totient function $\emptyset\ (N)$ as

$\emptyset\ (N) = (P-1) * (Q-1)$

$\emptyset\ (N)$ = (3-1) * (5-1) = (2) * (4) = 8

(c) Choose an integer for public key 'E' such that $1<E<\emptyset\ (N)$ and 'E' is co-prime to $\emptyset\ (N)$ i.e., $GCD\ (E, \emptyset\ (N))$ = 1. So the selected public key is 'E' = 5.

(d) Compute private key 'D' which should satisfy congruence relation.

$E*D\ mod\ \emptyset\ (N)$ =1 (or) $E*D = K*\emptyset\ (N) + 1$, where K is an integer. For K = 48 the private key is given as 'D' = 77.

(e) Perform encryption using public key to obtain cipher 'C'.

Step-3: The encrypted secret message is embedded in Zigzag position of the pixels (as shown in Fig. 2) in cover image binary text file which is known as stego binary file and corresponding image is known as stego image.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Message bits	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8
Pixels	1	0	1	0	1	0	1	0

Embedding the Secret Information in Pixels							
M_1	0	1	0	1	0	1	0
1	M_2	1	0	1	0	1	0
1	0	M_3	0	1	0	1	0
1	0	1	M_4	1	0	1	0
1	0	1	0	M_5	0	1	0
1	0	1	0	1	M_6	1	0
1	0	1	0	1	0	M_7	0
1	0	1	0	1	0	1	M_8
1	0	1	0	1	0	M_7	0
1	0	1	0	1	M_6	1	0
1	0	1	0	M_5	0	1	0
1	0	1	M_4	1	0	1	0
1	0	M_3	0	1	0	1	0
1	M_2	1	0	1	0	1	0
M_1	0	1	0	1	0	1	0

Fig. 3: Embedding Patient's Secret Information

VI. RESULT & ANALYSIS

In this section, a vivid analysis of the simulation results has been explained. The Fig. 5 shows the binary text file of RGB medical cover image (Fig. 4 (a))which consists of 8 bits for every pixel i.e. R component with 3 bits, G component with 3 bits and B component with 2 bits. In that text file, the secret information is embedded in zigzag manner. The corresponding medical cover images, stego images and their respective histograms are shown in Fig. 4 using MATLAB tool.

Xilinx simulation result shown in Fig. 6 consists of data, address of every pixel, public key (E), private key (D), modulus of public and private key (N), decrypted message. The Fig. 7 shows the hardware implementation of stego image [15] which is implemented on Nexys2 1200E board. The table I shows that the resulting comparison of proposed method and the existing methods like LSB, MSB embedding [5], [8], [16].

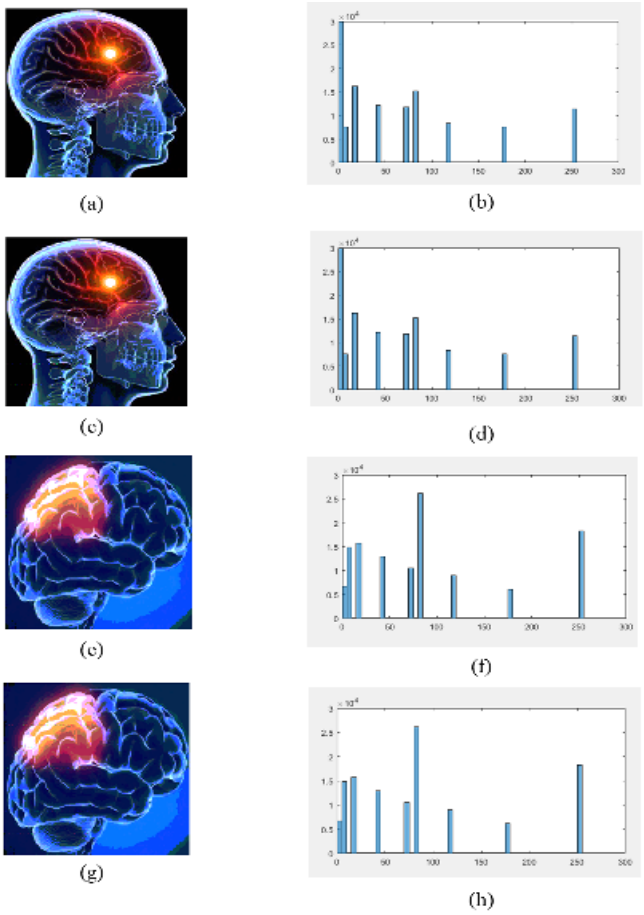

Fig. 4: (a), (e) represents medical cover images and (c), (g) represents their stego images respectively; (b), (d) represents histograms of medical cover images and (g), (h) represents histograms of their stego images respectively

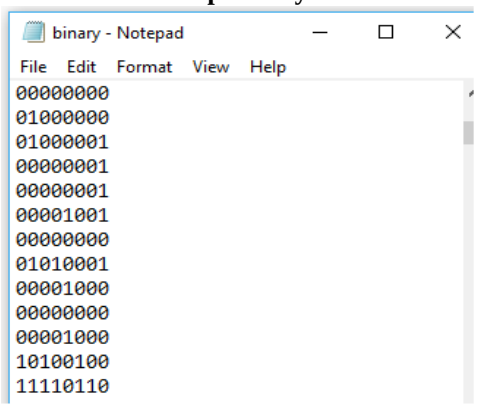

Fig. 5: Binary conversion of medical cover image (Fig. 4 (a))

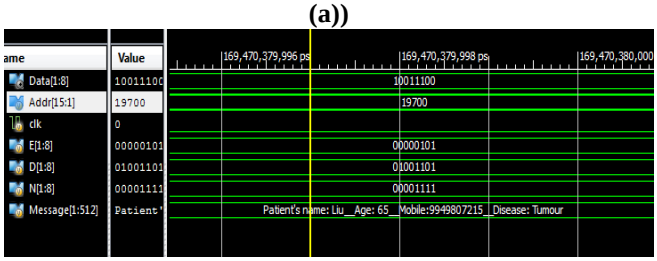

Fig. 6: Simulation Result of Decrypted Message

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

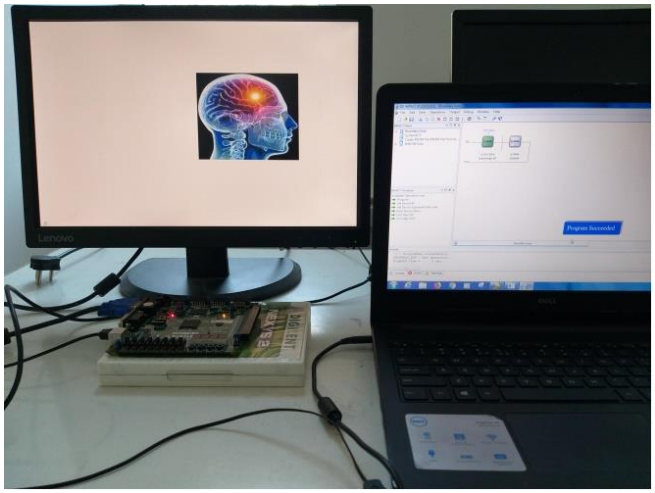

Fig. 6: Hardware implementation of stego image

Table I Comparison with other methods of steganography

Research Article	Method	Security	Encryption
Kamal joshi [5]	LSB	Less secure (Most of the hackers will focus on LSB)	Single layer of encryption
Ammad Islam [8]	MSB	Better secure	Single layer of encryption
Rajkumar Yadav [16]	LSB-S	Better secure	Steganography along with RSA
Proposed method	Zigzag	More secure (Difficult to hack the data)	Steganography along with RSA

VII. CONCLUSION

In this paper, the proposed method uses RSA algorithm to provide encryption for patient's secret medical data in a stego image. At steganography level, a new method is proposed to conceal the data from unauthorized persons. The amalgamation of both cryptography and steganography provides high complexity of encryption which is very high to break the system. Different medical cover, stego images and their respective histograms are generated in MATLAB tool and the medical cover image is implemented on Nexys 2 1200E FPGA technology. The above analysis concluded that the proposed method is better as compared to others.

REFERENCES

1. 'Privacy , Confidentiality : and Electronic Medical Records Abstract The enchanced Goals of Informantional Security In Health Care', 1996.
2. 'Summary of the HIPAA Security Rule', pp. 1–8, 2019.
3. M. E. Hellman, 'M. E. Hellman, "An Overview of Public Key Cryptography," IEEE Commun. Mag ., vol. 16, no. 6, May 2002, pp. 42–49.', no. 6, pp. 42–49, 2002.
4. J. Gupta, 'A Review on Steganography techniques and methods', vol. 1, no. 1, pp. 1–4, 2015.
5. K. Joshi, P. Dhankhar, and R. Yadav, 'A new image steganography method in spatial domain using XOR', in *12th IEEE International Conference Electronics, Energy, Environment, Communication, Computer, Control: (E3-C3), INDICON 2015*, 2016.
6. K. H. Jung and K. Y. Yoo, 'Steganographic method based on interpolation and LSB substitution of digital images', *Multimed. Tools Appl.*, 2015.
7. F. Huang, Y. Zhong, and J. Huang, 'Improved algorithm of edge adaptive image steganography based on LSB matching revisited algorithm', *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8389 LNCS, no. 2, pp. 19–31, 2014.
8. C. G. Tappe and A. V Deorankar, 'An Improved Image Steganography Technique based on LSB', *Int.Res. J. Eng. Technol.*, pp. 2395–56, 2017.
9. J. Mielikainen, 'LSB matching revisited', *IEEE Signal Process. Lett.*, vol. 13, no. 5, pp. 285–287, 2006.
10. V. M. Potdar and E. Chang, 'Grey level modification steganography for secret communication', Ind. Informatics, 2004. INDIN '04. 2004 2nd IE, no. June, pp. 223–228, 2004.
11. D. George, 'RSA Encryption System Using Encoded Multiplier and Vedic Mathematics', pp. 19–22, 2013.
12. F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, 'Information Hiding — A Survey', vol. 87, no. July, pp. 1062–1078, 1999.
13. Y. P. Astuti, D. R. Ignatius, M. Setiadi, E. H. Rachmawanto, and C. A. Sari, 'Simple and Secure Image Steganography using LSB and Triple
14. XOR Operation on MSB', pp. 191–195, 2018.
15. M. Jain and S. K. Lenka, 'Diagonal queue medical image steganography with Rabin cryptosystem', *Brain Informatics*, vol. 3, no. 1, pp. 39–51, 2016.
16. S. Debnath, M. Kalita, and S. Majumder, 'A review on hardware implementation of steganography', *Proc. 2nd Int. Conf. 2017 Devices Integr. Circuit, DevIC 2017*, pp. 149–152, 2017.
17. K. Joshi and R.Yadav, 'A new LSB-S image steganography method blend with cryptography for secure communication', Proc. 2015 3rd Int. conf. image Inf. Process. ICIIP.2015,pp-86-90, 2016.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)