Improvisation of Security aspect of Steganographic System by applying RSA Algorithm

*Manoj Kumar Ramaiya
Research Scholar, Computer Engineering
Suresh Gyan Vihar University
Jaipur, India

**Dr. Dinesh Goyal
Professor & Principal, School of Engineering
Suresh Gyan Vihar University
Jaipur, India

Dr. Naveen Hemrajani
Professor & Head, Computer Engineering
JECRC University
Jaipur, India

***Abstract*—The applications accessing multimedia systems and content over the internet have grown extremely in the earlier few years. Moreover, several end users or intruders can simply use tools to synthesize and modify valuable information. The safety of information over unsafe communication channel has constantly been a primary concern in the consideration of researchers. It became one of the most important problems for information technology and essential to safeguard this valuable information during transmission. It is also important to determine where and how such a multimedia file is confidential. Thus, a need exists for emerging technology that helps to defend the integrity of information and protected the intellectual property privileges of owners. Various approaches are coming up to safeguard the data from unauthorized person.**

Steganography and Cryptography are two different techniques for security data over communication network. The primary purpose of Cryptography is to create message concept unintelligible or ciphertext might produce suspicious in the mind of opponents. On the other hand, Steganography implant secrete message in to a cover media and hides its existence. As a normal practice, data embedding is employed in communication, image, text or multimedia contents for the purpose of copyright, authentication and digital signature etc.

Both techniques provides the sufficient degree of security but are vulnerable to intruder's attacks when used over unsecure communication channel. Attempt to combines the two techniques i.e. Cryptography and Steganography, did results in security improvement. The existing steganographic algorithms primarily focus on embedding approach with less attention to pre-processing of data which offer flexibility, robustness and high security level. Our proposed model is based on Public key cryptosystem or RSA algorithms in which RSA algorithm is used for message encryption in encoding function and the resultant encrypted image is hidden into cover image employing Least Significant Bit (LSB) embedding method.

Keywords—Image Steganography; Cryptography; LSB insertion; Public key Cryptosystem; RSA algorithm

I. INTRODUCTION

While in multimedia communications, the need of privacy and confidentiality gains more and more significance, mostly in open networks like the Internet. In the era of worldwide electronic connectivity, of viruses and hackers, of electronic eavesdropping and electronic fraud, there is indeed a need to protect information from passing before curious eyes or, more importantly from falling into wrong hands. Thus, multimedia security is much to consider in distributing digital information safely.

The past three or four decade led to the wide spread transfer of data from one end to the other end of the world. The remarkable evolution of the internet also evolved and eased various E- Commerce applications. This demand the assurance of security of information. Further the communication between private parties demanding absolute privacy also necessitate the data transmission in modified or encoded mode.

In multimedia communication the necessity of privacy and confidentiality gains additional importance mainly in open, unsecure communication network like internet. Present era of universal connectivity, of viruses, intruders, eavesdropping and digital fraud need to safe-guard information from releasing into erroneous hand.

Cryptography techniques [5, 6] scramble a source message in to unintelligible form so it cannot be understood while steganography hides the message in to other media, so it cannot be perceived. The term steganography [2, 3] originates from the Greek Steganos which means "covered" and Grafia means "writing" i.e. Steganography means "covered writing "[4].

Cryptography and Steganography are extensively used in the field of information hiding [1] and has received attention from the businesses and academic world in the past. Former conceals the original data but latter conceal the very fact that data is hidden.

Public Key Cryptosystem

A different concept of achieving the same results as from digital signature [11, 12] and steganography is the asymmetric key crypto system [7, 10] using two key termed as public key and private key. In symmetric encryption, the key need to be communicated before at both senders and receiver. Also to make the digital authentication look analog to the current practice some sort of identification like signature need to be inserted. To fulfill the above requirements Diffie and Hellman proposed the most widely accepted and implemented principle in 1976 termed as Public Key Cryptosystem [8, 9].

In contrast to symmetric key encryption, asymmetric key cryptosystem employ one key for encryption and different but related key for decryption. To fulfill the security requirement the approach need to have the following characteristics:

* First Author ** Corresponding Author

1) The cryptographic algorithm be such that it is infeasible to find the decryption key if only the encryption key and cryptographic algorithm is available.

2) Either of key pair (two related keys) can be used for encryption and the other used for decryption.

Fig. 1. Basic Model of Public key Cryptosystem

The process of encryption be as follows:

1) Each user generate a pair of keys for the encryption and decryption of the massage.

2) Each user place one of the two key in public or in open domain, accessible to all. This key is termed the public key. On the other hand, the companion key is kept private with each of them, and is termed the private key.

The messages from A are encrypted using the B's public key. On receiving the message, B decrypt using his private key. Since the private key of B has been generated and kept safe by B himself, the message remains secure.

Here the private keys have been generated by each locally and never transmitted nor distributed, thus remains protected and secrete, and hence providing the requirement of security

The rest of the paper is organized as follows. Section 2, literature surveyed dealt with techniques involving purely combination of cryptographic method or steganography methods. Section 3 proposed highly secured system which combines both cryptography and steganography techniques in order to provide higher payload, more robust and secure. In Section 4, the proposed hybrid techniques were tested on various standard images set namely Cameraman, Lena and Baboon etc. The PSNR (Peak Signal to Noise Ratio) value, to evaluating the quality of reproduced image (cover image and stego image) qualitatively. Finally, Section 5 concludes this paper.

II. The Related Work

Considering the strength and weakness of steganography and cryptography, researchers tried to combining them in practice, so that the new method would simultaneously possess the advantages of steganography and cryptography while overcoming the respective shortcomings.

The literature surveyed dealt with techniques involving purely cryptographic method or steganography methods. Both of the techniques have shortcoming from the view point of a degree of security and robustness against attacks and efficiency and ease of implementation in terms of hardware and runtime.

Attempt to combines two techniques [21, 22] to ensure more secure encoding have been made. In the most of the cases, techniques involved works on plaintext and very rare attempt have been made to encode images.

The major techniques comprises cryptography and steganography detailed in the literature can be broadly be classified into five categories, four being in the special domain while others one encrypt in the transform domain. They are as follows:

1) Idea employing the two techniques in tandem. Shouchao Song et Al [15] suggested a protocol merging cryptography and steganography techniques based on LSB matching method and well developed Boolean function in stream cipher. The protocol accomplishes the encryption and hiding all at once resulting in less computation them all the existing methods. The LSB method is used for hiding the encrypted message in cover image.

2) Text encryption with Data Encryption Standard (DES) and LSB insertion Dhawal Seth et Al [14] combines cryptography and steganography, so as to ensure more security over insecure communication channel. DES cryptographic algorithm being used for encrypting the text message in conjunction with LSB substitution for embedding the encrypted message in the cover image.

3) The techniques proposes compressing the signal before encrypting and employing steganographic techniques. It also proposed use of hash function so as to generate a message authentication code by hashing the key. The resulting model is claimed to survive image manipulation and attacks. Khalil Challita and Hikmat Farhat [16] proposed multiple encryption. Embedding the encrypted text secret message in more than one cover objects.

4) For a highly secure communication Ankit Uppal et Al [17] proposed dual security method by combining the RC5 enhance algorithm for encrypting and JPEG LSB coding for steganography.

5) The techniques proposed by Dipti Kapoor Sarmah and Neha Bajpai [13] apply Advance Encryption Standard (AES) encryption techniques for secrete message. The encrypted message is embedded in the Discrete Coeficint Transform (DCT) of the cover image. The DCT of image is obtained and the coefficient is embedding in the image.

The slight variant in the combined techniques is proposed by Pye Pye Aung and Tun Min Naing [18], using the same AES algorithm for encryption. In the steganographic a part of encrypted message as a key is used to hide in DCT of a cover image.

III. Proposed Hybrid Model

Proposed steganographic model is based on RSA Algorithms is depicted in figure 2.

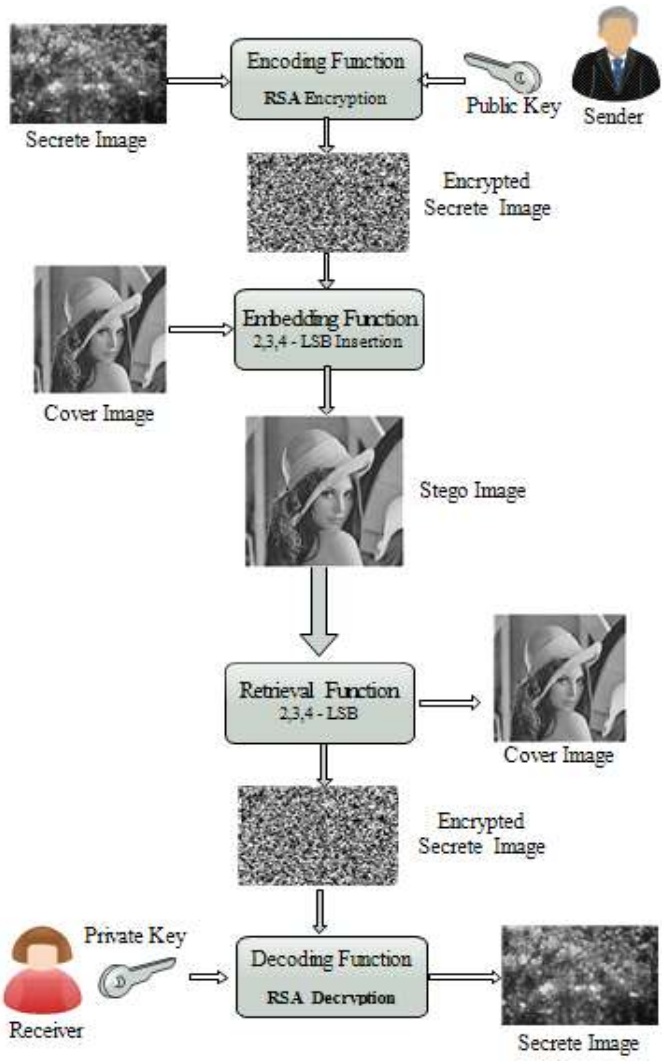

Fig. 2. Proposed Steganographic Model

A. RSA Encoding Function

First the secrete image is selected (e.g. of 256 × 256). The intensity value of each pixel of secrete image are converted from binary to decimal value. Now the first pixel values from secrete image is inputted to RSA encoding function as described below.

The RSA algorithm [22, 23] is implemented to encrypt input pixel value as follows:

1) Two prime number p and q are chosen such that they are the prime numbers.

2) $n = p \times q$ is calculated and made available to public.

3) e is chosen such that gcd $(\varphi(n), e) = 1$; $1 < e < \varphi(n)$ made public.

4) d is private and calculated as $d = e^{-1} \varphi(n)$.

Then the private key pair is (d ,n) and public key pair is (e ,n) .

The equivalent cipher value for first pixel is now calculated by using public key pair (e ,n)

$$C = M^{e} \bmod n$$

After the execution of RSA, first pixel value is now encrypted and this value are placed at first position by again convert it into decimal value. Now taking second pixel value convert it into decimal and inputted to RSA encoding function getting the second pixel encrypted value, likewise sequentially take pixel one by one, input to encoding function and obtain encrypted value of encrypted image.

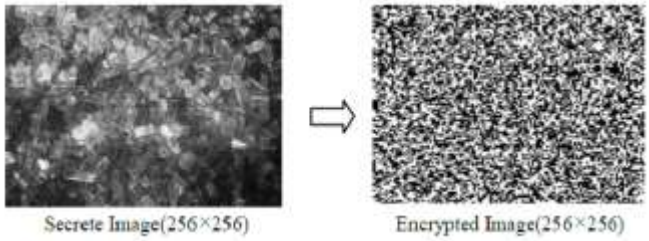

Fig. 3. Conversion of Secrete Image to Encrypted Secrete Image

B. Embedding Function using LSB Method

1) Bit Division: Taking the cipher encrypted image, the values are converted from decimal to binary.

The binary value of $(173)_{10} = (1\ 0\ 1\ 0\ 1\ 1\ 0\ 1)_2$

Next divide this 8 bit value into 4 part taking 2 bits in each. After bit division, value of b1 = 1 0 , b2 = 1 0 , b3 = 1 1 , b4 = 0 1 are getting.

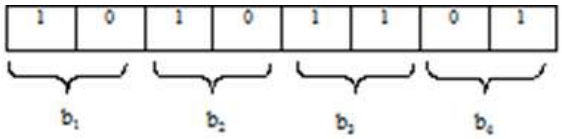

Fig. 4. Bit Division for LSB Embedding

2) Insertion of Bit value into the cover image: After receiving the values of b1, b2, b3, b4, these values are inserted into the cover image. The 2 bit LSB of the four consecutive pixels in cover image are replace. Taking the pixels one by one from the cover image, the 2 LSB bits are replaced by 10,10,11,01 respectively.

3) Formation of Stego Image: After receiving the new pixel value the stego image is formed by replacing these values at their original position. Likewise the pixels value one by one from encrypted secrete image and insertion into the cover image and replaced them. Result becomes the stego image.

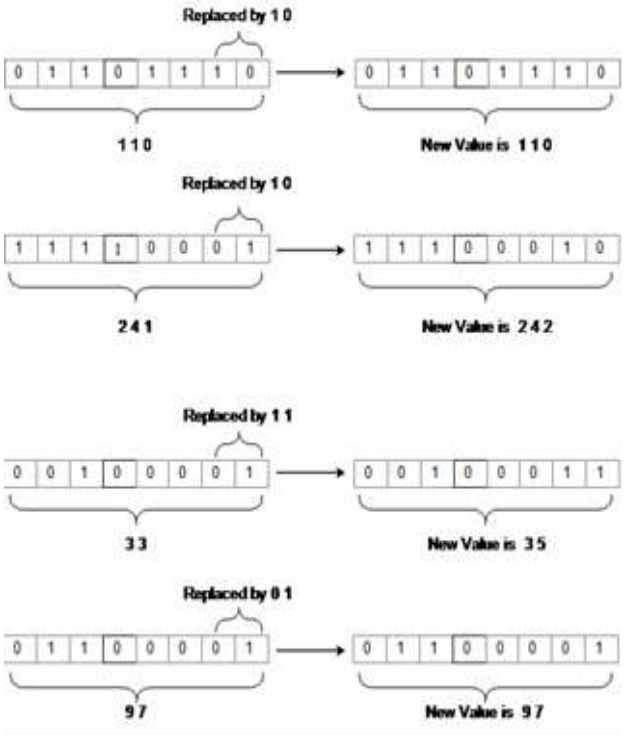

Fig. 5. Insertion of Bits into cover Image

C. Image Retrieval function

At the receiving end, decoding of stego image perform the following process:

1) Generate the 2 LSB bits from the stego Image: The pixels value are handled one by one from the stego image. Convert these pixel value from decimal to binary values and take 2 LSB bits from first four consecutive pixel values:

Similarly taking next three pixels. i.e. 242, 35, 97;

$(242)_{10}$ = $(1\ 1\ 1\ 1\ 0\ 0\ 1\ 0)_2$
$(35)_{10}$ = $(0\ 0\ 1\ 0\ 0\ 0\ 1\ 1)_2$
$(97)_{10}$ = $(0\ 1\ 1\ 0\ 0\ 0\ 0\ 1)_2$

Getting,

$b_1 = 1\ 0$; $b_2 = 1\ 0$; $b_3 = 1\ 1$; $b_4 = 0\ 1$;

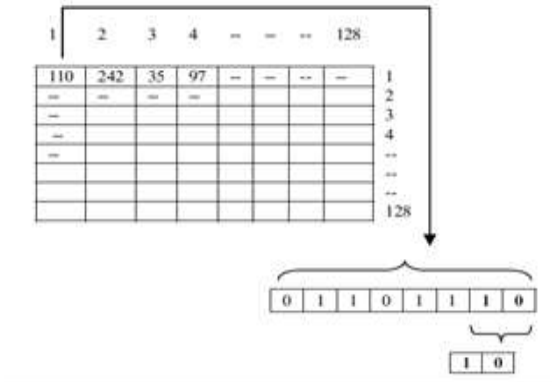

Fig. 6. LSB (2- bits) Extraction of Stego Image

2) Concatenation of bits: Now concatenating the input, the 8 bits of first pixel value of encrypted secrete image is acquired as

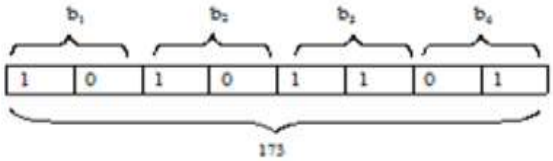

Fig. 7. Concatenation of Bits (Extracted)

3) Reformation of Encrypted Secrete Image: Now the generated value is placed into first position. Similarly taking the next four pixel value from stego image, the process is repetitive and the whole encrypted secrete image is recovered.

D. RSA Decoding Function

1) Creation of Secrete image: In decoding function the pixel value from the encrypted secrete image are again inputted to the RSA decoding function by using private key pair (d,n) to obtain pixel value of original secrete image as follows:

$M = C^d \bmod n$

After execution of decoding function for every pixel, the secrete image or original image is created.

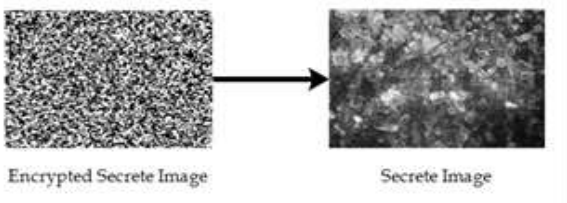

Fig. 8. Conversion of Encrypted Secrete Image to Secrete Image

IV. Results and Analysis

Proposed model using RSA algorithm is robust Steganography technique because without knowing the receiver secrete keys the extraction of secrete image from the stego image is impossible. Here the private keys have been generated by each user locally and never transmitted nor distributed via any transmission media , thus key remains protected and secrete, and hence system providing the requirement of security and authentication. Furthermore in embedding process quality of cover image is also not degrading due to variation in two LSB of each pixel which replicates only 0 – 3 difference in pixel value.

Moreover the proposed system is capable of not just scrambling data but it also changes the intensity of the pixels which contributes to the safety of the encryption.

TABLE I. Capacity and PSNR

Name of Image	Size (Pixel)	Capacity	PSNR In DB
Baboon.jpg	256× 256	25 %	44.23
Cameraman.jpg	256×2564	25 %	44.86
Lena.jpg	256× 256	25 %	44.48
pirate_gray.jpg	256× 256	25 %	44.36

V. CONCLUSION

In the proposed RSA based steganographic model is more secure as compare to the traditionally symmetric cryptosystem because in public key cryptosystem the private keys have been generated by each user locally and never transmitted nor distributed, thus no question of stealing or discloser of key, improves image quality and security compare to existing systems. Steganography, especially combined with the cryptography is a powerful tool which enables to communicate safely with the little computational overload in the system

REFERENCES

[1] N.F. Johnson, S. Jajodia, Exploring steganography: seeing the unseen, IEEE Computer 31 (2) (1998) pp.26–34.

[2] Ross J. Anderson, Fabien A.P. Petitcolas , "On The Limits of Steganography ", IEEE Journal of Selected Areas in Communications, 16(4):474-481, May 1998.

[3] N. Provos, P. Honeyman, "Hide and Seek: an Introduction to Steganography", IEEE Security and Privacy 1 (3) (2003) 32–44.

[4] J.C.Judge, "Steganography: past, present, future", SANS Institute publication, /http://www.sans.org/reading_room/whitepapers/stenganography/552.phpS, 2001.

[5] Lt. James Caldwell ,U.S. Air Force , "Steganography " , CROSSTALK The Journal of Defense Software Engineering , June 2003 , pp. 25 – 27 .

[6] N. Provos, P. Honeyman, "Hide and Seek: an Introduction to Steganography", IEEE Security and Privacy 1 (3) (2003) 32–44.

[7] Mohammed AbuTaha, Mousa Farajallah, Radwan Tahboub, Mohammad Odeh, "Survey Paper: Cryptography Is the Science of Information Security ", International Journal of Computer Science and Security (IJCSS), Volume (5): Issue (3): 2011, pp. 298 – 309.

[8] James L. Massey, "An Introduction to Contemporary Cryptology ", Proceedings of the IEEE, VOL. 76, NO. 5, MAY 1988, pp. 543 – 549.

[9] Alexander W. Dent, "Choosing key sizes for cryptography ", Information Security Technical Report, Vol. 15 No 1, 2010 Elsevier, pp. 21-27.

[10] Amin Daneshmand Malayeri , Jalal Abdollahi , "Modern Symmetric Cryptography methodologies and its applications " , IEEE Transactions On Information Theory, Vol. 97, No. 6, October 2009 , pp. 505 -509.

[11] Anthony T.S. Ho, Siu-Chung Tam, Kok-Beng Neo, Sim-Peng Thia , "Digital Steganography for Information Security", Internet Business99, 1999 - researchgate.net , pp. 1-9.

[12] Christoph Busch, Klara Nahrstedt, Ioannis Pitas, "Image Security", IEEE Jan – Feb 1999, pp. 16.

[13] Dipti Kapoor Sarmah, Neha Bajpai," Proposed System for Data Hiding Using Cryptographyand Steganography", International Journal of Computer Applications (0975 – 8887) Volume 8– No.9, October 2010, pp. 7- 10.

[14] Dhawal Seth, L. Ramanathan, Abhishek Pandey, "Security Enhancement: Combining Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887) Volume 9– No.11, November 2010, pp. 3-6.

[15] Shouchao Song, Jie Zhang, Xin Liao, Jiao Du, Qiaoyan Wen," A Novel Secure Communication Protocol Combining Steganography and Cryptography", Advanced in Control Engineering and Information Science , Procedia Engineering 15 (2011) , pp. 2767 – 2772

[16] Khalil Challita, Hikmat Farhat," Combining Steganography and Cryptography: New Directions", International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(1): pp.199-208.

[17] Ankit Uppal, Rajni Sehgal, Renuka Ngapal, Aakash Gupta, "Merging Cryptography& Steganography Combination of Cryptography: Rc6 Enhanced Ciphering and Steganography: JPEG ", International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-2, Issue-10, Oct.-2014, pp. 85-87.

[18] Pye Pye Aung, Tun Min Naing,"A Novel Secure Combination Technique of Steganography and Cryptography ", International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No. 1, February 2014. Pp 55-62.

[19] Vijay Kumar Sharma, Vishal Shrivastava ," A Steganography Algorithm For Hiding Image In Image By Improved Lsb Substitution By Minimize Detection " , Journal of Theoretical and Applied Information Technology 15th February 2012. Vol. 36 No.1 © 2005 - 2012 JATIT & LLS. All rights reserved.

[20] Abhinav Gupta, Anurag Pandey, Himanshu Agarwal," Analysis on Comparison of Cryptography and Steganography over an Open Channel", MIT International Journal of Computer Science and Information Technology, Vol. 5, No. 1, January 2015, pp. 8-12

[21] Z. V. Patel, S. A. Gadhiya," A Survey Paper on Steganography and Cryptography ", RESEARCH HUB – International Multidisciplinary Research Journal (RHIMRJ), Volume-2, Issue-5, May-2015 .

[22] Tan, Wenxue, Wang,Xiping , Xi, Jinju , Pan,Meisen , "A mechanism of quantitating the security strength of RSA key " , Third IEEE International Symposium on Electronic Commerce and Security 2010 , pp. 357- 361.

[23] Rajan.S.Jamgekar, Geeta Shantanu Joshi, "File Encryption and Decryption Using Secure RSA", International Journal of Emerging science and Engineering (IJESE) ISSN: 2319–6378, Volume-1, Issue-4, February 2013, pp. 11-14.