An Amended RSA Algorithm for Secure Communication

Nisha P.Shetty
Department of Information and Communication Technology
Manipal Institute of Technology, Manipal-576104, Karnataka, India
Email-nisha.pshetty@manipal.edu

Abstract- One of the foremost challenges faced while communicating in this digitized world is security. The need for legitimate and accredited information exchange is so great that it has become one among the major research areas today. This paper presents a three layer security model which expedites a safe and sound information exchange between the end users. The message from the sender is first scrambled using RSA algorithm and the cipher text is cloaked within an image. The correct Stego-image is shared with the receiver only if he answers the previously shared (only between sender and receiver; undisclosed to others) question correctly. The receiver first gleans the cipher text from the Stego-image and thenceforth proceeds to crack the extracted cipher text to obtain the original message.

Keywords – Steganography, RSA, Encryption, Cipher, Stego-Image

I. INTRODUCTION

In this era of Internet, where many people rely on online sector for their day to day deeds, ranging from banking to simple e-mail communication, major setbacks suffered by the Communication Zones is the breach of genuineness, authorization and solitude of information. To thwart this misuse and interception of essential data by illegal entities techniques like cryptography, steganography [1], digital signatures etc. have been introduced.

"Cryptography" originates from the amalgamation of two Greek words "Krypto" meaning "hidden" and "graphene" meaning "writing"[2]. It has ranged over a period of 4000 years tracing back to Egyptian 'hieroglyph' as its source [3].

There are 3 types of cryptosystems [4]:

- Secret Key Cryptosystem: Encryption and decryption is done via one key.
- Public Key Cryptosystem: 2 keys i.e. 1 for encryption and other for decryption is used.
- Hash Function: Makes use of a hash value having fixed length calculated on the plain text to warrant that the file has not been altered by an imposter or a virus.

Benefits [5]:

1. Protects from unlicensed revelation, spoofing and forgeries.
2. Promotes data veracity and non-repudiation.

Drawbacks [5]:

1. Huge Time and money Costs.
2. Even if the Cipher text can't be deciphered, an attacker can destroy or remove the text from the system making it inaccessible to all, owing to poor design of the system. This introduces the need to conceal from public eye.

"Steganography" [6] arising from Greek words "steganos", or "covered," and "graphie", or "writing" takes cryptography a step beyond by hiding the coded message within any other normal message in such a way that its presence can't be suspected. Many legends over the time has shown some or the other type steganography. One such fascinating legends is that of the Pirates who tattooed a secret maps on the heads so that it is cloaked by human hair. Most common digital steganography technique is "Watermarking" [7] which administers the copyright of content conveyed across internet by enclosing a concealed message (invisible watermark) in images, moving pictures, sound files, texts etc.

Pros [5]:

Vital Information masked from human eye useful in preventing hacking

Limitations [5]:

Care should be taken to ensure that the hidden message does not compromise the quality of the original message.

This paper combines the benefits offered by the systems (Public Key Cryptosystems and Steganography) in its design .The remaining parts of the paper is ordered in the ensuing fashion. Section II periodicals the allied work and section III partakes the suggested methodology. Finally, inference and future work is chronicled in section IV.

II. RELATED WORKS

Among various cryptographic algorithms such as RSA, AES, DES or hash functions such as MD5, SHA etc. RSA is the most popular algorithm till date. This section briefly expounds on some research done in the field of cryptography and steganography. Below research of some of the prominent people in the field are listed.

Dan Boneh et al in [8] researched on four variants of RSA designed with the intention of speeding up the decryption process in RSA. Their research concluded that while Batch RSA was fully backward compatible with the existing RSA techniques, Multi-factor RSA and Rebalanced RSA offered better rapidity while decrypting.

Anshuman Rawat and Shabsi Walfish in [9] divided the message into small parts and hash code generated for each block is concatenate with the message blocks. Subsequently the integrated string is encoded. At the receiver each block is processed parallel to obtain the speedup. Even though this method increases the security, it is not suitable for applications offering low bandwidth where short messages must be exchanged.

Weng-Long Chang et al in [10] tried to solve the utmost intricate part of RSA algorithm is the factoring the product of two large prime numbers by developing three new DNA-based procedures which are parallel subtractor, parallel comparator, and parallel modular arithmetic

In [11] authors S Chandra et al examined various Symmetric and Asymmetric Key Cryptographic algorithms emphasizing on their importance, pros, cons and future scope.

Authors Asif Hameed Khan et al in [12] researched on how genetic algorithm can be applied to the process of cryptanalysis by highlighting the work done by various researchers in that field.

Authors Sapna Saxena and Bhanu Kapoor in [13] divided the data into smaller chunks and distributed these chunks among various available cores of processors to imbibe simultaneous processing. Finally these pieces were unified together to get the entire data set.

Poonam Jindal and Brahmjit Singh in [14] presented the horometrical survey of the RC4 algorithm back from its inception. Being simple and robust, this algorithm is enticing many researchers nowadays. The paper expounds on various research opportunities in the field.

In [15] Bahadori M. et al employed a Smartcard furnished with a crypto-coprocessor and a true random number generator to achieve 50 percent reduction in key pair bearing time .Their technique produces large prime numbers in a lesser time effectively reducing the time requisite for spawning key pair. During key generation process an apt public key is chosen from a lot of pre-demarcated public keys and Euclid's extended algorithm is used to create private keys.

Authors P. Johri et al have done a detail study of steganography in all possible domains in [16].

Various works are done in the field of steganography such as video steganography built on genetic algorithm [17] and using the vertical and horizontal reflection symmetry properties of the characters in individual sentences of the document to camouflage the messages [18].

Prem Singh et al made use of null spaces (2 spaces for 1 and 1 space for 0) to embed the secret message in the cover text [19]. A great deal of spaces were needed to encode a small message as each character i.e. 8 bits required 8 spaces.

In [20] authors modified the alphabets in the cover text to hold bits of the secret memo in such a way that the structural alteration of the letters is not easily discernable.

C. H. Yang, C. Y. Weng, S. J. Wang and H. M. Sun used edge areas of images for hiding data rather than using smooth areas in [21].Pixel Value differentiation was used to find the edge areas of the images and LSB method was used for embedding the secret value.

P and B frames in video were used for secret text transmission and frame I contained control information in [22]. Authors, at the decryption end, extracted control information first, based on which implanted message was extracted.

The various advancements made in the field of steganography using digital audio as the carter are illustrated in [23].

III. PROPOSED METHOD

Steps followed during encryption and decryption are shown in Figure 1 and Figure 2 respecticvely. During Encryption process the cipher text generated after applying RSA is hidden in an image and is sent to the reciever. Also to certify the sacredness of the stego-image a classified question is decided among the sender and reciever . Reciever gets the correct stego-image only after answering the secret question correctly and then he applies the proposed steganalysis algorithm to it to generate the cipher text . Decryption of cipher text then yields the plain text.

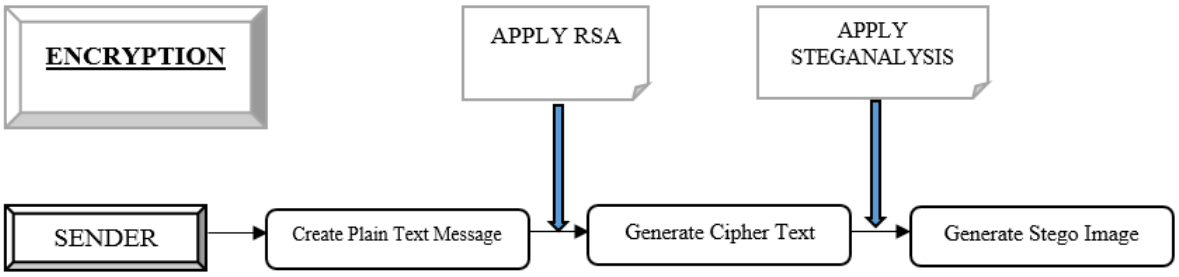

Figure 1. Encryption Process

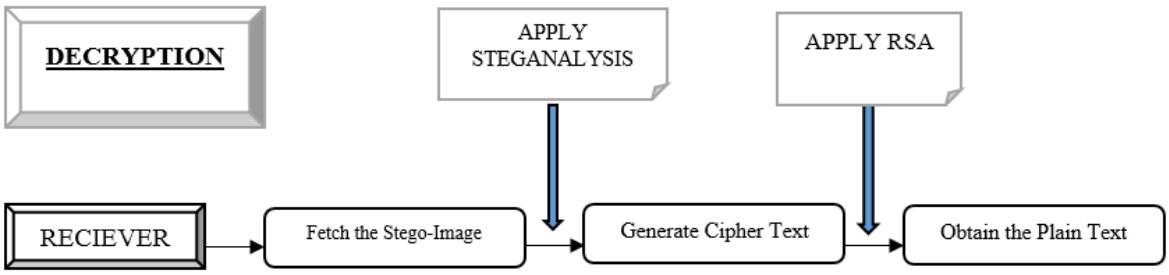

Figure 2. Decryption Process

3.1 Stegnography Algorithm

Below the algorithm used for hiding cipher text in the cover image is given and also is illuatrated in Figure 3 [24].

"Encoding [25]:

i. Choose a Cover Image from the database of available images.

ii. Select a Secret Key.

iii. Select a Secret Question (which is communicated prior between sender and receiver to retrieve the Stego-image from the database).

iv. Transfer and zip the Secret Text (Cipher Text) obtained from RSA into a Zip file.

v. Convert Zipped Text File to Binary Codes

vi. Transform Secret Key into Binary Codes

vii. Initialize BitsPerUnit to Zero

viii. Hide two binary codes from the series within a pixel of the chosen image

ix. Echo viii. until all codes are enciphered.

x. OUTPUT: Stego-image

Decoding [25]:

i. Answer the Secret Question to retrieve the correct Stego-Image.

ii. Enter the Secret Key

iii. Compute BitsPerUnit

iv. Retrieve 2 binary codes from each pixel

v. Decipher all the retrived binary codes and convert it into original format,

vi. Compare the Secret Key entered by the receiver with the embedded secret key.

vii. If match found , display the cipher text .

viii. If no match found display error messges.

ix. OUTPUT: Secret Text (Cipher Text) ".

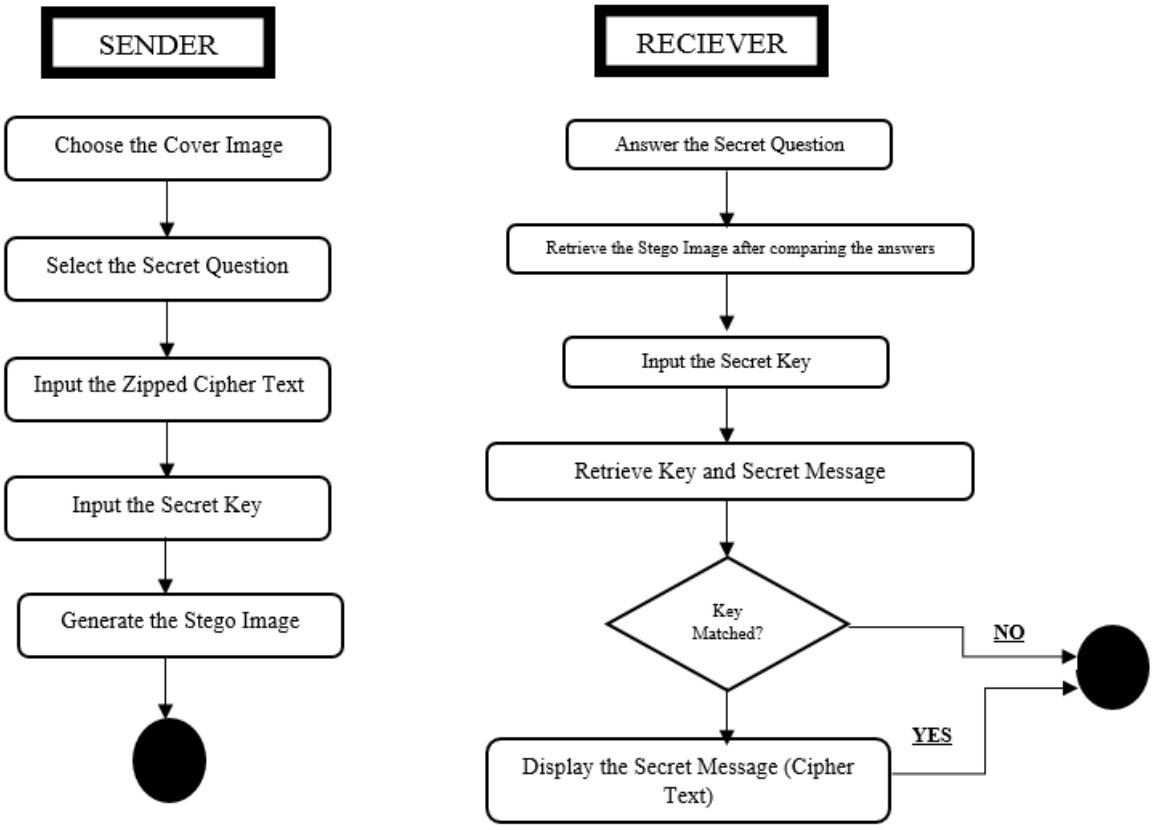

Figure 3. Block diagram of Stegnography process

Simple Embedding Zip files into image Commands on Windows and Unix Platforms
For embedding message in Image:
In Windows Platform:
"copy /B picture.gif+YourMenu.zip newfile.gif"
In Linux Platform:
"cat image.png secret.zip > image2.png"
Here**:**

i. The original image is picture.gif/image.png
ii. YourMenu.zip/secret.zip is the zip file to be hidden in the image.
iii. newfile.gif/image2.png is the Stego-image

For extracting the hidden message from the Image:
"unzip image2.png/newfile.gif"

3.2 RSA Algorithm

This algorithm, proposed by Rivest, Shamir & Adleman [26], is one of the most widely used algorithms till date. It involves 3 steps as shown in Figure 4 and shown below:

I. "Key Generation:
- Choose any two prime numbers p and q

- Compute n = p * q
- Compute φ(n) = (p - 1) * (q - 1)
- Choose e such that 1 < e < φ(n) and e and φ (n) are coprime.
- Compute a value for d such that (d * e) % φ(n) = 1.

Pubic Key Generation:

- Public key is (e, n)

Private Key Generation:

- Private key is (d, n)

II. Encryption:

ABC wants to send DEF an encrypted message *M* so she obtains his RSA public key (e,n) and generates Cipher text using $C= M^e \bmod n$

III. Decryption:

DEF uses his private key (d, n) to decrypt the message $M = C^d \bmod n$ “

Example:

Let, e=3, d=7, n=33.

To encrypt the message “SUN” numeric value of the character is incremented by one and is used as plain text message. While decrypting the plain text number obtained from cipher text is decremented by one and its corresponding character is fetched. The process is depicted in Table-1 and Table-2 shown below.

Table -1 Encryption

Symbol	Original Number	M = (Number+1)	M^3 mod 33=C
S	19	20	14
U	21	22	22
N	14	15	9

Table -2 Decryption

Cipher	C^7 mod 33 =M	Original Number (Number -1)	Symbol
14	20	19	S
22	22	21	U
9	15	14	N

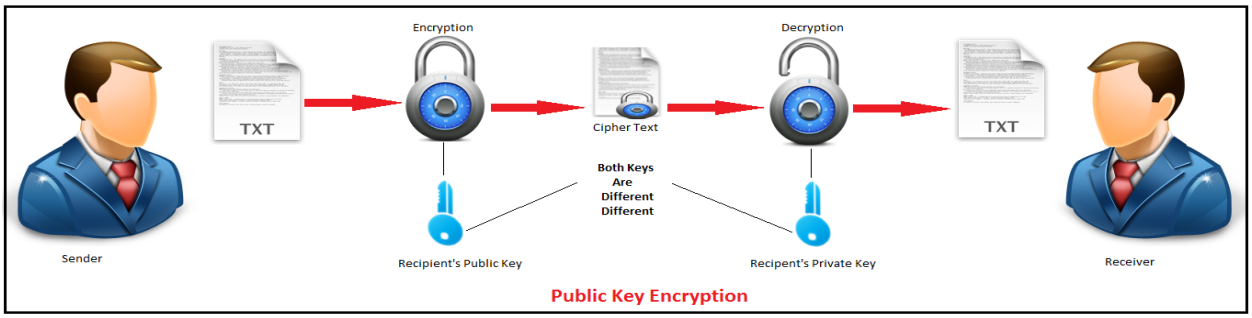

Figure 4. Block diagram of RSA process

IV.CONCLUSION

Steganography is the art of concealing data within other data and is used to transfer the messages stealthily avoiding a “hack”. The proposed technique presents a three tier security model where RSA based encryption, secret question and steganography techniques together shields the crucial data. As the Stego-images does not suffer from any noticeable changes that could be discerned by a human eye at a glance, it provides a vital protection for imperative information such as credit card information so that they can be protected from eavesdroppers (man in the middle attack). The presented method addresses the losses suffered by RSA on account of Brute Force attack and Chosen Cipher Text attacks [26] by avoiding the capture of cipher texts by unauthorized entities. Future work in this area would be improving the efficiency of the presented methodology by using some advanced algorithms such as elliptic curve cryptography or AES for encryption without compromising on the quality of the Stego-image (having higher PSNR (Peak signal to- noise ratio)) or incorporating signatures using hashing or digital signatures to endorse authenticity .Extending the work to develop Stego-videos can also be a future step in this direction.

REFERENCES

[1] S. Kaur, S. Bansal and R. K. Bansal, "Steganography and classification of image steganography techniques," 2014 *International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, 2014, pp. 870-875.doi: 10.1109/IndiaCom.2014.6828087

[2] S. Ahmad, K. M. R. Alam, H. Rahman and S. Tamura, "A comparison between symmetric and asymmetric key encryption algorithm based decryption mixnets," 2015 *International Conference on Networking Systems and Security (NSysS)*, Dhaka, 2015, pp. 1-5.doi: 10.1109/NSysS.2015.7043532

[3] Ahmed Al-Vahed and Haddad Sahhavi ,” An overview of modern cryptography”, *World Applied Programming*, Vol (1), No (1), April 2011, pp 55-61.

[4] Rajesh R Mane,” A Review on Cryptography Algorithms, Attacks and Encryption Tools”, *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 3, Issue 9, September 2015.

[5] Haripriya Rout and Brojo Kishore Mishra,” Pros and Cons of Cryptography, Steganography and Perturbation techniques”, *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*, PP 76-81.

[6] S. Kaur, S. Bansal and R. K. Bansal, "Steganography and classification of image steganography techniques," 2014 *International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, 2014, pp. 870-875.doi: 10.1109/IndiaCom.2014.6828087

[7] C. I. Podilchuk and E. J. Delp, "Digital watermarking: algorithms and applications," in *IEEE Signal Processing Magazine*, vol. 18, no. 4, pp. 33-46, Jul 2001.doi: 10.1109/79.939835

[8] Dan Boneh and Hovav Shacham, "Fast Variants of RSA”, *CryptoBytes*, Vol.1, No.5, pp. 1--9, 2002.

[9] A Rawat, S Walfish,” A Parallel Signcryption Standard using RSA with PSEP”, *Project Report*, 2003.

[10] Weng-Long Chang, Minyi Guo and M. S. H. Ho, "Fast parallel molecular algorithms for DNA-based computation: factoring integers*," in IEEE Transactions on Nano Bioscience*, vol. 4, no. 2, pp. 149-163, June 2005.doi: 10.1109/TNB.2005.850474

[11] S. Chandra, S. Paira, S. S. Alam and G. Sanyal, "A comparative survey of Symmetric and Asymmetric Key Cryptography," *2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE)*, Hosur, 2014, pp. 83-93.

[12] Asif Hameed Khan, Auqib Hamid Lone and Firdoos Ahmad Badroo, “The Applicability of Genetic Algorithm in Cryptanalysis: A Survey”, *International Journal of Computer Applications*, 130(9):42-46, November 2015. Published by Foundation of Computer Science (FCS), NY, USA.

[13] S. Saxena and B. Kapoor, "An efficient parallel algorithm for secured data communications using RSA public key cryptography method," 2014 IEEE International Advance Computing Conference (IACC), Gurgaon, 2014, pp. 850-854.doi: 10.1109/IAdCC.2014.6779433.

[14] Poonam Jindal, Brahmjit Singh, “RC4 Encryption-A Literature Survey”, *Procedia Computer Science*, Volume 46, 2015, Pages 697-705, ISSN 1877-0509, http://dx.doi.org/10.1016/j.procs.2015.02.129.

[15] M. Bahadori, M. R. Mali, O. Sarbishei, M. Atarodi and M. Sharifkhani, "A novel approach for secure and fast generation of RSA public and private keys on SmartCard," Proceedings of the 8th IEEE International NEWCAS Conference 2010, Montreal, QC, 2010, pp. 265-268.doi: 10.1109/NEWCAS.2010.5603937.

[16] P. Johri, A. Mishra, S. Das and A. Kumar, "Survey on steganography methods (text, image, audio, video, protocol and network steganography)," *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, 2016, pp. 2906-2909.

[17] Kousik Dasgupta, Jyotsna Kumar Mondal, Paramartha Dutta, “Optimized Video Steganography Using Genetic Algorithm (GA) “, Procedia Technology, Volume 10, 2013, Pages 131-137, ISSN 2212-0173, http://dx.doi.org/10.1016/j.protcy.2013.12.345.

[18] Anandaprova Majumder, Suvamoy Changder,” A Novel Approach for Text Steganography: Generating Text Summary Using Reflection Symmetry”, *Procedia Technology*, Volume 10, 2013, Pages 112-120, ISSN 2212-0173, http://dx.doi.org/10.1016/j.protcy.2013.12.343.

[19] Prem Singh, Rajat Chaudhary and Ambika Agarwal,” A Novel Approach of Text Steganography based on null spaces”, *IOSR Journal of Computer Engineering (IOSRJCE)*, ISSN: 2278-0661,Volume 3, Issue 4 (July-Aug. 2012), PP 11-17.

[20] Souvik Bhattacharyya, Pabak Indu, Sanjana Dutta, Ayan Biswas and Gautam Sanyal,”Hiding Data in Text Through Changing in Alphabet Letter Patterns (CALP)”, *Journal of Global Research in Computer Science*, Volume 2, No. 3, March 2011.

[21] C. H. Yang, C. Y. Weng, S. J. Wang and H. M. Sun, "Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems," *in IEEE Transactions on Information Forensics and Security,* vol. 3, no. 3, pp. 488-497, Sept. 2008.doi: 10.1109/TIFS.2008.926097.

[22] Changyong Xu, Xijian Ping and Tao Zhang, "Steganography in Compressed Video Stream," First International Conference on Innovative Computing, Information and Control - Volume I (ICICIC'06), Beijing, 2006, pp. 269-272.doi: 10.1109/ICICIC.2006.158.

[23] I. Bilal, R. Kumar, M. S. Roj and P. K. Mishra, "Recent advancement in audio steganography," 2014 *International Conference on Parallel, Distributed and Grid Computing*, Solan, 2014, pp. 402-405.doi: 10.1109/PDGC.2014.7030779.

[24] Rosziati Ibrahim and Law Chia Kee,”MoBiSiS: An Android-based Application for Sending Stego Image through MMS”, *ICCGI 2012: The Seventh International Multi-Conference on Computing in the Global Information Technology,* 2012.

[25] Rosziati Ibrahim and Teoh Suk Kuan,” Steganography Algorithm to Hide Secret Message inside an Image”, *CoRR,* pp- 102-108, 2011.

[26] E. Suresh Babu, C. Nagaraju, and MHM Krishna Prasad. 2015,"A Secure Routing Protocol against Heterogeneous Attacks in Wireless Adhoc Networks", *In Proceedings of the Sixth International Conference on Computer and Communication Technology 2015 (ICCCT '15), ACM*, New York, NY, USA, 339-344. DOI=http://dx.doi.org/10.1145/2818567.2818670