ISSN No. 0976-5697

Volume 4, No. 8, May-June 2013

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Statistical Analysis of Secret Message Hiding in Steganography Using Asymmetric Cryptosystem

VeerendraKumar.Chotupalli[#1]
[#1] Department of computer science and Engineering M.Tech scholar, Sri Vasavi Engineering College Tadepalligudem, Andhra Pradesh, India
mail2veerendrakumar@gmail.com

Venkata Mutyalu Kavidi [#2]
[#2] Department of I.T, Sri Vasavi Engineering College Tadepalligudem, Andhra Pradesh, India
venkatmutyalu @gmail.com

Abstract— In recent trends, information security is playing a vital role in data transmission. Steganography, cryptography is a play a major roles in the field of information security, Steganography Embed the text into cover image and cryptography convert plain text into the cipher text vice versa. Various algorithms proposed for Steganography, cryptography for safe transmission of the data. But intruder will also indentify the secret message in the, in this paper combine[1] the both cryptography and Steganography methods and a comparison is done by stegano image generate a stegano image. Various statistical parameters are analyzed and compare with resultant image and cover image. In this paper Secret message are converted into cipher text then embed the cipher text into the image. In this paper use two techniques, RSA[2,3] and NTRU[4,5]. Both are asymmetric cryptosystem techniques.RSA is the most popular and oldest techniques, NTRU (Nth degree truncated ring unit polynomial) is a collection mathematical algorithms perform simple operations of very small integers. LSB[6] method is used for the Steganography, in this method has less distortion and embeds more data into the cover image.. Compare stego image with some statistical methods[7] and identify. The proposed method prevents the possibilities of steganalysis also.

Keywords: Steganography,Cryptography,RSA,NTRU,LSB.

I. INTRODUCTION

In the present world of communication, one of the necessary requirements to prevent data theft is securing the information. Cryptography and Steganography are two important techniques for to provide the security in the transformation channel. Various cryptography and Steganography methods available for provide security of the secret message. Cryptography is method for convert the plain text into cipher text. Steganography is technique for embed the secret data into the cover image. Now in this paper we combine the both techniques.

A. Cryptography:

NTRU and RSA are two different techniques for converting plain text into cipher text. NTRU and RSA are asymmetric cryptography algorithms. Both techniques generate two keys one is public key and other is private. Public key is used for encrypt the secret data means convert chipper text. Private Key is used for the decrypt the cipher text into plain text. The main reasons which made Public-Key cryptography algorithms are more reliable are the area of greater secrecy.

B. Steganography:

Least significant bit[5] is the Steganography technique, which converts secret message and cover image into stegano image. In Steganography intruder will not identify the message because message visibility is very less.

C. Statistical methods:

In this approach embed the information by varying some statistical properties[7,8] of a cover image and use the hypothesis testing in the extraction process. The above process achieve by modifying the cover image in such a way that some statistical characteristics changed significantly.

Chi-Square test[10] on such a data-hiding scheme reveals the existence of the hidden data.

II. PROBLEM DEFINATION

A. Problem statement:

The aim of the paper is to send data with security. Cryptography and Steganography provide the security ant to send file to the destination and intruder retrieving of the secret data in done.

B. Problem solution:

The proposed method should provide better security with help of some techniques and user can select bets technique while transforming data or message in the form of images file.

III. PROPSED TECHNIQUES AND RELATED WORK

A. LSB technique:

Least significant bit (LSB)[6] insertion is a simple approach to embedding information in image file. The simplest Steganography techniques embed the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence Modulating the least significant bit does not result in human perceptible difference because the amplitude of the change is small. In this technique, the embedding capacity can be increased by using two or more least significant bits. At the same time, not only the risk of making the embedded message statistically detectable increase but also the image fidelity degrades. Hence a variable size LSB embedding schema is presented, in which the number of LSBs used for message embedding/extracting depends on the local characteristics of the pixel. The advantage of LSB-based method is easy to implement and high message pay-load.

a. Sender side:

Algorithm 1 The Encoding process in sender side

a) 1: for i = 1, ..., l(m) do
b) 2: p ← LSB(c_i)
c) 3: if p ≠ m_i then
d) 4: c_i← m_i
e) 5: end if
f) 6: end for

b. Receiver side:

Receiver receives the stego image then receiver first get the pixel color intensities and convert each pixel into binary format. The binary data send to LSB Decoder. Decoder decodes (extract) data from the each pixel intensities. Extracted data is decrypted. After completion of the process the receiver get the original or secret information from the image.

Algorithm the Decoding process

a) 1: for i = 1, ..., l(s) do
b) 2: m_i ← LSB (s_i)
c) 3: end for

B. NTRU technique:

NTRU[4,5] was originally presented by Jeffer Hoffstein and Jill pipher and joseph.H. Silverman. NTRU is based on the algebraic structure of certain polynomial ring. NTRU operation is based on the polynomial addition and multiplication. The basic collection of objects used by the NTRU is the ring R that consists of all truncated polynomial of degree N-1 integer coefficient.

The following are parameters for implementation of NTRU cryptosystem.

N is the Polynomial in the truncated polynomial ring having degree is N-1.Q is the large modulus: usually, the coefficient of the truncated polynomial will be reduced mod q. P is the small modulus, as the final step in decryption, the coefficient of the message is reduced mod p. Compute f_p and f_q. f_p is the private polynomial, f_q is the public polynomial.

a) Select randomly two small polynomial f and g in the ring of truncated polynomials.
b) Compute the inverse of the polynomial f^{-1} modulo q called as f_q and f^{-1} modulo p called as f_p .
   f* f_p =1 (mod p) f* f_q =1 (mod q)
c) Compute the public key
   h=p* f_q *g (mod q) .
   f_q*g is the multiplication of the two polynomial.
d) Encryption
   E=r*h+m (mod q).
   r is any small random polynomial .
   E is the encrypted message.
   Sender sends the message e to receiver.
e) Decryption
   A=f*E (mod q) Coefficients lie between (–q/2, q/2).
   B=A(mod p) Coefficients is lies between (-p/2, p/2).
   C=f_p*B (mod p).
   The polynomial C is the original message.

a. Encryption:

Process: first convert message into binary format. Each character length is N bits. Encrypt N bit binary into cipher text.

b. Decryption:

Collect N characters in cipher text decrypt the data into N bit binary format, convert into plain text.

N=11 is the degree of the polynomial ring. f, g is the polynomial of the ring whose degree is N-1=10, Q=32and P=3 is small integer means polynomial coefficient is lies between the {-1, 0, 1}.

$f=-1+X+X^2-X^4+X^6+X^9-X^{10}$

$g=-1+X^2+X^3+X^5-X^8-X^{10}$

Compute the inverse modulo of the p, q.

$fp=1+2X+2X^3+2X^4+X^5+2X^7+X^8+2X^{9.}$

$fq=5+9X+6X^2+16X^3+4X^4+15X^5+16X^6+22X^7+20X^8+18X^9+30X^{10}$

h=p*fq*g(mod q) (1)

Select random polynomial r for encrypt the message.

Steps for Encryption

a) Compute the public key h.
b) Select the any small random polynomial r.
c) Convert the message in the form of N^{th} degree polynomial.
d) e=r*h+m (mod q). (2)

Send message e

Steps for Decryption

a) a=f*e (mod q) (3)
b) b=a (mod p) (4)
c) c=fp *b(mod p). (5)

Get original message c.

C. RSA technique:

The RSA[2,3] algorithm was publicly described in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The letters **RSA** are the initials of their surnames. The RSA algorithm involves three steps: key generation, encryption and decryption.

Creation of key:

a) Choose two distinct two random prime numbers p, q.
b) Compute the product n=p*q;
c) Compute $\varphi(n) = \varphi(p)\,\varphi(q) = (p-1)(q-1)$.
d) Choose an integer e such that $1 < e < \varphi(n)$ and gcd $(e, \varphi(n)) = 1$; i.e., e and $\varphi(n)$ are co prime. e is released as the public key exponent.
e) Determine d as $d^{-1} = e \pmod{\varphi(n)}$

i.e., d is the multiplicative inverse of e (modulo $\varphi(n)$).This is more clearly stated as solve for d given $de = 1 \pmod{\varphi(n)}$.

a. Encryption:

Seder transmits her public key (n, e) to receiver and keeps the private key secret. Receiver then wishes to send message M to sender computes the cipher text c corresponding to the message m then transmit to the receiver

$C=M^e \pmod n$ (6)

b. Decryption:

Receiver can decrypt the message c with help of private key. Given m, recover the original message M.

$M=C^d \pmod n$ (7)

p = 23, q = 89, n = p * q=2047,

$\varphi(n) = (1 - p) * (1 - q)=1936$

Select e = 31;

Gcd (e, $\varphi(n)$) =gcd (31, 1936) =1.

Public key is (n, e) = (2047, 31).

Select d, d*e=1(mod φ (*n*)), d=687;
687*31=21297 (mod 1936)
(1936*11+1)=21297
Private Key (n, d) = (2047, 687*)*.

IV. PROPOSE SYSTEM ARCHITECTURE

A. Sender side:

First convert the secret message into cipher text. Each character in cipher text is converting into binary format. And take any cover image, get pixel of the cover image. Embed data into the cover image directly using LSB encoder and send to the receiver.

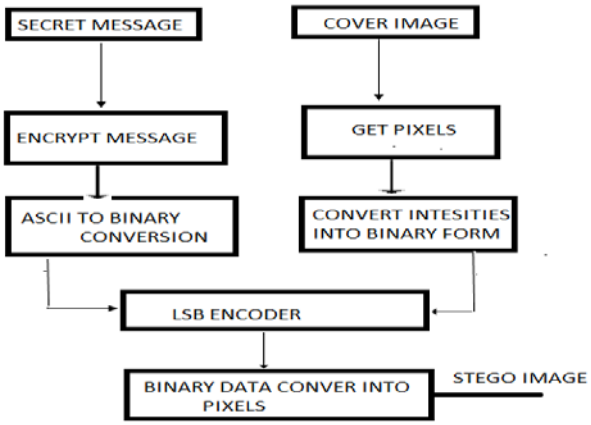

Figure 1: convert plain text into cipher and Embeds into the image.

B. Receiver side:

Receiver receive the stego image, extract data from the image using LSB decoder then it produce a cipher text. Receiver Decrypt the message it form a original plain text.

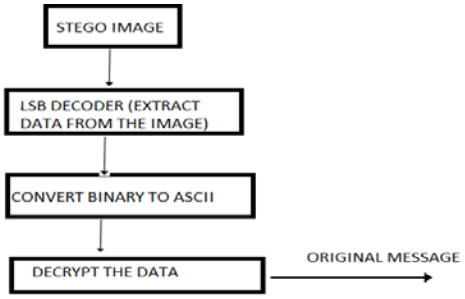

Figure 2: Extract data from the stego image and decrypts text.

V. EXPRIMENTAL RESULT

The stego images are got by using Normal Steganography, RSA, NTRU stego images are compared and various statistical parameters are used analyze the images and finally end user can select any one of the stego image for transmission. This is the main advantage of the proposed work.

A. Images:

Various images are used for analysis and identify the better Steganography technique.

a. Original image:

Original image is used for apply the Steganography and compare the stego images using statistical parameters.

Figure 3: orginal image

b. Normal stego image:

Plain text is directly embeds into the cover image.

Figure 4: Image quality using Pure Steganography

c. NTRU stego image:

Plain text is converting into cipher text with help of NTRU cryptosystem and embeds cipher text into the image.

Figure 5: Image quality using NTRU and Pure Steganography.

d. RSA stego image:

Plain text is converting into cipher text with help of RSA cryptosystem and embeds cipher text into the image.

Figure 6: Image quality using RSA and Pure Steganography

The NTRU algorithm is more secured than the RSA algorithm when combine pure Steganography. There is a slightly changes in image quality is evidence from the image. Above stego images are compared with the original image depends upon some statically methods.

B. Statistical Analysis:

a. Mean:

Mean [7] or Average is defined as the sum of all the given elements divided by the total number of elements.

$$\mu = \frac{\sum_{i=0,j=0}^{N-1,M-1} P_{i,j}}{N * M} \quad (8)$$

$P_{ij}=P_{ij.R}+P_{ij.B}+P_{ij.G}/3$, Where $P_{ij.R}$, $P_{ij.B}$,$P_{ij.G}$ are Red, Blue and Green color intensities.

b. Root mean square (RMS):

The RMS[7] also known as the quadratic mean, is a statistical measure of the magnitude of a varying quantity

$$MSR = \sqrt{\frac{\sum_{i=0,j=0}^{N-1,M-1} P_{i,j}^{2}}{N * M}} \quad (9)$$

c. Standard deviation (SD):

The S.D[7] shows how much variation or dispersion there is from the average.

$$\sigma = \sqrt{\frac{\sum_{i=0,j=0}^{N-1,M-1} (P_{i,j} - \mu)^2}{M * N}} \quad (10)$$

N and M is the width and Height of the image.

Table: 1 Results Of The Mean, RMS,And S.D Values Of The Above Four Images

Method and image	MEAN	RMS	S.D
Original image	102.2025	124.0655	68.7866
Pure Steganography	102.1935	124.0567	68.7779
NTRU and Pure Steganography	101.9913	123.8114	68.6837
RSA and Pure Steganography	102.1993	124.0648	68.7791

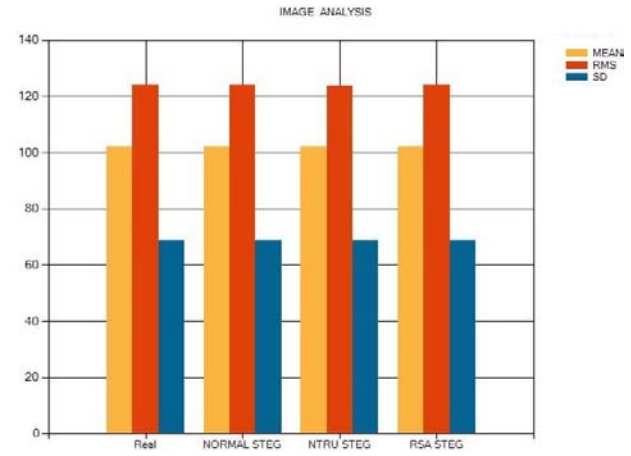

Figure 7: Graphical reprsenatiopn Mean,RMS and S.d of the above images.

d. Correlation Coefficient:

Correlation coefficients [7] are used to comparing two images for the purpose of the image reorganization and display measurement. If the coefficient result is "+1" then two images are absolutely identical. If result is "zero" then two images are completely uncorrelated. If result is "-1" then two images are anti correlated.

e. Chi-square test:

The χ^2 test[9,10] described how steganalysis can successfully detect steganalysis produced by sequential embedding approaches. The success of the test heavily relies on knowing the original order that the message was embedded in such that we can re-scan the values in the same order to yield the x^2statistic.

Table: 2 correlation coefficient comparisons and χ^2 values comparisons

Compare original	Correlation Coefficient	Chi-square
Pure Steganography	0.99999	0.0019
NTRU and Pure Steganography	0.99990	0.0284
RSA and Pure Steganography	0.99998	0.0029

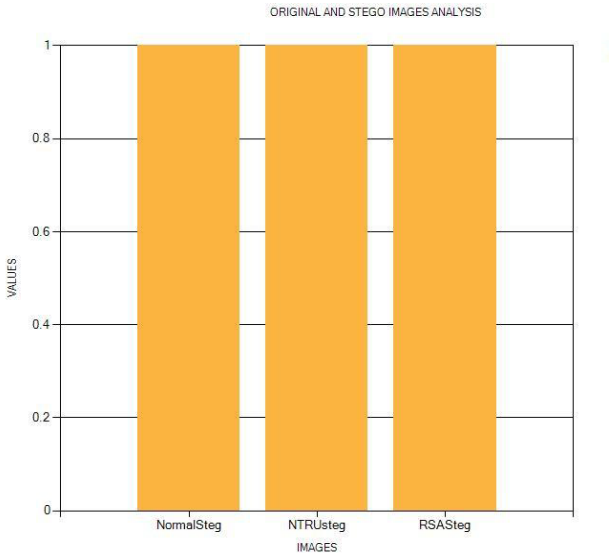

Figure 9: Graphical reprsenation of correlation coeffcient

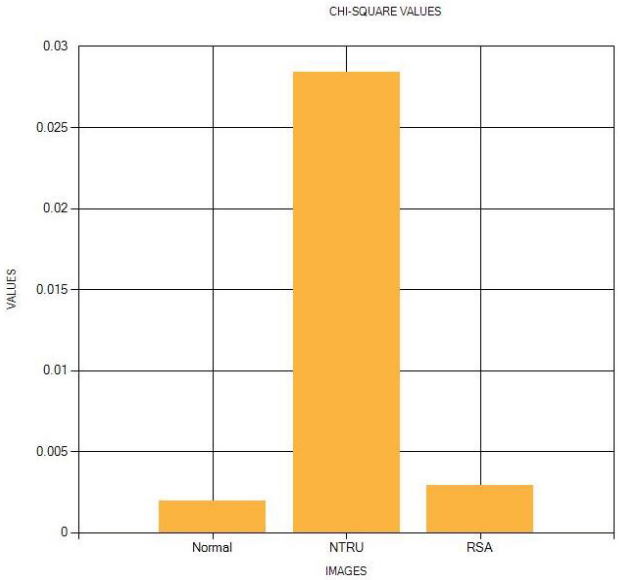

Figure 9: Graphical reprsenation of χ^2 values

VI. CONCLUSION

The proposed system used in this paper encrypts the secret message before embedding into the image. From the analysis we compared NTRU and RSA based on correlation coefficient and Chi-square methods and conclude that RSA is suitable for secret message hiding in Steganography. The end user selects the image for security of the message and prevents the possibilities of steganalysis.

VII. ACKNOWLEDGMENT

This paper is part of our M.Tech and we are grateful to our project guide for valuable suggestions, comments and contribution for completion.

VIII. REFERENCES

[1] Sujay Narayana and Gaurav Prasad " TWO NEW APPROACHES FOR SECURED IMAGE STEGANOGRAPHY USING CRYPTOGRAPHIC TECHNIQUES AND TYPE CONVERSION" signal and image processing: An International Journal (SIPIJ) vo1.1,No.2,December 2010.

[2] DI management –RSA Algorithm http://www.di-mgt.com.au/rsa_alg.html

[3] A book of "Cryptography and Network Security: principles and practices", William Stallings, Pearson education first Indian reprint 2003

[4] A. Naresh reddy ,Rakesh Nayak, S.Baboo "Analysis and performance characteristics of cryptography using image files" m International conference of computer applications ,2012.

[5] NTRU Cryptosystems, The NTRU Encrypt Public Key Cryptosystem Basic Tutorial available: http://www.ntru.com/cryptolab/tutorial_pkcs.html

[6] Shailender Guptha,ankur goyaland Bharat Bhusan "Infromation hiding using Least significant Bit stegnography and cryptography" international journal of Moderen Education and computer Sciences,2012,6,27-34 online publication.

[7] Shihua Zhou, Qiang Zhang,Xiaopeng Wei," Iimage Encryption Algorithm based on DNA Sequences for the Big image", , International Conference on Multimedia Information Network and Security, 2010.

[8] K.Sumathy,R.Tamilselvi 'Comparison of Encryption Level for image security using Various Transformation" international conference on information and Network Technology IPPCSIT vol.4(2011) IACSIT Press, Singapore.

[9] S. Guillermito, "A few tools to discover hidden data," 2004. [Online].Available: http://www.guillermito2.net/stegano/tools/index.html

[10] Westfeld, A., Pfitzmann, A.: Attacks on Steganographic Systems. In: Pfitzmann, A. (ed.) IH 1999. LNCS, vol. 1768, pp. 61–75. Springer, Heidelberg (2000)

[11] Hoffstein, J. Pipper, and J. H. Silverman, "NTRU: A Ring Based Public Key Cryptosystem", in Proc. of Algorithmic Number Theory: Third International Symposium (ANTS 3) (J. P. Buhler, ed.), vol. LNCS 1423,Springer-Verlag, June 21-25 1998, pp. 267-288.