Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 03, March -2018

An Improved Method of Steganography Combined with Cryptography

N. Sandeep[1], Sk. Heena Mobeen[2], V. Vijaya Lakshmi[3], S. Sivaji[4], V. Gopi Krishna[5]

[1.2.3.4.5] *Department of Electronics and Communication Engineering, Bapatla Engineering College*
P. Ravi[6], Asst. Professor, ECE Dept., Bapatla Engineering College.

Abstract: *Cryptography and Steganography are the two popular methods for secure data hiding and transmission available broadly. The techniques used information in order to cipher or cover their existence respectively. Cryptography is the science of using mathematics to encrypt and decrypt data; the data are converted into some other gibberish form, While Steganography is the art and science of hiding communication, a stenographic system, thus embeds hidden content in the unremarkable cover media so as not to provoke an eavesdropper's suspicion. This paper focuses on improved LSB information hiding algorithm of data using RSA cryptographic algorithm, combining information hiding and cryptography, increasing the human eye visual features and the encryption algorithm to improve the security of information hiding. Finally we get a better encryption technique than LSB algorithm which provides high PSNR and embedding capacity. Thus the two techniques are usually combined for enhanced security to a great extent.*

Keywords: *information security; public key; private key; image hiding; LSB; encryption.*

I. INTRODUCTION:

In the present world of communication, computer and internet are the major media that connects different parts of the world as one global virtual world in this modern era. So we can easily exchange lots of information within seconds of time, but the confidential data that needs to be transferred should be kept confidential. So by using steganography and cryptography we can secure the confidential data. But individually steganography and cryptography provides confidentiality to the data but they have some vulnerability so by combining steganography with cryptography we have more security.

Steganography is the art and science of writing hidden messages in such a way that no one, except the sender and receiver, suspects the existence of the message, a form of security through hiding the message.ie., Steganography is concealed writing and is the scientific approach of inserting the secret data within a cover media such that the unauthorized viewers do not get an idea of any information hidden in it.

Cryptography is also known as the science of secret writing. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, entity authentication, integrity of data and message origin authentication The goal of cryptography is to make data unreadable by a third party.

Cryptography algorithms are divided into symmetric (secret-key) and asymmetric (public-key) network security protocols. Symmetric algorithms are used to encrypt and decrypt original messages (plaintext) by using the same key. While Asymmetric algorithms uses public-key cryptosystem to exchange key and then use faster secret key algorithms to ensure confidentiality of stream data. In Public-key encryption algorithms, there is a pair of keys, one key is known to the public, and is used to encrypt information to be sent to a receiver who owns the corresponding private key. The private and public keys are both different and need for key exchange.

They are so many other techniques used for data security such as digital watermarking, finger print detection, Digital signature authentication techniques etc.

Individually both steganography and cryptography provides security to the data but they have some vulnerability. So by combination of steganography and cryptography we have more confidentiality and security. There are different techniques available in steganography and cryptography so can we have different combinations of steganography.

Main applications of cryptography and steganography are confidential communication and secret data storing, protection of data alteration, access control system for digital content distribution, Media database systems, electronic cash, threshold systems, credentialing systems

II. COMPARISION BETWEEN STEGANOGRAPHY AND CRYPTOGRAPHY:

STEGANOGRAPHY	CRYPTOGRAPHY
1) Outsider doesnot know the message is sending. 2) Steganography prevents the discovery of the very existence of communication. 3) Once the outsider knows there is information then easy to extract it. 4) Steganography does not alter the structure of the secret message.	1) Outsider knows the message is sending. 2) Encryption prevents an unauthorized person from discovering the contents of communication. 3) Once the outsider knows there is information but requires large computing power for cracking. 4) Cryptography alters the structure of the secret message.

In this paper we compare different techniques available in steganography based on their security. And on the improved LSB based steganalysis combined with RSA algorithm of cryptography.

III. RELATED WORKS:

In the present world of technology we have seen a rapid growth of data security and the threat of stealing the secret information has been an ever been concern for communication. Steganography and cryptography are the techniques used to overcome this threat. Both these techniques have gain lot of attention to overcome the data stealing. S. Kumar [7] has proposed an encryption technique combining both steganography with cryptography. Instead of encrypting the data once, here the data is encrypted twice. Bharati and A.R.Soni proposed a method by combining steganography with cryptography to hide the date using color image. Haffaya Abdulzara proposed an encryption technique in order to lower the space of representing characters used in secret message. Kandarand Maiti proposed a technique of well-known k-n secret sharing for color images using a variable length key with share division using random numbers. In [6], the authors proposed a highly-secure steganography technique by combining DNA sequence with Hyper-elliptic Curve Cryptography. This approach achieved the benefits of both techniques to obtain a high level of secure communication, besides other benefits of applying DNA cryptography and steganography. The algorithm hides a secret image in another cover image by converting them into DNA sequence using the nucleotide to the binary transformation table.

IV.STEGANOGRAPHY TECHNIQUES

Steganography is the art of hiding the existence of data in another transmission medium to achieve secret communication.In steganography the secrete data is embedded into the cover image in such waythat only cover image is visible which is sent from transmitter to receiver without scrambling. It does not replace cryptography but it can be used to improve the security of cryptography.

1) LSB-STEGANOGRAPHY:

In Least Significant Bit (LSB) steganography [5] embed the text message in least significant bits of digital picture. In which data is embedded by replacing the LSB of cover carrier with the data to be send.ie first read the cover image and text message which is to be hidden in the cover image, then convert text message in binary. Calculate LSB of each pixels of cover image. Replace LSB of cover image with each bit of secret message one by one so we get an image in which data is hidden.

2) DCT –STEGANOGRAPHY:

The hidden message is converted into binary stream of “1” and “0” are insert the into the DCT domain of the cover image. The color-based transformation converts the image (cover image) into 8x8 blocks of pixels. [8] Next, take larger positive coefficients need to embed in the cover image in the low-mid frequency range. DCT can divide the image into high, middle

and low frequency components. As the high frequency coefficients are vulnerable and less robust on the quality of image. The main issue of this work is robustness against with high quality of image, thus the low and mid frequency coefficients are the most appropriate. The selected coefficients c_i are modified by the corresponding bit in the message stream. This K quantity represents the persistence factor. As soon as the i^{th} term of message bit s(i) is "1", the coefficient of the image is added with a quantity K; otherwise the same quantity is subtracted from it.

3) DWT-STEGANOGRAPHY

A discrete wavelet transform (DWT) is any wavelet transform [6] for which the wavelets are discretely sampled. This is one of the frequency domains in which steganography can be implemented. DCT is calculated on blocks of independent pixels, a coding error causes discontinuity between blocks resulting in annoying blocking artifact. This drawback of DCT is eliminated using DWT because DWT applies on entire image. DWT offers better energy compaction than DCT without any blocking artifact. DWT splits component into numerous frequency bands called sub bands known as

LL – Horizontally and vertically low pass

LH – Horizontally low pass and vertically high pass

HL - Horizontally high pass and vertically low pass

HH - Horizontally and vertically high pass

Since Human eyes are much more sensitive to the low frequency part (LL sub band) we can hide secret message in other three parts without making any alteration in LL sub band. As other three subbands are high frequency sub-band they contain insignificant data. Hiding secret data in these subbands doesn't degrade image quality that much.

S.NO	Technique	MSE	PSNR
1	LSB	4.9929	11.812
2	DCT	7.055	20.059

V. CRYPTOGRAPHY TECHNIQUES

Cryptography is the study of sending messages in cipher form so that receiver only can able to read the message. It is performed by converting messages into encrypted by using symmetric key algorithm and asymmetric key algorithm. In symmetric key algorithm a single key is used for both encryption and decryption. In asymmetric key algorithm we use public key for encryption purpose and private key for decryption purpose.

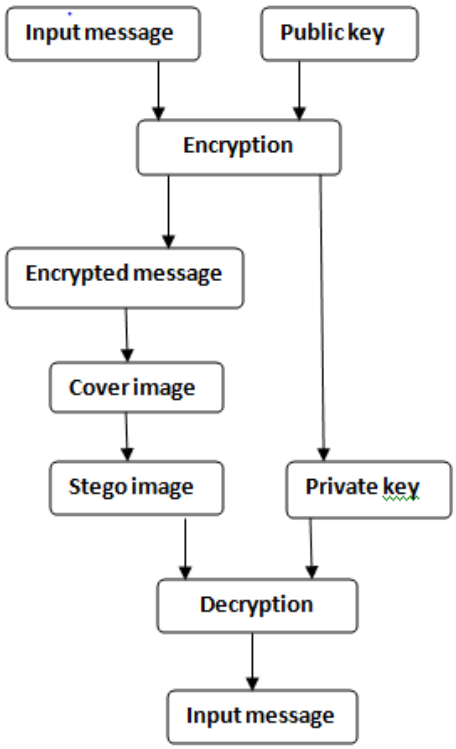
VI. RSA ALGORITHM

RSA was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology. RSA is one of the earliest public-key cryptosystems and it is widely used for securing data transmission. Here encryption key is public and decryption key is private, it kept secret. RSA is based on factorizing two large prime numbers. The public and the private key-generation algorithm is the most complex part of RSA cryptography. We can consider two prime numbers, x and y,. A modulus is calculated by multiplying x and y. This number is used by both the public and private keys and provides the link between them. Its length is called the key length.

VII. PROPOSED METHOD FORCOMBINING STEGANOGRAPHY WITH CRYPTOGRAPHY

In this paper we proposed a new technique for hiding secrete data into an image by combination of steganography with cryptography which enhances the data security and robustness of the message:

1)PROPOSED ALGORITHM FLOWCHART:



2) EMBEDDING ALGORITHM:

we choose to hide a message in a cover image of size 256x256 .this message can be of sequence of characters, and symbols sent by us. Suppose the message is PROJECT.

3) ENCRYPTION STAGE (FROM SECRET TEXT TO ENCRYPTED TEXT):

Step 1: In the secret message each character is converted into ASCII values.

Step 2: By using RSA algorithm we generate a public key and private key.

RSA ALGORITHM: TO GENERATE PUBLIC AND PRIVATE KEY:

Step 1: Select random prime numbers p and q and check that p! =q

Step 2: Compute modulus n=p*q

Step 3: Compute ø= (p-1) (q-1)

Step 4: Select public exponent e, 1<e< ø

Step 5: Such that GCD (e, ø)=1

Step 6: Compute the private exponent d= (e^-1) mod ø

Step 7: Public key is e,private key is d

Step 8: Encryption c= (m^e) mod n

Step 9: Decryption m=(c^d)mod n.

Here, the sender encrypts the message by using public key and we get an encrypted message.

Step 3: This encrypted message is converted into bit stream before embedding into the cover image.

4)STEGANOGRAPHY STAGE:

Step 1: In steganography we use LSB technique to hide the message.

Step 2: In this technique we embed the encrypted message into cover image by replacing the least bit of pixel of cover image then we get a stego image

Step 3: Then this stego-image is transmitted by using internet or any other medium.

4) DECRYPTION STAGE:

Step 1: Receive the stego image.

Step 2: Extract LSB bit of each pixel in the received image.

STEP 3: Split the LSB bits into group of 8 bits.

STEP 4: Decrypt these bits by applying private key generated by RSA algorithm to get the original message.

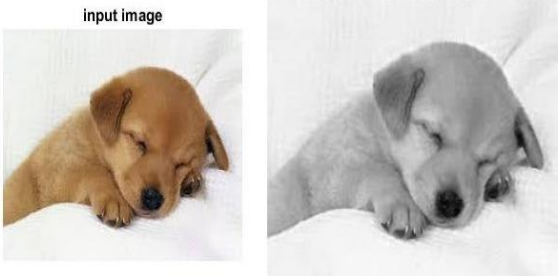
VIII. EXPERIMENT RESULTS

In this paper we use a cover image of size 256X256. LSB (least significant bit of the cover image is used to hide the encrypted message.

Input image

Stego image

Stego image



In the objective evaluation method the most commonly used index is the PSNR value and histogram changeability to show the better performance of the proposed method.

1) PSNR (peak to signal noise ratio):

It is defined as the ratio of peak square value of pixels by MSE. It is expressed in decibel. It measures the statistical difference between the cover and stego-image, is calculated using Equation :

$$PSNR=10\log_{10}\left[\frac{255^2}{MSE}\right]^{db}$$

2) MSE (Mean Square Error):

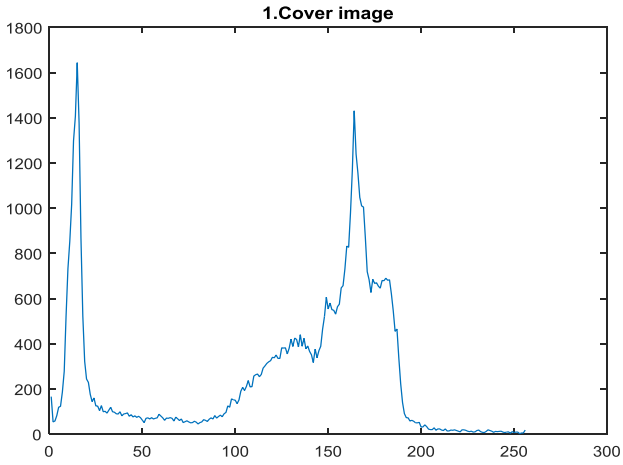
It is defined as the square of error between cover image and stego-image [2]. The distortion in the image can be measured using MSE and is calculated using Equation:

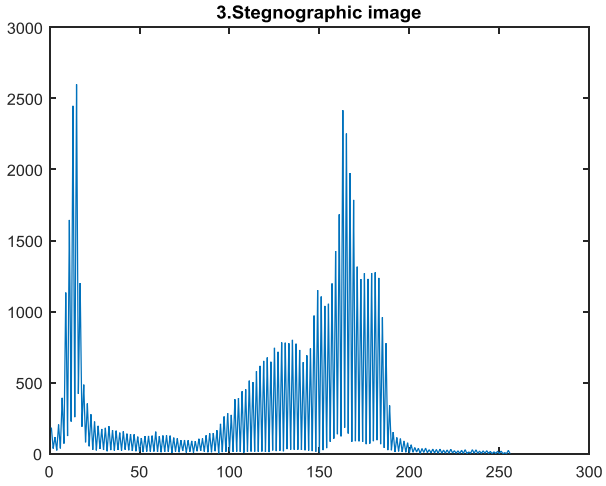
$\text{MSE} = \left(\frac{1}{M-N}\right)^2 \sum_{i=0}^{n} \quad \sum_{i=0}^{n} \quad (Xij - X'ij)^2.$

Where XIJ: The intensity value of the pixel in the cover image. M*N: Size of an Image.

Host image	Simple LSB		Proposed method	
	PSNR	MSE	PSNR	MSE
Cameraman	36.3	9.553	50.2691	6.25
puppy	32.9	8.726	48.82	5.92

IX. HISTOGRAM COMPARISON





X. CONCLUSION

Ensuring data security is a big challenge for computer users. Businessmen, professionals, and home users all have some important data that they want to secure from others. Even though both methods provide security, to add multiple layers of security it is always a good practice to use Cryptography and Steganography together. The present study is designed to combine the features of both cryptography and steganography, which will provide a double level of security and high PSNR value so that outsider so outsider cant able to recognize the change in cover image. In future the work will try increase the embedding capacity of cover image.

XI. ACKNOWLEDGEMENT

We would like to thank ECE department and our guide P.RAVI Asst. Prof and Head of ECE Department Dr.B.CHANDRA MOHAN, M. Tech, Ph.D., who guided and encouraged us in every step of the seminar work and paper work.

XII.REFERENCE

1. Usha, S., Kumar, G. A. S., and Boopathy bagan,K. A secure triple level encryption method using cryptography and steganography,0Computer Science and Network Technology (ICCSNT), International Conference, Vol.2, No.2.11, 2011 ,pp. 1017-1020.IEEE.

2.Bharti,P.,and Soni, R.,A New Approach of Data Hiding in Images using Cryptography and Steganography, International Journal of Computer Applications,Vol.58,No.18,2012,pp1-5

3. Xia, X., C. G. Boncelet, and G. R. Arce, "A Multi-resolution Watermark for Digital Images," in Proceedings of the IEEE International Conference on Image Processing (ICIP'97), 1997.

4. Kandar. S, and Maiti. A., Variable Length Key based Visual Cryptography Scheme for Color Image using Random Number, International Journal of Computer Applications (0975 –8887) Vol.19, No.4, 2011, pp 35-40.

5.Umamaheswari, M., Siva subramanian, S. and S.Pandiarajan S., Analysis of Different Steganographic Algorithms for Secured Data Hiding, IJCSNS International Journal of Computer Science and Network Security, Vol.10,No.8, 2010, pp 154-160.

6.Vandana Rajput,Sandeep Kumar Tiwari" Improved RSA Algorithm", in International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016.

7.Bairai, A. K., ASCII based Even-Odd Cryptography with Gray code and Image Steganography: A dimension in Data Security, ISSN 2078-5828 (Print), ISSN 2218-5224 (Online), Vol.01,No.2,2011, pp 37-41,Manuscript Code: 110112.

