KIU Journal of Social Sciences Copyright©2019
Kampala International University ISSN: *2413-9580*; 5(2): 345–351

A Residue Number System Based Data Hiding Using Steganography and Cryptography

JOSEPH B. ESEYIN
University of Jos, Nigeria

KAZEEM A. GBOLAGADE
Kwara State University, Malete, Nigeria

Abstract. Cryptography and Steganography are two distinct approaches for protected data hiding and diffusion that are widely obtainable. One hides the presence of the message and the other garbles the message. The practices made use of information to cipher or cover their existence correspondingly. Cryptography is the science of using mathematics to encrypt and decrypt data; the data are transformed into some other gibberish form, and then the encrypted data are diffused. While Steganography is the art and science of hiding messages, steganography embeds hidden content in an unexceptional cover media to avoid spy's suspicion. In steganography the clandestine message embeds in an undisruptive looking cover such as a digital image file and the image file is transmitted. In our proposed method, we use Steganography procedure where secret message is implanted within a hauler image file and the existence of message is hidden from the prowler. To prevent disclosure of contents of the covered file RSA algorithm is used with Steganography to enhance the sturdiness of the system. Usually in practice RSA public and private exponents are chosen to be very large this makes the decryption process slow. And to speed it up we employ the use of Chinese Remainder Theorem which concentrates on modulus calculation. This paper proposes a faster RSA-CRT algorithm for decryption of data. And by employing this technique on RSA algorithm by matching data to an image, there is less chance of an attacker being able to use steganalysis to recover data. Before hiding the data in an image, the application first encrypts it.

Keywords: RSA algorithm, cryptography, steganography, LSB method, Chinese Remainder Theorem

1. Introduction

The increasing usage of the Internet and availability of public and private digital data and its distribution has motivated industry professionals and researchers to pay a serious attention to information security. Internet users regularly need to store, send and receive private information and this private information needs to be protected against unauthorized access and attacks. Presently, three main methods of information security being used: watermarking, cryptography and steganography. In watermarking, data are hidden to convey some information about the cover medium such as ownership and copyright. Cryptography techniques are based on rendering the content of

a message garbled to unauthorized people. Steganography techniques are based on hiding the existence of information by embedding the secret message in another cover medium. While all three are information security techniques cryptography and steganography are having wide application as watermarking is limited to having information particularly about the cover medium. With the growth of computer network, security of data has become a major concern and thus data hiding technique has attracted people around the globe. Steganography techniques are used to address digital copyrights management, protect information, and conceal secrets.

As digital information and data are transferred over the internet and securing sensitive messages need to discover and developed more often than ever before, new technologies for protecting and securing the sensitive messages needs to realize and develop. Because cryptography and steganography methods always exposed to attacks by Steganalysis, so we constantly need to develop and look for new modes. Cryptography and Steganography are well-known and widely used techniques that handle information in order to cipher or hide their existence respectively. Steganography is the art and science of communicating in a way, which hides the existence of communication. On the other hand, cryptography is the enciphering and deciphering of data and information with a secret code so it cannot be understood. The Steganography hides the message so it cannot be seen. But, cryptography systems can be broadly classified into symmetric-key systems that use a single key, both the sender and the receiver have, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses. In Cryptography, a cipher message, for instance, might provoke. Suspicion on the part of the recipient while an invisible message created with steganographic methods will not. However, steganography can be useful when the use of cryptography is illegal. Where cryptography and strong encryption are barred, steganography can avoid such policies to pass the message secretly. However, steganography and cryptography differ in the way they are judged. Cryptography fails when the "enemy" is able to access the content of the cipher message, while steganography fails when the "enemy" detects that there is a secret message present in the steganographic medium. The combination of these two methods will enhance the security of the data embedded. This combination will satisfy the requirements such as capacity, security, and robustness for secure data transmission over an open channel. Thus, to speed up the encryption and decryption process we employ the use of Chinese Remainder Theorem which concentrate on moduli calculation and proposes a faster RSA-CRT algorithm for decryption of data.

2. Literature Review

With the high awareness and the rapid growth of communications and the use of internet services there is a great security and threat of a snooper gaining access to secret information. This has prone a strenuous concern for data communication experts. Cryptography and steganography are the most commonly used techniques to overcome this threat. These techniques received more attention from the research community. The reason for this growing interest is due to the combination of these two techniques together which can often achieve a higher level of security.

Ushl et al. proposed an encrypting system, by combining the techniques of cryptography and steganography with data hiding. Instead of using a single level of data encryption, the message is encrypted twice. Conventional techniques have been used for this purpose. Then the cipher is hiding inside the image in the encrypted format for further use. It uses a reference matrix for the selection of passwords depending on the properties of the image.

Bharti and Soni proposed a novel scheme based on steganography and cryptography to embed data in color images. This method shows its larger capacity for hiding data than other methods without loss of indistinctness integer wavelet transform and Genetic algorithm. The method is very efficient, especially when applied to those images whose pixels are scattered homogeneously and for small data. Marwaha and Paresh used traditional cryptographic techniques to achieve data encryption and visual

steganography algorithms have been used to hide the encrypted data. Multiple cryptography proposed where the data was encrypted into a cipher and the cipher will be hidden into a multimedia image file in the encrypted format.
Umamaheswari compress the secret message, encrypt it by the receiver's public key along with the stego key, and embed both messages in a carrier using an embedding algorithm.
Kandar, and 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.
Bairagi describes how such an even-odd encryption based on ASCII value is applied and how encrypted message converting by using Gray code and embedding of picture that can secure the message and thus makes cryptanalyst's job difficult.
The aim of this proposed scheme is to make a more secure and robust method of information exchange so that confidential and private data must be protected against attacks and illegal access. In order to achieve the required robustness and security cryptography and steganography is combined. Image is taken as a cover medium for steganography and RSA algorithm is used for encryption. However, RSA cryptosystem is known to be slower than symmetric key alternative in the area of cryptographic algorithms due to their basis in modular arithmetic. Therefore, how to enhance the speed of RSA algorithm has been our main focus in enhancing computer security. The encryption operation given by $c = m^e \bmod n$ requires an expensive computing procedure. As a result, we need to first provide optimizations to simplify the RSA cryptosystem. In this proposed method the advanced LSB bit manipulation method is used for embedding the message in the image file and the message is itself encrypted using the existing RSA encryption method. For embedding the text in image file firstly both the text and image file are converted into binary equivalent and then text is encrypted using RSA. The encrypted text is then embedded into the image file using the advanced LSB algorithm. Thus, we proposed a faster RSA-CRT algorithm for decryption of data. Contrary to other methodologies which try to detect embedded data or accomplish a time-consuming computation as part of their processes we focused on an all-inclusive Steganographic prevention which works in real time on any image data.

3. Steganography

Steganography is a longstanding technique of information hiding. Steganography refers to the science of invisible communication. Unlike cryptography, where the goal is to secure communications from an eavesdropper, steganographic techniques strive to hide the very presence of the message itself from an observer. The term Steganography is bifurcated from the Greek words "stegano"s meaning "cover" and "graphia" meaning "writing" defining it as covered writing. Before performing steganography, we need three primary frills which are Secret message, cover medium and one or more embedding algorithm(s). Besides these,` we can also use secret key for better security purpose. In the process of steganography, the cover medium can be a text file, an image, an audio file or it can be a video file but among these the most popular is the image steganography.

3.1 Combination of cryptography & steganography

Steganography must not be confused with cryptography that involves transforming the message so as to make its meaning obscure to malicious people who intercept it. In this context, the definition of breaking the system is different. In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganographic system needs the attacker to detect that steganography has been used and he is able to read the embedded message. Steganography provides a means of secret communication, which cannot be removed without significantly altering the data in which it is embedded. In addition, the security of classical steganography system relies on secrecy of the data encoding system. Once the encoding system is known, the steganography system is defeated.

However, it is advisable to use Cryptography and Steganography together for adding multiple layers of security. By combining, the data encryption which can be done by a software and then embed the cipher text in an image or any other media with the help of steganographic key. The combination of these two methods will enhance the security of the data embedded. This combined chemistry will satisfy the requirements such as the size, security and sturdiness for secure data transmission over an open channel. The figure below depicts the combination of cryptography and steganography.

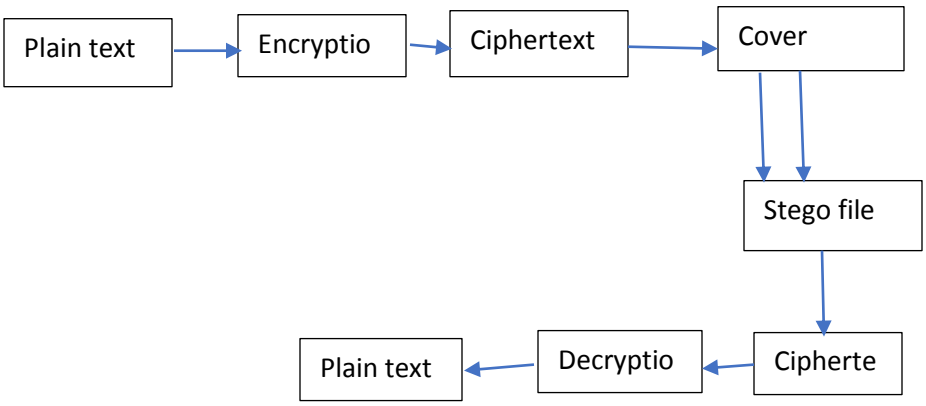

Fig 1: Combination of Cryptography and Steganography

4. The Proposed RSA – CRT Based Data Hiding Using Steganography and Cryptography

The two algorithm LSB (Least Significant Bit) and RSA (Rivest Shamir Adleman) are joint together to offer more level of protection. The message is first encrypted using cryptography to a cipher text. This cipher text is then embedded in a cover media using Steganography. This combined approach will satisfy the three goals of data hiding, security, capacity and robustness. The Least significant bit (LSB) coding is used to embed the information in a digital image file by substituting the least significant bit of each sampling point with a binary message. The LSB data hiding technique is one of the methods used for injecting data into digital signals in noise free environments, which embeds secret message-bits in a subset of the LSB planes of the image.

RSA is one of the first practicable public-private key cryptosystems and is widely used for secure data transmission. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers. A user of RSA creates and then publishes a public key based on the two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.

Both RSA and LSB algorithm are implemented together. Steganography is responsible for data hiding and cryptography does the scramble of the data sequences, these dual approaches will enhance the data security.

To extract a secret message from a LSB encoded image file, the receiver needs access to the sequence of sample indices used in the embedding process. Normally, the length of the secret message to be encoded is smaller than the total number of samples in an image file. Extraction process is exactly reverse of the embedding process. The secret message embedded in the image file is given as the input which is called the stego image file. In the extraction process data is extracted from the embedded file.

The security of the RSA cryptosystem is based on two mathematical problems: the problem of factoring large numbers and the RSA problem. Full decryption of an RSA cipher text is thought to be infeasible on the assumption that both of these problems are hard. The RSA problem is defined as the task of taking e^{th} roots modulo a composite n: recovering a value M such that $C \equiv M^e \pmod{n}$, where (n, e) is an RSA public key and C is an RSA cipher text.

CRT decryption is much more effective than RSA decryption.CRT guarantees that there is a solution because in this case all moduli are pairwise relatively prime. When the numbers are much larger, using CRT is much more efficient than directly performing the calculation. Chinese Remainder Theorem (CRT) speeds up the private key operations. The CRT remainder techniques are useful in developing code that detects errors. In cryptography, the CRT is used in secret sharing through error-correcting code. The CRT is itself a secret-sharing scheme without any need for modification.

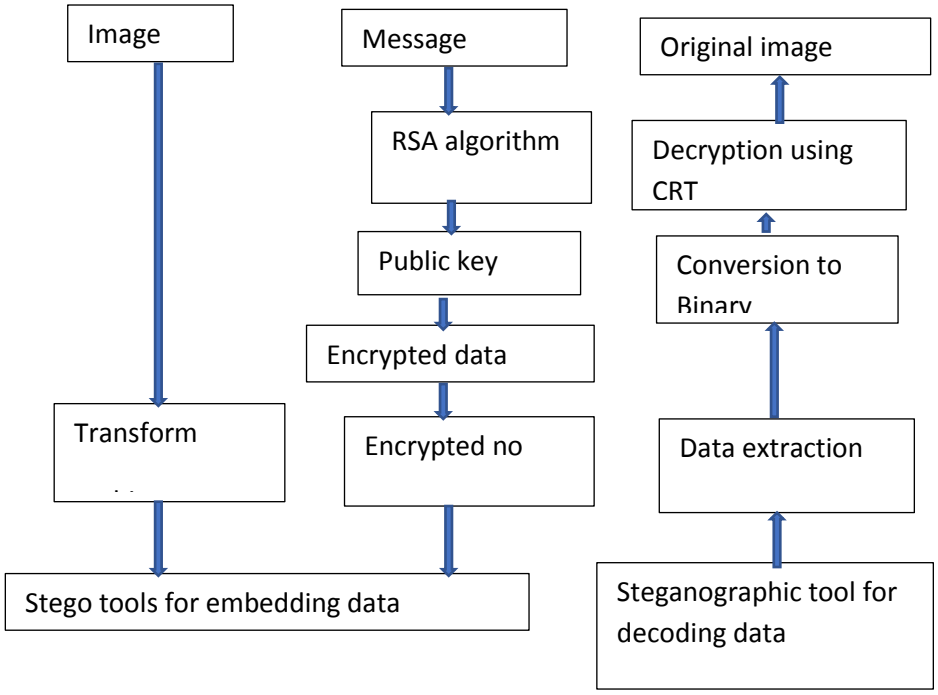

Fig. 2 Block diagram of the proposed system

Chinese Remainder Theorem, CRT, is one of the main theorems of mathematics. The RSA-CRT is employed during decryption process. It enhanced a faster decryption than modular exponentiation. RSA-CRT differs from the standard RSA in key generation and decryption.

When destination node receives the encrypted message, it decrypts this encrypted message using CRT in the following manner:

dp=d mod(p-1).
dq=d mod(q-1).
qinv =q-1 mod p.
m1 = C^{dp} mod p.
m2 = C^{dq} mod q.
h = (qinv * (m1- m2)) mod p.
M = m2 + h*q

Where,
p, q = Two prime numbers such that
N = p.q.
d, N= private key of destination node

5. Experimental Process, Results and Discussions

The proposed method is designed for bmp images. It first compares the length of the message to be concealed with the size of the image to ensure that the image can hold the

secret file. If the size of secret file is more, then a new image is selected. When using a 24-bit color image, a bit of each of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel. So, one layer between R, G, B is selected and message is inserted in the selected layer. Thus, an 800 × 600-pixel image can contain a total amount of 800x600x1=480.000 bits (60.000 bytes) of secret data. It has three levels of security as follows:

Level I-The message is inserted at a random pixel value of the image as inserted by the sender. It can be any row and column of the image matrix. But precaution must be taken such that message length should not exceed matrix size.
Level 2-The message to be sent is encrypted using an RSA encryption
Level 3-The encrypted message is inserted to image using LSB technique. In LSB technique encrypted message is converted to binary form and inserted in the least significant bit of pixel value as inserted before.

These are the three levels of security that enable the process to be highly secured. If anyone try to break into the system then he has to know the starting position of the message then encryption method used and method of insertion. This made it difficult and most discouraging for the infiltrators.

5.1 Algorithm for Concealing messages (Sender Side)

Input: message, cover image

Output: stego image (containing message)

store location of image where message is to be hidden

Insert the message

Encrypt the entered message

Convert the encrypted message to unsigned integer form

Find the length of the message inserted

Now convert it in to binary form

Transform the binary number to its residue number system

Store the message in a one row matrix

Store the message length in a predefined position of image

Now insert the binary format message in to image

Save the image

End

5.2 Algorithm Extraction message (Receiver side)

Input: stego image(containing message)

Output: hidden message

Enter location to start (Stego key)

Retrieve the size of the hidden message

Retrieve the message by same insertion method

Decrypt the retrieved message

Convert the residue number system to the conventional number system

Display the message

End

The same stego key is used for decoding of secret message from the stego image. The stego key is used to generate the same random number with which selection of the pixels is done and the order of block.

6. Conclusion

In this paper a new way of hiding information in an image with less variation in image bits have

been proposed which makes our technique secure and more efficient than LSB? In our proposed method, we use Steganography procedure where secret message is implanted within a hauler image file and the existence of message is hidden from the prowler. To prevent disclosure of contents of the covered file RSA algorithm is used with Steganography to enhance the sturdiness of the system. Usually in practice RSA public and private exponents are chosen to be very large this makes the decryption process slow. And to speed it up we employ the use of Chinese Remainder Theorem which concentrates on modulus calculation. This paper proposes a faster RSA-CRT algorithm for decryption of data. And by employing this technique on RSA algorithm by matching data to an image, there is less chance of an attacker being able to use steganalysis to recover data. Before hiding the data in an image, the application first encrypts it. This technique also applies a cryptographic method. RSA algorithm to secure the secret message so that it is not easy to break the encryption without the key. RSA algorithm itself is very secure that's why we choose the technique to increase the security of the secret message. The results obtained showed that CRT is better to deal with RSA cryptosystem complexity. Experimental results indicate that our schemes substantially outperform the related state-of-art RSA cryptosystem in terms of computational cost, speed and security.

References

K.Hemachandran, "Study *of Image Steganography using LSB, DFT and DWT",* International Journal of Computers & Technology, Vol 11, oct.25 2013, pp. 2618-2627

Zin.w, soe. N "*Implementation and Analysis of three Steganographic Approaches*", University of Computer Studies, Mandalay, 2011, pp. 456-460

Manoj.s,"Cryptography *and Steganography*", International Journal of Computer Applications (0975- 8887), 2010, Vo1-No.12, pp. 63-68

Adewole Kayode S. and Oladipupo Ayotunde J. *"Efficient Data Hiding System using Cryptography and Steganography*", International Journal of Applied Information Systems (IJAIS), Volume 4– No.11, December 2012, pp. 6-11

Anil kumar, Rohini Sharma "*A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique"* International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013

Muhammad Asad, Junaid Gilani, Adam Khalid "An enhanced Least Significant Bit Modification Technique for Audio Steganography",2011 international conference on Computer Networks and Information Technology (iCCNIT),pages143-147.

Masoud Nosrati, Ronak Karimi "*An Introduction to Steganography Methods"* World Applied Programming, Journal, Vol (1)-No (3), August 2011. 191-195

Application of steganography. Internet source http://www.datahide.com/BPCSe/applications-e.html

G.N. Shinde and H.S. Fadewar," Faster RSA Algorithm for Decryption Using Chinese Remainder Theorem" ICCES, Vol.5, No.4, pp.255-261.