ISSN No:-2456-2165

Data Veiling Using Residue Number System based Encryption in Cybersecurity

Eseyin Joseph B.
ICT Directorate,
University of Jos, Jos Nigeria

Akanni Gabriel A.,
Kwara State College of Education
(Tech), Lafiagi, Kwara State

Kazeem A. Gbolagade
Department of Computer Science
College of Library and Information Technology
Kwara State University, Malete, Ilorin

Abstract:- In today's technologically advanced world, providing a secure communication route has become a difficult task. There is an extraordinary need for protection as risks to privacy become more prevalent. Cryptography and steganography are critical security approaches, however with the upsurge in network invaders, these approaches must adapt quickly to dodge these perils. The focus of this work is on image steganography, where the asylum instrument is a picture. We propose in the report a multilayer security approach for converting message text to its residue number system equivalent, using asymmetric encryption method, and embedding the ciphertext in the least significant bits of an image before sending it over the network to the intended recipient. The information is buried from the interloper in this approach, if it is discovered, decoding it would be problematic, providing a four-layer of security. The embedding and the extraction memory used were measured to show the whacking capability of the model and the histogram of the message to ensure that the distortion on the image imperceptibility is not visible.

Keywords:- *Least Significant Bits, Steganography, Cryptography, Residue Number System, Image Embedding, Image Extraction, ASCII Code.*

I. INTRODUCTION

For secure transmission the sender turned the plaintext to an indecipherable ciphertext and the receiver translating the ciphertext overturn it to its initial

text using secret keys. Cryptography's role is to ensure data's confidentiality, integrity, and authenticity. Aside from the old customary methods, there are twin types of secret-key cryptography: symmetric and asymmetric cryptographies.

Encryption is simply defined as turning a plain text into ciphertext and decryption as transforming the ciphertext into the original plaintext. While steganography is the method of keeping veiled data in digital material such as imageries, aural files, and audiovisual files.

These digital media serve as concealment for sensitive information and aid in transmission. The focus of this study is on image steganography, where the cover medium is a picture. Both approaches are significant, but operate superlatively when used together. When cryptography is employed alone, the intruder has access to the ciphertext, and security can be undermined if sufficient cryptanalysis is performed. When used alone, steganography hides data, however, if discovered by an invader, decrypting the data isn't difficult. As a result, the combined method is recommended since it ensures data confidentiality, integrity, authenticity and concealment. The information is secreted from the impostor in this approach, and if it is discovered, decoding it might be tough, providing a multilayer of security. In Steganography, the stego image modelled after the clandestine message concealment must not be slanted too much and necessarly be parallel to the original image. When steganographic security is conceded due to distortions Peak Signal Noise Ratio (PSNR) values are measured to determine the extent of alterations. This research present a strategy for improving PSNR using asymmetric or public-key encryption and picture steganography.

The remaining part of the paper discusses the literature review, the proposed method, the sample working model, the experimental results, and the conclusion.

II. LITERATURE REVIEW

Cryptography refers to data encryption, that transform plain text to ciphertext that is aimed at securing data for transmission. Cryptanalysis is the decryption procedure of information deprived of the awareness of encryption schemes.William Stallings [8] discusses several forms of enciphering and deciphering schemes.

Undisclosed information is veiled in a cover media, and picture steganography is one type of steganography in which the cover media is image.

Steganography is accomplished using a variety of techniques, one of which is LSB replacement, which involves replacing the image's least significant bits with the message to convert the innovative image into a stego image. As a result lone restricted data can be buried in the asylum image as explained in [9]. This paper examines the implanting ability of shielding pictures using LSB-based approaches for image

ISSN No:-2456-2165

steganography, to make stego pictures indistinguishable. A considerable quantity of bits must be adjusted when employing LSB substitution-based approaches. In [7], a bit charting scheme is described, in which bits from the shelter channel and undisclosed data that is reasonably organized into braces, these collections bits of secret data are charted to the most significant bits of the concealment medium, and the charting position is conserved by using two-bit LSB substitution. An improved form of the LSB replacement is the reversed LSB technique suggested in [3,] which complements the stealthy communication before applying the reversed LSB technique to arbitrarily designated pixels of the image. Because the number of vicissitudes in bits of pixels of the inventive image is less in this method than in unpretentious LSB approaches, the PSNR assessment is improved. Concerning [4] and [3], various steganographic methods for information concealing in images in JPEG format and spatial representation are investigated, with highlight on imperceptibility, resilience, and hiding capacity and associated methods for steganalysis. There are cryptographic and steganographic systems for data security, but individual procedure has their own set of issues. As a result, a combined technique as proposed in [1] is used, It uses enhanced PVD picture steganography developed in [2] for data concealing and modified AES for encryption to increase data security and image embedding capacity.

Another example of combining cryptography and steganographic procedures is revealed in [10], in which surreptitious file to be communicated is first compressed, then AES algorithm is expended to generate the ciphertext. For pixel selection, the ciphertext is subsequently concealed in the asylum media. The clandestine file is further sheltered thanks to the employment of a genetic algorithm. The inherited algorithm is grounded on the notion of persistence of the fittest. [7] adapts a vibrant approach that uses mutually crypto and steganographic approaches through the RSA algorithm as the cryptosystem. RSA cryptosystem is employed to act on the secret data, in this case, the outcome and concealment media are arranged to blocks. These cipher blocks are dynamically assigned to circular queues using adaptive LSB substitution mechanism. RSA cryptosystem and uses were examined in [8] with the operation of RSA Public key cryptosystem, even for very long communications an approache to improve the RSA cryptosystems, were reviewed in [9]. This includes a look into the RSA algorithm's performance. A Residue Number System signifies a huge numeral using set of smaller integers, so that computation may be performed more efficiently. It relies on the Chinese Remainder Theorem (CRT) of modular arithmetic for its operation. RNS comprises a set of moduli that are independent of each other. An integer is represented by the residue of each of the modulus and arithmetic operations are based on residues individually. The advantage of using the RNS over the conventional system includes “carry-free” operation, fault tolerance, parallelism, and modularity [5]. These inherent features make RNS to be widely used in Digital Signal Processing(DSP) applications such as digital filtering, convolution, fast Fourier transform, and image processing. [6].

III. PROPOSED METHOD

Our suggested message security solution is combination of cryptography with steganography. The flow diagram depicts the stages that were taken as shown in Figure 1

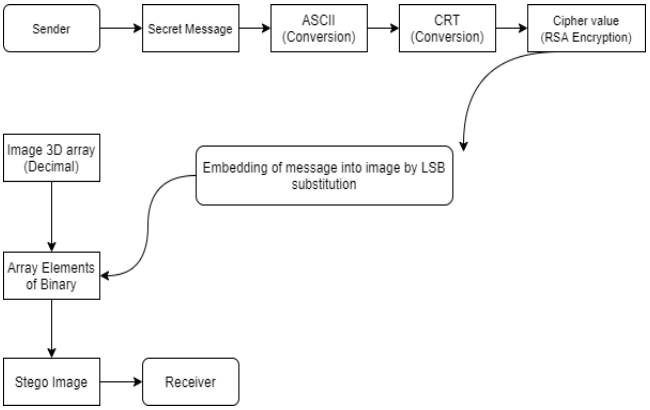

Fig 1 Flow diagram of Encryption and embedding of the stealthy message

➢ Encryption and embedding algorithm

Steps in Encryption and Embedding Algorithm

1. The stealthy message sent is encoded in ASCII characters. Then retrieve the message's decimal values

2. The message is transformed to its residue number system equivalent.

3. The values are then encrypted utilizing the RSA public-key cryptosystem

4. use the sender's private key with the receiver's public key to produce encrypted data in decimal format.

5. Transform The decimal-formatted encrypted values to binary format.

6. Paddled, the binary values of respective character with 0s as needed to generate a value with specified constant bits,

7. Read the image as three-dimensional array representing the RGB values of the pixels.

8. In the first few bits of the first row of the image, encrypt the number of characters in the covert message, followed by the message bits being encoded in the subsequent rows.

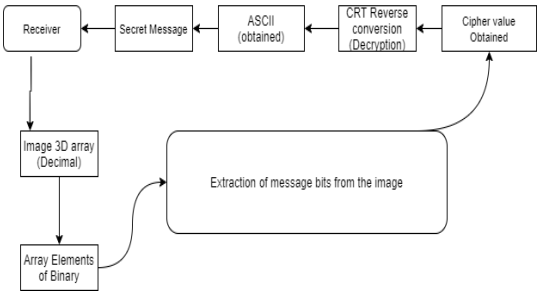

Fig 2 *Flow diagram of Decryption and Extraction of the stealthy message*

The decryption and extraction algorithm is the reverse of the encryption and embedding algorithm.

Before embedding in the picture array are transformed to binary representation and substitution is used for embedding. Each picture array element's two least significant

bits are sequentially replaced with two-two bits of the message. It is delivered to the receipient after embedding the full message into an image to generate a biased image known as a stego image.

➢ *Decryption*

The receiver got the message and did the following: -

1. *The receipient takes the stego image as three-dimensional array of RGB for the pixels, extracting the picture length from the initial row. The elements of the picture array are first converted from decimal to binary format then the last two bits of individual element are received and combined. Characters may be extracted deprived of issue because the size of individual character is chosen as a constant during encryption.*
2. *After that, the message bits are separated into sets of bits, each set including the number of constant bits selected for individual character during encryption.*
3. *Because step [4] of encryption is completed during encryption, individual set is transformed to decimal form to acquire the values in binary format.*
4. *To acquire enciphered values, the values of individual set acquired are transformed from binary to decimal format.*
5. *The initial decimal values are obtained by decrypting the decimal values using the RSA technique and the sender's public key and receiver's private key.*
6. *Each decimal value in individual set corresponds to the ASCII value of the secret message character, with each of the decimal values translated into a string to acquire the stealthy message.*

Asymmetric key cryptography, or RSA, is a system that uses asymmetric keys. The recipient is given a public and a private key, both of which result from the combination of two separate prime numbers. Both the sender and the public can be aware of the former. without compromising security, whereas the later required be kept hidden from the transmitter. The sender encrypts the message and directs it to the receiver by means of the public key. The recipient uses the private key to decode the message. The usage of two keys is referred to as asymmetric key cryptosystem. Concerning Stallings, 2017, the algorithm for key creation, encryption, and decryption is examined. Peak signal to noise ratio (PSNR) metrics is used to determine the alterations amongst the asylum picture and the stego picture.

The following formulas can be utiised to determine PSNR:

$$\text{PSNR} = 10 \log_{10}\left(\frac{MAX}{MNE}\right)^2$$

$$= 20 \log_{10}\frac{MAX1}{\sqrt{MSE}}$$

$$20\log_{10}(MAX_I) - 10\log_{10}(MSE_2)$$

$$MSE = \frac{1}{mn}\sum\sum[I(i,j) - k(i,j)]\,2$$

I(i,j) is the original image.

The image K(i,j) has been rebuilt.
The image dimensions are m,n.
MAXI is the image's maximum pixel value.

➢ *Sample Working Model*

Text message: - Eseyinj Key: - Hello

Step 1: Adjust the key and text message to ASCII code.

From the ASCII code table:
Hello is transformed in
H [5] = {72,101,108,108,111}
Eseyinj is changed to
E [7] = {69,115,101,121,105,110,106}
Step 2: Swab the text message to the length of the key.
Eseyinj has 7 characters and the key has 5 letters,
so the first five letters of the text will vary according to the key and at the end, the two-letter left is padded with the letter z for filling to make the precise size of the message.
*Eseyinj Eseyi**njzzz***
E [7] = {67,115,101,121,105,110,106, 122,122,122}
l = length of key

Step 3: Process with residue number system the encryption get two arrays Xtxt and Xkey of the dimension of the lengthof text message and key and imbuse it with zeros.
perform this procedure until the dimension of the key

In using the key:

```
for k=1to l
J=1
for  i=1 to g              (g  is the length of padded text)
{
if(j>l)
  {j=1
   e[i] =e[i] +  h[j]j++
}
else
{          e[i] =e[i] + h[j] j++
}
End for
```

To hide the key:

```
Do
for j=1 to l-1

  e[g]=e[g]+e[g+1]
end for

e[l]=e[l]+e [1]

End for
```

Step 4. Transform array H and E in to character:

```
For i=1 to g
 While
  e[i]>256
 e[i]=e[i]-256
Xtxt[i]+=1
 end while
```

ISSN No:-2456-2165

end for
for i=1 to l
while
h[i]>256
h[i]=h[i]-256
Xkey[i]+=1
end if
end for

Step 5. Process the Decryption Algorithm
Perform CRT decryption
Transform the encrypted text message to ASCII code:
E [12] = {20,143,29,231,256}
H [20] = {10,2,230,19,23}
The decryption of data and keys:
for i=1 to l (l is the dimension of padded text)
while
Xtxt[i]! =0
e[i]=e[i]+256
Xtxt[i]
end while
end for
for i=l to l
while
Xkey[i]! =0
h[i]=h[i]+256
Xkey[i]
end while
end for

for k=l to l
h[l]=h[l]-h[1]
for j=l-1 to 1
h[j]=h[j]- h[j+1]
end for
j=1
for i=1 to l
if(j>l)
j=1
e[i]=e[i]-h[j]
end if
end for
end for

Step. 6 Pixel processing

After the conversion, the information in scrambled form is to be patched with the information in the image.

*1111100**0*** ⟶ *11111001*

The modification is merely one bit, allowing for a simple data transmission and minimal impact on the image's intensity. T update an image with data: -

select a source image,
find the values of the pixels,
choose the pixel where data is to be inserted.

Inset the data values in pixels, for example, a grid for An image with 24 bits can have the following 3 pixels:
*0010110**1** 0001110**0** 1101110**0***
*1010011**0** 1100010**0** 0000110**0***
*1101001**0** 1010110**1** 0110001**1***

When the letter H from Hello(Xkey) is to be embedded, its decimal value is 72 with the binary representation of 01001000. The generated grid is as follows when the least significant bit of this area of the image is entered.:
*0010110**0** 0001110**1** 1101110**0***
*1010011**0** 1100010**1** 0000110**0***
*1101001**0** 1010110**0** 0110001**1***

e Decimal =101, binary = 01100101
*0010110**0** 0001110**1** 1101110**1***
*1010011**0** 1100010**0** 0000110**1***
*1101001**0** 1010110**1** 0110001**1***
l Decimal = 108, binary= 01101100
*0010110**0** 0001110**1** 1101110**1***
*1010011**0** 1100010**1** 0000110**1***
*1101001**0** 1010110**0** 0110001**1***
l Decimal = 108, binary= 01101100
*0010110**0** 0001110**1** 1101110**1***
*1010011**0** 1100010**1** 0000110**1***
*1101001**0** 1010110**0** 0110001**1***
o Decimal = 111, binary = 01101111
*0010110**0** 0001110**1** 1101110**1***
*1010011**0** 1100010**1** 0000110**1***
*1101001**1** 1010110**1** 0110001**1***

Because the intensity of the image only changes by 1 or 0 after the information is hidden, the least significant bit is used for data patching.. This embedding process is equally performed for the text message Eseyinj (Xtxt)

IV. EXPERIMENTAL RESULT

The recommended technique in this work is simulated in MATLAB, yielding the following results. To obtain the stego images, four diverse ordinal images were acquired and clandestine messages of length 800 were encrypted and placed in individual of the images.

➢ *Findings and discussions on Data Shrouding in steganography using CRT based RSA Encryption*

- *The Embedding Memory and Extracting Memory*

The cover images with the embedding memory are in table 1.

Table 1 The RSA embedding and RSA- CRT embedding memory

	RSA: Embedding Memory	**RSA-CRT: Embedding memory**
Eagle	3.25E+09	1.20E+09
Baboon	2.21E+09	1.19E+09
Gold Fish	2.18E+09	1.18E+09
Pepper	3.22E+09	1.17E+09
Lena	2.20E+09	1.21E+09
Babooon	2.90E+09	1.20E+09
Redroses	3.30E+09	1.20E+09
Dog	1.91E+09	1.22E+09

ISSN No:-2456-2165

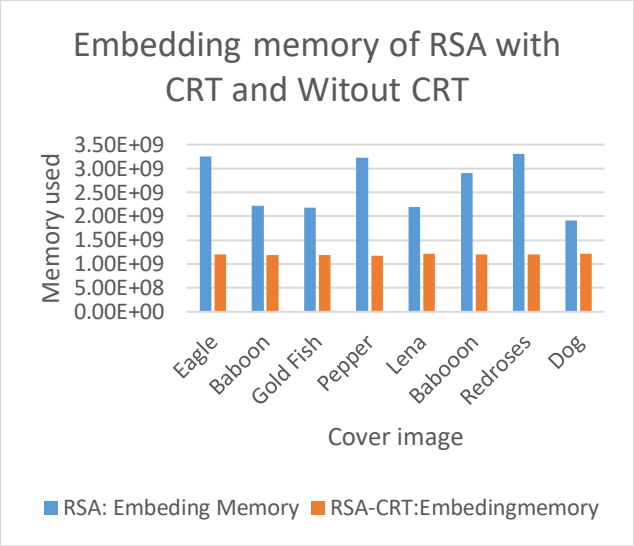

Fig 3 Embedding memory RSA and RSA with CRT

Using Chinese Remainder Theorem on the RSA encryption process before embedding, it is seen from Table 1 and Figure 3 that the memory used is significantly lower than RSA embedding without the CRT. It thus conserved memory and minimized resource utilization.

Table 2 The RSA extraction memory and RSA- CRT extraction memory

Cover image	RSA: Extraction Memory	RSA-CRT: Extraction memory
Eagle	2.26E+09	1.20E+09
Baboon	1.27E+09	1.02E+09
Gold Fish	2.08E+09	1.19E+09
Pepper	1.43E+09	1.03E+09
Lena	1.60E+09	1.01E+09
Babooon	1.51E+09	1.21E+09
Redroses	2.21E+09	1.01E+09
Dog	3.22E+09	1.22E+09

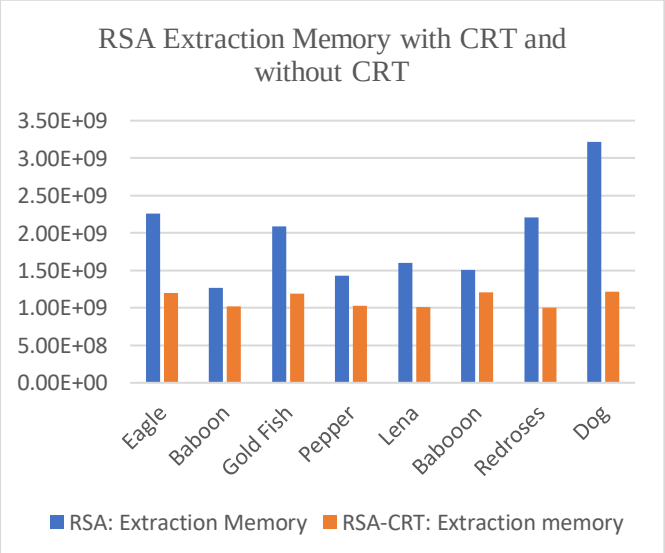

Fig 4 Extraction memory of RSA and RSA with CRT

V. CONCLUSION

In today's fast-paced communications ecosystem, data protection from unwanted access is a serious worry. One of the furthermost effective strategies we mentioned is using the most efficient RSA and LSB algorithms to create the most reliable and secure systems. The improvement of hiding data in the asylum image is greater. To solve decryption at a sluggish pace, fast RSA-CRT algorithms are used. We employed the RSA encryption technology to protect two layers, and we discovered that decryption of RSA-CRT is faster than standard RSA and with an enhanced reduction in decryption memory. To identify the flaws in the RSA decryption memory, an analytical comparison of the RSA and RSA-CRT decryption algorithms is designed and implemented. Initial results demonstrate that utilizing CRT to decrypt with RSA improves decryption memory performance significantly.

REFERENCES

[1]. Marwa E. Saleh, Abdelmgeid A. Aly, and Fatma A. Omara, "Data Security Using Cryptography and Steganography Techniques",(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 6, 2016.

[2]. M. E. Saleh, A. A. Aly, and F. A. Omara, "Enhancing Pixel Value Difference (PVD) Image Steganography by Using Mobile Phone Keypad (MPK) Coding", International Journal of Computer Science and security (IJCSS), Volume (9), Issue (2), pp. 397 - 397, 2015.

[3]. Rupali Bhardwaj and Vaishali Sharma, "Image Steganography Based on Complemented Message and Inverted bit LSB Substitution", 6th International Conference On Advances In Computing & Communications, ICACC 2016, 6-8 September 2016, Cochin, India.

[4]. Bin Li, Junhui H, Jiwu Huang, and Yun Qing Shi, "A Survey on Image Steganography and Steganalysis", Int. J. Inf. Hiding Multimedia Signal Process. 2 (2011) 142–172.

[5]. Eseyin, J. B. and Gbolagade, K. A A residue number system based data hiding using steganography and cryptography. KIU Journal of Social Sciences, [S.l.]. 2019;5(2):345-351. July. ISSN 2519-0474.

[6]. Eseyin J. B. and Gbolagade K.A. Data Hiding in Digital Image for Efficient Information Safety Based on Residue Number System. Asian Journal of Research in Computer Science 8(4): 35-44, 2021; Article no.AJRCOS.68473 ISSN: 2581-8260

[7]. Marghny H. Mohamed and Loay M. Mohamed, (2016), "High Capacity Image Steganography Technique based on LSB Substitution Method", Applied Mathematics & Information Sciences, Appl. Math. Inf. Sci. 10, No. 1, 2016, pp.: 259- 266.

[8]. W. Stallings, "Cryptography and Network Security: Principles and Practices, 6th edition".

[9]. R. Chandramouli and N. Memon, "Analysis of LSB Based Image Steganography Techniques", Image Processing Proceedings. 2001 International Conference on, vol. 3, pp. 1019-1022.
[10]. A. Zakaria, M. Hussain, A. Wahab, M. Idris, N. Abdullah and KH. Jung, “High-capacity image steganography with minimum modified bits based on data mapping and LSB substitution”, Appl Sci. 2018; 8(11):2199.