An Improved Cryptographic Key Generation and Data Transmission Technique Using Images

Manchineni Chudamani, Narendrababu Tatini

Abstract: Providing security to the data is a very important aspect in communication system. The importance of security lies in each and every region like e-commerce, industry, education and data ware house. The two main methods used for protecting data from an intruders while transferring over an open channel network are cryptography and steganography. The encryption of data is done in cryptography and steganography hides the secret image in a cover image. In this paper we are encrypting the data with a new cryptographic algorithm called affine cipher. The alphabets and special characters are transformed into numerical values equivalent to them. The encrypted data is embedded into a cover image which is binded with a key generated from an binary image in order to provide much more security. The system using this process has the better security in transferring the secret messages from sender to the receiver through public channels

Index Terms: Cryptography, Encryption, steganography, affine cipher

I. INTRODUCTION

Cryptography is an art within which data is encrypted or reworked into some indecipherable format referred to as cipher text. Solely the licensed user having the key code, through that they will decipher the received message. The two major groups for encryption algorithm includes symmetric and asymmetric key encryptions.

In symmetric key encryption, the same key is used by sender and receiver for encryption and decryption. Whereas the 2 keys public key and private key are used in case of asymmetric key encryption. This type of encryption is called public key encryption. Key should be exchanged between the communication entities before the transmission of data. Key is one of the important factor of theses algorithms. Weak keys can easily be attacked by the attackers as compared to longer keys which are difficult to break. Symmetric key encryption algorithms are still widely used as powerful techniques in secure communication channel.

Steganography refers to the art of secret writing which places personal information into another data with the help of various rules and techniques. As a result only few i.e., authorized users can recognize the information embedded into other format. One more issue lies in how safely we are restricting the information with a key. The primary significance lies in how arbitrarily we are producing a key. Solanki and Patel attempted to improve the advanced information .

Gray scale image and color image are the two kinds of images available. The main variation between these two lies in number of bits in the pixel. The number of bits for each pixel is 8 in case of gray scale and it is 24 bits in case of color image. These 24bit color image has red, blue and green colors.

The two propagation techniques used for images are loss full and lossless domain. In loss full method the image is changed after insertion of data and in lossless image processing the original cover image is remained as it is. In this process it inserts the data into the place where the intensity of pixel value is not changed even after placing the data. So that the original form of cover image not change.

II. RELATED WORK

In this section we are going to discuss some previous methodologies and their corresponding techniques and limitations.

Out of various ways in key generation schemes, this paper[1] uses EEG signals to generate keys because they differ from person to person. A particular task is performed by the authorized person and the waveform is monitored through neurosky device. The device shows the electrical activity of brain membranes in the form of wave patterns. Later with the help of noise filters and ADC converters the wave pattern is changed to the binary format. The first 128 bits are used as key. The limitation with this is the same person wave patterns differ at two different trails.

This paper[2] uses distributed source encoding scheme for hiding data in the image. Here the image is encrypted and MSB bits of the each pixel is selected. The data is inserted in the MSB positions randomly. Due to this the original form of cover image is changed to some disturbed format. The one more limitation lies in increase of payload.

Instead of transmitting data directly over the public channel network, this paper proposes a method to modify data with the image. The image generally requires 16X16 matrix form. The proposed algorithm converts plaintext into ASCII format and then inserts the predefined user offset value to generate a matrix format. From the matrix format the image is plotted in the histogram of the matlab[3].

Steganography includes various ways of inserting data. Out of them the distortion technique inserts data on selected pixels. So that image distortion takes place and image appears in blur form. The second technique is masking and filtering insertion which is similar to waterrmasking which is the older method. Here[4] data is inserted on the front surface of the image but not visible.

So that compression of image takes place.

Revised Manuscript Received on April 18, 2019.

Manchineni Chudamani, Ecm, Kl Deemed To Be University, Vijayawda, India.

Narendrababu Tatini, Ecm, Kl Deemed To Be University, Vijayawda, India.

This compression further has the probability of loosing data. The third one is LSB insertion, where data is inserted in the lest significant position of the pixel bits. The insertion has the very minute modifications in the original image structure. The advantages are less robust in nature. It also embeds huge amount of data into image. The fourth method is transform domain technique which is difficult compared to others. The data insertion happens in frequency domain instead of time domain and the image compression also less. The author Rachmavati and Budiman[5] proposed a method that uses the affine cipher extended from ceaser cipher with a modified functionality. The formula used is c=((axp)+k)mod 26. It solves the puzzle problem by extending it to z/pz results in modular arithmetic.

Instead of using binary codes or short texts as keys, the author proposed a method to generate a key from an image. With the pixel x, y locations (2D-plane) of the image and formatting them to row-column wise. All the locations obtained are formed into a new matrix in row column form. By selecting the random pixel locations from the matrix and formed into the new column array and used as a key to bind the data. The decryption side the exact pixel locations have to find in order to retrieve the original key.

In this paper the authors[6] proposed a method that provides security in communication over the internet. The entire process includes 4 phases. Those are database creation, key generation, encryption and decryption. A complete data base with various color images(RGB) is created and used at both sides of transmission channel.

The authors uses logistic map and logic map techniques to generate key sequence[7]. The security is analyzed in terms of probability of error, entropy and visual properties. The histogram results obtained from both of them show that the encrypted image is uniform compared with the original key image. But the maps alone usage produces disturbed waveforms.

III. PROPOSED MODEL

For the purpose of improved security in transmission, we are encrypting the message that need to transmit with affine cipher algorithm. The generated encrypted data i.e., cipher text is placed into an image called cover image and protected them by binding with a key. Most generally short texts or key generating algorithms are used to generate keys. For improved security purpose key is generated from another image and transmitted prior before the communication. The image with hidden data is transmitted at the next step. At the receiver section the exact reverse operation is obtained i.e., at the first step key is generated from the first transmitted image and then the cipher text is retrieved from the second image. The final step includes decrypting the original message from cipher text using affine cipher algorithm.

IV. BLOCK DIAGRAM AND EXPLANATION

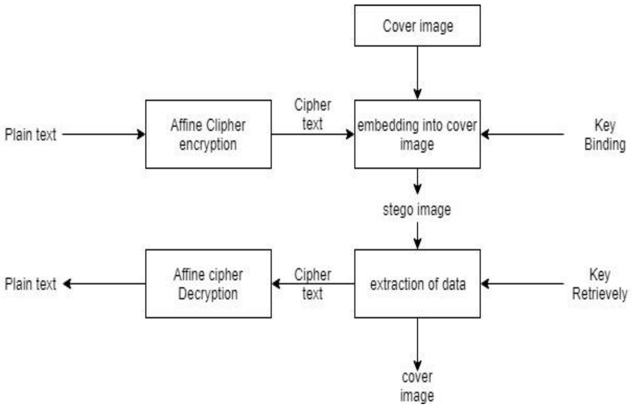


Fig.1: Block diagram of the proposed method

AFFINE CIPHER ALGORITHM:

This algorithm is used to encrypt the data. It takes each letter and special characters as an alphabet and mapped to the numerical proportional. The encoding process is done by using a scientific function and changed over back to the letter. So here each letter in the message appears like letters only but not the actual ones. This implies a basic standard substitution for the data over the image. Later with the help of ASCII codes, each letter obtained from the above function is changed to the ASCII format. The ASCII format is rearranged into binary codes for the improved security. The ASCII format is rearranged into binary codes for the improved security. This scramble information is inserted inside the picture.

STEPS:

1. Select the original message.
2. Find the numerical value (X) of each letter in the original message.
3. E(X)=(aX+b)mod m This function calculates the encrypted numerical value. where a and b are any agreed values between sender and receiver
   m= 26 (Total number of value in the alphabet)
4. E(X) is resultant number equivalent
5. Convert this numerical values to letters.
6. Generating the ASCII code for the above encrypted letters.
7. ASCII to binary format conversion.

EXAMPLE:

original text: encryption
assume a=2, b=4

Original text	**X**	**(2X+4)**	**(2X+4) mod 26**	**Cipher text[X]**
e	**4**	**12**	**12**	**m**
n	**13**	**30**	**4**	**e**
c	**2**	**8**	**8**	**i**
r	**17**	**38**	**12**	**m**
y	**24**	**52**	**0**	**a**
p	**15**	**34**	**8**	**i**

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

t	19	42	16	q
i	8	20	20	u
o	14	32	16	g
n	13	30	4	e

ASCII= 109 101 105 109 097 105 113 117 103 101
BINARY= 01101101 01100101 01101001 01101101 01100001 01101001 01110001 01110101 01100111 01100101

KEY GENERATION:

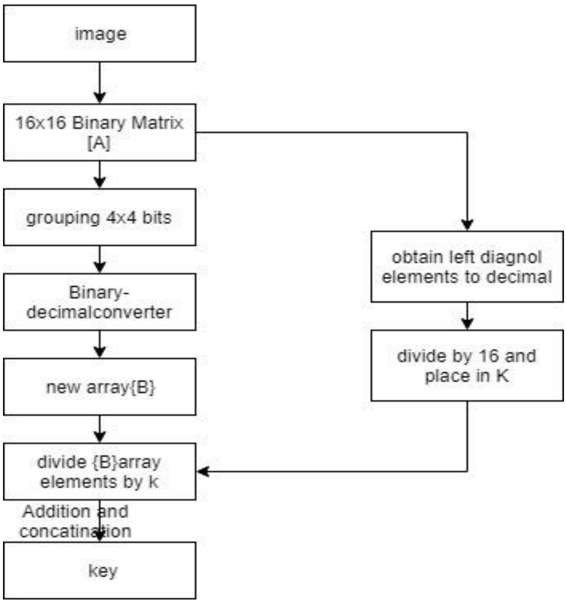


image
16x16 Binary Matrix [A]
grouping 4x4 bits
Binary-decimalconverter
new array{B}
divide {B}array elements by k
Addition and concatination
key
obtain left diagnol elements to decimal
divide by 16 and place in K

Fig.2: flow of key generation from image

The digital image used for generating key is represented by 16X16 matrix [A]. This is of binary form 0's and 1's. Then we are grouping the matrix [A] elements into 4X4 matrix form and converted to decimal form. Resultant shows 4X4 matrix [B] with decimal equivalents. For generating value to a variable K the left diagonal elements of original matrix [A] are taken, converted into decimal form and divided with 16. The resultant obtained is assigned to k. Now divide the elements of array[B] with k, then it shows new array [B']. Add row elements in the obtained array and then concatenate to generate the key.

DATA EMBEDDING:

Out of various ways , LSB is the basic methodology of inserting message into the picture. In case of gray scale image the 8th bit of each byte is rewritten to bit of secret message. For color image, the shades of every part like (red, blue, green) are changed. Any of the formats like BMP, JPG, GIF can be used. After inserting data the image file is changed to BMP format because of their lossless nature in compression. The algorithm has two types of encoding schemes sequential encoding and random encoding. In sequential encoding scheme, pixel values of the image is taken sequentially and LSB of the pixel is obtained in the same order. In random encoding scheme, the pixel value of the image is taken randomly with an agreed number from sender and receiver. The modulus 2 is calculated for each pixel value. It returns 0 or 1 based on the number is even or odd. Compare this value with the binary code generated from the affine cipher algorithm. If they are same then insert the data, otherwise modify the data with the message bit and calculate the next pixel value. This process is repeated till the complete data insertion completes. The receiver side operation is simpler if the above steps are used in reverse order.

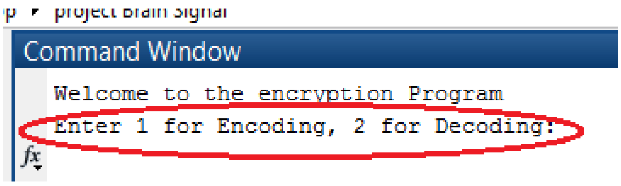
Data Insertion Algorithm:

1. Find out the pixel values from the cover image.
2. Choose the text message.
3. Select the encoding scheme.
4. Insert the first data bit at the 1st pixel LSB position.
5. Repeat step4 until data insertion completes.

Data Extraction Algorithm:

1. Find the pixel values from the stego image.
2. extract the data bits placed at the LSB position of the pixel data.
3. Repeat step2 until complete extraction of data takes place.

V. RESULTS



```
Welcome to the encryption Program
Enter 1 for Encoding, 2 for Decoding:
```

Fig.3: simulation results in encryption phase

The above result allow the user to select the requirement of task. In the sender section encryption is chosen and at the receiver section decryption is chosen.

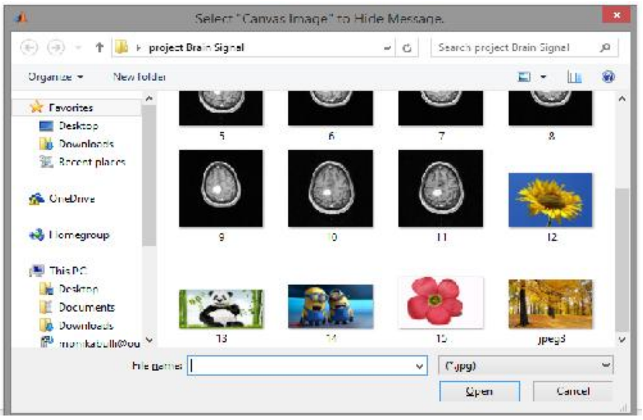
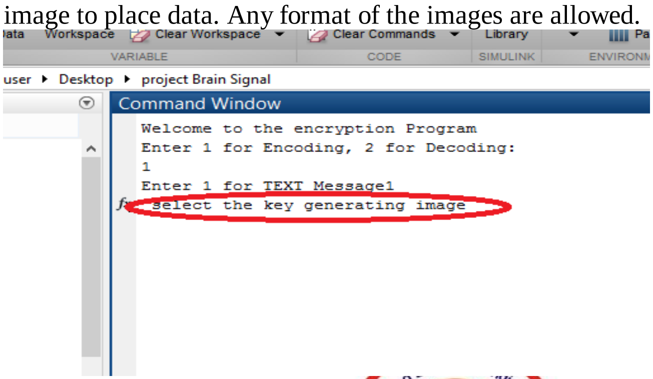


Fig.4: selecting the image for hiding data

Out of the jpg images from database the user selects the cover image to place data. Any format of the images are allowed.

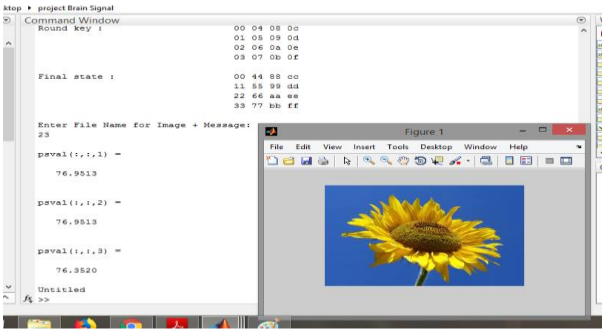


```
Welcome to the encryption Program
Enter 1 for Encoding, 2 for Decoding:
1
Enter 1 for TEXT Message1
select the key generating image
```

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Fig.5:Selecting the binary image for key generation

User selection of image for binding data. The binary images from the database is chosen at the encryption side and this image is transmitted to the receiver section.



```
ktop ▸ project Brain Signal
Command Window
  Round key :                              00 04 08 0c
                                           01 05 09 0d
                                           02 06 0a 0e
                                           03 07 0b 0f

  Final state :                            00 44 88 cc
                                           11 55 99 dd
                                           22 66 aa ee
                                           33 77 bb ff

  Enter File Name for Image + Message:
  23

  psval(:,:,1) =

     76.9513


  psval(:,:,2) =

     76.9513


  psval(:,:,3) =

     76.3520

  Untitled
fx >>
```

Fig.6: Image after data insertion

The generated image after data insertion will be save in .bmp format.

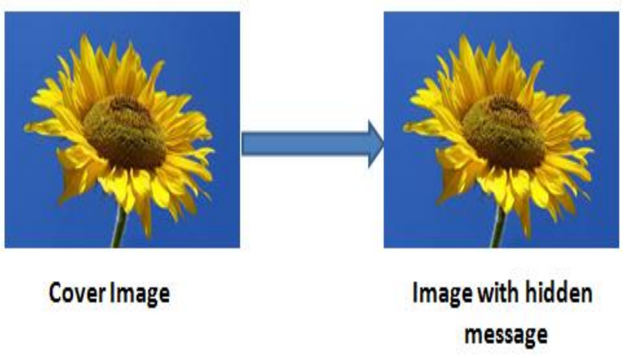


Fig.7: Image comparison before and after data insertion

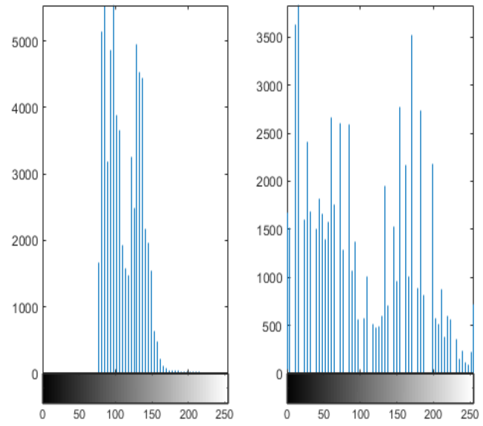


Fig 8: Histogram of cover image and encrypted image

Appearance of both the images looks similar, but the histogramic patterns vary due to data insertion

VI. CONCLUSION

This paper explained the overview of merging cryptography and steganography techniques in order to improve security for embedding data. By encrypting the data storing in image using latest algorithms improves the efficiency and the LSB type of insertion helps to place huge amount of data with distortion less changes in image. The key binding feature includes difficulty in hacking by the intruder. The overall findings provide improved security in transmission compared to previous techniques.

VII. REFERENCES

1. Dang Nguyen, Dat Tran, Dharmendra Sharma "On The Study Of EEG-based Cryptographic Key Generation". EL SEVIER 2017
2. Zhenxing Qian, Xinpeng Zhang, "Reversible Data Hiding in Encrypted Image with Distributed Source Encoding". IEEE 2015
3. Rahulkrishna P K , Eshwari R , Shree Harsha N J, "Enhanced Network Security Using Text to Image Encoding". IC-SSS 2015
4. Ashadeep Kaur , Rakesh Kumar, Kamaljeet Kainth, "Review Paper on Image Steganography". IJARCSSE 2016
5. D. Rachmawati, M. A. Budiman, "New Approach toward Data Hiding by Using Affine Cipher and Least Significant Bit Algorithm". IEEE 2017
6. Mazhar Islam , Mohsin Shah , Zakir Khan , Toqeer Mahmood, Muhammad Jamil Khan., "A New Symmetric Key Encryption Algorithm using Images as Secret Keys". IEEE 2015
7. Sukant Kumar Chhotaray , Animesh Chhotaray† and Girija Sankar Rath, "A new method of generating public key matrix and using it for image encryption". IEEE 2015
8. Rohith S, B K Sujatha, "Image Encryption and Decryption Using Combined Key Sequence of Logistic map and Lozi map". IEEE 2015
9. W. Stallings, "Cryptography and Network Security", Third Edition, Prentice Hall, 2003
10. S.K. Chhotaray, Animesh Chhotaray, G.S. Rath, "Orthonormal matrices and image encryption", International Conference on Circuits, Devices and Communication, BIT Mesra, 12-13 September 2014.
11. [11]. J.J. Amador and R.W. Green, "Symmetric-key block cipher for image and text cryptography," International Journal of Imaging Systems and Technology, vol. 15, pp. 178-188, 2005.
12. William Stallings ‚‚Cryptography and Network Security Principles and Practice" 5th Ed, Prentice Hall Publishers, 2011
13. MATLAB© website, http://in.mathworks.com/products/matlab/ .

AUTHORS PROFILE

Manchineni Chudamani, Mtech Student at KLEF

Dr.Tatini Narendra Babu, (Ph.D) Associate professor at KLEF