Watermark based Substitution technique Hill Cipher applied on Images

L. Ravi Kumar
Assistant Professor, Department of Information Technology
PVP Siddhartha Institute of Technology
Vijayawada, India

P.Ravi Prakash
Assistant Professor, Department of Information Technology
PVP Siddhartha Institute of Technology
Vijayawada, India

G.Venu Gopal
Assistant Professor, Department of Information Technology
PVP Siddhartha Institute of Technology
Vijayawada, India

D. Leela Dharani
Assistant Professor, Department of Information Technology
PVP Siddhartha Institute of Technology
Vijayawada, India

Dr.B.V.Subba Rao
Professor ,Department of Information Technology
PVP Siddhartha Institute of Technology
Vijayawada, India

Abstract**: In today's world it became very important to hide messages like images, audio, documents, and videos. The redundant data which we want to protect must be hidden. Cryptography is a method of storing and transmitting data in a particular form ie., encoding and decoding, so that only those for whom it is intended can read and process it. steganography is the practice of concealing messages or information within other non-secret text or data ie., hiding of a secret message within an ordinary message. In this we use Hill Cipher algorithm for encryption and decryption and to hide our text under image. Along with this we hide a image under another image using Least significant bit(LSB).**

Keywords: encryption, decryption, hill cipher, lsb, steganography

I. INTRODUCTION

With the wide use of Internet in every organization security becomes a serious problem. This is due to that there is scope for an attacker to attack the message. Here arises the Data Security problem which means protecting data, such as a text, image, database etc from destructive forces, and from the unwanted actions of unauthorized users. This must be perform at both encryption and decryption. encryption is the process of encoding messages or information in such a way that only authorized parties can read it.

In an encryption , the message or information, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. Decryption is the reverse process. Here we use a secure key for performing the encryption and decryption process. In symmetric-key schemes, the encryption and decryption keys are the same. Thus communicating parties must have the same key before they can achieve secret communication.

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. The term is most often associated with scrambling plaintext into cipher text a process called encryption, then back again known as decryption. Steganography is the art and science of hiding information by embedding messages within other harmless messages like image, audio, etc. In this paper we use both the Cryptography and Steganography along with Hill cipher key hiding technique. Here we hide the key and text in our image and image under the another image which is water marking technique.

II. HILL CIPHER

In classical cryptography, the Hill cipher is a polygraphic substitution cipher based on linear algebra. It was invented by Lester S. Hill in 1929, it was the first polygraphic cipher in which it was practical to operate on more than three symbols at once. Unlike other ciphers Hill Cipher can't broken easily besides Hill Cipher completely hides plain text. In particular requires the user to have an elementary understanding of matrices. It also make use of Modulo Arithmetic. Because of this, the cipher has a significantly more mathematical nature than some of the others. However it's safe against cipher text attacks.

For encryption the algorithm takes successive plain text and assign numbers like 0,1 and so on. This can be explained by using an example. Consider the plain text as HELP assign the numerical values like h=8, e=5, l=12, p=16. Arrange it as 2*2 matrix form.

Let us take our desire key as [7 7 1 2]. Now at Encryption we perform multiplication and modulus operations. initially we consider the first column of the plain text matrix and multiply with the key and perform modulos to it. we get as [9 1 18]mod 26, here we take 26 as our key space is 26. now after performing mod we get the values as follows 91mod26=13 and 18mod26=18, whose value are M,R respectively. Now we will consider another part of our text perform the same process then we will get 14 and 44 which are N,R respectively. This is our encryption.

For decryption we have to perform det, inverse modulo, matrix multiplication operations . after completion of encryption we get MRNR as cipher text. initially we perform det operation then we get 1/(ad-bc)[d -b -c a]= 1/7[2 -7 -1 7] mod 26. next we perform inverse modulo as 7-1 mod 26m=15 [2 -7 -1 7]mod 26=[30 -105 -15 105]mod 26 . Here we use euclidean algorithm then we get the matrix as [4 25 11 1]. Now we perform matrix multiplication for generated matrix and the first column of the cipher text matrix. we get [502 161]mod 26. after applying modulo we get 502 mod 26=8 and 161 mod 26=5 whose alphabetical values are H,E. now repeat the same process for the second column of the cipher text ,which we get the values as L,P. Finally our text after decryption is HELP which is our plain text.

For encryption: C = Ek (P) = KP

For decryption: P= Dk (C) = K-1 C = K-1 KP = P

DISADVANTAGES

1. Brute force attacks and chosen cipher attack will be possible.

2. High Computation is required for encrypting.

3. Social engineering works.

III. PROPOSED ALGORITHM

Here we consider an image and we hide the cipher text which we get after encryption along with key as first step. Next we transmit that image . At the receiver side from the cipher text we get plain text after performing inverse hill cipher algorithm. along with this we hide an image with another image and we use bit plane values here besides LSB technique. The noise also added to the image then the two images get blurred image.

Image Steganography has many types like: Image definition, Image Compression, Image and Transform Domain. In Image Domain there is Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image. The least significant bit , the 8th bit of some or all of the bytes inside an image is changed to a bit of the secret message.

When using a 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data.

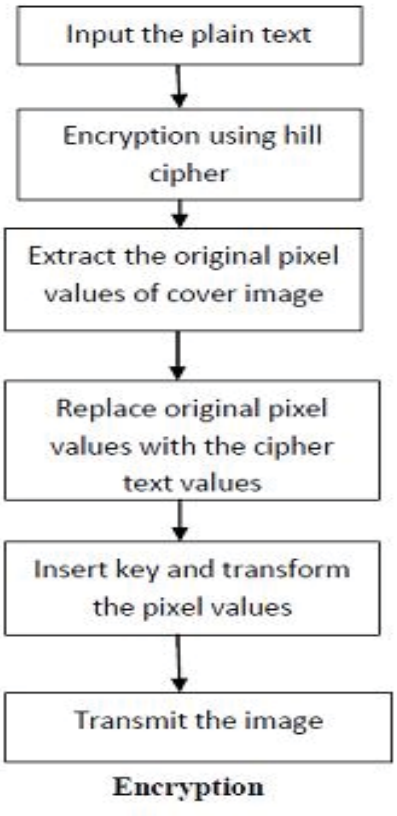

Figure1.Encryption

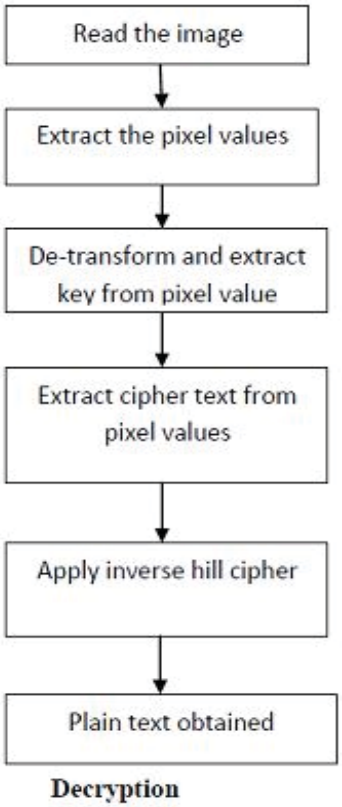

Figure2:Decryption

For example a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)

(10100110 11000100 00001100)

(11010010 10101101 01100011)

When the number 200, which binary representation is 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

(00101101 00011101 11011100)

(10100110 11000101 00001100)

(11010010 10101100 01100011)

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size. Since there are 256 possible intensities of each primary colour, changing the LSB of a pixel results in small changes in the intensity of the colours. These changes cannot be perceived by the human eye - thus the message is successfully hidden.

With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference.

In the above example, consecutive bytes of the image data – from the first byte to the end of the message – are used to embed the information. This approach is very easy to detect. A slightly more secure system is for the sender and receiver to share a secret key that specifies only certain pixels to be changed. Should an adversary suspect that LSB steganography has been used, he has no way of knowing which pixels to target without the secret key.

In its simplest form, LSB makes use of BMP images, since they use lossless compression. Unfortunately to be able to hide a secret message inside a BMP file, one would require a very large cover image. Nowadays, BMP images of 800 × 600 pixels are not often used on the Internet and might arouse suspicion. For this reason, LSB steganography has also been developed for use with other image file formats.

Here, the below figure was the inputed image behind that we are hiding the original text. The algorithm used here is hill cipher. By using this strategy we are hiding the message i.e, text in the image. Here we perform the matrix multiplication based on the hill cipher .The plain text is converted into the ascii code then the code is given key by taking random primes. Having primes gives us a lot of alternatives. By the use of keys the plain text was changed into the cipher text.

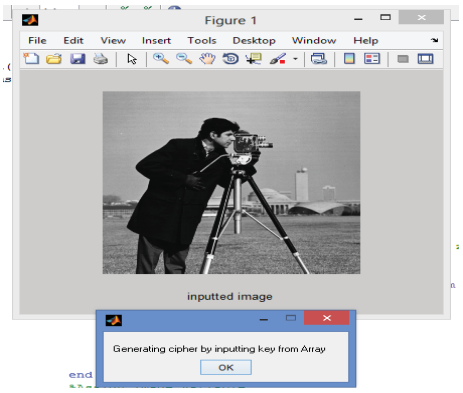

Figure 3 Description: Input image

we have certain resolutions for the inputted image which may be 256 X 256, 360 X 480, 240 X 480 etc. It has length and width which shows rows and columns and each point shows certain pixel information. Pixel value ranges from 0 to255. It is based upon the intensity , colour and position of the particular image**.**

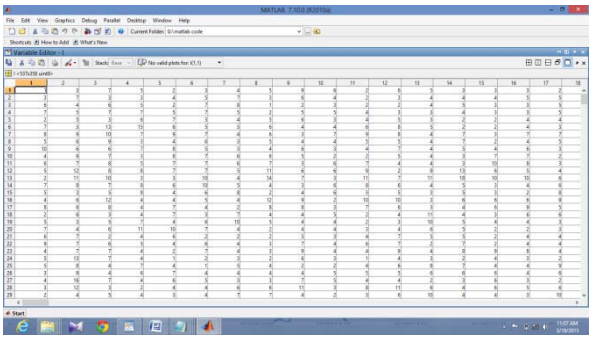

Figure 4 Description: pixel values

Here it is shown clearly that inputted image is converted into the blurred image after applying Hill Cipher algorithm. This is the encrypted image which we get after scrambling the pixel values**.**

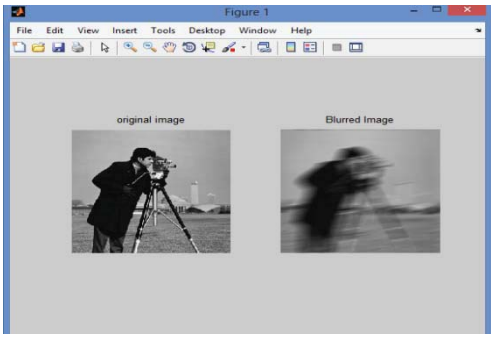

Figure 5 Description: Blurred image after encryption

The below figure shows that noise is added to the blurred image. The noise affect is less on dark area and more on lighten area.

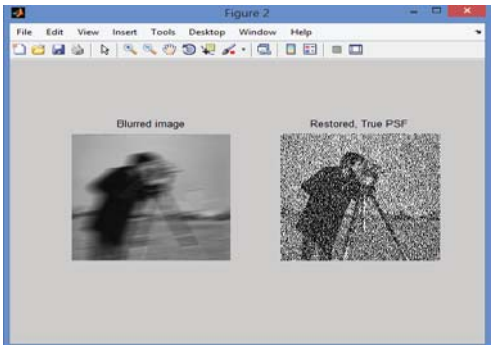

Figure 6 Description: Noise added Image

While decryption the blurred image changes into the original image with the use of key similarly the text given is also decrypted into the plain text with the use of hill cipher algorithm.The decrypted text is pvpsit which was given as a input.

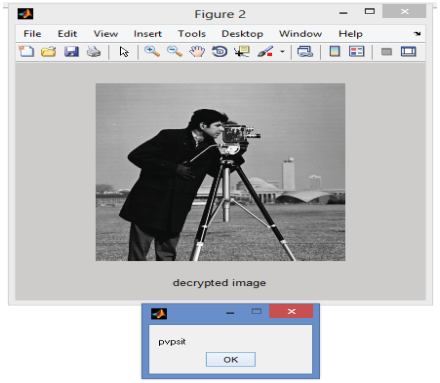

Figure 7 Description: Image after decryption

Image hidden in an image:

Here we are hiding an image with the help of another image.Here at first it asks for a bit plane value. Bit plane value says about the sharpness of hidden image in the original image.

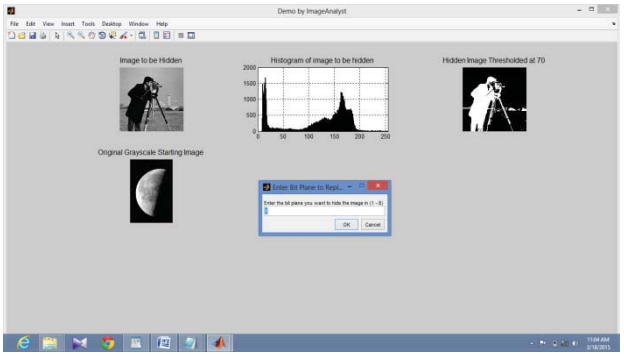

Figure 8 Description: passing bit map values

The figure describes the initial image in first position, histogram of pixel values, threshold image, the image which we place upon our hidden image, watermarked image, noise added images follows.

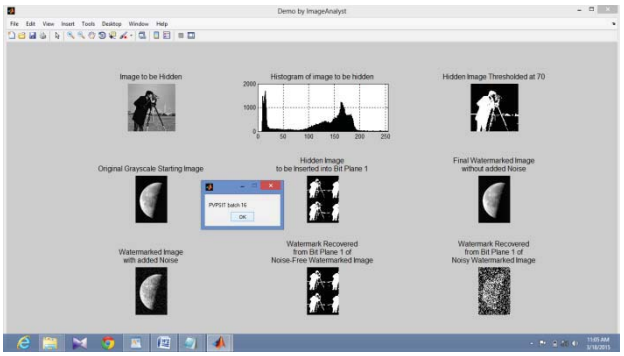

Figure 9 Description: output images after passing bitmap value as 1

The figure show our bit plane value as 8.

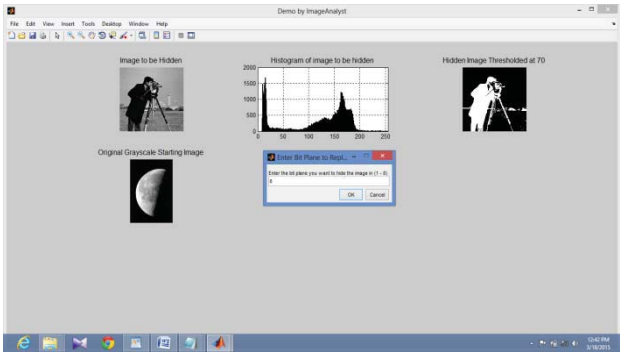

Figure 10 Description: bitmap value 8

The figure show the changes of images after giving bit plane value as 8. Then we get the output images changes in the hidden image and the image which we hide. The 6th position show the change in image.

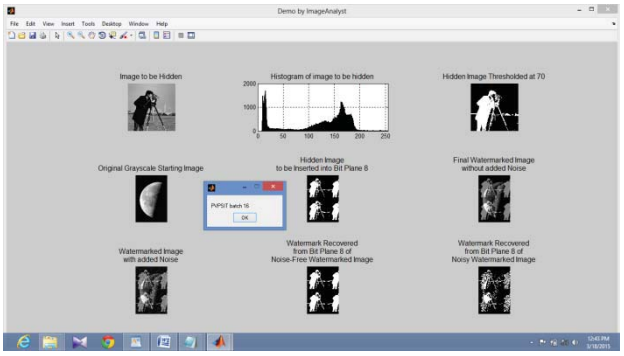

Figure 11 Description: output images with bitmap 8

ADVANTAGES:

1. Key space is so large
2. Encrypted image does not reveal actual image because key will be need

III. CONCLUSION

In this paper, we successfully implemented the hiding using Image steganography along with Hill Cipher, LSB. The key which we used is hide in the image efficient manner. The image also hid under another image by using bit map and LSB technique. Thus making the system highly secure for various network applications.

REFERENCES

[1] Bibhudendra Acharya, Saroj Kumar Panigrahy and Debasish Jena. Image encryption using self invertible key matrix of Hill cipher algorithm. Ist International Conference on Advances in Computing. Chikhli, India. 21-22 February 2008.

[2] Bibhudendra Acharya, Girija Sankar Rath, Sarat Kumar Patra, Saroj Kumar Panigrahy. 2007. Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm, International Journal of Security, Vol 1, Issue 1, 2007.

[3] S.K.Muttoo1, Deepika Aggarwal, Bhavya Ahuja. A Secure Image Encryption Algorithm Based on Hill Cipher System, Buletin Teknik Elektro dan Informatika (Bulletin of Electrical Engineering and Informatics) Vol.1, No.1, March 2012, pp. 51~60.

[4] W. Stallings, "Cryptography and Network Security", 4th edition, Prentice Hall, 2005

[5] Amogh Mahapatra Rrajballav Dash .Data encryption and decryption by using hill cipher technique and self repetitive matrix. Department of Electronics & Instrumentation Engineering National Institute of Technology Rourkela 2007