A Novel Approach of Steganography using Hill Cipher

Sainik Kumar Mahata[1], Anupam Mondal[2], Deepak Kumar[3], Pinaki Majumdar[4]
[1, 2 and 3]: Assistant Professor, Dept. Of CSE, JIS College of Engineering, Kalyani, Nadia, West Bengal, India.
[4]: B.Tech (CSE), JIS College of Engineering, Kalyani, West Bengal, India.

ABSTRACT

In the modern technological world, where data or image transfer through the internet has gained utmost importance, security of the data has become a major issue. We use cryptography for the security of the above mentioned data. By the help of cryptography, we convert plain text into cipher text, or data that is unreadable to the attacker. Another approach is to hide data in image and then send it to the receiver. This is known as steganography. Various approaches of steganography has been discovered earlier, which includes changing of data in pixels with the data that the sender needs to send. In the discussed approach, we will also find out the pixel matrix of an image, but we will multiply the found out matrix with a cipher matrix. In this way, we will convert the original image into encrypted image and then subject it to communication.

Keyword

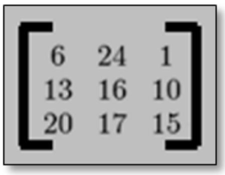
Cipher, Cipher text, Cryptography, Decryption, Encryption, Matrix, Plaintext.

1. INTRODUCTION

Going by the recent trend, images play a very important role in cryptography. We can always go by hiding an image in another image, but much advancement has been made in this field. In this paper we will present a new approach of cryptography using Hill Cipher. An image may be considered as a matrix of pixels. We will generate a random key matrix of the same dimension as that of the source image. Using the key matrix we will encrypt the source image. For decryption purpose, we will use the same key matrix.

2. HILL CIPHER

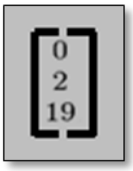
The Hill Cipher was invented by Lester. S. Hill in 1929. In this scheme, each letter is represented using modulo 26. Often, the simple scheme goes around like this: A=0, B=1..........Z=25. To encrypt a message, each block of n letters in multiplied by nXn cipher matrix. To decrypt the message, each block is multiplied with the inverse of the cipher matrix used for encryption purpose. Consider the message 'ACT', and the cipher matrix below (or GYBNQKURP in letters):



$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

Figure 1: the cipher matrix.

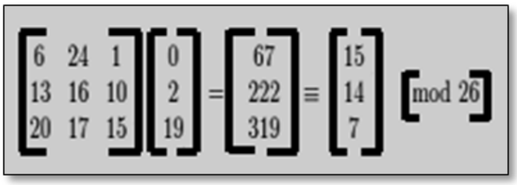
Since 'A' is 0, 'C' is 2 and 'T' is 19, the message is the vector:



$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

Figure 2: the plaintext vector.

Thus the enciphered vector is given by:

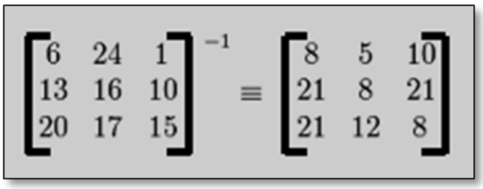


$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \begin{bmatrix} \bmod 26 \end{bmatrix}$$

Figure 3: calculation to find out the ciphertext.

After encryption, ACT is converted into POH.

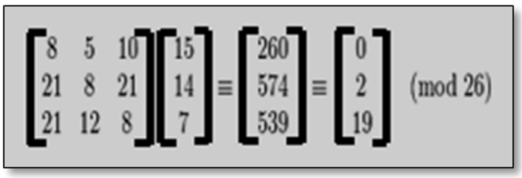
For the decryption process, inverse of the cipher matrix is found out.



$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} \equiv \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix}$$

Figure 4: calculation to find out inverse of the cipher matrix.

Then, we multiply the inverse of the cipher matrix with the encrypted matrix.



$$\begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix}\begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} \equiv \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \pmod{26}$$

Figure 5: Calculation to find out the plaintext.

From the above mentioned results, a formula can be derived such as

a. Ci = Cm* Pt
(1)
b. Pt = Cm^{-1}*Ci
(2)

Where,
Ci = Cipher Text
Cm = Cipher Matrix
Pt = Plain Text

3. PROPOSED ALGORITHM

In our approach, we encrypt an image rather than any data.

The algorithm for encryption and encryption is given below.

Encryption Algorithm:

1. We find out the pixel matrix for the image that is to be encrypted.

2. After finding the pixel matrix of the image to be encrypted, we will generate a random matrix which will have the same dimensions as that of the pixel matrix of the image that is to be encrypted.

3. We will then, apply the concept of hill cipher. But as we will work on an image of size 256X256, the mod element will be modified to 256 rather than 26.

4. So the formula will result as Ci = Cm*Pt mod 256 (3)

Where, Ci is the matrix of the cipher image.

Cm is the random cipher matrix.

Pt is the matrix of the image that is to be encrypted.

Decryption Algorithm:

1. For decryption purpose, we find out the pixel matrix of the cipher image.

2. We will inverse the cipher matrix that was used to encrypt the normal image.

3. We will then multiply the inverse cipher matrix and the pixel matrix of the cipher image.

4. The above step will be done using the formula

Pt = C^{m-1}*Ci mod 256
(4)

Where, Ci is the matrix of the cipher image.

Cm is the random cipher matrix.

Pt is the matrix of the image that is to be encrypted.

4. IMPLEMENTATION

The implementation part has been done in MATLAB. The image that was encrypted is shown Figure 6.

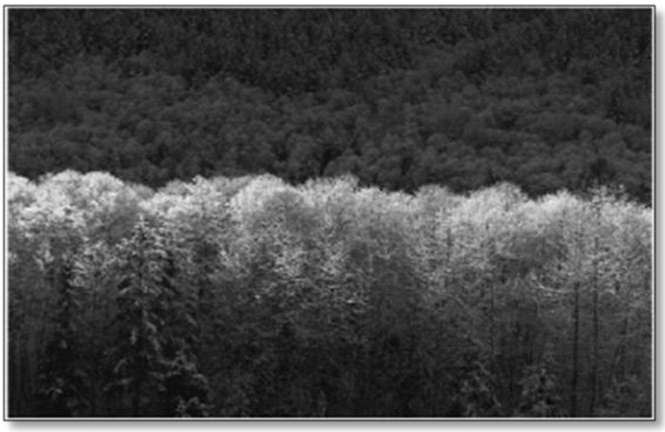
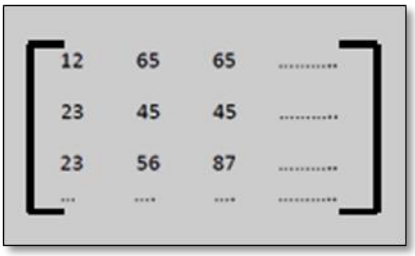


Figure 6: the image that is to be encrypted.

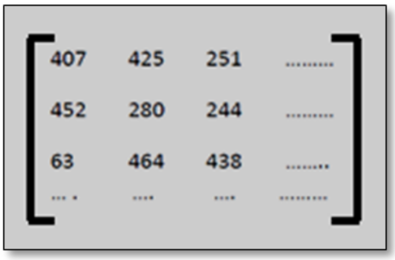
The pixel matrix for figure 6 has been found out and is given below in figure 7.



$$\begin{bmatrix} 12 & 65 & 65 & \cdots \\ 23 & 45 & 45 & \cdots \\ 23 & 56 & 87 & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{bmatrix}$$

Figure 7: pixel matrix of the image shown in figure 6.

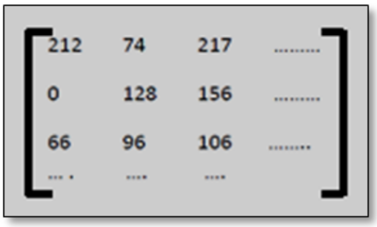
Then, we have generated a random cipher matrix with MATLAB with the same dimensions as that of the pixel matrix. The matrix is shown in figure 8.



$$\begin{bmatrix} 407 & 425 & 251 & \cdots \\ 452 & 280 & 244 & \cdots \\ 63 & 464 & 438 & \cdots \\ \cdots & \cdots & \cdots & \cdots \end{bmatrix}$$

Figure 8: random generated cipher matrix.

Multiplying the two matrix in figure 7 and figure 8 with the help of formula (3), we get a resultant matrix that is shown in figure 9.



$$\begin{bmatrix} 212 & 74 & 217 & \cdots \\ 0 & 128 & 156 & \cdots \\ 66 & 96 & 106 & \cdots \\ \cdots & \cdots & \cdots & \end{bmatrix}$$

Figure 9: result after multiplication using formula (3).

From the matrix in figure 9, we generate the cipher image. The results also show that we can generate the actual image from the encrypted image by using the formula (4). Figure 10 and figure 11 shows the actual image and the encrypted image respectively.

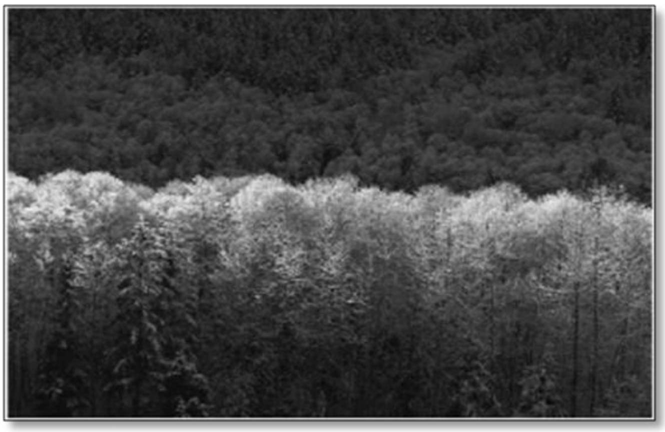


Figure 10: the image that is to be enccrypted.

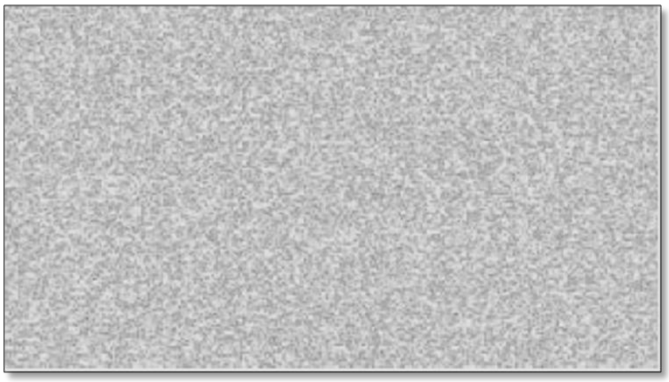


Figure 11: the encrypted ot the cipher image.

5. CONCLUSION

This is a novel approach for steganography and time taken to implement the algorithm and the procedure is less. And as it is a new approach, it is immune to attacks by hackers. The above algorithm is able to utilize optimum hiding capacities in every cover image. This allows users to hide files of larger sizes while at the same time preserve the general appearance of any cover image used. Furthermore, the implementation of various security measures provides a high level of protection for the hidden data. Although limited to lossless image formats, which are in any case standard and considerably widespread, the above algorithm is still useful in real-world applications especially in cases wherein large volumes of sensitive data need to be transmitted secretly over public communications channels such as the Internet.

6. REFERENCES

[1] R.J. Anderson and F.A.P. Petitcolas, "On the Limits of Steganography," *J. Selected Areas in Comm.*, vol. 16, no. 4, 1998, pp. 474–481.

[2] F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn, "Information Hiding—A Survey," *Proc. IEEE*, vol. 87, no. 7, 1999, pp. 1062–1078.

[3] J. Fridrich and M. Goljan, "Practical Steganalysis—State of the Art," *Proc. SPIE Photonics Imaging 2002, Security and Watermarking of Multimedia Contents*, vol. 4675, SPIE Press, 2002, pp. 1–13.

[4] B. Chen and G.W. Wornell, "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding," *IEEE Trans. Information Theory*, vol. 47, no. 4, 2001, pp. 1423–1443.

[5] N.F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen," *Computer*, vol. 31, no. 2, 1998, pp. 26–34.

[6] A. Kerckhoffs, "La Cryptographie Militaire (Military Cryptography)," *J. Sciences Militaires (J. Military Science,* in French*)*, Feb. 1883.