IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 11, Issue 5 (May. - Jun. 2013), PP 47-50
www.iosrjournals.org

Image Steganography Based On Hill Cipher with Key Hiding Technique

Pavan N[1], Nagarjun G A[2], Nihaar N[3], Gokul S Gaonkar[4], Mrs.Poonam Sharma[5]
Department of Electronics and Communication, Dayananda Sagar College of Engineering, Bangalore, INDIA

Abstract : *In today's digital world invisible ink and paper have been replaced by much more versatile and practical covers for hiding messages – digital documents, images, video, and audio files. As long as an electronic document contains irrelevant or redundant information, it can be used as a "cover" to hide secret messages. Cryptography is the study of encoding and decoding secret messages where as Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message.*

In this paper we implement Hill Cipher algorithm, for hiding our text behind the cover image and decrypt the cover image to get original text. The highlight of this paper is that, the key is encrypted and scrambled within the cover image.

Keywords : *Encryption, Decryption, Hill Cipher, Steganography, Symmetric Key Encryption.*

I. INTRODUCTION

With the rapid advancement in network technology especially Internet, it has become possible to transmit any type of data across networks. This has raised concern for the security of the transmitted data as access to data which has become easier by interception of communication media. Hence, data security is becoming an imperative and critical issue in data storage and transmission to prevent it from attacks. Images are widely used in several processes. Therefore, the protection of image data from unauthorized access is important. Encryption refers to the algorithmic schemes that encode the original message referred to as plain text using a key into non-readable form, a coded message known as cipher text so that it is computationally infeasible to be interpreted by any eavesdropper. The receiver of the cipher text uses a key to retrieve back the message in original plain text form.

Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there *is* a hidden message. By contrast, cryptography obscures the meaning of a message, but it does not conceal the fact that there *is* a message. Today, the term Steganography includes the concealment of digital information within computer files. For example, the sender might start with an ordinary looking image file, then adjust the color of every 100th pixel to correspond to a letter in the alphabet—a change so subtle that someone who isn't actively looking for it is unlikely to notice it. Steganography and cryptography are used together to ensure security of the covert message. In this paper we propose a method in which the key is transformed and is hidden in the cover image which also has the cipher text hidden in it. Thus eliminating the requirement of a key distribution centre and also eliminating the need for a secure channel for transmission of key to sender and receiver from the key distribution centre.

II. EXISTING SYSTEM

The Hill cipher is a polygraphic block cipher based on linear algebra developed by Lester Hill in 1929. Using frequency analysis, substitution ciphers like mono-alphabetic ciphers can be easily broken. But Hill cipher completely hides single letter frequencies by encrypting pairs of plain text and so it's safe against cipher-text only attacks. It provides good diffusion as change in one letter of plain text affects all letters in the cipher text. All arithmetic is done modulo some integer z that is the total number of possible symbols.

For encryption, the algorithm takes m successive plain text letters and instead of that substitutes m cipher letters. Each character is assigned a numerical value like a = 0, b = 1 and so on. The substitution of cipher text letters in the place of plain text letters leads to m linear equation. For m = 3, the system can be described as follows

$$C1 = (K11P1+K12P2+K13P3) \bmod 26 \quad (2.1)$$
$$C2 = (K21P1+K22P2+K23P3) \bmod 26 \quad (2.2)$$
$$C3 = (K31P1+K32P2+K33P3) \bmod 26 \quad (2.3)$$

This case can be expressed in terms of column vectors and matrices: or simply C = KP , where C and P are column vectors of length 3, representing the plain text and cipher text respectively, and K is a 3×3 matrix, which is the encryption key. All operations are performed mod 26 here. Decryption requires using the inverse of the matrix K. The inverse matrix K^{-1} of a matrix K is defined by the equation $KK^{-1} = K^{-1} K = I$, where I is the Identity matrix.

But the inverse of the matrix does not always exist, and when it does, it satisfies the preceding equation.

K^{-1} is applied to the cipher text, and then the plain text is recovered. In general term, we can write as follows:

For encryption: $C = Ek(P) = KP$ [4]

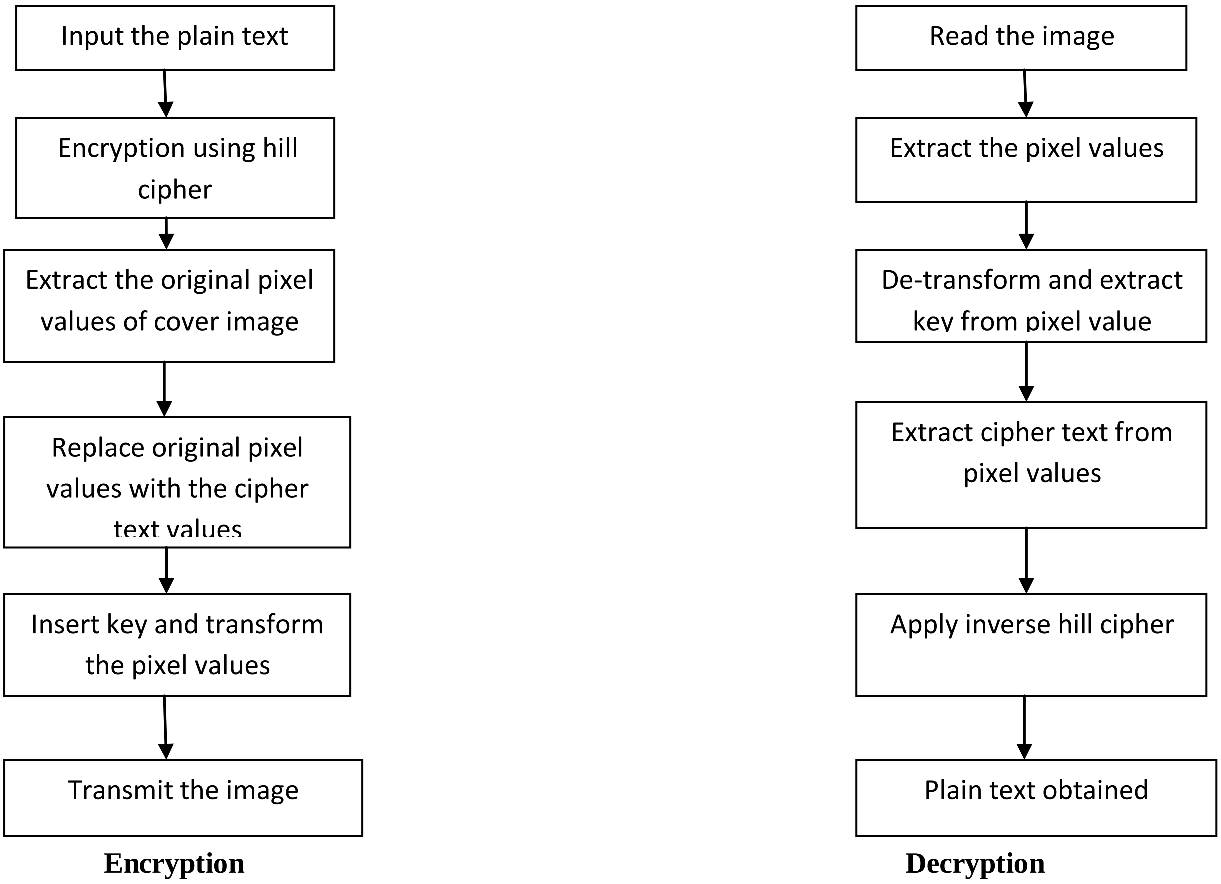
For decryption: $P = Dk(C) = K^{-1}C = K^{-1}KP = P$ [4]

If the block length is m, there are 26m different m letters blocks possible, each of them can be regarded as a letter in a 26m letter alphabet. In this paper, we have used Hill Cipher for encryption of data. All arithmetic has been done modulo 256 (8 bits per pixel for gray scale and 8 bits for RGB per color component).

III. PROPOSED SCHEME

In this paper, we have implemented Hill Cipher technique. We consider an image which acts a cover for hiding the cipher text as well as the key. As first step, we add the cipher text which is obtained by using Hill cipher technique to the cover image. In the second step, we add the encrypted key into the cover image which forms the encrypted image. The encrypted image is communicated over unsecured channel. At the receiver side the key is extracted from the cover image and by using its inverse the plain text is obtained.

IV. Flowchart


Input the plain text
Encryption using hill cipher
Extract the original pixel values of cover image
Replace original pixel values with the cipher text values
Insert key and transform the pixel values
Transmit the image
Encryption
Read the image
Extract the pixel values
De-transform and extract key from pixel value
Extract cipher text from pixel values
Apply inverse hill cipher
Plain text obtained
Decryption

V. Illustration Of The Method

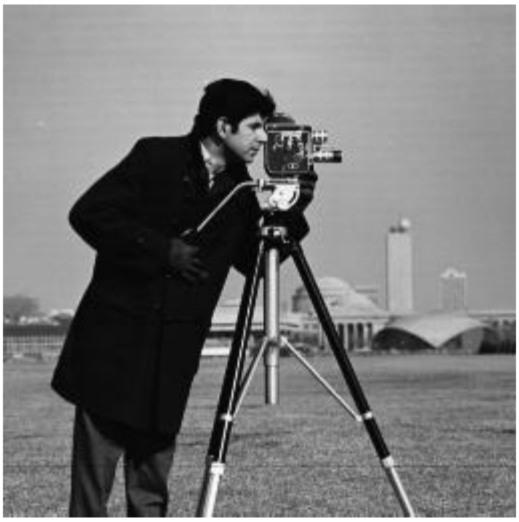


Figure 4.1 Original cover image

$$\text{key} = \begin{bmatrix} 5 & 8 \\ 17 & 3 \end{bmatrix}$$

Initial key insertion into the image pixels.

5 159 158 155 158 156 159 158 157 158 158 159 160 156
8 154 157 158 157 159 158 158 158 160 155 156 159 158
17 159 158 155 158 156 159 158 157 158 158 159 160 160
3 154 157 158 157 159 158 158 158 160 155 156 159 158

Due to space constraints, we are displaying only 4 rows of the 256x256 pixel matrix containing the key.

Figure 4.2 Encrypted image before transformation

Figure 4.3 Encrypted image after transformation

Transformed key matrix within the pixels of the image.

154	159	158	155	158	156	159	158	157	158
146	154	157	158	157	159	158	158	158	160
142	159	158	155	158	156	159	158	157	160
151	154	157	158	157	159	158	158	158	160

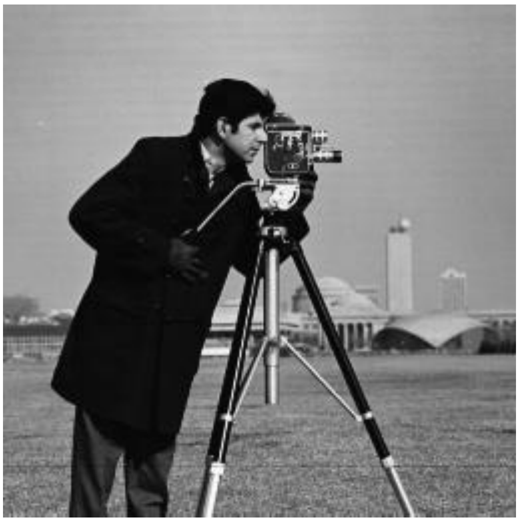


Figure 4.4 Decrypted cover image

CONCLUSION

In this paper, we perform image steganography based on Hill cipher technique. We have successfully implemented a scheme which eliminates the use key distribution system. The key is transformed in manner such that it is diffused within the pixel values, thus making the key invisible amongst the pixel values. The transformation is highly efficient since the encrypted data and also encrypted key similar values of the neighboring pixels. 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