Australian Journal of Basic and Applied Sciences, 6(7): 55-61, 2012
ISSN 1991-8178

Amalgamation of Scanning paths and Modified Hill Cipher for Secure Steganography

[1]B. Karthikeyan, [2]Jagannathan Chakravarthy, [1]Ramasubramanian S

[1]School of Computing, SASTRA University, Thanjavur, Tamilnadu, India
[2]School of Electrical & Electronics Engineering, SASTRA University, Thanjavur, Tamilnadu, India

Abstract: In the era of modern technology, secured exchange of information is of high priority. Security is needed to exchange range of data from military intelligence to personal information. Therefore, it is important to develop methods to exchange this information through insecure channels without being compromised. In this paper a new method is proposed to hide information in a gray scale image. The secret data is encrypted using a modified version of Hill cipher algorithm. The encrypted data is then embedded in the cover image. The method used is LSB substitution. In this paper, various methods of scanning patterns have been proposed that can be used embed the secret image inside a cover image. Scanning patterns are the patterns of accessing the pixels in the image. The scanning patterns used in this paper are raster horizontal, raster vertical, snake horizontal, snake vertical, Z horizontal and Z vertical.

Key words: Scanning paths, Modified Hill Cipher, LSB Substitution.

INTRODUCTION

The popularity of internet and its technologies increase day by day and so are the threats to the security of our information transmitted through the internet. The unauthorised or illegal access of the data or tampering of data is very high. In order to provide security of data being accessed by unauthorized people, information hiding is required.

Steganography refers to the science of "invisible" communication. It deals with the various methods that can be used to hide data (Petitcolas, F.A.P., et al., 1999).The object where the data is hidden is called a cover object and the hidden data is called secret data. The resultant object obtained after the process is called a stego-object. The process is referred as embedding. The cover object can be anything like text, image, audio or video files.

Among various branches of steganography is the image steganography which is the science of hiding secret data in an image (Bender, W., et al., 1996). Many techniques have been proposed in recent years to embed secret data in an image, among which is the LSB substitution method which is very simple and famous method of embedding scheme. It proposes that the least significant bits of each pixel can be substituted by the bits of data (Abbas cheddad, et al., 2010). This method, due to its simplicity, is very easy to target for intruders and the data is easily detected with less difficulty.

Various methods have been proposed to introduce randomness in order to increase the complexity of the LSB substitution (Katzenbeisser, S., F.A.P. Petitcolas, 2000). The complexity of detection of secret data can be increased by varying the number of bits to be used for embedding in each pixel. The complexity can be increased by embedding data in the image in a pseudo random manner rather than embedding them in an orderly manner. This is done by using the SCAN patterns (Chan, C.K., L.M. Chen, 2004) where the pixels to be embedded are selected using a pattern.

In this paper we propose various scanning patterns to introduce randomness during embedding data.

MATERIALS AND METHODS

Various methods have been proposed to improve the efficiency of hill cipher algorithm (Wang, R.Z., 2000). Hill cipher algorithm is used to encrypt data by a non-singular matrix as the key and the data is converted to vertical vector. The encryption is done by post multiplying the key matrix with data vector.

Various works have been done on scanning patterns too (Maniccam, S.S., N.G. Bourbakis, 2001). A scanning pattern is one which gives the order in which the pixels are to be accessed for embedding. In (Karthikeyan, B., et al., 2012), the authors have proposed a new method to send long text strings by using random keys without explicit change in the original image. In papers (Siva Janakiraman, 2011) and (2012), the authors have proposed new methods to hide data not only in the LSB of the cover image but also in other bits so that the security is increased. This is achieved by using a decoder circuit.

Corresponding Author: B. Karthikeyan, School of Computing, SASTRA University, Thanjavur, Tamilnadu, India

Proposed methodology:

In this paper, a method has been proposed to encrypt the data before embedding, using a modified version of Hill cipher. The Hill cipher algorithm used here has a key matrix K and the data image M. By multiplying the matrix M with K, we get the cipher text. In order to decrypt the cipher text is multiplied with the inverse of the key matrix K.

$$\begin{bmatrix} M11 & M12 \\ M21 & M22 \end{bmatrix}\begin{bmatrix} K11 & K12 \\ K21 & K22 \end{bmatrix} mod\ 256 = \begin{bmatrix} C11 & C12 \\ C21 & C22 \end{bmatrix}$$

$$\begin{bmatrix} C11 & C12 \\ C21 & C22 \end{bmatrix}\begin{bmatrix} K^{-1}11 & K^{-1}12 \\ K^{-1}21 & K^{-1}22 \end{bmatrix} mod\ 256 = \begin{bmatrix} M11 & M12 \\ M21 & M22 \end{bmatrix}$$

Encryption,
M.K = C
Decryption,
C.K'=M

This paper focuses on the various scanning methods that can be used to embed the secret data which is encrypted using the hill cipher. The proposed scanning patterns are Raster horizontal, Raster vertical, snake horizontal, snake vertical, Z horizontal and Z vertical.

A scanning pattern is the pattern or order in which the pixels are accessed to embed data. Instead embedding the first k bits in first pixel, second k bits in second pixel and so on, the data bits are embedded in a pseudo-random order.

We use three scan methods Raster scan method, snake scan, and Z scan method each in both horizontal and vertical embedding schemes.

In Raster horizontal scanning method, the secret data is embedded in a row wise manner. After embedding data in a row, the next row is scanned starting from the first pixel. In Raster vertical the scanning is done vertically, in a column wise manner.

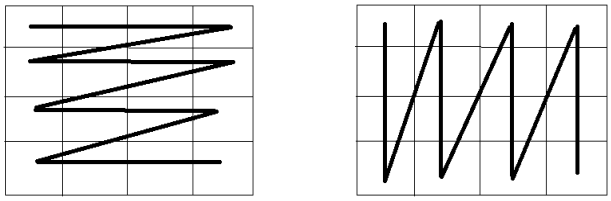

Fig. 1: a Raster scan Horizontal b) Raster scan Vertical

Snake horizontal embeds in the cover image by scanning the image in a snake like manner. The first row is scanned normally and the second row is scanned in the reverse order starting from the last pixel and the third row normally again and so on. Snake vertical scans the same way but done so column wise instead of row wise.

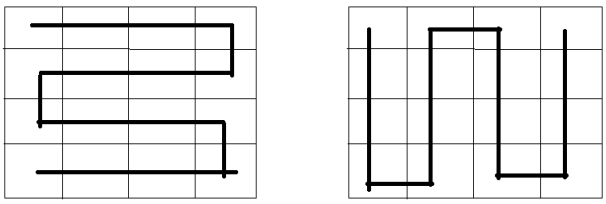

Fig. 2: a Snake Horizontal b) Snake Vertical

Z horizontal does the embedding in a Z wise manner. The whole image is divided into a number of 4x4 matrices and each matrix is scanned in a horizontal Z manner. In Z vertical the whole image is divided into a number of 4x4 matrices and each matrix is scanned in a vertical manner.

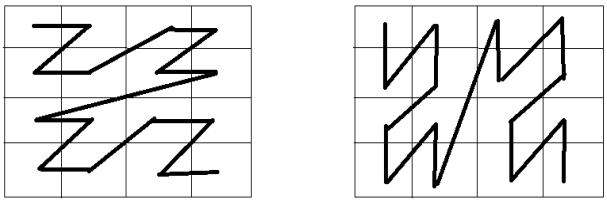

Fig. 3: a Z Horizontal b) Z Vertical

Thus by using the pattern the next pixel is selected and the data is embedded with the LSB substitution method.

Algorithm for embedding:

Step 1: Encrypt the secret image using Hill cipher algorithm with a key.
Step 2: Find the pixel in which the data has to be embedded using the pattern.
Step 3: Embed the data using LSB substitution.
Step 4: If any more data left go to step 2.
Step 5: End.

Flow chart for embedding:

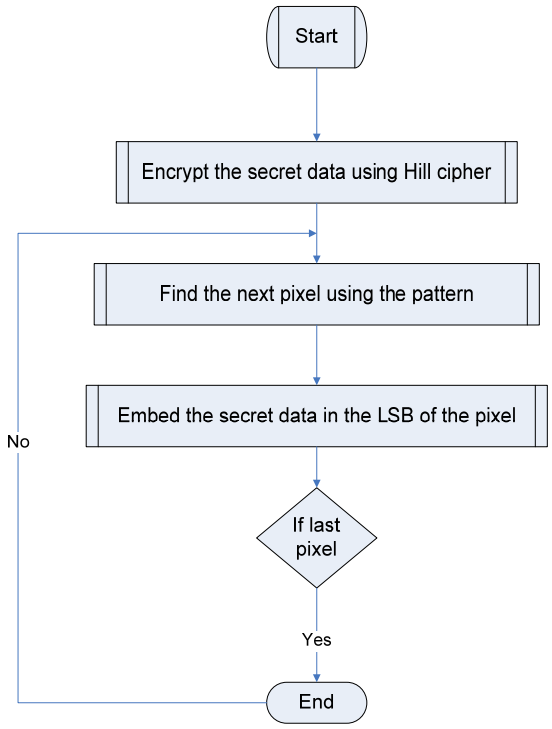

Fig. 4: Flow chart for Embedding

Algorithm for extracting:

Step 1: Start.
Step 2: Identify the pixel from which the data has to be retrieved using the pattern.
Step 3: Extract the last two bits of data from that pixel.
Step 4: If there is more data to be retrieved, go to step 2.
Step 5: Decrypt the data using Hill cipher.
Step 6: End.

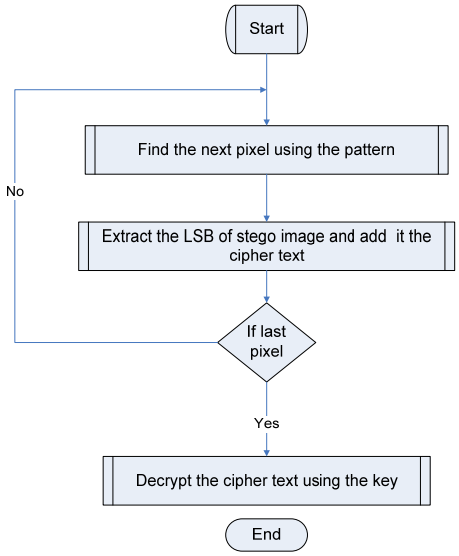

Fig. 5: Flow chart for Extraction

Results:

The above method is implemented using four different 128x128 gray images Lena, photographer, stone, and pepper as cover images (figure 6 a, b, c, and d).

Fig. 6: Cover images a) Lena b) Photographer c) Stone d) Pepper

Three 64x64 gray images namely Gandhi, moon and temple (figure 7 a, b, and c) are used as secret images in order to evaluate the performance.

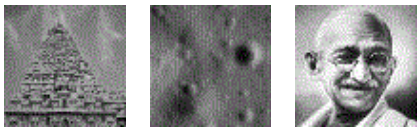

Fig. 7: Secret images a) temple b) moon c) Gandhi

Each secret image is embedded in the all the four cover images by using the two bit LSB substitution method. The performance and quality of the stego image obtained is done by calculating the MSE and PSNR values using the formula,

$$\text{MSE} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(X_{i,j} - Y_{i,j})^2$$

where Xi,j is the value of stego pixel and Yi,j is the value of cover pixel.

$$PSNR = 10\log_{10}\left(\frac{I_{\max}^2}{MSE}\right)dB$$

Where MSE is the mean square error value and Imax is the maximum intensity value.

The stego image for each of the scanning patterns is given in the figure 8 to 13.
Stego images:

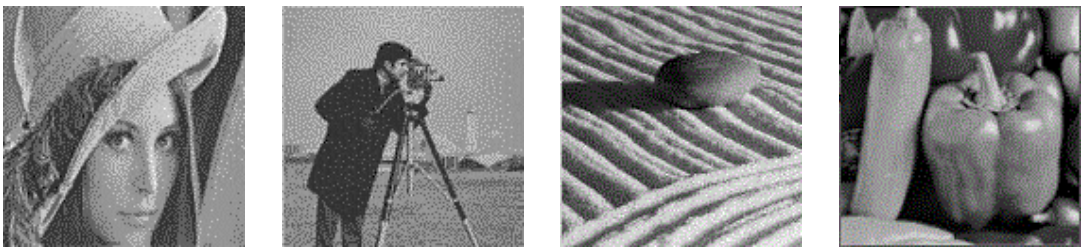

Fig. 8: Raster Horizontal a) Lena b) Photographer c) Stone d) Pepper

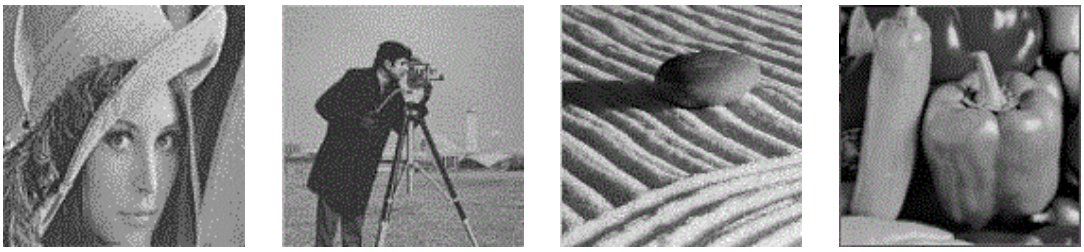

Fig. 9: Raster Vertical a) Lena b) Photographer c) Stone d) Pepper

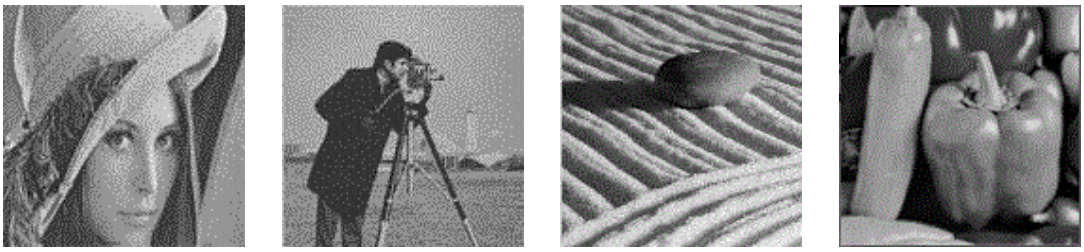

Fig. 10: Snake Horizontal a) Lena b) Photographer c) Stone d) Pepper

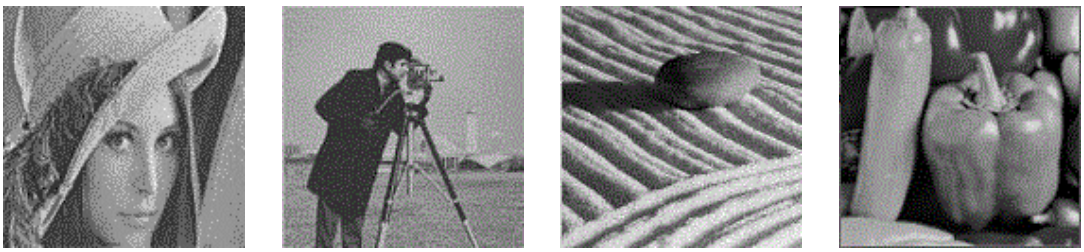

Fig. 11: Snake Vertical a) Lena b) Photographer c) Stone d) Pepper

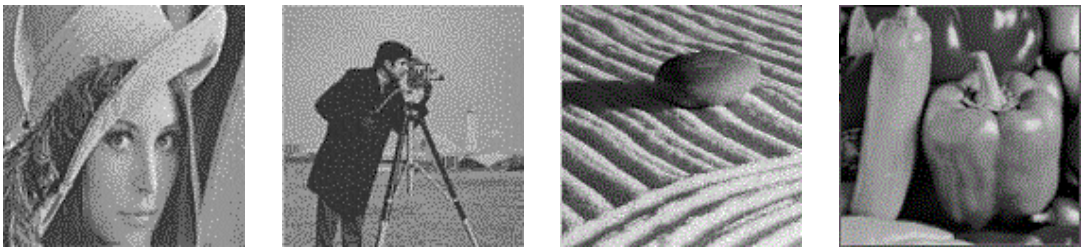

Fig. 12: Z horizontal a) Lena b) Photographer c) Stone d) Pepper

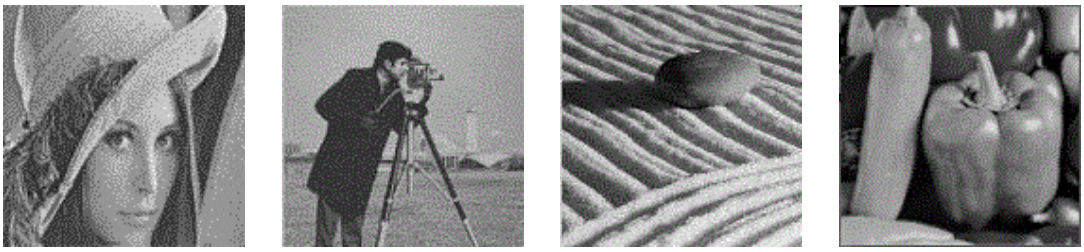

Fig. 13: Z vertical a) Lena b) Photographer c) Stone d) Pepper

Secret image: Gandhi

COVER IMAGE	RASTER H		RASTER V		SNAKE H		SNAKE V		Z H		Z V	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
LENNA	2.38	44.35	2.39	44.33	2.36	44.39	2.36	44.38	2.38	44.35	2.34	44.43
PHOTO GRAPHER	2.39	44.34	2.34	44.42	2.37	44.38	2.35	44.41	2.36	44.39	2.38	44.36
STONE	2.21	44.67	2.24	44.62	2.22	44.65	2.24	44.62	2.21	44.67	2.25	44.60
PEPPER	2.47	44.19	2.46	44.20	2.44	44.25	2.49	44.15	2.45	44.22	2.47	44.19

Secret image: Moon

COVER IMAGE	RASTER H		RASTER V		SNAKE H		SNAKE V		Z H		Z V	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
LENNA	2.39	44.33	2.38	44.35	2.36	44.39	2.38	44.35	2.40	44.32	2.33	44.45
PHOTO GRAPHER	2.42	44.29	2.34	44.42	2.41	44.30	2.34	44.42	2.42	44.28	2.34	44.42
STONE	2.24	44.61	2.23	44.63	2.23	44.64	2.25	44.59	2.25	44.60	2.26	44.58
PEPPER	2.52	44.10	2.49	44.15	2.48	44.17	2.51	44.12	2.45	44.23	2.47	44.20

Secret image: Temple

COVER IMAGE	RASTER H		RASTER V		SNAKE H		SNAKE V		Z H		Z V	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
LENNA	2.48	44.17	2.41	44.29	2.48	44.16	2.41	44.29	2.45	44.22	2.42	44.28
PHOTO GRAPHER	2.41	44.29	2.41	44.30	2.42	44.29	2.43	44.27	2.41	44.29	2.44	44.25
STONE	2.36	44.40	2.31	44.47	2.34	44.43	2.33	44.44	2.33	44.44	2.34	44.42
PEPPER	2.55	44.04	2.53	44.08	2.58	44.00	2.59	43.99	2.59	43.99	2.57	44.02

Discussion:

The secret images are embedded in the cover images using different scanning methods such as Raster Horizontal, Raster Vertical, Snake Horizontal, Snake Vertical, Z Horizontal and Z Vertical. The stego images obtained after the embedding process are also shown. The tabulation shows the Mean Square Error and PSNR values obtained after embedding each secret image in different cover images.

As observed from the table, the MSE values are low, indicating that the embedding has introduced only very small errors. Also, the high PSNR values show that the stego images obtained after embedding have high fidelity. The stego images obtained also show that they do not differ much from the original cover images. The results obtained are at par with the results obtained from simple 2 bit LSB substitution but are more secure. Two layers of security have been introduced - One in the form of modified Hill Cipher and another in the form of scanning paths. Only if these two parameters are known, the embedded image can be successfully retrieved. Thus, apart from the high fidelity characteristic of LSB substitution, this method has the added advantage of two layers of security.

The maximum size of the secret image can be of dimensions 64x64 for a 128x128 cover image. Hence 25% of the cover image can be used to embed the data. This is the maximum embedding capacity for 2 bit LSB substitution. The embedding capacity can be increased by increasing the number of bits embedded in every pixel.

Conclusion and Future Work:

This paper proposes a way to decrease the error caused due to the embedding of secret image within the cover image by analysing different scanning paths and choosing the one with least error values. As the data are embedded in different ways, this method proves to be highly secure and decreases the probability of detection of the secret data present in the cover image by steganalysis. Also, as a modified version of Hill cipher is used, the retrieved data is rendered useless without the key for the cipher. Therefore, this paper provides two layers of security to transmit the information securely. As a future work, many other scanning methods can be analysed. Also, in the same image, a composite scanning path can be introduced by incorporating different scanning paths in different areas of the image. Many such combinations can be tried and the combination which gives best results can be chosen for embedding the message.

REFERENCES

Abbas cheddad, Joan Condell, Kevin Curran and Paul Mckevitt, 2010. Digital image steganography an overview: survey of current methods (90).

Bender, W., D. Gruhl, N. Morimoto, A. Lu, 1996. Techniques for data hiding, IBM Systems Journal, 35 (3&4): 313-336.

Chan, C.K., L.M. Chen, 2004. Hiding data in images by simple LSB substitution, Pattern Recognition., 37(3): 469-474.

Karthikeyan, B., V. Vaithiyanathan, B. Thamotharan, M. Gomathymeenakshi, S. Sruti, 2012. LSB Replacement Stegnography in an Image using Pseudo randomised Key Generation, Research Journal of Applied Sciences, Engineering and Technology, 4(5): 491-494.

Katzenbeisser, S., F.A.P. Petitcolas, 2000. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, Norwood, MA.

Maniccam, S.S., N.G. Bourbakis, 2001. Lossless image compression and encryption using SCAN, Pattern Recognition., 34: 1229-1245.

Petitcolas, F.A.P., R.J. Anderson, M.G. Kuhn, 1999. Information hiding - a survey. In the proceedings of IEEE 87(7): 1062-1078.

Siva Janakiraman, Anitha Mary. A, Jagannathan Chakravarthy, Rengarajan Amirtharajan, K Thenmozhi and John Bosco Balaguru Rayappan, 2011. Smart Bit Manipulation for k bit Encoded Hiding In k-1 Pixels. In the proceedings of 3rd International Conference on Trendz in Information Science and Computing, pp: 86-91.

Siva Janakiraman, Anitha Mary.A, Jagannathan Chakravarthy, Rengarajan Amirtharajan, K Thenmozhi and John Bosco Balaguru Rayappan, 2012. Pixel Bit Manipulation for Encoded Hiding - An Inherent stego. In the proceedings of International Conference on Computer Communication and Informatics.

Wang, R.Z., C.F. Lin, J.C. Lin, 2000. Image hiding by optimal LSB substitution and genetic algorithm, Pattern Recognition., 34(3): 671-683.