ISSN No. 0976-5697

Volume 3, No. 4, July- August 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Cryptography of a Gray level Image Using Generalized Hill Cipher Involving Different Powers of a Key, Mixing and Substitution

V.U.K.Sastry*
Department of computer Science and Engineering, SNIST
Hyderabad, India,
vuksastry@rediffmail.com

Ch. Samson
Department of Information Technology, SNIST
Hyderabad, India,
samchepuri@gmail.com

Abstract: In this investigation we have obtained an encrypted image of a gray level image by applying the Generalized Hill Cipher Involving Different Powers of a Key, Mixing and Substitution which we have developed in the recent past. In this paper we have taken a gray level image and found the corresponding encrypted image which does not have any resemblance with the original image. All this has happened on account of multiplication with the powers of a key and functions such as Mix( ) and Substitute( ) which are responsible for a through mixing of the binary bits corresponding to the gray level values of the image.

Keywords: Encryption, Decryption, Gray level image, Generalized Hill cipher, Mixing, Substitution.

I. INTRODUCTION

Converting an image from one form to another by adopting a procedure available in cryptography is an interesting area of research, as an image can be kept in a secret manner and transmitted in a comfortable way. In recent years several authors have devoted their attention to the study of the cryptography of gray level images [1-7].

In a recent investigation [8], we have generalized the classical Hill cipher by including several plaintext matrices, obtained by decomposing a single plaintext matrix, and introducing different powers of a key matrix subjected to mod operation. In this analysis, we have taken a typical example wherein the size of the plaintext matrix is 16x16, (decomposed into sixteen square matrices of size 4), the size of the key matrix is 4x4, and the keys utilized in this analysis are of different powers of the original key matrix ranging from 1 to 16. In this analysis, we have made use of a pair of functions called Mix ( ) and Substitute ( ) for creating diffusion and confusion in each round of the iteration process involved in the cipher. Thus the cryptanalysis of this cipher clearly indicates that this cipher is a strong one.

In the present paper, our objective is to study the cryptography of a gray level image by adopting the generalized Hill cipher involving mixing and substitution operations. In this investigation, the gray level image is represented in terms of pixels where each pixel value is lying in [0,255], where 0 and 255 correspond to the dark pixel and the bright pixel respectively. The matrix corresponding to the image is taken to be of size 256x256, and this is divided into 256 square matrices wherein each one is of size 16x16. Here our interest is to see how the image gets encrypted on adopting the generalized Hill cipher under consideration.

In what follows we present the plan of the paper. In section 2, we study the development of a procedure for the cryptography of a gray level image. In section 3, we present an illustration of the cryptography of a portion of the image.

Finally in section 4, we mention the computations that are carried out in this analysis and draw conclusions.

II. DEVELOPMENT OF A PROCEDURE FOR THE CRYPTOGRAPHY OF A GRAY LEVEL IMAGE

Consider a gray level image G. Let us represent this in the form of a matrix given by

$G = [G_{ij}]$, i=1 to 256 and j= 1 to 256. (2.1)

Let us take a key matrix K which is given by

$K = [K_{ij}]$, i=1 to 4 and j= 1 to 4. (2.2)

On using the relations

$K_1 = K$, and

$K_i= (K_{i-1} * K_1) \bmod N$, i=2 to 16, (2.3)

Where N is a positive integer chosen appropriately, we have 16 matrices denoted as K_1 to K_{16}.

On focusing our attention on a portion of the image G, say P = $[P_{ij}]$, i=1 to 16 and j= 1 to 16), we get 16 plaintext matrices given by

$[P_{ij}]$, i=1 to 4 and j= 1 to 4, $[P_{ij}]$, i=1 to 4 and j= 5 to 8,
$[P_{ij}]$, i=1 to 4 and j= 9 to 12, $[P_{ij}]$, i=1 to 4 and j= 13 to 16,
$[P_{ij}]$, i=5 to 8 and j= 1 to 4, $[P_{ij}]$, i=5 to 8 and j= 5 to 8,
$[P_{ij}]$, i=5 to 8 and j= 9 to 12, $[P_{ij}]$, i=5 to 8 and j= 13 to 16,
$[P_{ij}]$, i=9 to 12 and j= 1 to 4, $[P_{ij}]$, i=9 to 12 and j= 5 to 8,
$[P_{ij}]$, i=9 to 12 and j= 9 to 12, $[P_{ij}]$, i=9 to 12 and j= 13 to 16,
$[P_{ij}]$, i=13 to 16and j= 1 to 4, $[P_{ij}]$, i=13 to 16and j= 5 to 8,
$[P_{ij}]$, i=13 to 16and j= 9 to 12, $[P_{ij}]$, i=13 to 16and j= 13to 16.

These matrices (taken in row wise order one after the other) can be denoted, as $P_1, P_2 \ldots P_{16.}$ Following the basic idea of the generalized Hill cipher [8], we use the relation

$C_i= (K_i\, P_i) \bmod N$, i=1 to 16, (2.4)

and obtain C_1 to $C_{16.}$ On using the these component ciphertext matrices, we get the cipertext C in the form,

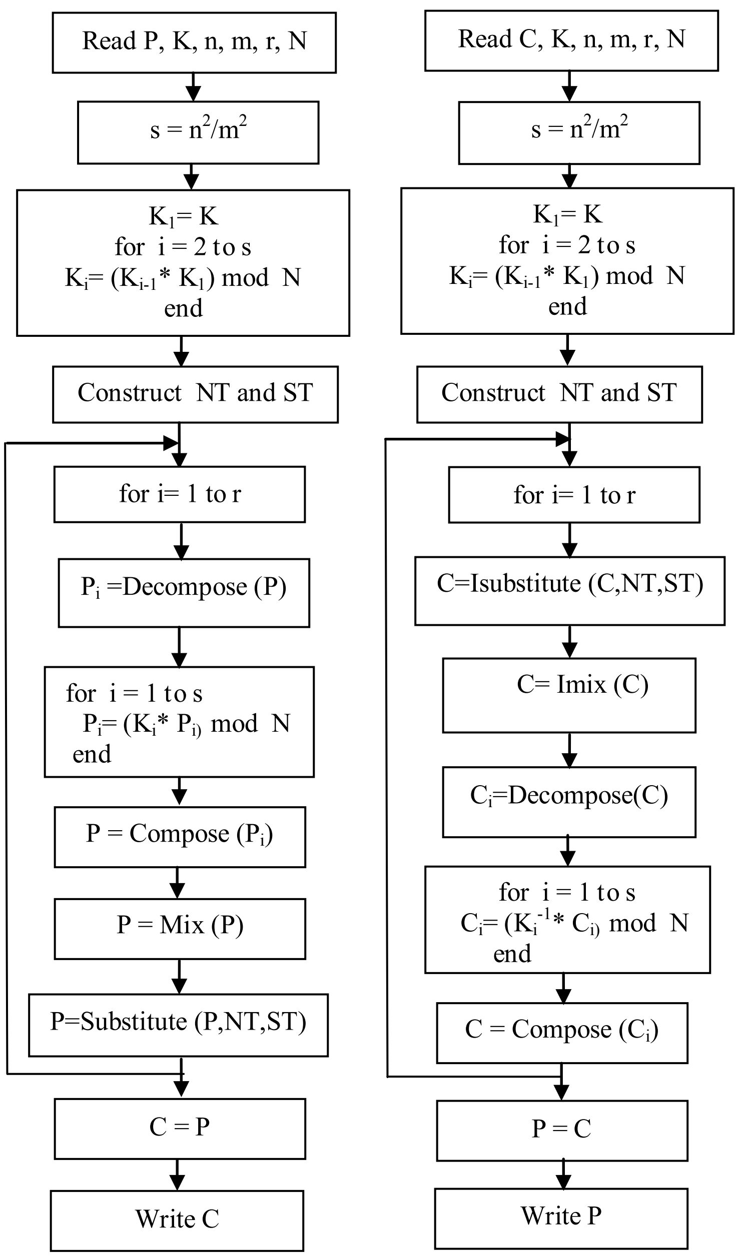
$$C = \begin{bmatrix} C_1 & C_2 & C_3 & C_4 \\ C_5 & C_6 & C_7 & C_8 \\ C_9 & C_{10} & C_{11} & C_{12} \\ C_{13} & C_{14} & C_{15} & C_{16} \end{bmatrix} \qquad (2.5)$$

© 2010, IJARCS All Rights Reserved

This can be written in the form,

$C = [C_{ij}]$, i=1 to 16 and j= 1 to 16. (2.6)

The schematic diagram of the flow charts and algorithms for encryption and decryption are given below.



(a) Process of Encryption (b) Process of Decryption

Figure 1. Schematic diagram of the Cipher

NT and ST are a pair of tables which are explained later.Here r denotes the number of rounds in the iteration process and it is taken as 16. Further, we have N=256 as we have used EBCDIC code in the development of the cipher. In this analysis, the number of rounds, denoted by r, is taken as 16.

Algorithm for Encryption

a. Read P,K, n, m, r, N
b. $s= n^2/m^2$
c. Initialize $K_1= K$
d. for i = 2 to s
   $K_i= (K_{i-1}* K_1) \bmod N$
   end
e. Construct NT and ST
f. for i = 1 to r
   P_i =Decompose (P)
   for i = 1 to s
   $P_i= (K_i* P_i) \bmod N$
   end
   P = Compose (P_i)
   P= Mix(P)
   P=Substitute (P,NT,ST)
   end
g. C = P
h. Write C

Algorithm for Decryption

a. Read P,K, n, m, r, N
b. $s= n^2/m^2$
c. Initialize $K_1= K$
d. for i = 2 to s
   $K_i= (K_{i-1}* K_1) \bmod N$
   end
e. Construct NT and ST
f. for r = 1 to r
   C=Isubstitute (C, NT, ST)
   C= Imix (C)
   C_i=Decompose(C)
   for i = 1 to s
   $C_i= (K_i^{-1}* C_i) \bmod N$
   end
   C = Compose (C_i)
   end
g. P = C
h. Write P

For a detailed discussion of the functions Decompose ( ), Mix( ), Substitute(),Compose( ), Imix( ) and Isubstitute() we may refer to [8].

III. ILLUSTRATION OF CRYPTOGRAPHY OF AN IMAGE

Consider a gray level image given below.

Figure. 2. Input image of Mahatma Gandhi

On representing this image in terms of its pixel values, we get a matrix of the form

$[G_{ij}]$, i=1 to 256 and j= 1 to 256, (3.1)

wherein each number lies in [0,255].

© 2010, IJARCS All Rights Reserved

Now we focus our attention on the portion of the image which lies in between the rows 113 and 128, and columns 113 and 128 This can be considered as

$P = [P_{ij}]$, i=1 to 16 and j= 1 to 16. (3.2)

and it is given by

$$P = \begin{bmatrix} 62 & 60 & 59 & 61 & 65 & 66 & 65 & 62 & 68 & 70 & 75 & 77 & 77 & 79 & 77 & 68 \\ 66 & 63 & 61 & 62 & 66 & 68 & 67 & 66 & 63 & 67 & 75 & 77 & 74 & 73 & 72 & 68 \\ 63 & 61 & 60 & 60 & 64 & 67 & 68 & 68 & 60 & 64 & 74 & 78 & 72 & 68 & 69 & 70 \\ 58 & 57 & 58 & 60 & 64 & 67 & 69 & 69 & 64 & 65 & 73 & 77 & 72 & 68 & 73 & 76 \\ 57 & 59 & 61 & 64 & 67 & 69 & 70 & 70 & 71 & 68 & 72 & 76 & 74 & 74 & 79 & 82 \\ 61 & 62 & 64 & 66 & 67 & 68 & 69 & 70 & 75 & 70 & 70 & 73 & 74 & 77 & 81 & 80 \\ 65 & 65 & 64 & 63 & 63 & 65 & 69 & 72 & 73 & 69 & 69 & 71 & 71 & 75 & 75 & 70 \\ 68 & 67 & 64 & 61 & 61 & 65 & 71 & 76 & 69 & 67 & 69 & 69 & 68 & 71 & 69 & 60 \\ 66 & 61 & 60 & 59 & 59 & 65 & 72 & 73 & 65 & 62 & 60 & 66 & 74 & 71 & 64 & 63 \\ 62 & 61 & 61 & 58 & 54 & 57 & 63 & 66 & 67 & 70 & 68 & 68 & 75 & 77 & 70 & 64 \\ 62 & 62 & 62 & 60 & 57 & 55 & 56 & 58 & 66 & 74 & 73 & 67 & 71 & 74 & 68 & 59 \\ 62 & 61 & 59 & 60 & 62 & 59 & 54 & 53 & 64 & 71 & 70 & 65 & 68 & 70 & 65 & 59 \\ 57 & 57 & 54 & 54 & 59 & 57 & 54 & 58 & 63 & 65 & 65 & 66 & 70 & 69 & 66 & 67 \\ 53 & 56 & 52 & 50 & 54 & 52 & 54 & 66 & 63 & 61 & 59 & 63 & 67 & 62 & 58 & 63 \\ 54 & 56 & 51 & 51 & 59 & 56 & 53 & 62 & 64 & 59 & 55 & 58 & 61 & 56 & 52 & 57 \\ 55 & 54 & 46 & 52 & 67 & 62 & 49 & 50 & 63 & 59 & 55 & 58 & 63 & 60 & 58 & 61 \end{bmatrix} \quad (3.3)$$

This conspicuous portion is taken into consideration so that we shall have a clear picture.

Let us now consider the key matrix

$$K = \begin{bmatrix} 231 & 245 & 155 & 238 \\ 90 & 224 & 181 & 207 \\ 170 & 137 & 103 & 140 \\ 9 & 201 & 59 & 177 \end{bmatrix} \quad (3.4)$$

On using the encryption algorithm, we get the ciphertext C in the form

$$C = \begin{bmatrix} 183 & 38 & 82 & 189 & 35 & 119 & 140 & 70 & 70 & 162 & 21 & 108 & 245 & 61 & 55 & 29 \\ 98 & 164 & 102 & 251 & 91 & 69 & 181 & 111 & 185 & 217 & 65 & 182 & 123 & 116 & 123 & 20 \\ 91 & 175 & 137 & 49 & 61 & 212 & 76 & 125 & 201 & 214 & 66 & 190 & 170 & 103 & 1 & 102 \\ 249 & 42 & 238 & 208 & 54 & 168 & 38 & 69 & 144 & 206 & 234 & 172 & 76 & 17 & 244 & 145 \\ 7 & 165 & 247 & 103 & 167 & 135 & 40 & 145 & 145 & 103 & 248 & 169 & 26 & 113 & 37 & 36 \\ 249 & 32 & 19 & 65 & 15 & 201 & 7 & 107 & 134 & 13 & 200 & 237 & 102 & 230 & 140 & 105 \\ 191 & 216 & 123 & 18 & 29 & 193 & 181 & 105 & 82 & 167 & 15 & 222 & 64 & 169 & 181 & 64 \\ 195 & 178 & 166 & 136 & 144 & 75 & 192 & 231 & 139 & 86 & 170 & 128 & 65 & 83 & 190 & 159 \\ 121 & 41 & 179 & 189 & 212 & 169 & 56 & 196 & 62 & 73 & 114 & 11 & 63 & 46 & 54 & 243 \\ 194 & 152 & 230 & 37 & 144 & 98 & 156 & 183 & 234 & 14 & 226 & 31 & 156 & 116 & 202 & 113 \\ 249 & 86 & 84 & 12 & 204 & 62 & 50 & 117 & 5 & 146 & 234 & 166 & 95 & 210 & 43 & 223 \\ 133 & 243 & 131 & 167 & 49 & 213 & 255 & 49 & 155 & 52 & 33 & 124 & 38 & 130 & 175 & 90 \\ 95 & 126 & 57 & 74 & 34 & 18 & 213 & 200 & 4 & 192 & 79 & 101 & 194 & 183 & 133 & 55 \\ 45 & 19 & 65 & 193 & 219 & 32 & 154 & 251 & 97 & 218 & 192 & 238 & 184 & 101 & 86 & 195 \\ 2 & 11 & 186 & 255 & 199 & 64 & 32 & 224 & 94 & 220 & 122 & 230 & 145 & 99 & 145 & 121 \\ 79 & 9 & 103 & 101 & 92 & 74 & 218 & 141 & 215 & 133 & 204 & 131 & 87 & 74 & 30 & 220 \end{bmatrix} \quad (3.5)$$

As the portion under consideration is very small, we do not find any special features exhibited in the encrypted image, despite the fact that we have made use of the functions Mix( ) and Substitute( ) in carrying out the encryption process. Here we have made use of the decryption algorithm and obtained the corresponding original image for a checkup.

IV. COMPUTATIONS AND CONCLUSIONS

Consider the gray level image mentioned in the preceding section (See Figure. 2) . Let us focus our attention on the matrix

$[G_{ij}]$, i=1 to 256 and j= 1 to 256, given in (3.1). This can be divided into 256 matrices, wherein, each matrix is of size 16x16. Now on employing the encryption algorithm on each 16x16 matrix separately, we get the ciphertext corresponding to each portion. On combining these ciphertext portions in an appropriate manner, we get the ciphertext matrix corresponding to the entire image. The encrypted image is shown in Figure. 4.

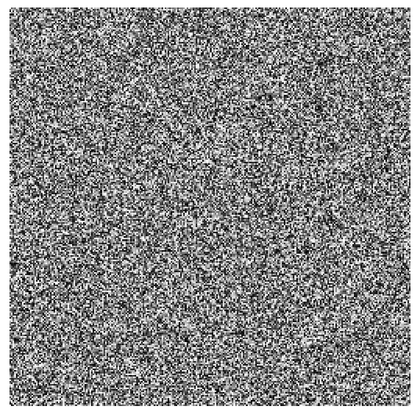


Figure 4. Encrypted image of Mahatma Gandhi

The programs for encryption and decryption are written in MATLAB [9].

As the generalized Hill cipher utilized in this analysis of image encryption is including several features such as multiplication with several powers of key matrix, modular arithmetic, mixing and substitution, the strength of the cipher is remarkable as we have seen in [8]. Thus it is totally impossible to recognize the original image basing upon the encrypted image by breaking the cipher in any way.

On comparing Figure 2 in section 3 and Figure 4 in section 4, it is interesting to note that the encrypted image does not show any resemblance with the original image. This feature makes the analysis worthy in its own way.

IV. REFERENCES

[1] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah, " Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images", International Journal of Computer, Information, and Systems Science, and Engineering, Vol. 1, No. 1, pp. 33 – 39, 2007.

[2] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, " A Modified AES Based Algorithm for Image Encryption", World Academy of Science,

Engineering and Technology, Vol. 27, pp. 206 – 211, 2007.

[3] Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda, "Image Encryption Using Advanced Hill Cipher Algorithm", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.

[4] Dr. V. U. K. Sastry, Prof. D. S. R. Murthy, Dr. S. Durga Bhavani, "Cryptography of a Gray Level Image Using a Modified Feistel Cipher", International Journal of Advanced Research in Computer Science (IJARCS), Vol. 1, No. 3, Sep. – Oct 2010.

[5] Dr. V. U. K. Sastry, Prof. D. S. R. Murthy, Dr. S. Durga Bhavani, "Cryptography of a Gray Level Image Using a Novel Block Cipher Involving Feistel Structure and Modular Arithmetic", International Journal of Advanced Research in Computer Science (IJARCS), Vol. 1, No. 3, Sep. – Oct 2010.

[6] Dr. V. U. K. Sastry, Prof. D. S. R. Murthy, Dr. S. Durga Bhavani, " Cryptography of a Binary Image Using Modified Hill Cipher", International Journal of Computer and Network Security (IJCNS), Vol. 2, No. 6, June 2010.

[7] Dr. V. U. K. Sastry, Prof. D. S. R. Murthy, Dr. S. Durga Bhavani, "Cryptography of a Gray Level Image Using Modified Hill Cipher", International Journal of Computer and Network Security (IJCNS). Vol. 2, No. 6, June 2010.

[8] VUK Sastry, Ch.Samson," A Generalized Hill Cipher Involving Different Powers of a Key, Mixing and Substitution", International Journal of Advanced Research in Computer Science (IJARCS), Vol. 3, No. 4, July-August 2012.

[9] http://www.mathworks.com/products/matlab

Short Bio Data for the Authors

Dr. V. U. K. Sastry is presently working as Professor in the Dept. of Computer Science and Engineering (CSE), Director (SCSI), Dean (R & D), SreeNidhi Institute of Science and Technology (SNIST), Hyderabad, India. He was Formerly Professor in IIT, Kharagpur, India and worked in IIT, Kharagpur during 1963 – 1998. He guided 12 PhDs, and published more than 70 research papers in various international journals. He received the best Engineering College Faculty Award in Computer Science and Engineering for the year 2008 from the Indian Society for Technical Education (AP Chapter) and Cognizant- Sreenidhi Best faculty award for the year 2012. His research interests are Network Security & Cryptography, Image Processing, Data Mining and Genetic Algorithms.

Mr. Ch. Samson obtained his Diploma from Govt Polytechnic, Hyderabad in 1994 , B.E . from Osmania University in 1998 and M. E from SRTM University in 2000. Presently he is pursuing Ph.D. from JNTUH, Hyderabad since 2009. He published 10 research papers in international journals and two papers in conferences. He is currently working as Associate Professor and Associate Head in the Dept. of Information Technology (IT), SNIST since June 2005. His research interests are Image Processing, Image Cryptography and Network Security.

© 2010, IJARCS All Rights Reserved