International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

An Investigation of Different Image Encryption Techniques based on Hill Cipher

Manju Sharma[1], Manju Meena[2]

[1]Lecturer (Sel. Grade) Govt. Women polytechnic College, Ajmer, Rajasthan, India
[2]Lecturer Govt. Women polytechnic College, Ajmer, Rajasthan, India

ABSTRACT

In recent times, security of multimedia data is an important issue. With the advancement and easier availability of internet at low cost, as lead to increased use of multimedia data. Till date large number of image encryption methodologies have been proposed to protect image data from unauthorized use. In this paper we review different image encryption techniques using hill cipher & compare the results obtained from different techniques.

Keywords : Image Encryption, Hill Cipher, Symmetric Key Cryptography, Asymmetric Key Cryptography

I. INTRODUCTION

With the rapid advancement in network technologies, security of confidential data has become a major problem. Image encryption is commonly used for hiding secret information from unauthorized access. Encryption is a process used to encode original message commonly referred to as plain text into non-understandable message referred to as cipher text. Decryption process restores plain text from cipher text. The many schemes used for encryption constitute the area of study known as cryptography.

Two types of cryptosystem are commonly used – symmetric and asymmetric cryptosystem. Symmetric cryptosystem make use of same key for encryption and decryption process. Asymmetric cryptosystem make use of different keys (public-private key pair) for encryption and decryption process. Symmetric cryptosystem make use of substitution and/or transposition techniques. In substitution technique letters of plaintext are replaced by other letters or by numbers or symbols. Monoalphabetic cipher, polyalphabetic cipher, playfair and hillcipher are some of substitution technique. Monoalphabetic cipher uses fixed substitution for the entire message where as polyalphabetic cipher uses different types of substitution over different parts of message. Hill cipher is a type of monoalphabetic polygraphic substitution cipher. In transposition technique some type of permutation is applied on plaintext.

Hill Cipher is multi letter cipher and was developed by mathematician Lester Hill. The core of Hill cipher is matrix manipulations. For encryption, algorithm takes m successive plaintext letters and instead of that substitutes m cipher letters. In Hill cipher, each character is assigned a numerical value like $a = 0$, $b = 1, \ldots, z = 25$. The substitution of ciphertext letters in the place of plaintext letters leads to m linear equation. For $m = 3$, the system can be described as follows:

$$C_1 = (K_{11}P_1 + K_{12}P_2 + K_{13}P_3) \bmod 26$$
$$C_2 = (K_{21}P_1 + K_{22}P_2 + K_{23}P_3) \bmod 26$$
$$C_1 = (K_{31}P_1 + K_{32}P_2 + K_{33}P_3) \bmod 26$$

CSEIT1831390 | Received : 12 Feb 2018 | Accepted : 25 Feb 2018 | January-February-2018 [(3) 1 : 1581-1586]

This case can be expressed in terms of column vectors and matrices:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix}$$

or simply we can write as $C = KP$, where C and P are column vectors of length 3, representing the plaintext and ciphertext respectively, and K is a 3×3 matrix, which is the encryption key. 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. In general term we can write as follows:

For encryption:

$C = Ek(P) = KP$

For decryption:

$P = D_k(C) = K^{-1} C = K^{-1}KP = P$

II. LITERATURE REVIEW

Bibhudendra Acharya et al. (2009) [2] proposed an advanced hill cipher algorithm for image encryption using involutry matrix. They explain generation of involutry matrix of size m. The image is divided into m x m block size. Level of security is added by taking the i^{th} pixel from each block to form a temporary block which is encrypted using hill cipher , block is then transposed and again encrypted using hill cipher. Advance hill cipher is more secure and faster since randomly generated involutry matrix is used which overcome the problem associated with hill cipher and computational complexity is reduced. Experimental result shows that algorithm works well for images consisting of large area of same color or gray level images.

Sheetal Khobrekar & Nayana Shenvi (2016) [4] proposed an image encryption algorithm which applies k modulus transformation to each pixel for image compression. The image is divided into blocks. Each block is encrypted using hill cipher after applying DCT & quantization. Experimental results shows that image compression is highly increased by used of k modulus along with DCT. Also peak signal to noise ratio (PSNR) is around 32.53 db for Lena image.

K Mani & M Viswambari (2017) [5] explains generation of key matrix for hill cipher using magic rectangle. Hill cipher can't encrypt the image properly if the image is gray or if image consist of large area of same color. This drawback of hill cipher can be removed by using a proper key matrix. They proposed a deterministic method for generation of key matrix of higher order k from magic rectangle. Any number of sub matrices of any order k can be generated from the magic rectangle and can be used as key matrix for hill cipher. Security of method is enhanced because of large number of possible keys. Also for large block sizes can be encrypted using higher value of k.

Panduranga H T & Naveen Kumar S K (2012) [6] describes a partial image encryption algorithm using two stage hill cipher. Each stage used slightly different keys for generating self-invertible matrix. By controlling the dependency of second stage self-invertible matrix on the first stage self-invertible matrix amount of partial encryption is controlled.

M G Vara Prasad and P Sundarayya (2016) [7] explained generation of self-invertible reflection matrix key for hill cipher and affine hill cipher under modulation of prime number. Homogenous linear equation and a prime number are used for generation of self-invertible key matrix which reduces computational complexity at the time of decryption. Experimental result shows that algorithm is well suited for grey and color images.

Rakesh Ranjan, R. K. Sharma and M. Hanmandlu (2016) [8] explained color image encryption and decryption using two stage Hill Cipher method with Arnold Transformation. The RGB image is first divided into blocks of size $m \times m$. Keys for Hill Cipher are generated from $SL_n(F_q)$ domain where n divides m. $SL_n(F_q)$ is the set of all $n \times n$ matrix that contain elements of $GL_n(F_q)$ whose determinant is one over the domain F_q where F_q is a finite field containing q elements and q is a large prime number. Since determinant of key matrix is one, inverse of key matrix equals to adjoint of key matrix. Also different keys are used for encoding of RGB components. The encoding process first applies Hill Cipher on m × m block, performs Arnold Transform and then again applies the Hill Cipher on the block. Six keys are used for Hill Cipher and two keys are used for Arnold Transform. Since large number of keys are possible and number of ways in which they can be used is still larger, the attacker will not be able to recover the original image.

M. D. Randeri et.al. (2017) [9] proposed an image encryption using key matrix generation from biometric mixed fingerprint image for two level security. In this method, fingerprint of all users is saved in a secured server database called enrollment phase. Whenever a sender wants to transmit image, the system takes the fingerprint of the sender and matches with the stored database for the authentication of the sender. If matching is successful, a key matrix for hill cipher is generated by mixing the minutiae points from fingerprint image of the sender and region points from fingerprint image of the receiver and this key is used for encryption of image using hill cipher.

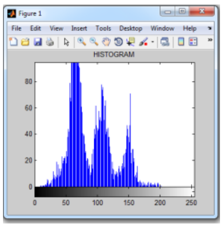
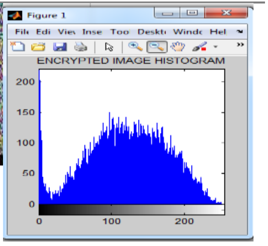
Andysah putera utama Siahaan (2017) [10] proposed a genetic algorithm for generating key matrix for Hill Cipher encryption. The method generates a random matrix of size 20 × 9, where each element is in the range of 0 to 255. Each row of the matrix is treated as hill cipher chromosome. Random matrix with 20 rows indicate that the population size is 20. For every chromosome i.e. for every row, fitness (determinant), probability and cumulative probability is calculated. The process of selection, crossover and mutation is carried over the random matrix to generate next generation population structure. The process is repeated for thirty times to generate next generation population structure. The matrix obtained from the last round is used for key formation for hill cipher. More than one key are formed from the last stage population matrix which enhances the level of security.

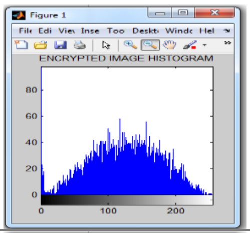
Mohammad Hadi Valizadeh [12] proposed modified hill cipher algorithm vulnerable to zero plaintext attack. In this method a random number a_0 is selected and use to calculate $a_1, a_2, \ldots a_n$ where $a_i = H(a_{i-1})$. H( ) is one way hash function. Random number a_0 is securely transmitted to receiver. A row vector $V_t = (v_1, v_2, \ldots v_n)$ for t changing from 1 to n is computed as $j_i = (v_{i-1} \bmod n) + 1$ and $v_i = (k_i\, j_i + \hat{v}_{i-1} v_0)(\text{mod } p)$ where vector v_{i-1} depends on value of v_{i-1} and $v_0 = a_t\,(\text{mod } p)$. Matrix

$V_{n\times n}$ is formed from these row vectors. Plaintext X is encrypted as $Y_{n\times n} = X_{n\times n} * K' + V'_{n\times n}$ where $K' = ACM(K, \bar{a})$ and $V' = ACM(V, \bar{a})$. $\bar{A}$ is average of $a_1, a_2, \ldots a_n$, ACM is Arnold transform and K is the key matrix.

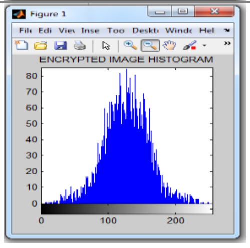
Rakesh Kumar Jangid et. al. (2014) [11] explained hybrid approach of image encryption using DNA cryptography and TF hill cipher. In this method, first they converted the RGB image into gray image and then converted each pixel value into binary and rotated the binary value by a count of four. DNA code is then calculated for this binary value and converted into amino acids. This matrix is then encrypted using TFine hill cipher.

III. EXPERIMENTAL RESULTS

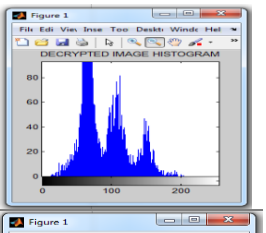
Original Image		
Encrypted Image using Review Paper I, II,III method-ologies		

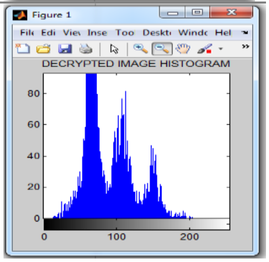


Compressed & Encrypted Image

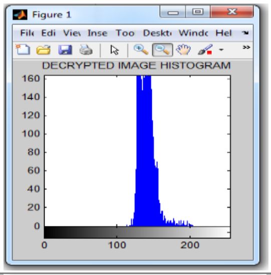


Decrypted Image using Review Paper I, II,III Methodo-logies

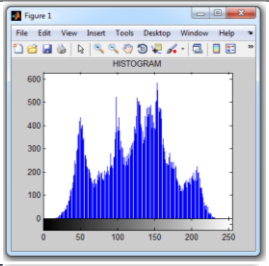




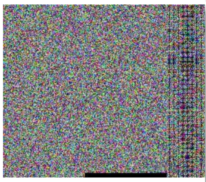
Compressed Image

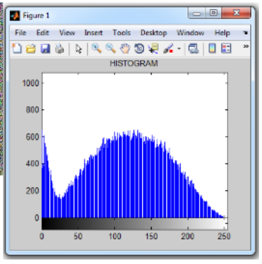


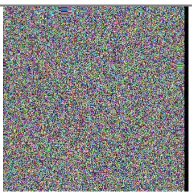
Original Image

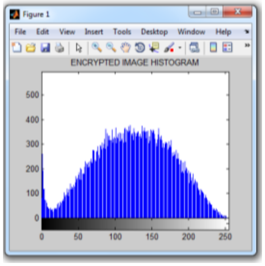


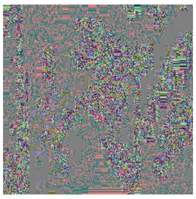
Encrypted Image using Review Paper I, II,III method-ologies

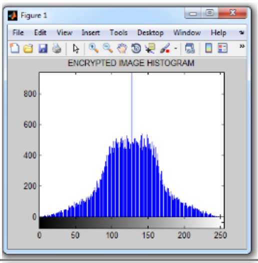




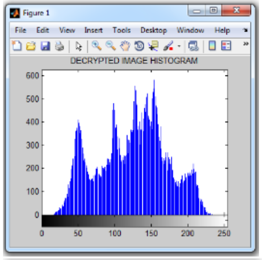


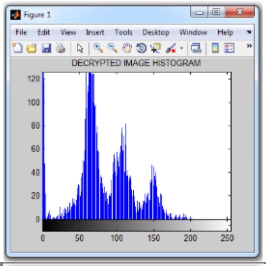


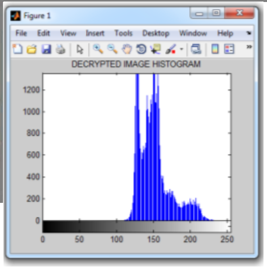




Decrypted Image using Review Paper I, II,III Methodo-logies







CONCLUSION

In today's digital world, secure transmission of images over open network is a must. In this paper, we surveyed different papers on image encryption using hill cipher technology. All methodologies are suitable for real-time application and provide high security against different types of crypto attacks. All methodologies have certain qualities –some are fast, more secure, less computational cost. Depending upon the application, a well suited methodology can be selected.

IV. REFERENCES

[1]. 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, pp. 14-21.

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

[3]. Stallings, W. Cryptography and Network Security.2005. 4th Edition, Prentice Hall.

[4]. Sheetal Khobrekar, Nayanashenvi.2016. "Effect of K- Modulus Method on JPEG Compression and Hill Cipher Encryption", International Journal of Technology and science, Issue 1, 2016 pp. 13-16

[5]. K. Mani, M. Viswambari, 2017. "Generation of Key Matrix for Hill Cipher using Magic Rectangle". Advance in Computational Science and Technology, Volume 10, Number 5 (2017) pp. 1081-1090

[6]. Panduranga H T , Naveen Kumar S K .2012. "Advanced Partial Image Encryption using Two- Stage Hill Cipher technique". International Journal of Computer Applications(0975-8887) Volume 60-no. 16 December 2012

[7]. M.G Vara Prasad, P. Sundarayya. "Generalized Self-Invertiblekey Generation Algorithm by using Reflection Matrix in Hill Cipher and Affine Hill Cipher". International journal of pharmacy & Technology. ISSN; 0975-766X, 2016

[8]. Rakesh Ranjan, R. K Sharma and M.Hanmandlu . "Color Image Encryption and decryption using Hill Cipher associated with Arnold Transform". Application and applied Mathematics an International Journal. Vol. 11, Issue 1 (June 2016), pp. 45-60

[9]. M.D Randeri, S.D. Degadwala , A. Mahajan. "A Study on Image Encryption Using Key Matrix Generation from Biometric Mixed Fingerprint Image for Two Level Security". International Journal of Scientific Research in Computer Science, Engineering and Information Technology. Volume 2, issue 6.

[10]. Andysah Putera Utama Siahaan , "Genetic Algorithm in Hill Cipher Encryption", American International Journal of research in Science, Technology, Engineering & Mathematics.

[11]. Rakesh Kumar Jangid, Noor Mohmmad, Abhishek Didel, Swapnesh Taterh.Hybrid . "Approach of Image Encryption Using DNA Cryptography and TF Cipher Algorithm", International conference on communication and Signal Processing, April 3-5, 2014

[12]. Mohammad Hadi Valizadeh . "Healing the Hill Cipher, Improved Approach to Secure Modified Hill against Zero-plaintext Attack".

[13]. Subhas Barman, Debasis Samanta and Samiran Chattopadhyay. "Fingerprint-based Crypto-Biometric System for Network Security". Journal on Information security (2015).

[14]. Bibhudenra Acharya, Debasish Jena, sarat Kumar Patra, and Ganapati Panda. "Invertible, Involutory and Permutation Matrix generation Method for Hill Cipher System". International Conference on Advanced Computer Control.

[15]. V.U.K Sastry and V.Janaki . "Modified Hill Cipher with Key Dependent Permutation and Circular Rotation", Journal of Computer Science, Volume 3(9).2007.

[16]. Abd Manaf et al. "On the affine Ciphers in Cryptogarphy" Springer-Verlag Berlin Heidelberg 2011,pp. 185-199.

[17]. Goutham L, Mahendra M S, Manasa A p, Mr. Prajwalasimha S N4, " Modified Hill Cipher Based Image Encryption Technique" .(IJRASET), Volume 5 Issue IV, April 2017.

[18]. Sharda Singh, Dr. J. A. Laxminarayana, "RSA Key Generation Using Combination of Fingerprints", IOSR Journal of computer Engineering (IOSR-JCE), e- ISSN: 2278-0661, (AETM'15).

[19]. Liu Z, Xu L, Liu T, Chen H, Li P, Lin C, Liu S. "Color image encryption by using Arnold Transform and Color-blend Operation in Discrete Cosine Transform Domains", Optics Communication, 2011; 284: 123-8

[20]. Analysis and Design of Affine and Hill Cipher, Journal of Mathematics Research Vol. 4, No. 1; February 2012.

[21]. Firas A. Jassim , "Increasing Compression Ratio in PNG Images by K-Modulus Method for image Transformation".

[22]. Saroj Kumar Panigrahy , "Image Encryption using Self- Invertible Key Matrix of Hill Cipher Algorithm".

[23]. Lerma, M.A., 2005. Modular Arithmatic. http://www.math.northwestern.edu/`mlerma/problem_solving/results/modular_airth.pdf.