Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 5 (2017) pp. 1081-1090

http://www.ripublication.com

Generation of Key Matrix for Hill Cipher using Magic Rectangle

K. Mani[*], M. Viswambari[#]

Department of Computer Science, Nehru Memorial College, Puthanampatti, Trichy, India

Abstract

Hill cipher encryption is one of the polygraph cipher of classical encryption in which if the encryption key matrix called key matrix is not chosen properly, obtaining the decryption key matrix is not possible. This is because the chosen key matrix must satisfy the criteria viz., it must be invertible and the determinant of the key matrix is also odd. If the key matrix is chosen randomly, sometimes it may fail to satisfy the said criteria and it is very difficult to obtain the correct key matrix in a single run. To avoid it, a deterministic method has been proposed in generating the key matrix based on magic rectangle of order m×n in this paper. The novelty in this paper is that higher order of key matrix is generated based on m. In order to generate the key matrix, first the magic rectangle of order m×n is converted into magic square of order m×m. From it the required key matrix is generated based on the rules proposed in this paper. As the order of magic rectangle is increasing the number of characters to be encrypted is also increasing and resulting in enhanced security.

Index Terms: Hill Cipher, Magic Rectangle, Magic Square, Sub Matrices, With and Without Overlapping.

1. INTRODUCTION

Hill cipher is a multiletter cipher classical encryption technique developed by the mathematician Lester Hill in 1929. It is a poly-graphic substitution cipher based on linear algebra, which has a few advantages in data encryption. But, it is vulnerable to known plaintext attack. Further an invertible key matrix is needed for decryption. It may become problematic since an invertible key matrix does not always exist. In Hill

cipher the encryption algorithm takes successive plaintext letters and substitutes ciphertext letters. The substitution is determined by linear equations in which each character is encoded either using alphabetical encoding as a=1, b=2, c=3,…, z = 26 or using ASCII encoding as a= 97, b=98,…, z=122 with modulus p=26 or 256 respectively. In Hill cipher, a matrix containing numbers called key matrix which is used for encryption process and the modular arithmetic inverse of encryption matrix called decryption matrix is employed in decryption process.

In order to encrypt the message using a n×n Hill cipher, suppose n plaintext-ciphertext pairs, each of length n, the pairs $P_j = (p_{1j}p_{2j\ldots}p_{nj})$, $C_j = (c_{1j}c_{2j\ldots}c_{nj})$ can be labeled as plaintext and ciphertext respectively such that $C_j = KP_j$ for $1 \leq j \leq n$ and for some unknown key matrix K. In general, the Hill cipher encryption and decryption are given by $C = KP \bmod p$ and $P = K^{-1}C \bmod p$, where P, C, K, K^{-1} represents plaintext, ciphertext, encryption key matrix and decryption key matrix respectively. It is noted that, not all the matrices have inverse and if so they will not be eligible as key matrices in the Hill cipher scheme. Further, the encryption key matrix must satisfy two important criteria viz., the key matrix should be invertible and the gcd(det[K], p)=1.

It is noted that there is no deterministic procedure available in generating the key matrix and it is generated randomly. As the key matrix is generated randomly, sometimes it is very difficult to obtain such a key matrix in a single run. Thus it is necessary to develop a deterministic procedure in generating the key matrix. For that a deterministic procedure based magic rectangle as proposed in [18] is considered. Once the magic rectangle has been generated, it is converted into magic square of order m. Let the block size chosen is k which is treated as the order of sub matrix in this paper. Thus a sub matrix K′ of order k is chosen from magic square preferably starting from the first element of magic square. Suppose the selected K′ fails to satisfy the said criteria, it is modified based on the rules as proposed in section 3.2. After applying the rules, now K′ satisfies the criteria and the resultant sub matrix is called key matrix K which is used for encryption. Once a suitable K is found, the modular inverse of encryption key matrix called decryption matrix which is then used for decryption.

The rest of the paper is organized as follows. Section 2 describes the various works related on Hill cipher key matrix. The proposed methodology in determining the encryption key matrix is illustrated in section 3. In section 4, encryption/decryption using Hill Cipher is described. Section 5 ends with conclusion.

II. RELATED WORKS

In [1], Bibhudendra proposed various methods of generating self- invertible matrix for Hill cipher algorithm. They emphasised less computational complexity as inverse of the matrix was not needed for Hill cipher decryption. In [2], V. U. K. Sastry, have modified the Hill cipher using permutation and circular rotation which depends on the

key. They developed a block cipher and analyzed avalanche effect. Bibhudendra Acharya [3], have developed an involutary, permuted and reiterative key matrix generation method for Hill cipher system. They eliminated the matrix inverses for Hill cipher decryption and reduced the decryption time.

In [4], P. Shanmugam, have developed a method from Hill cipher using self-invertible matrix for encrypting and decrypting the text and image. They also increased the order of self-invertible matrix and obtained better encryption quality and security level. A.V.N. Krishna [5], generated multiple ciphertexts by using modified output of classical Hill cipher. Randomization of ciphertext was made which was free from known plaintext and chosen ciphertext attacks with increased computational time. Adi Narayana Reddy [6], have presented an enhancement to Hill Cipher using circulant matrices. It shares a prime circulant matrix as a secret key and non-singular matrix as public key and the determinant of the coefficient matrix is zero.

B. Karthikeyan et.al, [7] proposed a new method to hide information in gray scale image. A modified version of Hill cipher algorithm was used to encrypt secret data by LSB substitution method. They also proved that the method was highly secure and decreased the probability of detection of secret data by steganalysis. In [8], Rahul R. Ravan presented a symmetric cipher which was the variant of Hill cipher. An algorithm was proposed which eliminated the usage of random key matrix for Hill cipher encryption. They also used different key for each block encryption and this increased resistance to various attacks.

Gurtaptish Kaur [9], has proposed a scheme in which image was taken as input and calculated the elapsed time for hidden text. The author combined advanced Hill cipher and DES techniques and secured confidential data from unauthorized users. D. C. Mishra [10], presented an approach for gray-scale image encryption and decryption using Random Hill Cipher (RHC) over $SL_n(F)$ which was associated with discrete wavelet transformation. The author also analyzed the robustness of the technique and also compared with other approaches in which security was increased without loss of information during transmission. In [11], Sarla Dewangan presented a competent method of encryption and proposed Two-Level Hill cipher. The method proposed was fast in encrypting and is robust against known plaintext attacks. The hybrid method achieved confidentiality and authentication of message.

In [12], Prerna proposed a modified a Hill cipher encryption and decryption techniques by involuntary key matrix and suggested efficient methods for generating self-invertible matrix for Hill cipher algorithm. They also provided security against different attacks like brute-force and known plaintext attacks. Komal Agarwal [13], proposed an idea in which Hill cipher is generated with Elliptic Curve Cryptography which increased the speed and decreased the memory. They analyzed the basis of key size and provided high security with shorter key size. Anand Joshi, [14], proposed a new approach for color image encryption and decryption using involuntary matrix associated with Arnold transmission. And also they discussed the security and sensitivity analysis in using digital RGB image processing.

In [15], Thangarasu. N have given formulae for the numbers of n*n involuntary matrices mod m and noted the decryption time. The size of the key was reduced and observed that if the dimension of the matrices was increased the key used was also large. Ashraf A. M. Khalaf [16], studied the security problem and presented a triple Hill cipher algorithm which provided more robust and high level security. They considered a block cipher with block length of 128 bits and key length of 256 bits at each stage. In [17], Andysah Putera, has designed a matrix in Hill cipher to perform encryption and decryption using genetic algorithm. They also determined the evaluation function in genetic algorithm in which the key was obtained and the time was reduced.

III. PROPOSED METHODOLOGY

To perform encryption, K must be a square matrix and the inverse of square matrix called decryption matrix using Hill cipher, K must satisfy two important criteria viz., it must be invertible and gcd(det[K], p)=1 where p is the base value of encoding scheme. In order to generate K for Hill cipher, K is normally obtained randomly and it could not be sometimes invertible. There is no deterministic method yet available in generating K. Thus, this paper focuses on a deterministic method in generating K. For this, it considers a magic rectangle of order m×n denoted as $MR_{m\times n}$ proposed in [18]. First $MR_{m\times n}$ is converted into square matrix of order m×m denoted as $SM_{m\times m}$. After converting into $SM_{m\times m}$, for each and every element in $SM_{m\times m}$ the modulus value p is taken depending on the encoding procedure used for encryption. From the SM, the K of order k is accepted as input.

A. Selection of K

It is noted that from $SM_{n\times n}$, the different sub matrices denoted as K' of order k are generated using two different ways.

Case (i): With overlapping of rows/columns.

In order to select K' of order k from $SM_{n\times n}$, start with row 1 and column 1, move up to column k horizontally and move downward from row 1 to row k. This is called first K' of order k. To get the next K', then start with column 2 and move up to column k+1 horizontally. The process is repeated till the last K' is obtained by selecting the column from (n-k) to k of row 1. The same process is repeated to get different K' for 2^{nd}, 3^{rd} …, $(n-k)^{th}$ row. Further, the total number of different possible K' of order k=2, 3, …,(n-2), (n-1) denoted as T_k is computed using

$$T_k = \sum_{k=1}^{n-2}(n-k)^2 \qquad \ldots(1)$$

For example, if n=5 then k=2, 3, 4. The different possible K' of order k are 2,3,4 and the sub matrices taken from the original matrix with overlapping are shown in fig.1.

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} \\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55} \end{bmatrix}$$

Fig 1(a). Original matrix of order n=5

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{bmatrix} \begin{bmatrix} a_{13} & a_{14} \\ a_{23} & a_{24} \end{bmatrix} \begin{bmatrix} a_{14} & a_{15} \\ a_{24} & a_{25} \end{bmatrix}$$

$$\begin{bmatrix} a_{12} & a_{13} & a_{14} \\ a_{22} & a_{23} & a_{24} \\ a_{32} & a_{33} & a_{34} \end{bmatrix} \begin{bmatrix} a_{13} & a_{14} & a_{15} \\ a_{23} & a_{24} & a_{25} \\ a_{33} & a_{34} & a_{35} \end{bmatrix}$$

$$\begin{bmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{bmatrix} \begin{bmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} a_{23} & a_{24} \\ a_{33} & a_{34} \end{bmatrix} \begin{bmatrix} a_{24} & a_{25} \\ a_{34} & a_{35} \end{bmatrix}$$

$$\begin{bmatrix} a_{22} & a_{23} & a_{24} \\ a_{32} & a_{33} & a_{34} \\ a_{42} & a_{43} & a_{44} \end{bmatrix} \begin{bmatrix} a_{23} & a_{24} & a_{25} \\ a_{33} & a_{34} & a_{35} \\ a_{43} & a_{44} & a_{45} \end{bmatrix}$$

$$\begin{bmatrix} a_{31} & a_{32} \\ a_{41} & a_{42} \end{bmatrix} \begin{bmatrix} a_{32} & a_{33} \\ a_{42} & a_{43} \end{bmatrix} \begin{bmatrix} a_{33} & a_{34} \\ a_{43} & a_{44} \end{bmatrix} \begin{bmatrix} a_{34} & a_{35} \\ a_{44} & a_{45} \end{bmatrix}$$

$$\begin{bmatrix} a_{32} & a_{33} & a_{34} \\ a_{42} & a_{43} & a_{44} \\ a_{52} & a_{53} & a_{54} \end{bmatrix} \begin{bmatrix} a_{33} & a_{34} & a_{35} \\ a_{43} & a_{44} & a_{45} \\ a_{53} & a_{54} & a_{55} \end{bmatrix}$$

$$\begin{bmatrix} a_{41} & a_{42} \\ a_{51} & a_{52} \end{bmatrix} \begin{bmatrix} a_{42} & a_{43} \\ a_{52} & a_{53} \end{bmatrix} \begin{bmatrix} a_{43} & a_{44} \\ a_{53} & a_{54} \end{bmatrix} \begin{bmatrix} a_{44} & a_{45} \\ a_{54} & a_{55} \end{bmatrix}$$

Fig 1(b). K′ of order k=2 with overlapping

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

$$\begin{bmatrix} a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \\ a_{41} & a_{42} & a_{43} \end{bmatrix}$$

$$\begin{bmatrix} a_{31} & a_{32} & a_{33} \\ a_{41} & a_{42} & a_{43} \\ a_{51} & a_{52} & a_{53} \end{bmatrix}$$

Fig 1(c). K′ of order k=3 with overlapping

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix} \begin{bmatrix} a_{12} & a_{13} & a_{14} & a_{15} \\ a_{22} & a_{23} & a_{24} & a_{25} \\ a_{32} & a_{33} & a_{34} & a_{35} \\ a_{42} & a_{43} & a_{44} & a_{45} \end{bmatrix} \begin{bmatrix} a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \\ a_{51} & a_{52} & a_{53} & a_{54} \end{bmatrix} \begin{bmatrix} a_{22} & a_{23} & a_{24} & a_{25} \\ a_{32} & a_{33} & a_{34} & a_{35} \\ a_{42} & a_{43} & a_{44} & a_{45} \\ a_{52} & a_{53} & a_{54} & a_{55} \end{bmatrix}$$

Fig 1(d). K′ of order k=4 with overlapping

Fig 1. SM with overlapping

Using (1),

$$T_k = (5-1)^2+(5-2)^2+(5-3)^2 = 16 + 9 + 4 = 29$$

Case (ii): Without overlapping of rows/columns

Before selecting elements of K′, the number of stages denoted as S is calculated using

$$S=\text{int}[n/k] \quad \ldots(2)$$

In order to get the first stage K′s of order k, start with row 1 and column 1 and move horizontally in SM up to column k. Then second K′ is selected by starting with $(k+1)^{th}$ column of row 1 and move up to 2k and the last K′ of first row is obtained from (n-

k)th column to k. To obtain the second, third,…,Sth stage K′, the same process is repeated with rows (k+1)th, (2k+1),…,(n-k)th rows respectively. Then T_k is calculated using

$$T_k = T_{k1} + T_{k2} \quad \ldots(3)$$

$$T_{k1} = \sum_{k=2}^{n1} q_k * q_k \qquad if\ n_1 \leq n/2 \quad \ldots(4)$$

$$T_{k2} = (n - n_1 - 1) \qquad if\ n_1 > n/2 \quad \ldots(5)$$

where n_1 = int[n/2]; q_k = int[n/k]. It is noted that if n=3 and k=2 then T_k=1, it is trivially rejected. The above formula is applicable only if n ≥ 4. But in case of without overlapping, for the same n=5, k=2,3,4 the different possible K′ are shown in fig.2.

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} \\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55} \end{bmatrix}$$

Fig 2(a). Original matrix k=3 of order n=5

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} a_{13} & a_{14} \\ a_{23} & a_{24} \end{bmatrix} \quad \begin{bmatrix} a_{31} & a_{32} \\ a_{41} & a_{42} \end{bmatrix} \begin{bmatrix} a_{33} & a_{34} \\ a_{43} & a_{44} \end{bmatrix}$$

Fig 2(b). K′ of order k=2 with overlapping

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

Fig 2(c). K′ of order with overlapping

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}$$

Fig 2(d). K′ of order k=4 with overlapping

Fig 2. SM without overlapping

Using (2), T_k = 4+1+1=6

B. Forming the Key Matrix K

After selecting K′ from MS, sometimes it may not satisfy the said criteria. It is noted that there are several K′s with order k are possible. Some modifications can be performed in K′ according to the following rules up to 10 to get at least one correct K.

K	Rule
4	$\forall i, if\ MS(i,i), i = 1, \ldots, k\ is\ already\ even, leave\ as\ it\ is.$ $Otherwise, MS(i,i) \leftarrow MS(i,i) + 1$
5 9	$\forall i, if\ MS(i,i)\ is\ already\ even, leave\ as\ it\ is.$ $Otherwise, MS(i,i) \leftarrow \begin{cases} MS(i,i) + 1, & i = 1,2, \ldots, (k-1) \\ MS(n,n) \leftarrow MS(n,n) + 1 \end{cases}$
6 8	$\forall i, if\ MS(i,i), i = 1,2, \ldots, n - 3, n\ is\ already\ even, leave\ as\ it\ is.$ $Otherwise, MS(i,i) \leftarrow \begin{cases} MS(i,i) + 1, \\ when\ i = (n-2), (n-1) \end{cases}$

7	$\forall i, i = 2, \ldots, 6$ $if\ MS(i,j)\ is\ already\ even, leave\ as\ it\ is.$ $Otherwise, MS(i,i) \leftarrow MS(i,i) + 1$
10	$\forall i, if\ MS(1,1), MS(n,n) is\ already\ odd, leave\ as\ it\ is.$ $Otherwise, MS(i,i) \leftarrow MS(i,i), MS(n,n) + 1$

Fig 3. Rules for obtaining k from K′

C. Determination of Key matrix

In order to get proper understanding of the work, let n= 16 with MSstart=4, MRcsum = 5000 is taken as input and MR is obtained as illustrated in [18].

617	4	613	16	601	24	28	593	589	40	577	48	565	52	569	64	553	72
611	18	615	6	20	605	42	587	591	30	44	581	567	66	563	54	68	557
12	609	8	621	603	22	585	36	32	597	579	46	56	561	60	573	555	70
10	619	14	607	26	599	595	34	38	583	50	575	62	571	58	559	74	551
545	88	541	76	529	96	521	100	505	112	517	120	497	124	493	144	136	481
539	78	543	90	92	533	515	114	116	102	519	509	491	138	495	485	126	140
84	549	80	537	531	94	108	513	507	525	104	118	132	489	128	142	501	483
82	535	86	547	98	527	106	523	122	511	110	503	130	499	134	479	487	146
469	148	473	160	457	168	449	184	445	172	433	192	425	196	409	208	421	216
471	162	467	150	164	461	443	174	447	186	188	437	419	210	212	198	423	413
152	465	156	477	459	166	180	453	176	441	435	190	204	417	411	429	200	214
158	475	154	463	170	455	178	439	182	451	194	431	202	427	218	415	206	407
401	220	397	240	385	232	244	377	373	256	361	264	353	349	268	280	337	288
395	234	399	389	236	222	258	371	375	246	260	365	347	351	282	270	284	341
228	393	224	387	238	405	369	252	248	381	363	262	276	272	345	357	339	286
226	403	230	383	242	391	379	250	254	367	266	359	274	278	355	343	290	335

Fig 4. $MR_{16\times18}$

Suppose, alphabetical encoding is used, the resultant modular rectangle is shown in fig. 3.

19	4	15	16	3	24	2	21	17	14	5	22	19	0	23	12
13	**18**	17	6	20	7	16	15	19	4	18	9	21	14	17	2
12	11	**8**	23	5	22	13	10	6	25	7	20	4	15	8	1
10	21	14	**9**	0	1	23	8	12	11	24	3	10	25	6	13
25	10	21	24	**9**	18	1	22	11	8	23	16	3	20	25	14
19	0	23	12	14	**13**	21	10	12	24	25	15	23	8	1	17
6	3	2	17	11	16	**4**	19	13	5	0	14	2	21	24	12
4	15	8	1	20	7	2	**3**	18	17	6	9	0	5	4	11
1	18	5	4	15	12	7	2	**3**	16	17	10	9	14	19	0
3	6	25	20	8	19	1	18	5	**4**	6	21	3	2	4	16
22	23	0	9	17	10	24	11	20	25	**19**	8	22	1	21	13
2	7	24	21	14	13	22	23	0	9	12	**15**	20	11	10	25
11	12	7	6	21	24	10	13	9	22	23	4	**15**	11	8	20
5	0	9	25	2	14	24	7	11	12	0	1	9	**13**	22	10
20	3	16	23	4	15	5	18	14	17	25	2	16	12	**7**	19
18	13	22	19	8	1	15	16	20	3	6	21	14	18	17	**5**

Fig 5. Modular Rectangle with order 16

Let k= 10, then the first 10×10 matrix is taken from fig.2 denoted as K′ it is shown in fig.4.

19	4	15	16	3	24	2	21	17	14
13	**18**	17	6	20	7	16	15	19	4
12	11	**8**	23	5	22	13	10	6	25
10	21	14	**9**	0	1	23	8	12	11
25	10	21	24	**9**	18	1	22	11	8
19	0	23	12	14	**13**	21	10	12	24
6	3	2	17	11	16	**4**	19	13	5
4	15	8	1	20	7	2	**3**	18	17
1	18	5	4	15	12	7	2	**3**	16
3	6	25	20	8	19	1	18	5	**4**

Fig 6. K′ of order 10

Since |K′| = 0, K′ is not invertible. Using rule 5, K′ is changed as,

19	4	15	16	3	24	2	21	17	14
13	**19**	17	6	20	7	16	15	19	4
12	11	**9**	23	5	22	13	10	6	25
10	21	14	**9**	0	1	23	8	12	11
25	10	21	24	**9**	18	1	22	11	8
19	0	23	12	14	**14**	21	10	12	24
6	3	2	17	11	16	**4**	19	13	5
4	15	8	1	20	7	2	**4**	18	17
1	18	5	4	15	12	7	2	**4**	16
3	6	25	20	8	19	1	18	5	**5**

Fig 7. Generation of K after applying the rule

Now, |K′| = 15. Further, gcd(|K′|, 26) ≠ even number and hence K′ is treated as K.

IV. ENCRYPTION/DECRYPTION USING HILL CIPHER

To perform encryption, let the plaintext P be taken for encryption is “kannanbaba” and alphabetical encoding is used (i.e., p = 26). Then, using Hill cipher encryption C = KP mod 26

$$C = \begin{bmatrix} 19 & 4 & 15 & 16 & 3 & 24 & 2 & 21 & 17 & 4 \\ 13 & 19 & 17 & 6 & 20 & 7 & 16 & 15 & 19 & 4 \\ 12 & 11 & 9 & 23 & 5 & 22 & 13 & 10 & 6 & 25 \\ 10 & 21 & 14 & 9 & 0 & 1 & 23 & 8 & 12 & 11 \\ 25 & 10 & 21 & 24 & 9 & 18 & 1 & 22 & 11 & 8 \\ 19 & 0 & 23 & 12 & 14 & 14 & 21 & 10 & 12 & 24 \\ 6 & 3 & 2 & 17 & 11 & 16 & 4 & 19 & 13 & 5 \\ 4 & 15 & 8 & 1 & 20 & 7 & 2 & 4 & 18 & 17 \\ 1 & 18 & 5 & 4 & 15 & 12 & 7 & 2 & 4 & 16 \\ 3 & 6 & 25 & 20 & 8 & 19 & 1 & 18 & 5 & 5 \end{bmatrix} \begin{bmatrix} 11 \\ 1 \\ 14 \\ 14 \\ 1 \\ 14 \\ 2 \\ 1 \\ 2 \\ 1 \end{bmatrix} mod\ 26 = \begin{bmatrix} 19 \\ 15 \\ 15 \\ 10 \\ 8 \\ 21 \\ 4 \\ 0 \\ 14 \\ 16 \end{bmatrix} = \begin{bmatrix} S \\ O \\ O \\ J \\ H \\ U \\ D \\ Z \\ N \\ P \end{bmatrix}$$

Thus the plaintext “kannanbaba” is converted into “SOOJHUDZNP”.

To perform decryption, Using Hill cipher decryption P = K^{-1} C mod 26

$$P = \begin{bmatrix} 3 & 2 & 23 & 9 & 4 & 25 & 9 & 23 & 23 & 10 \\ 0 & 13 & 24 & 1 & 18 & 18 & 3 & 4 & 17 & 14 \\ 5 & 12 & 17 & 14 & 4 & 14 & 9 & 4 & 25 & 12 \\ 20 & 7 & 12 & 21 & 23 & 9 & 9 & 25 & 10 & 11 \\ 16 & 6 & 8 & 20 & 18 & 21 & 2 & 10 & 23 & 12 \\ 15 & 18 & 22 & 9 & 0 & 21 & 9 & 2 & 12 & 2 \\ 24 & 24 & 20 & 23 & 24 & 22 & 16 & 25 & 16 & 18 \\ 15 & 6 & 18 & 5 & 23 & 12 & 4 & 7 & 4 & 24 \\ 16 & 10 & 20 & 22 & 23 & 2 & 20 & 20 & 1 & 20 \\ 1 & 20 & 24 & 25 & 21 & 22 & 17 & 6 & 17 & 7 \end{bmatrix} \begin{bmatrix} 19 \\ 15 \\ 15 \\ 10 \\ 8 \\ 21 \\ 4 \\ 0 \\ 14 \\ 16 \end{bmatrix} mod\ 26 = \begin{bmatrix} 11 \\ 1 \\ 14 \\ 14 \\ 1 \\ 14 \\ 2 \\ 1 \\ 2 \\ 1 \end{bmatrix} = \begin{bmatrix} k \\ a \\ n \\ n \\ a \\ n \\ b \\ a \\ b \\ a \end{bmatrix}$$

V. CONCLUSION

A deterministic method of generating the key matrix K of higher order k from magic rectangle for Hill cipher encryption is thought of and it is generated successfully. It is noted that the sub matrix K′ with order k selected from magic rectangle is not necessarily be invertible in generating the key matrix K. For that some rules have been proposed to obtain the correct K from K′. The rules are formed in such a way that it must satisfy the said criteria in determining the correct K. Further, in the proposed method as k is selected large, the block size for encrypting the plain text is also large. The novelty in this paper is that any number of sub matrices of order k can be taken with and without overlapping of rows/columns from the original MR. As many K are generated from magic rectangle, the eavesdropper may not know which K is taken for encryption which will prevent many cryptographic attacks.

REFERENCES

[1] Bibhudendra Acharya, Girija Sankar Rath, Sarat Kumar Patra, Saroj Kumar Panigrahy, "Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm", *International Journal of Security* (CSC Journals), Volume 1, Issue 1, 2007.

[2] 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.

[3] Bibhudendra Acharya, Sarat Kumar Patra, and Ganapati Panda, "Involutory, Permuted and Reiterative Key Matrix Generation Methods for Hill Cipher System", *International Journal of Recent Trends in Engineering*, Volume 1, No. 4, May 2009.

[4] P.Shanmugam & C.Loganathan, "Involutory Matrix in Visual Cryptography", *International Journal of Recent Research and Applied Studies* (IJRRAS), March 2011.

[5] Prof. A.V.N.Krishna, K.Madhuravani, "A Modified Hill Cipher using Randomized Approach", *I. J. Computer Network and Information Security*, June 2012.

[6] Adi Narayana Reddy K, Vishnuvardhan B, Durga Prasad K, "Generalized Affine Transformation Based on Circulant Matrices", *International Journal of Distributed and Parallel Systems (IJDPS)*, Volume 3, No.5, September 2012.

[7] B. Karthikeyan, Jagannathan Chakravarthy, Ramasubramanian S, "Amalgamation of Scanning paths and Modified Hill Cipher for Secure Steganography", *Australian Journal of Basic and Applied Sciences*, Volume 6(7), 2012.

[8] Rahul. R. Ravan, Atul R. Nigavekar, "Secured Data Communication using Novel Modification to Hill Cipher Algorithm with Self Repetitive Matrix", *International Journal of Science and Research* (IJSR), Volume 2, Issue 4, April 2013.

[9] Gurtaptish Kaur, Sheenam Malhotra, "A Hybrid Approach for Data Hiding using Cryptography Schemes", *International Journal of Computer Trends and Technology (IJCTT)*, volume 4, Issue 8, August 2013.

[10] D. C. Mishra and R. K. Sharma, "Grayscale-image encryption using Random Hill Cipher over SLn(F) associated with Discrete Wavelet Transformation", *Applications and Applied Mathematics: An International Journal* (AAM), Volume 8, Issue 2, December 2013.

[11] Sarla Dewangan, Mrs. Shikha Pandey, Mohammad Imroze Khan, "Design of a Cryptosystem Using Two-Level Hill Cipher", *International Journal for Advance Research in Engineering and Technology,* Volume 2, Issue I, January 2014.

[12] Prerna, Urooj, Meena kumari, Jitendra Nath shrivastava, "Image Encryption and Decryption using Modified Hill Cipher Technique", *International Journal of Information & Computation Technology*, Volume 4, Number 17, 2014.

[13] Komal Agrawal, Anju Gera, "Elliptic Curve Cryptography with Hill Cipher Generation for Secure Text Cryptosystem", *International Journal of Computer Applications,* Volume 106, No.1, November 2014.

[14] Anand Joshi, Maneesha Kumari, "Encryption of RGB image using Arnold transform and involutory matrices", *International Journal of Advanced Research in Computer and Communication Engineering* (IJARCCE), Vol. 4, Issue 9, September 2015.

[15] Thangarasu.N, Dr.Arul Lawrence SelvaKumar, "Encryption using Lester Hill Cipher Algorithm", *International Journal of Innovative Research in Advanced Engineering* (IJIRAE), Volume 2, Issue 12, December 2015.

[16] Ashraf A.M. Khalaf, Mona S. Abd El-karim, Hesham F. A. Hamed, "A Triple Hill Cipher Algorithm Proposed to Increase the Security of Encrypted Binary Data and its Implementation Using FPGA", *ICACT Transactions on Advanced Communications Technology (TACT)*, Volume 5, Issue 1, January 2016.

[17] Andysah Putera Utama Siahaan, "Genetic Algorithm in Hill Cipher Encryption", *American International Journal of Research in Science, Technology, Engineering & Mathematics*, June-August, 2016.

[18] Mani.K, Viswambari. M, "Enhancing the Security in Cryptosystems Based on Magic Rectangle", International Journal of Computer Network and Information Security (IJCNIS), Volume. 9, No.4, 2017.