A New Cryptographic Symmetric Key Algorithm Design by Clockwise 2D-Rotation Matrix

Ginny Bansal, Anuj Kumar and Naveen Kumar
Department of CSE, JPIET, Meerut.

ABSTRACT
Today huge amount of data are transforms over the network connected to internet. In recent day many social networking site, electronic mail, trades website etc. exchange information in term of audio, video, image, text. Here more concern is that how to secure such type of data from the various intruders. There are various algorithm is used to provide security from unauthorized of data over the network. The term cryptography is the technique to exchange the plain text (sender message) into cipher text (encoded form) and then convert it encoded message back into original message. Symmetric cryptographic is one of the cryptographic techniques where sender and receiver generate a common key that is used to encrypt and decrypt the message. Here, introduce a new emerging Geometry based Cryptography approach in the field of symmetric cryptography. In this technique used a 2-D clockwise Rotation and performs transformations such as on the object matrix to obtain cipher text. The basic idea behind this paper is that focuses on the symmetric key Cryptography approach, using the concepts of clockwise 2D-rotation of object and find out an algorithm that provide the better accuracy and security over the basic encryption algorithm.

I. Introduction
In the new era, data security is the major concern because of large amount of data transform over network via internet. More Security for that data is an important issue. The Cryptography technique provides the security where human-being is allowed to encrypt the data and decrypt can be performed without the aid of sender. At the same time, the security issues are a crucial problem in the transmission process. In symmetric key encryption, common key is shared by the sender and receiver. Text message are arranged in different 3*n matrices. When there is a need to send a message, the generated key as angle in rotation matrix. Again all the characters in the matrices are converted into hexadecimal. Now the data will be encrypted using rotation matrices. Then the encrypted message and Intermediate-key will be transmitted to the Destination. When the cipher-text reaches the Destination, the rotation key will be computed by using transpose matrix. Then the message will be decrypted.

Cryptography: The cryptography is a technique say: art and science of making a cryptosystem that is able of provides information security. Cryptography deals with the actual securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. You can think of cryptography as the establishment of a large toolkit containing different techniques in security applications.

Symmetric Cryptography: In the symmetric key encryption technique, the same key concept is used for encryption and decryption process of the text message. The basic advantage of symmetric algorithm is that, not consuming additional of computing power and symmetric key encryption technique works with very high speed in encrypted them. The symmetric key encryption used in two different modes either as a block ciphers or as a stream ciphers. In the block cipher, the complete data is divided into number of specified blocks. Which is based on the block length and the key is provided for encryption. In the stream ciphers mode provides, the data is divided as small as single bit and randomized then the encryption takes place. Symmetric key cryptosystems are much faster than the asymmetric key cryptosystems [7].

2-D Rotations: In 2-D rotation, rotate the particular object at specific angle θ (theta) from its origin. The Rotation may be counter clockwise and clockwise.

A rotation in the x-y plane by an angle θ measured counterclockwise from the positive x-axis is represented by the real 2x2 special orthogonal matrix,

\[
\begin{pmatrix}
\cos \theta & -\sin \theta \\
\sin \theta & \cos \theta
\end{pmatrix}
\]

A clockwise rotation on the row vectors will correspond to a counterclockwise rotation on the column vectors

\[
\begin{pmatrix}
\cos \theta & \sin \theta \\
-\sin \theta & \cos \theta
\end{pmatrix}
\]

Fig 1. Clockwise 2D-Rotation.
In the Figure, the point P(x, y) is located at angle φ from the horizontal X coordinate with distance r from the origin.
Here the object is move the angle theta in clockwise direction which is shown in figure.

The point P(x, y) can be represented as, In ΔOPA, cos φ=x/r, and sin φ=y/r, then

\[ x=r \cos \phi \] \[ y=r \sin \phi \]

Similarly, the point P’ (x’, y’) represent as in ΔOP’A, cos (φ-θ) =x’/r and sin (φ-θ) =y’/r, then

\[ x’=r \cos (\phi-\theta) = r \cos \phi \cos \theta - r \sin \phi \sin \theta \]
\[ y’=r \sin (\phi-\theta) = r \sin \phi \cos \theta - r \cos \phi \sin \theta \]

Using the eqn-3 and eqn-4, representing the matrix of clockwise 2D rotation in two dimension form as follow:-

\[ R(\theta) = \begin{bmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{bmatrix} \]

II. IV. Hill Cipher: Hill cipher is a polygraphic substitution cipher based on linear algebra. In this technique each letter of plain text message is represented by a number modulo 26 that is A = 0, B = 1… Z = 25 simple pattern is used, but this is not an essential feature of the cipher. Here to encrypt a message, to create various block and each block of n letters is multiplied by an invertible n x n matrix, against modulus 26. And for description of message, each block is multiplied by the inverse of the matrix used for encryption. In this technique, the matrix used for encryption is the cipher key, and it should be chosen randomly from the set of invertible n x n matrices (modulo 26). The substitution of cipher text letters in place of plaintext generates m linear equations . For m=n, the system can be described as follows:

\[ C_1 = (K_{11}P_1 + K_{12}P_2 + K_{13}P_3) \mod 26 \]
\[ C_2 = (K_{21}P_1 + K_{22}P_2 + K_{23}P_3) \mod 26 \]
\[ C_3 = (K_{31}P_1 + K_{32}P_2 + K_{33}P_3) \mod 26 \] (1)

The above equation can be written in column vector as well as Row Vector and Matrix:

\[ \begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix} \mod 26 \] (2)

The Equation (2) can be written in simple form as C=K P mod 26. Here K and P is the column vector which is length of vector is three that is representing the plaintext and cipher text respectively, and K is a 3x3 matrix, which is the encryption key. All operations are performed mod 26 here.

When decrypts the message to other end then used the inverse matrix of K that is K-1 of a matrix K and represent by the equation K K-1 = I , here I is the Identity matrix. But the inverse of the each matrix does not always exist it is the problem in this hill cipher, and when it does, it satisfies the preceding equation. Then K-1 is applied to the cipher text, and find out the original plaintext message. In general term we can write as follows:

i) For encryption
\[ C = E_K(P) = K P \]

ii) For decryption
\[ P = D_K(C) = K^{-1} C = K^{-1} K P = P \]

If the block length is m, there are 26mdifferent m letters blocks possible, each of them can be regarded as a letter in a26m-letter alphabet. In Hill cipher, the basic problem is arises that the every square matrix does not necessarily identity matrices.

II. Related Work

Deepthi Rana et.al. [1] Examines that, cryptography is the science or art of transforming an intelligible message (plaintext) into one that is unintelligible (cipher text) and then transforming the message back to its original form. Symmetric key Cryptography is a cryptographic approach where the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. Geometry based cryptography is a new and emerging approach in the field of cryptography. It uses geometric shapes such as circles; ellipses etc and perform geometric transformations on these figures to produce cipher text. The present work focuses on the Symmetric key Cryptography technique, using the concepts of Cartesian coordinate geometry and circle generation. Chakra algorithm, for symmetric key cryptography, is used as the basis for this work with some modifications in it for better results. Chakra is a Sanskrit term which means a circle or a disc. It plays a key role in encryption of data. Data is grouped into circles and each circle holds a portion of data. An improved geometric cryptographic algorithm is developed, that considers data into a 2- dimensional data grid, generate circles on the grid and apply some geometric transformations over data. This encryption technique adapts hybrid geometric transformations (i.e., translation followed by scaling) of the circumference points of every circle by some scaling factors (Sx, Sy) and translation factors (Tx , Ty). The proposed algorithm is an improvement in the basic Chakra algorithm in terms of accuracy.

Swapnali Krushmarao Londhe et.al.[2] emphasis on, Privacy for that data is an important issue. Cryptography is one of the technique used for stopping unauthorized access and increasing integrity of that data. In this research encryption and decryption scheme is used based on image pixel shuffling and transposition. We can use cipher algorithm for generating key using RGB values of the pixel. For that purpose we use m*n size image on which different operations are performed. This algorithm was implemented in java language.

Mohammad Jabeen Morshed Chowdhury et.al.[3], focus on Symmetric Key cryptography is one of the prominent means of secure data transfer through unreliable channel. It requires less overhead than Public Key Cryptosystem. We present here, a new algorithm based on 2-d geometry using property of circle, and circle-centered angle. It is a block cipher technique but has the advantage of producing fixed size encrypted messages in all cases. It incorporates low computational complexity with fairly high confidentiality.

Prerna Gaur et.al.[4] proposes a new method for security with symmetric key here Cryptography is the way to secure the data to achieve higher reliability during the communication process. There exist a number of cryptographic approaches. This paper defines a geometry based Symmetric cryptography algorithm that is used to encrypt the input data. As the name suggests the approach is based on the geometric figure to perform the cryptography. In this work, we will define elliptic shape geometry to generate the dynamic key so as to perform the dynamic symmetric encryption of input text. Based on the geometric elliptic figure’s properties the key will be generated and by using the key parameters the length and breadth of Cartesian plain will be defined. Once the area will be defined, the next work is to define a group of ellipses and to perform the translation and rotation of axis. By extracting the pixel positions on these ellipses and to place the input data respectively to these
locations the cryptography will be performed. The actual work of this algorithm is to change the data locations instead of changing the data. The secure and reliable encoding of the data is expected from the work.

Preeti Poonia et.al.[5] the research work of this paper focus on symmetric cryptographic technique based on hill cipher recent day’s drastic change in communication like social media network such as mobile communication and computer, all type of a data such as audio, video, images are used for the communication. More Security for that data is an important issue. Cryptography is the technique to transforming plain text (message) into one that is cipher text and then transforming the message back to its original form. Symmetric key Cryptography is a cryptographic approach where the sender and receiver of a message allocate a single, common key that is used to encrypt and decrypt the message. Geometry based Cryptography is a new and emerging approach in the field of cryptography. It uses 2-D Rotation and performs geometric transformations on the object matrix to produce cipher text. This work focuses on the symmetric key Cryptography technique, using the concepts of 2-D rotation of object. The main focus in this paper is to produce an algorithm. The proposed algorithm is an improvement in the basic encryption algorithm in terms of accuracy and security.

III. Proposed Methodology
This paper introduced new security algorithm based upon the clockwise 2D-rotation graphics transformation techniques and the symmetric key cryptographic approach. Here introduced new manipulation method for data encryption and decryption of any text. The main aim to develop a symmetric key algorithm where they have used clockwise 2D rotation matrix (2D transformation) for encryption and decryption methods.

In this paper, used a row vector of length 3, that is obtain from the ASCII value of plaintext message. If length of plaintext is less than 3 character then add required bogus (dummy) character and multiply this matrix with clockwise 2D rotation matrix and rotate with a random angle θ. Find out encrypted rotation matrix in rational format now convert this rotation matrix value into hexadecimal value. This hexadecimal rotation matrix is the encoded text i.e. ciphers text.

The matrix multiplication with row vectors. Say you have a matrix A of dimension m×n and a row vector V of dimension 1×m, then you can multiply the vector "from the left" as VA will be (1×m)(m×n) for which the product gives a 1×n vector. Similarly with column vectors, you can only multiply them from the right of a matrix (assuming dimensions match).

Following step for producing encryption of given message……

1. Enter the text message and convert it into ASCII value.
2. Create row vector of length three if less than three then add some bogus character.
3. Create clockwise 2-D rotation matrix with random angle theta.
4. Multiply row vector (from the left) with clockwise 2-D rotation matrix.
5. Obtain matrix convert into hexadecimal value (which is encrypted text) and repeated this process till the all block of length 3.

Following step for producing decryption of given encrypted message.

1. Enter Encrypted Hexadecimal Text Message and convert it into ASCII value in form row vector.
2. Obtained the Transpose the given clockwise 2-D rotation matrix.
3. Multiply transpose matrix with ASCII value row vector and find row vector
   Convert obtained value of this row vector into corresponding character and repeated this procedure until all data convert into original form.

IV. Algorithms

a) Clockwise 2D Rotation Algorithm for Encryption
1. Enter the input text message (plain text)
   Setmsg: = Plain Text
   Theta: = random θ (0,360)
2. If length(msg)<3 then
   Add bogus (dummy) character into the plain text to make length equal to three
End if
3. Generate ASCII value of each character of the msg.
   Ascii_value[i]=ascii(msg[i]) for all i=1 to length(msg)
4. Create plain text row vector of length 3 from ascii_value[i].
5. Multiplication of clockwise 2-D rotation matrix with plaintext row vector
   Rotation_plaintext=plain_text_row_vector (length 3(msg)) * Clockwise Rotation matrix (θ)
6. Convert the Rotation_plaintext matrix into hexadecimal values.
   Cipher_text=hexadecimal (Rotation_plaintext matrix) //encrypted message

b) Clockwise 2D Rotation Algorithm for Decryption
1. Convert encrypted hexadecimal Text to numeric row vector of length 3
   Cipher_Text[i]= hexadecimal_to_numeric(i)
2. Transpose of clockwise Rotation matrix.
3. Multiplication of transpose rotation matrix and cipher text row vector(from left)
   original_ascii_value [i,] = Transpose_Rotation_matrix(θ)* Cipher_Text_row_vector (length3(msg))
4. Convert original_ascii_value[i,] into character for all i=1 length 3 (msg)
5. Find original text message.

Fig 2. Block Diagram Clockwise 2D Rotation Algorithm for Symmetric Cryptography.
V. Experimental Works:

This paper presents a clockwise 2D rotation algorithm for encryption/decryption for the given text. The work of the algorithm depicted in figure to use experimental tool MATLABVER2011.

STEP BY STEP RESULT OF PROPOSED METHODOLOGY:

1. Algorithm applied to Fixed Length Input
   a. Fixed Length Encryption

   ![Fig 3. Encryption Result for Fixed Length Input.]

   Fixed Length Decryption

   ![Fig 4. Fixed Length Decryption.]

   b. Fixed Length Decryption

2. Algorithm applied to variable length input
   a. Variable Length Encryption

   ![Fig 5. Variable Length Encryption.]

   b. Variable Length Decryption:

   ![Table showing the encryption results.]

   Column 1 through 16:
   87.0000 69.0000 76.0000 67.0000
   97.0000 79.0000 86.0000 77.0000
   2.0000 1.0000 1.0000 1.0000
   79.0000 77.0000 65.0000 32.0000
   89.0000 87.0000 75.0000 42.0000
   1.0000 1.0000 1.0000 1.0000
   84.0000 70.0000 32.0000 74.0000
   94.0000 89.0000 42.0000 84.0000
   1.0000 1.0000 1.0000 1.0000
   80.0000 73.0000 65.0000 84.0000
   90.0000 83.0000 75.0000 94.0000
   1.0000 1.0000 1.0000 1.0000

   Original Message --->

   WELCOME TO JPIET

   ![Fig 6. Variable Length Decryption.]

   VII. Conclusion

   In this paper implement a new cryptographic technique based on clockwise 2-D rotation that encrypt and decrypt the plain text message. It overcomes the problem of hill cipher technique. In this work to encrypt the text message in decrypt form using different rotation angle and send it to receiver end. In future we can overcome complexity and apply different cryptography method and generate a new hybrid technique for key generation.

   References: