Abstract - Information security is the most important aspect of digital data communications. This demands an effective cryptographic algorithm to secure these information from an unauthorized access. This paper is aiming to apply a modification on the Elliptic Curve Cryptography which makes computations easier, faster and improve the performances of security. Hill Cipher with Circulant Matrix has been used to share the secret key and mapping the message instead of applying Koblitz Encoding method. In this paper, Image encryption and decryption processes have been implemented using the proposed new Elliptic Curve Cryptography Modified Hill Cipher algorithm. Security analysis was performed on the algorithm to make an evaluation.

Keywords - Circulant Matrix, Elliptic curve cryptography, Hill cipher, Security analysis.

I. INTRODUCTION

Nowadays the challenge of securing the data is now completely huge. These data turn into more importance and privacy like ATM card, e-commerce and military information. Cryptography is one of the methods used to protect data from unauthorized access. Generally, there are two types of cryptography: Symmetric Key Cryptography (SKC) and Asymmetric (Public) Key Cryptography (PKC).

In SKC, the same key is used for encryption and decryption, but in PKC, two separate keys are used. One key known as public key is obtained from the other key called private key.


ECC uses less key size to provide more security. ECC security is based on the intractability of a highly difficult problem, namely Elliptic Curve Discrete Logarithm Problem (ECDLP) [3].

The Hill cipher (HC) was invented by L.S. Hill in 1929 [4]. It is a type of a symmetric block cipher technique based on matrix transformation. HC is a monoalphabetic polygraphic substitution block cipher. Both sender and receiver should share and use the same key matrix for ciphering and deciphering. HC has resistant towards frequency analysis, high speed and high throughput. HC is vulnerable against known-plaintext attack.

II. REVIEW OF LITERATURE

Several studies have been presented by many researchers. For instance, Darrel Hankerson, Alfred Menezes and Vanstone in 2004 introduced why ECC is considered over other cryptography techniques [3].

In 2007, Bibhudendra proposed various methods of generating self-invertible matrix for HC algorithm [9] and Sastry have modified the HC using permutation and circular rotation which depends on the key [10]. Agrawal & Gera in 2014 produced a new method for encryption by using HC algorithm first to produce the ciphertext numerical values, and then convert it to points on the ECC by using scalar multiplication [11]. Ziad E. Dawahdeh in 2017 introduced combine ECC with HC to increase its security and efficiency of authentic HC [12].

III. ELLIPTIC CURVE OPERATION

ECC makes use of mathematical properties of the elliptic curves for both encryption and decryption. For cryptographic applications, ECC makes use of either the prime field or the binary field. An Elliptic Curve (EC) over a Prime Field ($P_f$) is defined by:

$$E_{C'}: y^2 \equiv x^3 + ax + b \ (mod \ p) \ (1)$$

where $a, b \in P_f, p\neq2,3$ and satisfy the condition:
\[4a^2 + 27b^2 \neq 0 \pmod{p}\] (2)

The Elliptic Curve Group (ECG) is the set of all points \((x, y)\) that satisfy the elliptic curve equation (1) beside a special point O at infinity [6]. The order of E is defined as the number of points of the curve and denoted by \(E\) [6].

The basic operations involved in ECC are: addition of points, doubling of points, multiplication of points and subtraction of points.

3.1. Addition of points

Consider two distinct points on an elliptic curve, \(M \) and \(S\) where \(M = (x_m, y_m)\) and \(S = (x_s, y_s)\) at \(M \neq S\). The addition of both these points results in another point on the given EC, \(L\), where \(L = (x_l, y_l)\). \(x_l\) and \(y_l\) are derived by following mathematical expressions:[6] \(M + S = L\)

\[x_l \equiv (\lambda^2 - x_m - x_s) \pmod{p}\] (5)

\[y_l \equiv (\lambda(x_m - x_l) - y_m) \pmod{p}\] (6)

If \(x_m = x_s\) but \(y_m \neq y_s\), then \(M + S = O\).

3.2. Doubling of points

Consider a point \(M = (x_m, y_m)\) on EC. Adding the point \(M\) to itself is called doubling point on an EC:[6] \(M + M = 2M = L\)

\[x_l \equiv (\lambda^2 - 2x_m) \pmod{p}\] (7)

\[y_l \equiv (\lambda(x_m - x_l) - y_m) \pmod{p}\] (8)

3.3. Multiplication of points

Scalar multiplication of point is obtained by multiplying a scalar \(k\) with a point \(M\) on the given EC. Scalar multiplication of point can be achieved either by repeated addition of points operation alone or by combining repeated addition and doubling operations [6].

The multiplication of a point \(M\) with a scalar \(k\) by using repeated additions and doubling is computed as follows let \(k = 0\)

\[9M = 2(2M) + M\] (11)

The multiplication of a point \(M\) with a scalar \(k\) by using repeated additions is computed as follows:

\[kM = M + M + \cdots + M\] (times) (12)

3.3. Subtraction of points

Consider a point \(M\) on EC. The negative of the point \(M\) [6].

\[\text{where} - S = (x_m, -y_m)\] At \(M + S = O\) (13)

IV. HILL CIPHER

HC is a block cipher algorithm where plaintext is divided into equal size blocks. In HC, the key is a matrix of size \(n \times n\) in which \(n\) is the size of the block. The plaintext \(P\) is encrypted as:

\[C = M_k \times P \pmod{m}\] (14)

Which \(C\) is the cipher text block and \(M_k\) is key matrix. The decryption of cipher text \(C\) produces plaintext as:

\[P = M^{-1}_k \times C \pmod{m}\] (15)

The encryption key matrix must satisfy two important criteria viz, the key matrix should be invertible and the gcd (det \(M_k\) )mod \(m\) = 1. \[w \cdot K \times M_k^{-1} = I\] (16)

Which \(I\) is the identity matrix. Both sender and receiver should use the same key matrix for deciphering and deciphering.

4.1. The Circulant Matrix

A Circulant Matrix (CM) [9] is matrix where each row is rotated one element to the right relative to the preceding row vector. Thus, a circulant matrix can be written as:

\[
C_m = \begin{bmatrix}
c_0 & c_1 & \cdots & c_{n-1} \\
c_{n-1} & c_0 & \cdots & c_{n-2} \\
\vdots & \vdots & \ddots & \vdots \\
c_1 & c_2 & \cdots & c_0 
\end{bmatrix}
\] (17)

V. THE PROPOSED ALGORITHM

5.1. Selection of ECG domain parameters

The domain parameters for EC over \((p, a, b, N)\) are \((p, a, b, N)\) where \(p\) is the prime number defined for finite field, \(a\) and \(b\) are the curve parameters and \(N\) is the order of EC.

5.2. Generation of ECG elements

An EC eq. (1) and satisfy the condition eq. (2) to generate points or group elements of EC.

5.3. Selection of Base Point

Select the Base Point \((BP)\) which is a point on the EC chosen for cryptographic operation \((BP_p, BP_y)\).

5.4. Generation of Secret Key

Sender selects a Private Key \((P_k)\) and is a random integer between 1 and \((N - 1)\), then calculates a PublicKey \((U_k) = BP \times P_k\) (18)

Receiver selects a Private Key \((P_r)\) and is a random integer between 1 and \((N - 1)\), then calculates a PublicKey \((U_r) = BP \times P_r\) (19)

Both the sender and receiver have the same Secret Key \(S_k:\)

\[w \cdot S \cdot K = P_s \times U_r = P_r \times U_s\] (20)

5.5. Generation of Secret Matrix

By using \(SK(S_{K_s}, SK_y)\) and \(BP (BP_p, BP_y)\), then computes

\[M_1 = BP \times SK_x\]

\[M_2 = BP \times SK_y\]

By using \(M_1, M_2\) we create a row of matrix \((M_1, M_2, M_1, M_2)\), then generate the initial Key matrix by using circulant matrix with dimension \((4 \times 4)\):

\[K_{cm} = \begin{bmatrix}
M_{11} & M_{12} & M_{21} & M_{22} \\
M_{22} & M_{11} & M_{12} & M_{21} \\
M_{21} & M_{22} & M_{11} & M_{12} \\
M_{12} & M_{21} & M_{22} & M_{11}
\end{bmatrix} \pmod{m}\]

The inverse of the key CM does not always exist. The receiver cannot decrypt the cipher message if the key CM not invertible.

To overcome this case, we use the self-invertible key
CM will be created and the identical key CM will be used for sender and receiver. The self-invertible key CM
\[
(SK_m) = \begin{bmatrix}
K_{cm} & I - K_{cm} \\
I + K_{cm} & -K_{cm}
\end{bmatrix} \mod m
\]
So, the secret key CM will be a matrix with dimensions \((8 \times 8)\).

\[
\begin{bmatrix}
M_{11} & M_{12} & M_{13} & M_{14} & M_{15} & M_{16} & M_{17} & M_{18} \\
M_{21} & M_{22} & M_{23} & M_{24} & M_{25} & M_{26} & M_{27} & M_{28} \\
M_{31} & M_{32} & M_{33} & M_{34} & M_{35} & M_{36} & M_{37} & M_{38} \\
M_{41} & M_{42} & M_{43} & M_{44} & M_{45} & M_{46} & M_{47} & M_{48} \\
M_{51} & M_{52} & M_{53} & M_{54} & M_{55} & M_{56} & M_{57} & M_{58} \\
M_{61} & M_{62} & M_{63} & M_{64} & M_{65} & M_{66} & M_{67} & M_{68} \\
M_{71} & M_{72} & M_{73} & M_{74} & M_{75} & M_{76} & M_{77} & M_{78} \\
M_{81} & M_{82} & M_{83} & M_{84} & M_{85} & M_{86} & M_{87} & M_{88}
\end{bmatrix}
\]

5.6. Encryption and Decryption for Image Security

The proposed algorithm of Elliptic curve cryptography modified Hill cipher dependent on Circulant matrix (ECCMHC). The main concept of this technique depends on divide the image into blocks consisting of the same size \(n\) depending on the key matrix size \(n \times n\). For encryption, separate the image pixel values into blocks to be a vector of size \(n \times 1\). \((p_1, p_2, \ldots, p_n)\), So, the ciphered vectors will be:
\[
C_n = SK_m \times p_n \mod 256 \quad (21)
\]
After that, reconstruct the ciphered image \(C\) from the values in the ciphered vectors and send it to the other party.

For decryption, separate the ciphered image pixel values into blocks to be a vector of size \(n \times 1\). So, the deciphered vector will be:
\[
p_m = SK_m \times C_n \mod 256 \quad (22)
\]
After that, reconstruct the original image \(p\) from the values in the deciphered vectors.

VI. SOFTWARE IMPLEMENTATION

MATLAB R2015a (8.5.0.197613) 64-bit software on Intel(R) Core(TM) i5-2410M CPU 2.3 GHz and RAM 4 GB will be used for encryption and decryption processes.

Suppose that user \(U\) wants to send a Image to user \(R\) and they agreed to use \(EC_{y^2 \equiv x^3 + x + 1 \mod 4397}\) and satisfies the condition in eq. (2) \(\neq 0\). The order \(N\) of the elliptic curve \(EC_{y^2 \equiv x^3 + x + 1 \mod 4397}\) is 4273 which is prime number. So, we choose any point from ECG as base point, let us choose \(BP = (3258,3592)\), \(P_x = 1152\) and \(P_y = 2560\).

Then compute the value of \(U_x = (911,3274)\) and \(U_y = (875,1608)\). So the generation of \(SK = (965,2096)\) and comput \(M_1 = (3610,282)\) and \(M_2 = (3213,4152)\).

![Elliptic Curve Points over Prime filed at a=1, b=1 and p=4397](image)

Fig. 1. Elliptic Curve Points over Prime filed at a=1, b=1 and p=4397

Now generate the circulant matrix key:
\[
K_{cm} = \begin{bmatrix}
26 & 26 & 141 & 56 \\
141 & 56 & 26 & 26 \\
26 & 141 & 56 & 26
\end{bmatrix} \mod 256
\]
And The self-invertible circulant matrix key \(SK_m\):
\[
\begin{bmatrix}
26 & 26 & 141 & 56 & -25 & -26 & -141 & -56 \\
141 & 56 & 26 & 26 & -141 & -56 & -141 & -56 \\
26 & 141 & 56 & 26 & -141 & -56 & -141 & -56 \\
26 & 141 & 56 & 26 & -25 & -141 & -56 & -141 \\
26 & 141 & 56 & 26 & -26 & -141 & -56 & -141 \\
26 & 141 & 56 & 26 & -25 & -141 & -56 & -141 \\
26 & 141 & 56 & 26 & -25 & -56 & -26 & -56
\end{bmatrix}
\]

At user \(S\) for encryption, Separate image pixel values into blocks of size \(8 \times 1\)
\[
P_1 = \begin{bmatrix}
156 \\
159 \\
158 \\
155 \\
158 \\
159 \\
156 \\
159
\end{bmatrix}, \quad P_2 = \begin{bmatrix}
157 \\
158 \\
158 \\
159 \\
160 \\
160 \\
160 \\
158
\end{bmatrix}, \quad p_{192} = \begin{bmatrix}
104 \\
103 \\
138 \\
126 \\
117 \\
133 \\
130 \\
113
\end{bmatrix}
\]

Compute \(C_n = SK_m \times p_n \mod 256\)
\[
\begin{bmatrix}
86 & 237 & 206 & 170 & 175 & 206 & 123
\end{bmatrix}, \quad \begin{bmatrix}
122 & 249 & 206 & 175 & 206 & 123
\end{bmatrix}, \quad \begin{bmatrix}
96 & 100 & 120 & 114 & 113 & 113
\end{bmatrix}
\]

Reconstruct the ciphered image \(C\) from the values in the ciphered vectors.
Elliptic Curve Cryptography Modified Hill Cipher Dependent on Circulant Matrix

AT user \( R \) for decryption, Separate cipher image into blocks of size \( 8 \times 1 \)

\[
\begin{bmatrix}
86 & 237 \\
170 & 66 \\
206 & 83 \\
122 & 100 \\
249 & 86 \\
175 & 175 \\
206 & 206 \\
123 & 244
\end{bmatrix}
\]

\[
C_1 = \begin{bmatrix}
122 \\
86 \\
175 \\
206 \\
123
\end{bmatrix}
\]

\[
C_2 = \begin{bmatrix}
249 \\
238 \\
70 \\
81 \\
244
\end{bmatrix}
\]

\[
\ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots 
\]

\[
C_{8192} = \begin{bmatrix}
96 \\
96 \\
100 \\
120 \\
114 \\
113 \\
113 \\
113
\end{bmatrix}
\]

Compute:

\[
p_1 = \text{SK}_m \times C_n \mod 256
\]

\[
\begin{bmatrix}
156 & 157 \\
159 & 158 \\
158 & 158 \\
155 & 159 \\
158 & 160 \\
156 & 160 \\
159 & 160 \\
158 & 113
\end{bmatrix}
\]

\[
p_2 = \begin{bmatrix}
104 \\
103 \\
138 \\
126 \\
117 \\
133 \\
130 \\
113
\end{bmatrix}
\]

Reconstruct the original image \( p \).

VII. SECURITY ANALYSIS

Security analysis of a cryptographic process is an essential process to ensure the strength of cryptographic algorithm. In this section we discuss some analysis of the implemented algorithm.

7.1. Histogram analysis

The histogram is a graph showing the number of pixels in an image at different intensity values found in the image. For a good encryption, the distribution in the encrypted image should be uniform. It is used to show how the algorithm is resistant to statistical attacks.

The original, encrypted and decrypted images. Their corresponding histograms are shown in Fig.3. There is no loss of the image data between the original and the decrypted images. The encrypted image's histograms are almost uniform, the algorithm ensures that the statistical analysis of the encrypted image is almost random.

7.2. Correlation Coefficient analysis

Normal images that we see every day have pixel values which have high correlation with their neighbors. A good cipher image will have a very low correlation to its neighbor pixel value. Correlation coefficient less than 0.1 between the original image and encrypted image is preferable. It is used to show how the algorithm is resistant to frequency attacks [13].

Correlation Coefficient is calculated as:

\[
CC = \frac{\text{cov}(x,y)}{\sigma_x \sigma_y}
\]

\[
\sigma_x = \sqrt{\text{var}(x)} \quad \text{and} \quad \sigma_y = \sqrt{\text{var}(y)}
\]

\[
\text{var}(x) = \frac{1}{N} \sum_{i=1}^{N} (x_i - \bar{E}(x))^2
\]

\[
\text{cov}(x,y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - \bar{E}(x))(y_i - \bar{E}(y))
\]

The correlation coefficient between original and encrypted image is \( CC = 0.0017 \). The correlation coefficient is small enough to state that there is no
correlation between the original and the encrypted images.

7.3. Entropy analysis
Entropy is one of the statistical scalar parameters used for the image encryption evaluation. It shows the most frequency occurring patterns. It depends on the probability of the pixels values and measures the degree of randomness.

The theoretical and ideal entropy value for the grayscale image of size 256×256 is eight, and the encrypted image efficiency is better if the entropy value is closed to eight. And is calculated as:

\[ E = \sum_{x=0}^{255} P(x) \times \log_2 \left( \frac{1}{P(x)} \right) \]  

(27)

At \( P(x) \) is the probability of the pixel value \( x \).

\[ P(x) = \frac{\text{frequency of the pixel value } x}{\text{Total number of the image pixels}} \]  

(28)

The entropy value is \( E = 7.9957 \). It very closed to 8.

7.4. Perceptual Security Analysis
Perceptual Security means that, the encrypted data are completely unintelligible, and it is hard for an attacker to retrieve any significant information about the original data. Peak Signal to Noise Ratio (PSNR) is an availability measurement of whether a significant original image data is embedded in the encrypted image data.

PSNR was calculated for the encrypted image that is shown in using MATLAB and it was \( \text{PSNR} = 8.3997 \text{ dB} \), which reflects that the encrypted data is not like the original data, so it is very unintelligible to an unauthorized user. It is so difficult for an attacker to retrieve the original image data.

7.5. (NPCR) and (UACI) analysis
The Number of Pixels Change Rate and The Unified Average Changing Intensity are designed to test the number of changing pixels and the number of averaged changed intensity, respectively, between ciphered and original image.

The two tests are used to show how the algorithm is resistant to differential attacks. if NPCR value is closed to 100% and if UACI value is very closed to 33.46% the algorithm is resistant to differential attacks.

NPCR is calculated as:

\[ \text{NPCR} = \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times \frac{100}{M \times N} \]  

(29)

\[ \text{where} \quad D(i,j) = \begin{cases} 0, & \text{if } i = j \\ 1, & \text{if } i \neq j \end{cases} \]

UACI is calculated as:

\[ \text{UACI} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|D(i,j)-C(i,j)|}{255} \]  

(30)

By Calculation of \( \text{NPCR} = 99.4431\% \) is very close to 100%

\( \text{UACI} = 31.1278\% \) is close to 33.46%. So, the algorithm is resistant to differential attacks.

A comparison between the proposed technique and other technique for cameraman grayscale image is shown in Table 1. The Entropy in the proposed technique is higher than the other technique and it is nearest to the theoretical value eight when \( E=7.9957 \). PSNR and UACI values in the proposed technique are also better than other technique at 8.3007 and 31.1278 respectively. from Table 1 we can conclude that the proposed technique is more efficient than the other technique

<table>
<thead>
<tr>
<th>The Method</th>
<th>Cameraman Image (256×256)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Entropy</td>
</tr>
<tr>
<td>ECCMHC</td>
<td>7.9957</td>
</tr>
<tr>
<td>ECCCHC [12]</td>
<td>7.9848</td>
</tr>
<tr>
<td>ECC Koblitz Encoding</td>
<td>6.5223</td>
</tr>
</tbody>
</table>

Table 1: Comparison of security analysis between ECCMHC, ECCCHC algorithm and ECC Koblitz encoding algorithm for cameraman image

CONCLUSIONS
In the proposed algorithm, ECCMHC. The experimental results and analyses of the proposed algorithm were very encouraging. This approach yielded a good uniform distribution for Histogram, The Entropy is 7.9957 which near to expected value, The Correlation Coefficient is 0.0017 which is very low correlation and The UACI is 31.1278% close to the ideal value. From the analyses results it is providing a high resistance to any overall attacks and the time consumed in encryption and decryption processes is very little. Consequently, the proposed it provided a highly secure data transmission in any communication session.

REFERENCES
Elliptic Curve Cryptography Modified Hill Cipher Dependent on Circulant Matrix
