Cryptography Based on Elliptic Curve and Special Matrix with Linear System Algorithm

Ameer Hasan Almuqdadi
Department of Mathematics, Faculty of Computer Science and Mathematics.
University of Kufa
Najaf, Iraq
ameerh.almuqdadi@student.uokufa.edu.iq
Orcid.org/0009-0003-5475-2152

Adil AL-Rammahi
Department of Mathematics, Faculty of Computer Science and Mathematics.
University of Kufa
Najaf, Iraq
adilm.hasan@uokufa.edu.iq
Orcid.org/0000-0003-3856-0663

DOI: http://dx.doi.org/10.31642/JoKMC/2018/110113

Received Aug. 14, 2023. Accepted for publication Oct. 9, 2023

***Abstract*—** *Elliptic Curve Cryptosystem, which offers a high level of security with a reduced key size, has emerged as the best option for public key encryption. Elliptic curve cryptosystem has proven to be the best solution for public key encryption, where it provides a good level of security with smaller key size. In this paper, we attempt to develop an enhanced image encryption algorithms based on ECC by use two keys as circulant matrix in one of them, while generation another key from simple linear system modulo to purpose of image cryptography. The results of the suggested algorithm comparison with recent research are used to assess it where results were better than previous works*

Keywords*— *Elliptic curve cryptosystem; circulant matrix; Logical operation XOR; Modulo and Multiplicative Inverses Modulo; Image encryption .

1.INTRODUCTION

Encryption has become more important on the modern Internet for ensuring data safety during transmission across the network. Various encryption techniques are used to prevent unauthorized access to sensitive information [1]. One common method to fortify photo safety is via encryption. It is the fundamental goal of photo encryption to prevent any outside party from being able to see the original image during transmission over a network. The special characteristics of image data, such as large storage capacity, high redundancy, and strong pixel correlation, increase the difficulty of any encryption method [2].

Algebraic structure [3] describes the combination of a set of integers and the methods used for the set's components, both of which are required for cryptography.

Since Roman times, people have employed cryptography, and secret writing, to keep communications private. The use of encryption and decryption to safeguard sensitive data is widespread. Cryptography primarily serves two purposes: encryption and decryption. During encryption, plain text (the original form of the message) is transformed into cipher text, which is unintelligible to humans. During decryption, a cipher text is transformed back into its plaintext form (plaintext). These features ensure that only the intended recipients can access sent communications. [4]- [5].

Two distinct varieties of cryptography exist: symmetric and asymmetric. Since both the sender and the recipient have the same secret key, symmetric cryptography (also known as symmetric key cryptography) ensures secure transmissions. To ensure the confidentiality of messages, asymmetric cryptography [6-7] uses both public and private keys. All references in this article to asymmetric will be underscored.

Protection of sensitive data like e-mail and financial transactions are only two of the many uses for cryptography. Ultimately, it ensures privacy, authenticity, integrity, and irrefutability [8].

For quite some time, mathematicians have been interested in elliptic curves, a particular arithmetic curve [9]. In 1985, Neil Kobletz [10] and Victor S. Miller [11] independently suggested using elliptic curves in cryptography; from 2004 to 2005, curve encryption techniques were widely used. In 2015, various scholars, including Singh [12], who had previously studied this problem, began using photo encryption using elliptic curve cryptography. Elliptic curve cryptography is used to encrypt, decrypt, and digitally sign the cipher picture to guarantee its authenticity and integrity. Ahmed [13] encrypted photos using a chaotic hybrid system and cyclic elliptic curve in 2013.

Using an external secret key of 256 bits and a chaotic system and this unique strategy generates an initial key stream in a feedback fashion. Points on a cyclic elliptic curve are used

to generate key sequences coupled with the key stream. A comprehensive analysis of the security and performance of the proposed encryption method is used to assess its efficacy. In 2015, Nagaraj [14] suggested a new approach of protecting photographs transferred over an unsecured channel by combining elliptic curve cryptography with a magic matrix operation.

Elliptic curve cryptography's main benefit is that it requires less space for storing and sending keys than other methods. In other words, a 256-bit e public key should deliver equal security to a 3072-bit RSA public key, and the elliptic array may provide the same degree of security as an RSA-based system with a greater parameter and proportionally larger key. The security of ECC is tied to how hard it is to solve the discrete logarithm problem for elliptic curves (ECDLP) [15].

We found the inverse of the matrix by using inverse modular to unlock the encryption and supported a linear system to distort the image further. This paper combines the coding by the elliptic curve with the circulant matrix, which will be key to encryption and algebraic operation such as dot product and XOR etc.

2.ELLIPTIC CURVE FUNCTION

elliptic curve cryptography is a kind of public-key encryption (ECC). A pair of keys, called a private key, and a public key and a set of operations for utilizing the keys to accomplish cryptographic tasks are shared between the sender and the receiver in public key cryptography. [16].

An elliptic curve E over a prime field is defined as follows:

$$E_P(a, b): y^2 = x^3 + ax + b \ modp,$$

This type of equation is called a Weierstrass equation.

where $p>3$, $a, b \in F$ are constants satisfy the condition:

$$4a^3 + 27b^2 modp \not\equiv 0.$$

This the condition ensures that the curve non-singular and does not contain any bend or intersect itself.

An elliptic curve is an abelian variety – that is, it has a group rule defined algebraically, with keeping to which it is an abelian group with O serves as the identity element.

The elliptic curve group (**Ep**) includes all points locations

(x, y) that fulfill the elliptic curve $E_P(a.b)$ and the infinity point. O_∞ [17, 18].

2.2ELLIPTIC CURVE OPERATIONS:

The elliptic curve scalar multiplication is the most time-consuming elliptic curve operation, both for

encrypting and decrypting, and it is also the most fundamental operation related to the elliptic curve's function. Point addition and point doubling are the two steps needed for scalar multiplication on an elliptic curve [19].

2.2.1. Point addition:

Let $p_1=(x_1, y_1)$ and $p_2=(x_2, y_2)$, where $p_1 \neq p_2$, are two points lie on an elliptic curve E_P (a,b). Adding the two points p_1 and p_2 giving a third point

$p_3=(x_3, y_3)$, as $x_3 \equiv (s^2 - x_1 - x_2) modp$,

$y_3 \equiv (s(x_1 - x_3) - y_1) modp$,

Where $s = \frac{y_2 - y_1}{x_2 - x_1} modp.$

(If $x_1 = x_2$ but $y_2 \neq y_2$, and $p_1, p_2 \neq \infty$ Then the line through p_1 and p_2 is a vertical line and therefore intersects E_P at ∞. Then reflecting across the x-axis gives ∞. Thus $p_1 + p_2 = \infty$).

p_3 should lie on the same curve E_P (a,b)[20].

2.2.2. Point doubling: Suppose $p_1=(x_1, y_1)$ is a point on an elliptic curve E_P (a,b), the point $R=2P=(x_1, y_1)$ that results from doubling the point P as:

$x_2 \equiv (s^2 - 2x_1) modp$, $y_3 \equiv (s(x_1 - x_2) - y_1) modp$

and $s = \frac{3x_1^2 + a}{2y_1} modp.$

(If $y_1 = 0$, the line undefined slope and is therefore vertical. Then $P1 + P2 = \infty$).

$R$is also point on an elliptic curve E_P (a,b)[20].

2.2.3. Elliptic curve scalar multiplication:

Let P represent a point on the elliptic curve a. Given a point P on a curve, we can get a second point Q by multiplying k by P, as follows:

KP = P + P + P + … + P for some scalar (integer) K and a point P = (x, y) that lies on the curve.

3.CIRCULANT MATRIX

Circular matrix is a square matrix with-i row elements for $i = 1.2.\cdots.p$ obtained by shifting the elements in the first row to the right by $i - 1$ steps[21].

The general form is:

let vector of any numbers v =$[c_0, c_1, c_2, \ldots, c_n, c_{n-1}]$ then

M([v])=c($[c_0, c_1, c_2, \ldots, c_n, c_{n-1}]$) =

$$\begin{bmatrix} c_0 & c_1 & c_2 & & \cdots & c_{n-1} \\ c_{n-1} & c_0 & c_1 & c_2 & & \vdots \\ & c_{n-1} & c_0 & c_1 & \ddots & \\ \vdots & \ddots & \ddots & \ddots & & c_2 \\ & & & & & c_1 \\ c_1 & \ldots & & c_{n-1} & & c_0 \end{bmatrix}$$

A circulant matrix C is one in which each row represents a cyclic shift of the row above it (generated by the first row). The matrix C is a unique kind of Toeplitz matrix [22].

Circulant matrix included with encryption; we will attempt to utilize this matrix to encrypt photos with a high degree of security [23].

Example (1):

Let v= [1,2,3,4,5,6] then the circulant matrix is

$$M([v])=c([1,2,3,4,5,6])=\begin{bmatrix}1&2&3&4&5&6\\6&1&2&3&4&5\\5&6&1&2&3&4\\4&5&6&1&2&3\\3&4&5&6&1&2\\2&3&4&5&6&1\end{bmatrix}.$$

4.LOGICAL OPERATION XOR

XOR is a commonly used logical operation in cryptography that compares two input bits to create a single output bit based on the comparison results. The logic is simple. If all the bits are the same, the result is 0. A result of 1 is produced if the bits are unique [24]. The capacity to do logical OR operations makes XOR useful in encryption. All four possible permutations of plaintext and key bits are detailed below. It seems to reason that encryption can't be cracked if the key or plaintext is unknown. [25].

Example (2):

Let x: 0101 1100 and y: 1001 1000

Then

0101 1100 XOR 1001 1000 = 1100 0100

5.MODULO

Let n be a positive integer . let a and b are two integers. Then a and b are called congruent modulo n , denoted by $a \equiv b \mod n$ if n divides $(a-b)$; that mean , $ab = kn$ for some integer k. $a \not\equiv b \mod n$ if n is not divides $(a-b)$, then a and b are not congruent modulo n [26].

Let n be a positive integer and let a be integer such that $\gcd(a.n) = 1$. If $x^2 = a \, mod \, n$ has a solution (solvable), then a is call quadratic residue of modulo n. Otherwise, it is quadratic nonresidue of module n[26].

6.MULTIPLICATIVE INVERSES MODULO

There exists a multiplicative inverse modulo n for any positive integer a lower than n that is relatively prime ton. The Euclidean algorithm produced this outcome. In the next example, we'll see why this must be the case. The multiplicative inverse modulo n does not exist for any positive integer a lower than n and not relatively prime such that (gcd (a, n) = 1) to n [27].

Integer a module n has an inverse in modular multiplicative x such that

$$a\text{^} - 1 \equiv x \ (mod \ n)$$

Then the inverse

$$a\text{^}1 \ x \ \equiv 1 \ (mod \ n)$$

7.MATERIALS AND METHODS

7.1. Proposed Algorithms

let's pretend that User A wants to transfer plaintext to User B through an insecure channel using this method. Ep (a, b) is the elliptic curve they agree on, and they must also agree on the domain parameters a, b, p, α,G, where G is the generating point. Then, both User A and User B must independently choose a private key from the range [1, p -1], and generate their respective public keys as $P_A = N_A$.G and $P_B = N_B$.G (N_B and N_B private key $\in$[1, p -1]). The starting key is calculated by multiplying each user's private key by the corresponding public key as:

$$O = N_A \cdot P_B = N_B \cdot P_A = N_A \cdot N_B \cdot G = (x, y)$$

then calculates

$$K_1 = x.\ G = (K_{11}, K_{12}) \ ; \ x \in O$$

$$K_2 = y.\ G = (K_{21}, K_{22}) \ ; \ y \in O$$

Next, the transmitter and receiver will each use a circulant matrix to generate a secret key matrix.

The secret key matrix has an inverse, which may be found by utilizing multiplicative inverses modulo to get the user B secret key.

There will be four-pixel-wide sections throughout the picture. Therefore, both sides generate the key matrix K_{E1}, where K_{E1} be a circulant matrix split into four square matrices.

K_{11}, K_{12}, K_{21} and K_{22}. So, we can rewrite K_{E1} as:

$$K_{E1} = \begin{bmatrix}K_{11}&K_{12}&K_{21}&K_{22}\\K_{22}&K_{11}&K_{12}&K_{21}\\K_{21}&K_{22}&K_{11}&K_{12}\\K_{12}&K_{21}&K_{22}&K_{11}\end{bmatrix}.$$

And generating the second secret key by linear systems as:

$$k_1 = ax_0 + by_0$$

$$k_2 = \alpha y_0$$

Where ($0 < \alpha < 1$) and a, b,x_0,y_0 $\in$N (integer number)

$$K_{E2} = \begin{bmatrix} k_1 \\ k_2 \end{bmatrix}.$$

Choosing the sender two pixel $(v_1 . v_2)$ from cipher image respectively and putting it in square matrix as:

H=$\begin{bmatrix} 1 & v_{1.} \\ v_{2.} & 1 \end{bmatrix}$, the receiver here does not need to calculate the inverse of the key that will be explained later.

7.1.1. Encryption of First case:

In this case, divide the picture pixel values into four-pixel blocks, with each block having the same size circulant matrix: b_1, b_2 , b_3,…. and we change any pixel equal to 0 by 256.

The next step is to calculate cipher matrix by using dot product operation $(*)$ such that

$C_i = K_{E1} * b_i$ mod (256+1) for all i=1,2,3,….

We have C_1, C_2 , C_3,…. ciphered matrix and using 257 to avoid having a zero value.

The last phase of the encryption procedure is reconstructing the ciphered picture from the values of Ci and transmitting it to party B.

7.1.2. Decryption processes of first case:

party B, will calculate inverse of (K_{E1}) and the ciphered image pixel values will separate into blocks of 4×4: C_1, C_2 , C_3,…. and replace any 256 by 0

The next step is computing b_1, b_2 , b_3,…. by

B_i= K_{E1}^{-1}.* C_i mod (256+1) for all i=1,2,3,….

The last stage of the decryption process consists of reconstructing the plain picture from the values of b_i $where$ i=1,2,3,… & replace every 256 by 0

7.1.3. Encryption of second case:

After the last phase of the encryption procedure in the first scenario, using the second key by separating the cipher tax picture pixels into pixel pairs (v_1, v_2) and placing in the matrix.

Such as $T_{i=}\begin{bmatrix} 1 & v_1 \\ v_2 & 1 \end{bmatrix} \cdot \begin{bmatrix} K_1 \\ K_2 \end{bmatrix}$

Next step calculate RQ_i =mod (V_i,Max) and

NL_i =(T_i- RQ)/Max

Then XOR operate between RQ_i and NL_i ,last step send cipher tax RV_i and ciphered matrix to the other party B.

7.1.4. Decryption processes of second case:

using the XOR between RQ_i and U_i then next step calculate H_i b y

$$H_i = NL_i \cdot Max + RQ_i$$

The last step computing V_i as:

v_1 =(h_{11}-k_1)/ k_2 , v_2 =(h_{12}-k_2)/ k_1

Then repeat all previous steps in first case.

8.MATERIALS AND METHODS FOR IMPLEMENTING THE PROPOSED ALGORITHMS

Assume that the transmitter (Bob) wishes to communicate the recipient (Alice) encrypted text and a "image" using the suggested technique. They will have agreed to utilize an elliptic curve and choose any prim number and two numbers a and b, such that the requirement is satisfied

$$a^3 + 27b^2 \bmod p \neq 0$$

Let, a=1, b=3 and p=37 and α=1/3

where $1^3 + 27(3)^2$ mod p =247 mod 37=25≠0 and

E_{37}(1,3): y^2=x^2+x+3 mod 37,

The points that satisfying E_{37} (1,3) are: (0,15), (0,22), (3,12), (3,25), (4,16), (4,21), (6,15), (6,22), (9,1), (9,36), (12,2), (12,35), (13,17), (13,20), (15,10), (15,27), (17,7), (17,30), (18,9), (18,28), (19,6), (19,31),(26,17), (26,20), (29,1), (29,36), (31,15), (31,22), (32,13), (32,24), (33,3), (33,34), (34,11), (34,26), (35,17), (35,20), (36,1) and (36,36). So # E37(1,3) =39. So, if we choose G= (0,15), the domain parameters for E37(1,3) are

{a ,b, α,P,G,}={1,3,1/3,37,(0,15)}.

Step 1: "Generating of keys"

–Bob choose the private key N_A = 11 ∈ [1,36]

– He computes the public key

P_A = $N_A \cdot G$ = 11(0,15) = (3,25)

– He computes the

$K = N_A . P_A$ = 11(26,20) = (26,17) = (x, y)

– He computes $K_1 = x. G$ = 26(0,15) = (26,17) = (K_{11}, K_{12}) and

$K_2 = y. G$ = 17(0,15) = (19,31) = (K_{21}, K_{22})

– He constructs K = [K_{11}, K_{11}, K_{11}, K_{11}] = [26, 17, 19, 31] by using a Circulant matrix, then the key is:

$$K_{E1} = \begin{bmatrix} 26 & 17 & 19 & 31 \\ 31 & 26 & 17 & 19 \\ 19 & 31 & 26 & 17 \\ 17 & 19 & 31 & 26 \end{bmatrix}$$

– He computes the second key by a small linear system

$k_1 = ax_0 + by_0$=1(0) +3(15) =45

And $k_2 = \alpha y_0$=1/3(15)=5

$$K_{E2} = \begin{bmatrix} 45 \\ 5 \end{bmatrix}$$

Remark (1): replace any value equal to 0 by 256 in the second key.

On the other side:

– Party (Alice) Chooses the private key $N_B = 13 \in [1,36]$

– He computes the public key $P_B = N_B . G = 13(0,15) = (26,20)$

– He computes $K = N_B . P_A = 13(3,25) = (26,17) = (x, y)$

– He computes $K_1 = x . G = 26(0,15) = (26,17) = (K_{11}, K_{12})$

and $K_2 = y . G = 17(0,15) = (19,31) = (K_{21}, K_{22})$

– He computes inverse key of K_{E1}

$$K_{E1}{}^{-1} = \begin{bmatrix} 89 & 121 & 230 & 199 \\ 199 & 89 & 121 & 230 \\ 230 & 199 & 89 & 121 \\ 121 & 230 & 199 & 89 \end{bmatrix}$$

– He computes the inverse of the second key K_{E2} by using two equations:

$h_i = nv_i \cdot * m + rv_i .$

$v_{11} = (h_{11} - k_1)/ k_2$, $v_{12} = (h_{12} - k_2)/ k_1$.

Remark (2): used for encryption and decryption processes MATLAB R2014a, 64-bit software

Step 2: Encryption of first case:

-He will cut the image into parts the same size 4×4 as kay "K_{E1}"

Let cipher image

IM=

$$\begin{bmatrix} 112 & 225 & 227 & 200 & 220 & 222 & 142 & 199 & \dots \\ 200 & 117 & 190 & 190 & 186 & 223 & 139 & 210 & \cdots \\ 213 & 165 & 175 & 145 & 179 & 111 & 175 & 156 & \cdots \\ 209 & 148 & 215 & 122 & 166 & 147 & 207 & 187 & \cdots \\ 225 & 110 & 148 & 240 & 142 & 197 & 209 & 188 & \cdots \\ 114 & 118 & 196 & 165 & 149 & 250 & 253 & 226 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{bmatrix}$$

Change any values equal to 0 in the cipher image by 256

So,

$$b_1 = \begin{bmatrix} 112 & 225 & 227 & 200 \\ 200 & 117 & 190 & 190 \\ 213 & 165 & 175 & 145 \\ 209 & 148 & 215 & 122 \end{bmatrix},$$

$$b_2 = \begin{bmatrix} 220 & 222 & 142 & 199 \\ 186 & 223 & 139 & 210 \\ 179 & 111 & 175 & 156 \\ 166 & 147 & 207 & 187 \end{bmatrix},\dots\dots..$$

- He computes the values of C_1, C_2 , … by using dot product (*) as:

$C_1 = K_{E1} * b_1 =$

$$\begin{bmatrix} 26 & 17 & 19 & 31 \\ 31 & 26 & 17 & 19 \\ 19 & 31 & 26 & 17 \\ 17 & 19 & 31 & 26 \end{bmatrix} * \begin{bmatrix} 112 & 225 & 227 & 200 \\ 200 & 117 & 190 & 190 \\ 213 & 165 & 175 & 145 \\ 209 & 148 & 215 & 122 \end{bmatrix} mod\ 257 =$$

$$C_1 = \begin{bmatrix} 85 & 227 & 201 & 32 \\ 32 & 215 & 146 & 12 \\ 192 & 232 & 181 & 152 \\ 212 & 242 & 240 & 88 \end{bmatrix}$$

$C_2 = K_{E1} * b_1 =$

$$\begin{bmatrix} 26 & 17 & 19 & 31 \\ 31 & 26 & 17 & 19 \\ 19 & 31 & 26 & 17 \\ 17 & 19 & 31 & 26 \end{bmatrix} * \begin{bmatrix} 220 & 222 & 142 & 199 \\ 186 & 223 & 139 & 210 \\ 179 & 111 & 175 & 156 \\ 166 & 147 & 207 & 187 \end{bmatrix} mod\ 257 =$$

$$C_2 = \begin{bmatrix} 66 & 176 & 128 & 1 \\ 112 & 144 & 50 & 135 \\ 60 & 100 & 181 & 82 \\ 252 & 223 & 249 & 236 \end{bmatrix}$$

Change any values equal 256 in the cipher image to 0

2- The plain image was reconstructed from the values of Ci as:

$EncIm1 =$

$$\begin{bmatrix} 85 & 227 & 201 & 32 & 66 & 176 & 128 & 1 & \dots \\ 32 & 215 & 146 & 12 & 193 & 144 & 50 & 135 & \cdots \\ 192 & 232 & 181 & 152 & 60 & 100 & 181 & 82 & \cdots \\ 212 & 242 & 240 & 88 & 204 & 186 & 249 & 236 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{bmatrix}$$

3-He sends it to the receiver (Alice).

Step 3: Decryption of first case:

1- The pixel values of the ciphered image were separated into blocks of size 4×4 as:

$$C_1 = \begin{bmatrix} 85 & 227 & 201 & 32 \\ 32 & 215 & 146 & 12 \\ 192 & 232 & 181 & 152 \\ 212 & 242 & 240 & 88 \end{bmatrix},$$

$$C_2 = \begin{bmatrix} 66 & 176 & 128 & 1 \\ 193 & 144 & 50 & 135 \\ 60 & 100 & 181 & 82 \\ 204 & 186 & 249 & 236 \end{bmatrix},\ldots\ldots$$

$$b_1 = {K_{E1}}^{-1} * C_1 = \begin{bmatrix} 89 & 121 & 230 & 199 \\ 199 & 89 & 121 & 230 \\ 230 & 199 & 89 & 121 \\ 121 & 230 & 199 & 89 \end{bmatrix} * \begin{bmatrix} 85 & 227 & 201 & 32 \\ 32 & 215 & 146 & 12 \\ 192 & 232 & 181 & 152 \\ 212 & 242 & 240 & 88 \end{bmatrix} mod\ 257=$$

$$b_1 = \begin{bmatrix} 112 & 225 & 227 & 200 \\ 200 & 117 & 190 & 190 \\ 213 & 165 & 175 & 145 \\ 209 & 148 & 215 & 122 \end{bmatrix}.$$

$$b_2 = {K_{E1}}^{-1} * C_2 = \begin{bmatrix} 89 & 121 & 230 & 199 \\ 199 & 89 & 121 & 230 \\ 230 & 199 & 89 & 121 \\ 121 & 230 & 199 & 89 \end{bmatrix} * \begin{bmatrix} 66 & 176 & 128 & 1 \\ 193 & 144 & 50 & 135 \\ 60 & 100 & 181 & 82 \\ 204 & 186 & 249 & 236 \end{bmatrix} mod\ 257=$$

$$b_2 = \begin{bmatrix} 220 & 222 & 142 & 199 \\ 186 & 223 & 139 & 210 \\ 179 & 111 & 175 & 156 \\ 166 & 147 & 207 & 187 \end{bmatrix}.$$

2- The plain image was reconstructed from the values of B_i as:

IM

$$= \begin{bmatrix} 112 & 225 & 227 & 200 & 220 & 222 & 142 & 199 & \ldots \\ 200 & 117 & 190 & 190 & 186 & 223 & 139 & 210 & \cdots \\ 213 & 165 & 175 & 145 & 179 & 111 & 175 & 156 & \cdots \\ 209 & 148 & 215 & 122 & 166 & 147 & 207 & 187 & \cdots \\ 225 & 110 & 148 & 240 & 142 & 197 & 209 & 188 & \cdots \\ 114 & 118 & 196 & 165 & 149 & 250 & 253 & 226 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \end{bmatrix}$$

Step 4: Encryption of second case:

After the second stage in encryption of first case, the second case of the proposed method will use a second key and repeat the preceding steps:

a- The pixel values of the ciphered image were divided into pairs of pixels and constructs as:

$$V_{2i} = \begin{bmatrix} 1 & v_1 \\ v_2 & 1 \end{bmatrix} = V_{21} = \begin{bmatrix} 1 & 85 \\ 32 & 1 \end{bmatrix}, V_{22} = \begin{bmatrix} 1 & 192 \\ 212 & 1 \end{bmatrix}, \ldots\ldots$$

b-He computes the values $T_1\ T_2, T_3$,…..as: $T_i = V_{i2} \cdot K_{E2}$

$$T_1 = V_{12} \cdot K_{E2} = \begin{bmatrix} 1 & 85 \\ 32 & 1 \end{bmatrix} \cdot \begin{bmatrix} 45 \\ 5 \end{bmatrix} = \begin{bmatrix} 470 \\ 1445 \end{bmatrix}$$

$$T_2 = V_{22} \cdot K_{E2} = \begin{bmatrix} 1 & 192 \\ 212 & 1 \end{bmatrix} \cdot \begin{bmatrix} 45 \\ 5 \end{bmatrix} = \begin{bmatrix} 1005 \\ 9545 \end{bmatrix}$$

$\vdots$

$\vdots$

c- He computes the RQ_i =mod (Ti,M)

$$rq_1 = \begin{bmatrix} 214 \\ 165 \end{bmatrix}, rq_2 = \begin{bmatrix} 237 \\ 73 \end{bmatrix},\ldots\ldots$$

d- He reconstructs all the rc

f- He computes the $NL_i = (\ Ti - RQ_i)$./M

$$NL_1 = (\ T_1 - RQ_1)\ ./\text{M} = \left(\begin{bmatrix} 470 \\ 1445 \end{bmatrix} - \begin{bmatrix} 214 \\ 165 \end{bmatrix}\right)./256 = \begin{bmatrix} 1 \\ 5 \end{bmatrix}$$

$$NL_2 = (\ T_2 - RQ_2)\ ./\text{M} = \left(\begin{bmatrix} 1005 \\ 9545 \end{bmatrix} - \begin{bmatrix} 237 \\ 73 \end{bmatrix}\right)./256 = \begin{bmatrix} 3 \\ 37 \end{bmatrix}$$

$\vdots$

$\vdots$

Then use XOR operation between NL_i and RQ_i ,

$U_1 = \begin{bmatrix} 215 \\ 160 \end{bmatrix}, U_2 = \begin{bmatrix} 238 \\ 108 \end{bmatrix},\ldots\ldots$

g- the cipher image was reconstructed from the values of U_i

last step send cipher image and RQ_i to the other party B.

Step 5: Decryption processes of second case:

using the XOR operation between cipher images U_i and RQ_i to find NL_i .

next step he calculates $H_i = NL_i * \text{M} + RQ_i$

$$h_1 = nl_1 * m + rq_1 = \begin{bmatrix} 1 \\ 5 \end{bmatrix} * 256 + \begin{bmatrix} 214 \\ 165 \end{bmatrix} = \begin{bmatrix} 470 \\ 1445 \end{bmatrix}$$

$$h_2 = nl_2 * m + rq_2 = \begin{bmatrix} 3 \\ 37 \end{bmatrix} * 256 + \begin{bmatrix} 237 \\ 73 \end{bmatrix} = \begin{bmatrix} 1005 \\ 9545 \end{bmatrix}$$

⋮

⋮

he calculate c_{ij} where c_{11} =(h_{11}-k_1)/ k_2 and c_{12} =(h_{12}-k_2)/ k_1

c_{11} =(470-45)/ 5 = 85, c_{12} =(1445-5)/ 45 = 32

c_{21} =(1005-45)/ 5 = 192, c_{22} =(9545-5)/ 45 = 212

then repeat all previous steps in first case to find B_i.

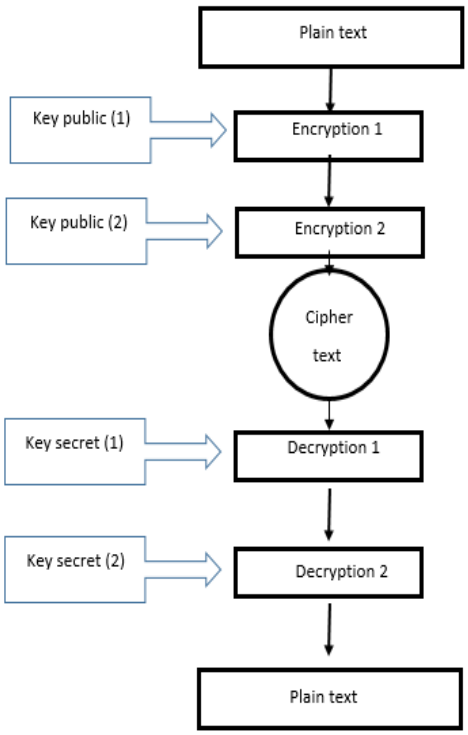
$$b_1 = {K_{E1}}^{-1} * C_1 = \begin{bmatrix} 89 & 121 & 230 & 199 \\ 199 & 89 & 121 & 230 \\ 230 & 199 & 89 & 121 \\ 121 & 230 & 199 & 89 \end{bmatrix}. \begin{bmatrix} 85 & 227 & 201 & 32 \\ 32 & 215 & 146 & 12 \\ 192 & 232 & 181 & 152 \\ 212 & 242 & 240 & 88 \end{bmatrix} mod\ 257=$$

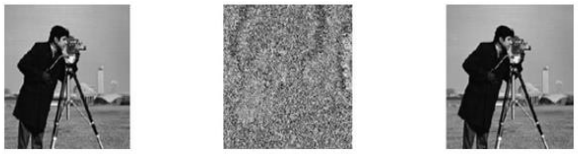
$$b_1 = \begin{bmatrix} 112 & 225 & 227 & 200 \\ 200 & 117 & 190 & 190 \\ 213 & 165 & 175 & 145 \\ 209 & 148 & 215 & 122 \end{bmatrix}.$$

$$b_2 = {K_{E1}}^{-1} * C_2 = \begin{bmatrix} 89 & 121 & 230 & 199 \\ 199 & 89 & 121 & 230 \\ 230 & 199 & 89 & 121 \\ 121 & 230 & 199 & 89 \end{bmatrix}. \begin{bmatrix} 66 & 176 & 128 & 1 \\ 193 & 144 & 50 & 135 \\ 60 & 100 & 181 & 82 \\ 204 & 186 & 249 & 236 \end{bmatrix} mod\ 257=$$

$$b_2 = \begin{bmatrix} 220 & 222 & 142 & 199 \\ 186 & 223 & 139 & 210 \\ 179 & 111 & 175 & 156 \\ 166 & 147 & 207 & 187 \end{bmatrix}.$$

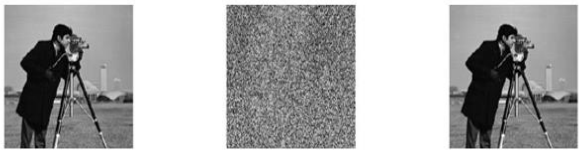
2- The plain image was restructured from the B_i values.





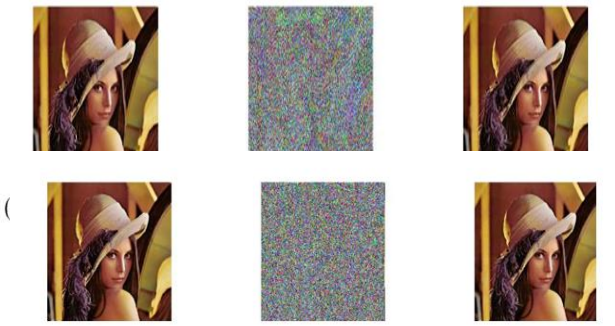
(a) Plain Imaged (b) Encrypted Image (c) Decrypted Image

Figure (2): use one keys on grayscale image



(a) Plain Imaged (b) Encrypted Image (c) Decrypted Image

Figure (3): use two keys on grayscale image.



(a) Plain Imaged (b) Encrypted Image (c)Decrypted Image

Figure (4): use one keys on color image.

Figure (5): use two keys on color image.

9. SECURITY ANALYSIS

for display the efficacy of the suggested algorithms by using the findings of a well-known encryption standard and displaying them in tables. To compare the impact of image enhancement algorithms on picture quality, it is required

constructing quantitative/empirical metrics. Several image enhancement algorithms may be systematically evaluated using the same collection of test photographs to determine which delivers superior results. If we can demonstrate that an algorithm or group of algorithms can restore a degraded version of a known picture such that it more closely resembles the original, then we may infer more correctly that it is a superior method.

9.1. NPCR and UACI Analysis

The two most important parameters for determining the strength of encryption techniques are the unified average changing intensity (UACI) and the number of pixels that change at a certain rate per second (NPCR). NPCR and UACI were introduced in 2004 [27, 28] by Yaobin Mao and Guanrong Chen. NPCR and UACI have now become two widely-used security evaluations for differential attacks in image encryption [[29]. NPCR is the measurement of the absolute number of pixels that change every second, while UACI calculates the average difference in color intensity between two photos when the change in one image is minor. NPCR and UACI values may be calculated using Equations (1) and (2).

$$NPCR = \frac{\sum D}{M \times N} \times 100\% \qquad (1)$$

D denotes the array bipolar, $D\,(i,j) = 0\ if\ X\,(i,j) = Y\,(i,j).otherwise\ D\,(i,j) = 1.$

$$UACI = \frac{1}{M \times N}\left[\frac{\sum |X-Y|}{255}\right] \times 100\% \qquad (2)$$

UACI is one of the differential studies used to measure the strength of image encryption, where the contrast between the encrypted and unencrypted picture is evaluated. The greatest UACI score (about 33.46%) indicates that the suggested approach is secure against diverse attacks. [28]

9.2. Correlation and PSNR Analysis

The correlation between neighboring encrypted picture pixels should be as minimal as feasible. To measure the correlation between pixels in a cipher picture, neighboring pixel pairs are selected randomly. The correlation coefficient is determined using an equation (3)

$$COR \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\left(X(i,j)-\overline{X(i,j)}\right)\left(Y(i,j)-E(Y)\right)}{\left[\sum_{i=1}^{N}\sum_{j=1}^{M}\left(X(i,j)-E(X)\right)^2 \sum_{i=1}^{N}\sum_{j=1}^{M}\left(Y(i,j)-E(Y)\right)^2\right]^{\frac{1}{2}}} \quad (3)$$

$$E(X) = \frac{1}{N \times M}\sum_{1}^{N}\sum_{1}^{M} X(i,j) \text{ and}$$

$$E(Y) = \frac{1}{N \times M}\sum_{1}^{N}\sum_{1}^{M} Y(i,j)$$

Where E(X) and E(Y) are the mean values of the elements $X(i,j)$ and $Y(i,j)$

Peak signal-to-noise ratio (PSNR) It measures the ciphered picture's accessibility based on whether or not crucial, unique image information has been installed [17]. It is defined by calculating the mean squared error (MSE) [27]. The PSNR equation is as follows:

$$PSNR = 10\log_{10}\frac{(255 \cdot 255)}{MSE} \qquad (4)$$

where

$$MSE = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\left(x(i,j) - y(i,j)\right)^2}{M \times N} \qquad (5)$$

$x(i\ ,j)$ and $y(i\ ,j)$ are the values of the pixels in the plain picture and the encrypted image.

TABLE (1): The analysis of our algorithm's accuracy in relation to worldwide standards.

Name photo	Measures	First case	Second case
Cameramen	COR	0.0355	0.0490
	NPCR	100	99.8199
	PSNR	8.1000	8.2500
	UACI	31.9877	31.3339
Lena	COR	0.0200	0.0690
	NPCR	99.4270	99.5370
	PSNR	7.5100	7.3100
	UACI	34.2382	35.2847
Baboon	COR	5.0000	0.0192
	NPCR	99.4569	99.7646
	PSNR	8.7800	8.8200
	UACI	29.8133	29.5633
Peppers	COR	0.0380	0.0181
	NPCR	100	99.3883
	PSNR	7.5400	7.7000
	UACI	34.1591	33.6137

TABLE (3): The analysis of another algorithm [20].

	Measures	First case	Second case
Lena	PSNR	9.2996	**9.2549**
	UACI	28.1854	**28.529**
Cameramen	PSNR	9.0097	**8.0926**
	UACI	26.9897	**32.092**
Baboon	PSNR	9.8015	**9.7765**
	UACI	27.0906	**27.188**

10. CONCLUSION

Comparing to the Global RSA cryptosystem (slower in generating keys), ECC offers similar security with a smaller key size and lower mathematical complexity. In this study, two elliptic curve cryptosystem-based picture encryption

algorithms are introduced. The first and second cases for the suggested methods require circulant matrices. Table 1 demonstrates that the suggested techniques for both scenarios on certain 256×256 photos produce excellent results. UACI and PSNR. Using the first and second suggested algorithms, PSNR was calculated for the ciphered picture and plain image, and the results were 8.1000 and 8.2500, respectively. Therefore, it would be challenging for an attacker to obtain the simple image. On the other hand, UACI was calculated for the plain image and ciphered image using the first and second proposed algorithms, and the results were 34.2382 and 35.2847, respectively. This indicates that it is difficult for an aggressor to recover the plain image, and the results were better compared with result another algorithm as table. (3) .

REFERENCES

[1] A Shreef, M., & K Hoomod, H. (2013). Image encryption using lagrange-least squares interpolation. International Journal of Advanced Computer Science and Information Technology (IJACSIT) Vol, 2, 35-55.

[2] John Justin, M., & Manimurugan, S. (2012). A survey on various encryption techniques. International Journal of Soft Computing and Engineering (IJSCE) ISSN, 2231, 2307.

[3] I.M.Alamsyah.(2014)."ALGEBRAICSTRUCTURES INCRYPTOGRAPHY " Algebra Research Group, Faculty of Mathematics and Natural Sciences..

[4] J. S. Chauhan and S. K. Sharma. (2015). "A Comparative Study of Cryptographic Algorithms," Int. J. Innov. Res., 24–28.

[5] Narasimham, C., & Pradhan, J. (2008). Evaluation of performance characteristics of cryptosystem using text files. Journal of Theoretical & Applied Information Technology, 4(1).

[6] Naureen, A., Akram, A., Maqsood, T., Riaz, R., Kim, K. H., & Ahmed, H. F. (2008, May). Performance and security assessment of a PKC based key management scheme for hierarchical sensor networks. In VTC Spring 2008-IEEE Vehicular Technology Conference (pp. 163-167). IEEE.

[7] S. Farah, M. Y. Javed, A. Shamim, and T. Nawaz.(2012) "An experimental study on Performance Evaluation of Asymmetric Encryption Algorithms," Recent advaces Inf. Sci., vol. 8,121–124.

[8] Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1997). Handbook of applied cryptography crc press. Boca Raton.

[9] Jurišic, A., & Menezes, A. (1997). Elliptic curves and cryptography. Dr. Dobb's Journal, 26-36.

[10] Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of computation, 48(177), 203-209.

[11] Miller, V. S. (1985, August). Use of elliptic curves in cryptography. In Conference on the theory and application of cryptographic techniques (pp. 417-426). Berlin, Heidelberg: Springer Berlin Heidelberg.

[12] Abd El-Latif, A. A., & Niu, X. (2013). A hybrid chaotic system and cyclic elliptic curve for image encryption. AEU-International Journal of Electronics and Communications, 67(2), 136-143.

[13] Nagaraj, S., Raju, G. S. V. P., & Rao, K. K. (2015). Image encryption using elliptic curve cryptograhy and matrix. Procedia Computer Science, 48, 276-281.

[14] Koblitz, N., Menezes, A., & Vanstone, S. (2000). The state of elliptic curve cryptography. Designs, codes and cryptography, 19, 173-193.

[15] Analytics, D. P. M. U. C. Computing, Communications and Informatics (ICACCI).

[16] Al Saffar, N. F. H., & Said, M. R. M. (2014). High Performance Methods of Elliptic Curve Scalar Multiplication. International Journal of Computer Application, 108(20), 39-45.

[17] Deb, S., & Haque, M. M. (2019). Elliptic curve and pseudo-inverse matrix based cryptosystem for wireless sensor networks. International Journal of Electrical and Computer Engineering (IJECE), 9(5), 4479-4492.

[18] Faz-Hernández, A., López, J., & Dahab, R. (2019). High-performance implementation of elliptic curve cryptography using vector instructions. ACM Transactions on Mathematical Software (TOMS), 45(3), 1-35.

[19] Faz-Hernández, et al., "High-performance implementation of elliptic curve cryptography using vector instructions," ACM Transactions on Mathematical Software, vol. 45, no. 3, pp. 1-35, 2019.

[20] Obaid, Z. K., & Al Saffar, N. F. H. (2021). Image encryption based on elliptic curve cryptosystem. International Journal of Electrical and Computer Engineering, 11(2), 1293.

[21] Biggs, N. (1993). Algebraic graph theory (No. 67). Cambridge university press.

[22] Gray, R. M. (2000). Toeplitz and circulant matrices: A review, 2002. URL http://ee. stanford. edu/~ gray/toeplitz. pdf.

[23] Arya, M. C., Chandra, N., Joshi, M. C., & Campus, D. S. B. (2018). A coincidence point theorem in partial metric space. Ganita J, 68, 1-6.

[24] L.Michael.(June 2012). "All About XOR". Overload. 2 ((109): 14–19.

[25] Paar, C., & Pelzl, J. (2009). Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media.

[26] D. M. Burton. (2009)."Elementary Number Theory", Seventh Edition, McGraw-Hill.

[27] Chen, G., Mao, Y., & Chui, C. K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals, 21(3), 749-761.

[28] C. X. Zhu, Z. G. Chen, and W. W. Ouyang. (2006)."A new image encryption algorithm based on general Chen's chaotic system," Journal of Central South University (Science and Technology .

[29] Wu, Y., Noonan, J. P., & Agaian, S. (2011). NPCR and UACI randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT), 1(2), 31-38.