An More effective Approach of ECC Encryption Algorithm using DNA Computing

Fatima Amounas
R.O.I Group, Computer Sciences Department, Moulay Ismaïl University, Faculty of Sciences and Technics, Errachidia, Morocco.
E-mail: F_amounas@yahoo.fr

Hassain Sadki
R.O.I Group, Computer Sciences Department, Moulay Ismaïl University, Faculty of Sciences and Technics, Errachidia, Morocco.
E-mail: sadki.hasain@yahoo.fr

Moha Hajar
R.O.I Group, Mathematical Department Moulay Ismaïl University, Faculty of Sciences and Technics Errachidia, Morocco.
E-mail: moha_hajjar@yahoo.fr

***Abstract*—**Now a day's Cryptography is one of the broad areas for researchers. Encryption is most effective way to achieve data security. Cryptographic system entails the study of mathematical techniques of encryption and decryption to solve security problems in communication. Elliptic Curve Cryptography (ECC) is one of the most efficient techniques that are used for this issue. Many researchers have tried to exploit the features of ECC field for security applications. This paper describes an efficient approach based elliptic curve and DNA computing. The security of the scheme is based on Elliptic Curve Discrete Logarithm Problem (ECDLP). Existing DNA based cryptography technique need more computational power and more processing time with larger key sizes to provide higher level of security. The main goal of our construction is to enhance the security of elliptic curve cryptosystem using DNA Computing. Both image and text data are encrypted successfully.

Keywords- *Cryptography,Elliptic Curve, Data Matrix, Deoxyribo Nucleic Acid (DNA).*

*****

I. INTRODUCTION

With the rapid growth of internet, information security in the present era is becoming very important in communication and data storage. Data encryption is an important issue and widely used in recent times to protect the data over internet. One of the mostly used in public key cryptographies is the Elliptic Curve Cryptography (ECC).

Elliptic curve cryptography is emerging as an attractive public-key cryptosystem for limited environments like smart cards. As compared to existing cryptosystems like RSA, it offers equivalent security with smaller key sizes, faster computation and lower power consumption. The performance of elliptic curve cryptosystem heavily depends on an operation called point multiplication [1,2]. The popularity of elliptic curve cryptography is due to the determination that is based on a harder mathematical problem than other cryptosystems. So, the adversaries are not able to attack ECC and solve ECDLP which is infeasible to be solved and has strength security against all kinds of attacks.

In the last years, DNA Cryptography seems to be a promising strategy for fulfilling the current information security needs. Several encryption schemes have been proposed by many researchers based on DNA computing that use biological properties of DNA sequences. For instance, the authors in [3] proposed symmetric key DNA cryptographic which combine the mathematical model of the algorithm with the DNA to define key sequences. In [4], a new asymmetric encryption and signature cryptosystem based on the DNA key features and amino acid coding is proposed. Next, the authors introduced a hybrid encryption scheme using DNA technology in [5]. Furthermore, the authors in [6] describe a novel DNA encoding algorithm. This encoding algorithm is based on a string matrix data structure, for generating the unique DNA sequences used to encode plain text as DNA sequences. Recently, P.Vijayakumar and al. proposed an algorithm hybrid multilevel DNA computing based color code cryptography scheme combined with elliptic curve cryptography in [7]. In this context, we attempt to provide an approach to enhance the security level of ECC cryptosystem using DNA computing. The rest of this paper is organized as follows: we start in section 2 with some basics notions on elliptic curve over finite field F_p and DNA cryptography. Section 3 is devoted to proposed approach. A detailed example is presented that outlines the working procedure of the proposed method in section 4. The performance and the security analysis of the proposed scheme will be discussed in section 5. Finally, the concluding remarks will be in the last section.

II. BACKGROUND INFORMATION

A. *Elliptic Curve cryptography*

Elliptic curve cryptography is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields [8]. ECC can be defined over two types of fields: one is the prime field F_p and the other is the binary field.

An elliptic curve E over a field F_p is defined by the equation of the form:

$$y^2 = x^3 + ax + b \mod p \qquad (1)$$

Where p = prime number for which the elliptic curve is defined a, b satisfy the equation:

$$(4a^3 + 27b^2) \mod p \neq 0 \qquad (2)$$

An elliptic curve E over F_p consists of the answers (x, y) distinct by (1) and (2), along with an supplementary element called Ω. The basic operation in ECC is point multiplication. Point multiplication is achieved by two basic curve operations[9]:

- *Point Addition*, R = P + Q,

$x_R = \alpha^2 - x_P - x_Q \bmod p$ and

$y_R = \alpha(x_P - x_R) - y_P \bmod p$

where

$\alpha = (y_Q - y_P / x_Q - x_P) \bmod p$,

- *Point Doubling*, R = 2P,

$x_R = (\alpha^2 - 2x_P) \bmod p$ and

$y_R = (\alpha(x_P - x_R) - y_P \bmod p$

where

$\alpha = (3x_p^2 + a) / \square\, 2y_p \bmod p$,

B. *DNA Computing*

The DNA cryptography is an emerging field in the area of DNA computing research. Some algorithms that are available in DNA Cryptography have limitations in that they still use modular arithmetic cryptography at their encryption and decryption processes.

- DNA map rules

DNA sequence contains four nucleic acid bases A (Adenine), C (Cytosine), G (Guanine) and T (Thymine), where A, T, C and G are complementary pairs. In the binary system, 0 and 1 are complementary, 00, 11, 10 and 01 also are complementary. If 00, 11, 10 and 01 are encoded with nucleic acid bases A, C, G and T, we can get 4!=24 kinds of encoding schemes. Due to the complementary relation between DNA bases, there are eight kinds of encoding combinations satisfying the principle of complementary base pairing, which are shown in Table 1.

TABLE 1. DNA MAP RULES

	A	T	G	C
R_1	00	11	01	10
R_2	00	11	10	01
R_3	01	10	00	11
R_4	01	10	11	00
R_5	10	01	00	11
R_6	10	01	11	00
R_7	11	00	01	10
R_8	11	00	10	01

III. MAIN RESULT

In this paper, an enhanced elliptic curve cryptosystem based on matrix approach will be proposed, which is divided into two basic parts: The first part of the algorithm deals with the ECC cryptosystem based matrix approach and enhanced using DNA computing. The second part which deals with the code computing based DNA mapping rules. Now, we discuss the algorithms in greater details to explain its working and features.

A. *Code Computing based DNA Encoding*

There are different processes to encode data and different DNA cryptography methodology that are used for secure data transmission like bio-molecular, one-time-pad [10,11,12]. The sender chooses a secure key. Instead of giving DNA map rule directly, secure key is mapped with DNA molecule to provide greater level of security which is not known to the eavesdropper who always tries to retrieve the secret. DNA sequence is generated by combining DNA molecules such as Adenine (A), Thymine (T), Guanine (G) and Cytosine(C) as shown in Table 1. In our case, each character is imbedded into code point that can be converted into data sequence. Then, the data sequence is mapped with DNA nucleotide using the Table 1. Inversely, the DNA sequence can be decoded into a code point. Here, we extend the concept of code computing to DNA nucleotide Code subtraction is the reverse operation of code addition [13]. Furthermore, a new DNA XOR operation is defined here. It can achieve exclusive XOR operation between two DNA sequences. If the DNA encoding rule R_1 is adopted, the code operation can be expressed as shown in Table 2.

TABLE 2. (a) CODE ADDITION OPERATION

-	**A**	**G**	**C**	**T**
A	T	C	G	A
G	A	T	C	G
C	G	A	T	C
T	C	G	A	T

(b) CODE SUBTRACTION OPERATION

+	**A**	**G**	**C**	**T**
A	G	C	T	A
G	C	T	A	G
C	T	A	G	C
T	A	G	C	T

(c) XOR OPERATION OF DNA SEQUENCE

⊕	**A**	**G**	**C**	**T**
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

B. *Key Generation Phase*

In the proposed approach, the domain parameters are (p, E, P, n) where p is the prime number, F_p denoted as field of integers modulo p. E is the elliptic curve over F_p is defined by the equation $y^2 = x^3 + ax + b$ where (a, b) are the real numbers over F_p and satisfy $4a^3 + 27b^2 \neq 0 \bmod p$.

Suppose Alice and Bob are two users wishing to communicate over insecure channel. Let us choose Alice as the sender who wants to encrypt and send a message M to the receiver Bob. Every entity needs to choose a private key. The private keys, n_A and n_B are positive integers chosen randomly from the interval [1, p-1]. The public keys for the users can be generated respectively as follows:

$$P_A = n_A P$$

$$P_B = n_B P$$

C. *Encryption Algorithm*

The proposed cryptosystem consists in the following steps:

Suppose that we have some elliptic curve E defined over a finite field F_p and that E and a point $P \in E$ are publicly known, as is the embedding system $M \rightarrow P_M$; which imbed plain text on an elliptic curve [14]. In our case, the embedding process

 ISSN: 2321-8169
13 – 18

will represent one character Unicode (Amazigh) by a code point. Then, when Alice wants to send a message to Bob, she proceeds thus:

Step 1. Take any sentence as input of algorithm.

Step 2. Imbed the given string into respective code point on elliptic curve and store them into square matrix of n×m.

$$PM = \begin{pmatrix} P_{11} & P_{12} & P_{13} & \dots & P_{1m} \\ P_{21} & P_{22} & P_{23} & \dots & P_{2m} \\ & & \dots & & \\ P_{n1} & P_{n2} & P_{n3} & \dots & P_{nm} \end{pmatrix}$$

Step 3. Choose a random integer k and computes: $K=kP_B$. (k_1, k_2). Then, generate two key matrices as follows:

$$PK_1 = \begin{pmatrix} X_{11} & X_{12} & X_{13} & \dots & X_{1p} \\ X_{21} & X_{22} & X_{23} & \dots & X_{2p} \\ & & \dots & & \\ X_{p1} & X_{p2} & X_{p3} & \dots & X_{pp} \end{pmatrix}$$

$$PK_2 = \begin{pmatrix} Y_{11} & Y_{12} & Y_{13} & \dots & Y_{1p} \\ Y_{21} & Y_{22} & Y_{23} & \dots & Y_{2p} \\ & & \dots & & \\ Y_{p1} & Y_{p2} & Y_{p3} & \dots & Y_{pp} \end{pmatrix}$$

Step 4. Divide the data matrix into sub matrices. Then, encrypt the obtained sub matrices using ECC technique.

Step 5. Choose DNA map rule and encodes the obtained points with the DNA nucleotide.

Step 6. Generate the DNA key matrix. Then, perform DNA XOR operation to produce data matrix B_i.

Step 7. Apply code addition operation of column vectors noted B and K as follow:

$$C_j=B_j + K_j$$

Step 8. Convert the result values into corresponding characters and send the encrypted data to the receiver.

D. Decryption Algorithm

The steps of the decryption algorithm are the reverse of those involved in encryption. The receiver uses the following steps to get the plaintext:

Step 1. Get the received data and convert the data sequence into binary form using the map DNA rule.

Step 2. Extract the secure key and multiply kP by his private key k_B to obtain K and generate a key matrices KP_1 and PK_2.

Step 3. Generate the DNA key matrix and apply code substraction operation as follow:

$$B_j = C_j - K_j$$

Step 4. Perform DNA XOR operation to produce data matrix.

Step 5. Convert the result code into code point and stored into data matrix.

Step 6. Decrypt the obtained points using ECC decryption process.

Step 7. Reverse the embedding to get back the original message.

Figure 1 shows detailed design of encryption/decryption module.

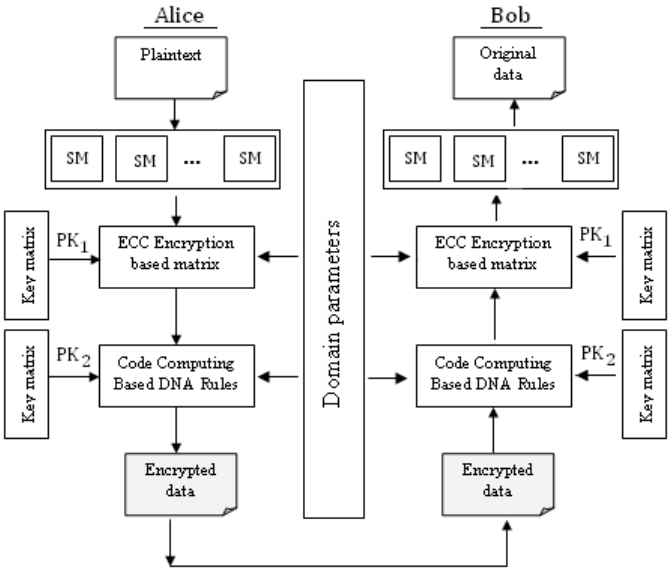

Figure 1. Flowchart of the proposed scheme.

IV. IMPLEMENTATION EXAMPLE

Assume that Alice and Bob are agreed to use the elliptic curve:

$$y^2 = x^3 - x + 188 \bmod 241$$

The following steps are used to find out the points on the elliptic curve $y^2 = x^3 - x + 188 \bmod 241$

Step 1. Compute y^2 mod 241 for y= 0 to 241.

Step 2. For x= 0 to 241, compute $y^2 = (x^3 - x + 188) \bmod 241$.

Step 3. Match the value of y^2 in step 2 with that in step 1.

Step 4. If match is found, then the corresponding x and y becomes a point on an elliptic curve.

Step 5. For any point on an elliptic curve, its inverse will also be present.

The set of points on the elliptic curve $E_{241}(-1,188)$ is shown below in Figure 2.

For the system parameters, we used the following data:
- p and n: two prime numbers (p=241 , n=268).
- E_{241} (-1, 188) an elliptic curve defined on finite field F_{241}.
- P (1, 46): a point on elliptic curve E with order n.
- Key values:
  - Alice's private key: n_A = 19, public key: (23, 102).
  - Bob's private key: n_B = 31, public key: (31, 233).
  - Let k be a random number: k=43 ➔ K=(208,124).
- DNA rules: R_1

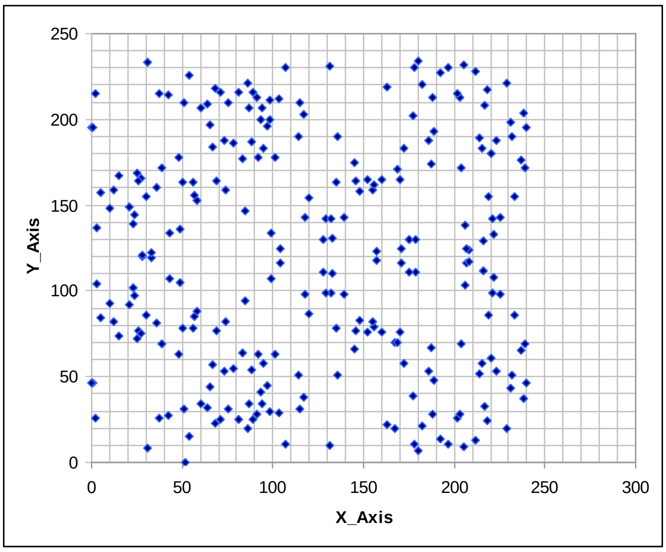

Figure 2. The points on $E_{241}(-1,188)$.

A. Results for Text Encryption and Decryption

Now the encryption-decryption process is illustrated by using the sample data in Amazigh language [14] as below:
"ⵉⴱⴹⴰ ⵓⵙⵍⵎⴰⴷ ⵉⴷⵍⵉⵙⵏ ⵅⴼ ⵉⵍⵎⴰⴷⵏ ⴳ ⵜⵉⵎⵍ".

That means:
"The teacher distributed books to students at the school."

After applying embedding process, we get:

SM1:

(220,180)	(42,27)	(218,24)
(131,231)	(220,180)	(12,159)
(58,153)	(220,180)	(12,159)

SM2:

(152,165)	(93,200)	(220,180)
(131,231)	(58,153)	(131,231)
(58,153)	(98,200)	(145,66)

SM3:

(42,27)	(42,27)	(131,231)
(220,180)	(58,153)	(98,200)
(220,180)	(104,125)	(220,180)

SM4:

(23,102)	(218,24)	(85,94)
(98,200)	(21,149)	(216,112)
(39,69)	(57,85)	(31,233)

Hence we shall assume that K= (208,124) and a secure key matrix generated is given as follows:

PK_1:

(180,7)	(114,190)	(3,137)
(78,186)	(239,69)	(33,119)
(99,107)	(205,9)	(36,160)

Therefore, the encrypted data using ECC technique based matrix approach is given as follows:

SC1:

(239,69)	(217,33)	(60,34)
(221,99)	(50,163)	(216,112)
(49,136)	(88,54)	(23,102)

SC2:

(10,148)	(238,204)	(128,130)
(167,70)	(115,31)	(81,25)
(37,215)	(28,120)	(101,178)

SC3:

(28,120)	(197,230)	(2,215)
(222,133)	(21,149)	(50,163)
(188,20)	(74,159)	(39,69)

SC4:

(48,63)	(206,103)	(27,166)
(21,149)	(155,82)	(5,84)
(180,7)	(197,230)	(10,148)

Next, we encrypt the result matrices with the secure key PK_2:

PK_2:

GAATATCG	GGGCTGTG	ATGCAATT
CGTGGTGC	TACTTGGG	CGCTGGAC
GTGCGCAC	CGACGATG	AATTGACC

Therefore, the encrypted data generated once encoding using DNA rules and applying code addition operation is given below:

AGTTTCCG	GGCTAGTA	AGGCGAAG
CCATAGGC	GGATGCGC	ACTAACGG
TACCTGGA	CTGGATTG	GAATCGCC

GGAGAGCG	CCTTCAAC	TGTCCAGG
ATACCCAT	GTGGACGC	GATCCTCC
GCATGCCT	GTGCCATT	GGCGTGCA

 ISSN: 2321-8169
13 – 18

GGCACTCT	GACCGGAC	GAAGACTA
GCGGATTT	AGTTAACA	CAAAGCTT
GGGCAGGA	AGTCGGGC	AAGGCGTG

ACAGGTCC	GAGAAGGT	TGGTCTGT
AGCTGACT	AGCAGGTA	CAATAACC
ATAACTAC	GGCGATTA	GTGGACGC

After converting the result values to binary form, and embedding into corresponding characters, we get:

“[illegible]”

Now, the result cipher text along with secure key is sent to the receiver.

At the receiving side, the recovery of cipher text is done as follows:

After receiving the cipher text, the receiver extracts the first entry that represents the secret. The second entry represents the encrypted data. Then, reverse the process to retrieve the original message.

B. Results for Image Encryption and Decryption

In this section, we extend the proposed method to encrypt the plain image using Netbeans 7.1 as tool [16]. Our algorithm has been tested using grayscale image. Every image consists of pixels. In grayscale images, each pixel has an 8-bit value of between 0 and 255. To encrypt an image using the proposed approach, each pixel should be mapped to a point on a predefined elliptic curve [17]. Then, the encryption process will be started.

The result obtained from practical implementation of the proposed method on Lena image is shown in the following Figures (Figure 3, Figure 4).

Figure 3. Experimental result of “Lena” image.

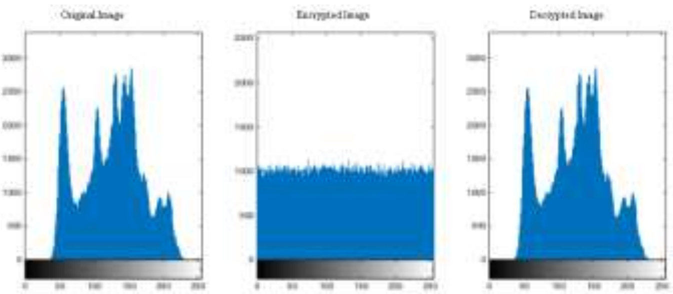

Figure 4. Histogram of the plain image and encrypted Image

Experiments using the proposed method resulted in a significantly different encrypted image and uniform histogram, as shown in the Figure 3 and Figure 4. From the result, it can be easily seen that the proposed scheme encrypts the image so well that nobody can recover the image. Further more, it is obvious that the histogram of cipher-image is uniform and significantly different from the histogram of the original image as shown in Figure 3, hence it does not provide any statistical attacks.

V. RESULT AND DISCUSSION

In this section, security aspects of the proposed approach will be discussed. The proposed approach has large key space that making brute force attack is infeasible. It has DNA and code computing and different combinations of them. So it resists the exhaustive of brute force attacks.

The proposed system is more efficient than the existing DNA cryptography [6] and Elliptic Curve Cryptography [13] in terms of security. Because, it uses elliptic curve cryptography mechanism for encryption and DNA computing in its encoding phase. So, the proposed system has two level of security first one in the encryption phase and the other is in the encoding phase. It would be hardly breakable by eavesdropper as it contains multi level of security.

VI. CONCLUSION

This paper introduces the concept of DNA computing as a promising approach to enhance the security of the elliptic curve cryptosystem. Our proposed approach is the combination of elliptic curve cryptography and DNA computing theory. In addition, the proposed system has multi level security one in ECC encryption steps and other in DNA encoding. The strength of the security is improved by means of elliptic curve discrete logarithm problem where retrieval of key is very difficult in both ECC encryption and decryption algorithm. Furthermore, the advantage of DNA computing is employed in the proposed scheme to enhance the security of system. Finally, we like to point out that the use of DNA computing will provide better performance in this regard.

REFERENCES

[1] Darrel R. Hankerson, A. Menezes and A. Vanstone, “Guide to Elliptic Curve Cryptography”, Springer, 2004.

[2] Ali M. Sagheer, “Elliptic curves cryptographic techniques”, proceeding of the 6th International Conference on Signal Processing and Communication Systems, 2012 IEEE, Gold Coast, Australia, , pp.12-14, 2012.

[3] Sherif T. Amin, Magdy Saeb, Salah El-Gindi "A DNA based Implementation of YAEA Encryption Algorithm," International Conference on Computational Intelligence, San Francisco, No. 20, 2006, .

[4] Lai, XueJia, "Asymmetric encryption and signature method with DNA technology", Science China Information Sciences 53.3, pp. 506-514, 2010.

[5] Grasha Jacob and Annamalai Murugan, “A Hybrid Encryption Scheme using DNA Technology”, The *International Journal of Computer Science and Communications Security*, Vol. 3, pp. 61-65, 2013.

[6] Noorul Hussain Ubaidur Rahman, Chithralekha Balamurugan, Rajapandian Mariappan, “A Novel String Matrix Data Structure for DNA Encoding Algorithm”, *International Conference on Information and Communication Technologies*, (ICICT 2014), 46, pp. 820-832, 2015.

[7] P. Vijayakumar, S. Indupriya1 and R. Rajashree, “A Hybrid Multilevel Security Scheme using DNA Computing based Color Code and Elliptic Curve Cryptography”, Indian Journal of Science and Technology, Vol 9, No.10, pp. 1-7, 2016.

[8] Darrel Hankerson, Alfred Menezes and Scott Vanstone, “Guide to elliptic curve cryptography”, Springer-Verlag, 2004.

[9] Ziad E. Dawahdeh, Shahrul N. Yaakob and Ali Makki Sagheer, “Modified ElGamal Elliptic Curve Cryptosystem using Hexadecimal Representation”, *Indian Journal of Science and Technology*, Vol. 8 (15), pp:1-8, 2015.

[10] A. Atito, A. Khalifa and S. Z. Reda, ”DNA-Based Data Encryption and Hiding Using Playfair and Insertion Techniques”, *Journal of Communications and Computer Engineering*, Vol. 2, Issue 3, pp. 44-49, 2012.

[11] Xing Wang, QiangZhang, “DNA computing -based cryptography”, Key Laboratory of Advanced Design and 1ntelligent Compuling (Dalian university), Ministry of education, Dalian, 116622, China IEEE, 2009.

[12] Fatma E. Ibrahim, M. I. Moussa and H. M. Abdalkader, “ A Symmetric Encryption Algorithm based on DNA Computing”, *International Journal of Computer Applications*, Vol. 97, No.16, pp. 41-45, 2014.

[13] F. Amounas and E.H. El Kinani, “Construction Efficiency of the Elliptic Curve Cryptosystem using Code Computing for Amazigh Alphabet”, International Journal of Information & Network Security, vol.2, No.1, pp. 43-53, 2013

[14] F.Amounas and E.H. El Kinani, "Fast mapping method based on matrix approach for elliptic curve cryptography", *International Journal of Information & Network Security*, Vol. 1, No. 2, pp. 54-59, 2012.

[15] Fatima Sadiqi, “The Teaching of Tifinagh (Berber) in Morocco”, Handbook of Language and Ethnic Identity The Success-Failure Continuum in Language and Ethnic Identity Efforts, Vol 2, Oxford University Press, pp. 33-44, 2011.

[16] Herbert Shildt, ”Java complete reference”, Tata McGraw-Hill, 2011.

[17] F. Amounas and E.H. El Kinani, “Security Enhancement of Image Encryption Based on Matrix Approach using Elliptic Curve”, International Journal of Engineering Inventions, Vol. 3, Issue 11, pp. 8-16, 2014.