International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

A Novel Image Encryption Scheme based on Elliptic Curve and Rubik's Cube

Salma Bendaoud[1], Fatima Amounas[1], El Hassan El Kinani[2]
[1]R.O.I Group, Computer Sciences Department, Faculty of Sciences and Technics, Moulay Ismaïl University, Errachidia Morocco
[2]M.M.S.C Group, ENSAM, Moulay Ismaïl University, Meknes, Morocco

Abstract*—In recent years, several encryption algorithms have been proposed to protect digital images from all types of attack, including statistical and brute force attacks. Encryption is a method to protect data against destruction by involving special algorithm and keys to transform digital data into unreadable format before transmission over the network. The decryption keys are used to get the original digital data back from the transmitted encrypted data form. RSA provide a good level of security but the size of encryption key is a big problem. ECC is a better alternative for public key encryption. In this paper, a new image encryption scheme based ECC using Rubik's cube is discussed. The original image is divided into six sub-images and these sub-images are divided amongst a number of blocks and attached to the faces of a Magic Cube. The faces are then scrambled using rotation of the Magic Cube. For simulation Matlab software is used. The results demonstrate that the proposed scheme have adequate security for the confidentiality of digital image.*

Keywords*— Encryption, elliptic curve, prime group field, scrambling, matrix, rubik's cube.*

I. INTRODUCTION

The security of images is of particular interest in this paper. Cryptography is a method of storing and transmitting data in a secured form so that only intended user can read and process it. It involves encryption and decryption of messages. Encryption is the process of converting a plain text into cipher text and decryption is the process of getting back the original message from the encrypted text. Cryptography is used to protect e-mail messages, credit card information etc. Cryptography provides confidentiality, authentication, Integrity and non-repudiation.

Elliptic curves are algebraic curves which have been studied by many mathematicians for a long time. In 1985, Neal Koblitz and Victor Miller independently proposed the public key cryptosystems using elliptic curve [1, 2]. Since then, many researchers have spent years studying the strength of ECC and improving techniques for its implementation. The main attraction of ECC is that it can provide better performance and security for small key size, in comparison of RSA cryptosystem. In ECC a 160-bit key provides the same security as compared to the traditional crypto system RSA with a 1024-bit key, thus in this way it can reduced computational cost or processing cost. The security of ECC depends on the difficulty of elliptic curve discrete logarithm problem. In fact for a given two points on E(K), it is computationally infeasible to solve the corresponding elliptic curve discrete logarithm problem. ECC is not easy to understand by attackers. So provides better security through insecure channels.

Digital images are an attractive data type that offers a widespread range of use. Any users are interested in implementing content protection methods to their images [3], [4]. In recent years, several image encryption methods have been proposed to secure multimedia information before transmission over unsecure channels [5-7]. ECC is a better method to transmit the image securely. In the literature, several Image encryption algorithms have been proposed [8], [9]. In [10], the authors have studied application of elliptic curves over finite fields for traditional key exchange and encryption of text. It has implemented the proposed scheme for encryption of images. In [11], the authors provide a novel image encryption algorithm based on Rubik's cube principle. The original image is scrambled using the principle of Rubik's cube. Then, XOR operator is applied to rows and columns of the scrambled image using two secret keys. In [12], the author uses the concept of Rubik's Cube to enhance the security of elliptic curve cryptosystem to protect Text message. In this paper, we attempt to extend this approach to secure digital images using data matrix. This approach will boost the security of the cryptosystem using scrambling process based on Rubik's Cube principle. The remaining of this paper is organized as follows. Section 2 gives some background information about the elliptic curve and Rubik's cube. Section 3 describes the proposed image encryption algorithm based on Rubik's cube principle. Experimental results are discussed in Section 4. Finally, we conclude in Section 5.

II. BACKGROUND INFORMATION

A. Elliptic Curve Cryptosystem

An elliptic curve E over a field K can be described as the subset of K×K satisfying the weirstrass equation:

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$$

given as

$$E=\{(x,y): y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6\}$$

For a given $a_i \in K$, along with another special point at infinity (denoted by ∞). The importance of elliptic curve stems from their rich structure, there is a rather simple addition law definable on elliptic curves which make them into a finite abelian group. The basic operations on elliptic curves are addition and doubling. A scalar multiplication with a point can be represented as a combination of addition operations.

For cryptographic propose it is sufficient to limit to non-singular elliptic curve defined by the equation of the form

Salma Bendaoud, Fatima Amounas, and El Hassan El Kinani, "A novel image encryption scheme based on elliptic curve and Rubik's cube," *International Research Journal of Advanced Engineering and Science*, Volume 2, Issue 2, pp. 144-147, 2017.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

$y^2=x^3+ax+b$ over a finite field noted GF(p), here p>3 is prime and a,b∈GF(p). The condition

$$4a^2+27b^3\neq 0$$

Implies that the curve has no "singular points", the set of all elliptic curve points is denoted by Ep(a, b) and defined as

$$E_p(a, b)= \{(x,y): y^2=x^3+ax+b \bmod p\}$$

together with the point at infinity, denoted O.

The basic operations on elliptic curves are addition and doubling [13].

Addition operation for two points P and Q over an elliptic group is given by specific rules indicated below:

$P+Q = R(x_3,y_3)$;

$$x_3=t^2 - x_1- x_2$$

$$y_3= t(x_3 - x_1) - y_1$$

where

$$t= \begin{cases} (y_1-y_2)/(x_1-x_2) & \text{if } P\neq Q \\ (3x_1^2+a)/(2y_1) & \text{if } P=Q \end{cases}$$

A scalar multiplication with a point can be represented as a combination of addition operations. Multiplication kP over an elliptic group is computed by repeating the addition operation k times. The strength of an ECC cryptosystem depends on the difficulty of finding the number of times; P is added to itself to get Q. This reverse operation is known as the Elliptic Curve Discrete Logarithm Problem (ECDLP) and is exploited in cryptography. For more details on the theory of elliptic curves, we refer interested reader to [14], [15].

B. *Rubik's Cube*

A Rubik's cube is built from 26 cubies, each able to make restricted rotations about a core of Rubik's cube. A face of Rubik's cube is a side as shown in Figure 1.

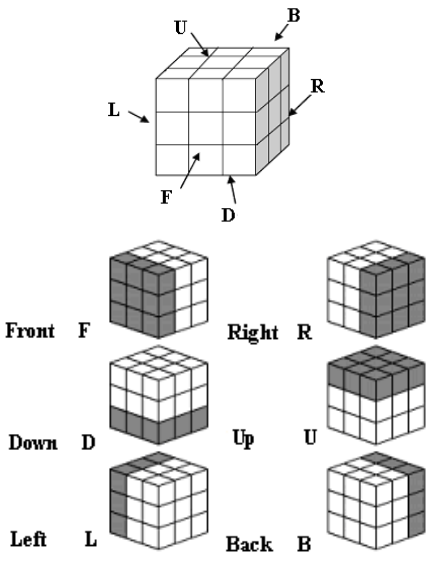

Fig 1. Rubik's cube.

Each face is divided into 9 facelets, where each of the 9 facelets is part of a distinct cubie. The cube was used in cryptography by writing and jumbling the message on the cube. It was very new technique in cryptography and it has given rise to further new suggested techniques. Many cryptography solutions have been implemented that use a cube [16]. Rubik's Cube's complexity is gives by the large number of permutations. In this work, we extended this structure to scramble the encrypted Image.

III. PROPOSED METHOD

In this section, we combine image processing based ECC with the scrambling technique using Rubik's cube. The main idea is that an image can be encrypted and scrambled by rotating the faces (sub-images) of the magic cube. This process generates a good disordering of the image.

Every image consists of pixels. In grayscale images, each pixel has an 8-bit value of between 0 and 255. A pixel in color images is represented by 3 octet values separately; indicate the Red, Green and Blue intensity. To encrypt an image using ECC, each pixel should be mapped to a point on a predefined elliptic curve [17]. The architecture of the image encryption process using the proposed algorithm is shown in Figure 2.

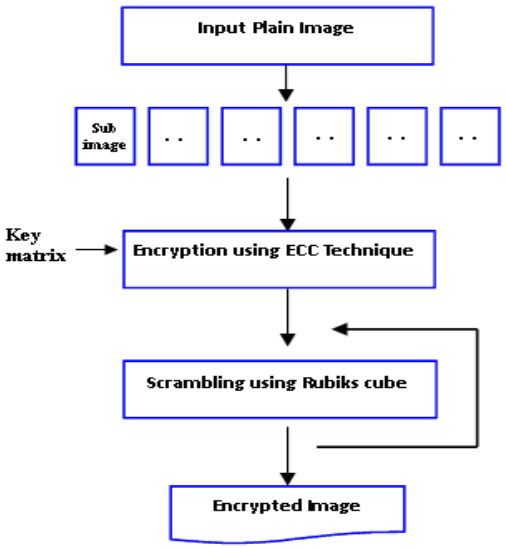

Fig. 2. Flowchart of the image encryption process.

A. *Encryption Process*

Input: Plain image
Output: Encrypted image

Step 1. Load the original image to be encrypted and resize the image such that can be divided into six sub-images.
Step 2. Imbed each pixel into point on the elliptic curve and arrange the mapping points into data matrix PM.
Step 3. Choose a random number and compute secure key K_1.
Step 4. Generate a key matrix KM=(k_{ij}), which are referred to as session keys.
Step 5. Encrypt the mapping points using ECC technique based on matrix approach. Then, arrange the result points into six sub-matrices.

Salma Bendaoud, Fatima Amounas, and El Hassan El Kinani, "A novel image encryption scheme based on elliptic curve and Rubik's cube," *International Research Journal of Advanced Engineering and Science*, Volume 2, Issue 2, pp. 144-147, 2017.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Step 6. Map the six sub-matrices on the six faces of a magic cube (Up (U), Front (F), Right (R), Left (L), Down (D) and Back (B).
Step 7. By rotating the rows and the columns of data matrix, the cipher text can be scrambled. The value of b is verified: if b=1, row transformation is applied on the sub-matrices that are attached to the faces of the magic cube F, U, B, D. If b=0, column transformation is to applied the sub-matrices that are attached to the faces of the magic cube F, R, B, L.
Step 8. Repeat step 7 for m of times.
Step 9. Then the encrypted image is created and sends it to the receiver.

B. Decryption Process

At the receiver side, the original image can be retrieved by an inverse of the scrambling process followed by ECC decryption. The encrypted image is divided into same sub matrices. First, apply a reversal of scrambling process to unscramble the encrypted points using Rubik's cube. Then, cryptographic key is used for ECC decryption to decrypt the result image.

IV. Simulation and Result

The proposed algorithm implemented and analyzed by Matlab programming language [18]. The proposed technique is tested on Matlab R2015a (Figure 3), to justify the effectiveness of the proposed algorithm with caramen image is taken as input image. The results of application of our algorithm on caramen image are given in Figures (Figure 4, Figure 5, Figure 6, Figure 7).

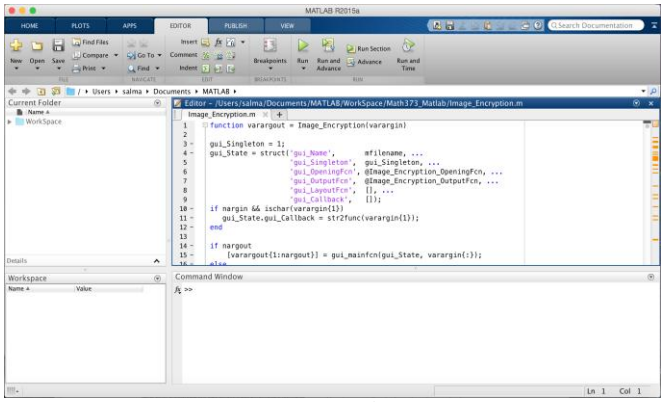

Fig. 3. Matlab software.

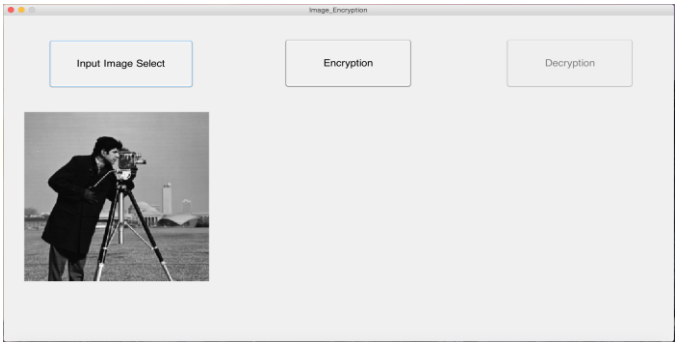

Fig. 4. Input plain image.

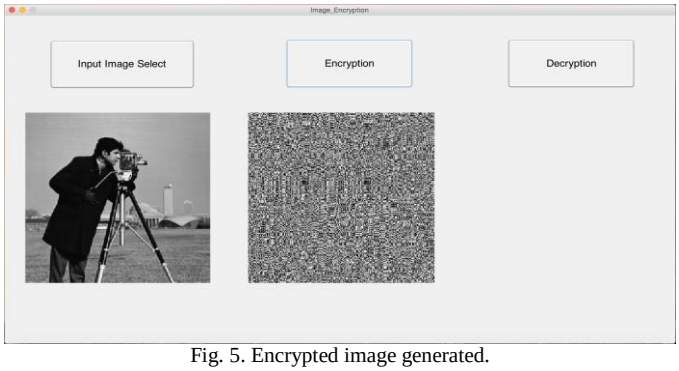

Fig. 5. Encrypted image generated.

The decryption algorithm perfectly recovers the original image as shown below:

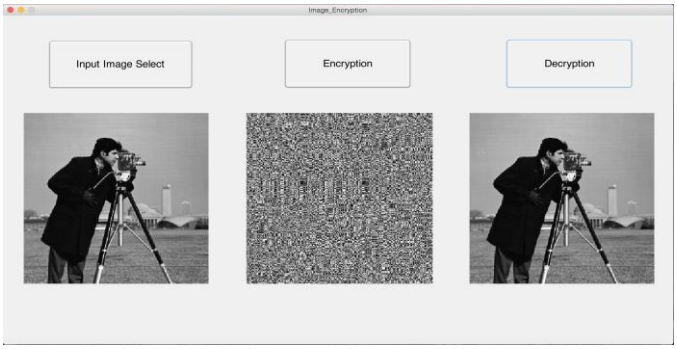

Fig. 6. Decrypted image of "Caramen image".

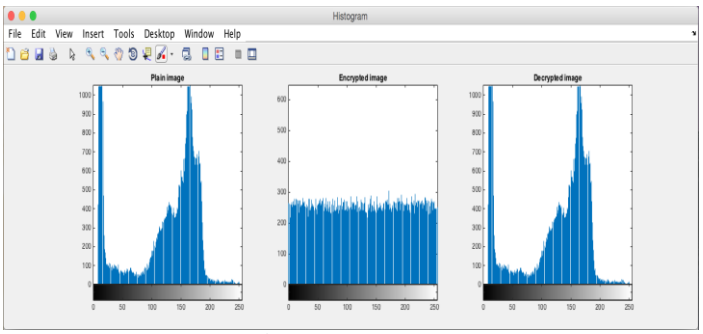

Fig. 7. Histogram of original image and encrypted image.

Experiments using the proposed method resulted in a significantly different encrypted image and uniform histogram, as shown in the Figure 6 and Figure 7. It can be easily seen that ECC encrypts the image so well that nobody can recover the image without possession of keys. The security offered by this proposed cryptosystem, lies in the generation of key matrix with entries on the elliptic curve. For attacking this cryptosystem, we should know the random point and we should know the private key. ECC's strength lies in solving the discrete logarithm problem for elliptic curves [19]. The experimental results show that the algorithm possesses high security and a large key space. Furthermore, a robust cipher image should has a uniform frequency distribution [20]. From Figure 7, it is obvious that the histogram of cipher-image is uniform and significantly different from the histogram of the original image. Hence it does not provide any statistical attacks to the algorithm.

Salma Bendaoud, Fatima Amounas, and El Hassan El Kinani, "A novel image encryption scheme based on elliptic curve and Rubik's cube," *International Research Journal of Advanced Engineering and Science*, Volume 2, Issue 2, pp. 144-147, 2017.

V. CONCLUSION

Image encryption algorithms based ECC are employed nowadays because of their better security and performance aspects. In this paper, a novel image encryption scheme is proposed. During encryption, the scrambling was performed using Rubik's cube principle. The experimental results show that the newly proposed image encryption scheme can achieve good encryption and can resist any cryptanalytic attacks.

In future, we can improve this method by reducing the length of secure key using compression technique. Furthermore, new modifications can be added on to the proposed system for making excellent multimedia applications.

REFERENCES

[1] V. Miller, "Uses of elliptic curves in cryptography", *Advances in Cryptology*, Springer-Verlag, vol. 85, pp. 417-426, 1986.
[2] N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation*, AMS, vol. 48, no. 177, pp. 203-208, 1987.
[3] Ali Soleymani, Zulkarnain Md Ali, and Md Jan Nordin, "A survey on principal aspects of secure image transmission", *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, vol. 6, no. 6, pp. 780-787, 2012.
[4] Omar Reyad, Zbigniew Kotulski and W. M. Abd-Elhafiez, "Image encryption using chaos-driven elliptic curve pseudo-random number generators", *Applied Mathematics & Information Sciences*, vol. 10, no. 4, pp. 1283-1292, 2016.
[5] Vinod Kumar Yadav, A.K. Malviya, D.L. Gupta, Satyendra Singh and Ganesh Chandra, "Public key cryptosystem technique elliptic curve cryptography with generator g for image encryption", *International Computer Technology & Applications*, vol. 3, no. 1, pp. 298-302, 2012.
[6] K. Brindha, Ritika Sharma, Sapanna Saini, "Use of symmetric algorithm for image encryption", *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 2, issue 5, 2014.
[7] Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh, "Image encryption using elliptic curve cryptography", *Eleventh International Multi-Conference on Information Processing-2015, Procedia Computer Science*, vol. 54, pp. 472-481, 2015.
[8] Romi Singh, Shipra Sharma and Shikha Singh, "Image encryption using block scrambling technique", *International Journal Computer Technology and Applications*, vol. 5, no. 3, pp. 963-966, 2014.
[9] Smithashree K and Sujatha M, "Image encryption using efficient elliptic curve cryptography", *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 3, special issue 5, 2015.
[10] Megha Kolhekar and Anita Jadhav, "Implementation of elliptic curve cryptography on text and image", *International Journal of Enterprise Computing and Business Systems*, vol. 1, issue 2, 2011.
[11] Khaled Loukhaoukha, Jean-Yves Chouinard and Abdellah Berdai, "A secure image encryption algorithm based on Rubik's cube principle", *Journal of Electrical and Computer Engineering*, vol. 2012, pp.1-13, Article ID 173931, 2012.
[12] Fatima Amounas, "Enhancing robustness of encrypting amazigh alphabet based ECC using scrambling method", *International Journal of Engineering and Innovative Technology*, vol. 5, issue 3, pp. 138-142, 2015.
[13] D. R. Hankerson, S. A. Vanstone, and A. J. Menezes, "Guide to elliptic curve cryptography", *Springer*, 2004.
[14] Lawrence C. Washington, *Elliptic Curves Number Theory and Cryptography*, Discrete Mathematics and its Applications. Chapman and Hall/CRC, University of Maryland College Park, Maryland, U.S.A., 2 editions, 2008.
[15] Williams Stallings, *Cryptography and Network Security*, Prentice Hall, 4th Edition, 2006.
[16] Rajdeep Chowdhury and Saikat Ghosh, "Normalizer based encryption technique (NBET) using the proposed concept of rubicryption", *International Journal of Information Technology and Knowledge Management*, vol. 4, no. 1, pp. 77-80, 2011.
[17] Fatima Amounas and El Hassan 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.
[18] Gonzalez R. C., Woods R. E., and Eddins S. L., *Digital Image Processing Using MATLAB*, Gatesmark Publishing A Division of Gatesmark, LLC, 2009.
[19] Lawrence C. Washington, *Elliptic Curves Number Theory and Cryptography*, Discrete Mathematics and its Applications. Chapman and Hall/CRC, University of Maryland College Park, Maryland, U.S.A., 2 editions, 2008.
[20] Gurpreet Singh and Lovleen Kaur, "Image cryptography based upon scrambling and random integer", *International Journal of Science and Research*, vol. 3, issue 9, 2014.

Salma Bendaoud, Fatima Amounas, and El Hassan El Kinani, "A novel image encryption scheme based on elliptic curve and Rubik's cube," *International Research Journal of Advanced Engineering and Science*, Volume 2, Issue 2, pp. 144-147, 2017.