New Digital Image Encryption Scheme based on Elliptic Curve Isogenies

Samia Bouaziz, Ramzi Hadaji, Abdellatif Mtibaa

National School of Engineering of Monastir, Tunisia

Abstract— *Due to the complexity of modern technological exchanges, the need of the security of the image remains till now a challenging problems. In this paper, we present a new encryption scheme based on a non-classical aspect of the elliptic curve cryptography and the Ramanujan graph to encrypt JPEG compressed image. Our algorithm operates on the hardness to predict the exact walk of the Pizer graph formed by the elliptic curve isogenies. The proposed approach has been compared with classical protocols.*

Keywords— Elliptic curve, Encryption, Digital Image, Ramanujan graph.

I. INTRODUCTION

The security of the data transmission become more and more important nowadays due to the multitude ways and uses for exchange many types of data, medicine, channel TV, satellite image, military transmission, etc. Data security is proved by encryption scheme and it has received huge amount of interest by researchers who have proposed hundreds of approaches, especially in recent decades using mathematical theories. A simple and an effective method remains an interesting topic for many researchers. Generally, the existing approaches of encryption scheme in cryptography are classified into two categories: private or public key encryption. Unlike text messages, the multimedia information including image data has some special characteristics like high capacity, redundancy and high correlation among pixels. Many techniques have been developed to the security of multimedia information. In some cases image applications require to satisfy their own needs like real time transmission and processing as in satellite image or TV channel. As known, there are three kinds of encryption techniques namely substitution, transposition or permutation and techniques that include both transposition and substitution.

Elliptic curve cryptography, ECC, rises and become one of the more important mathematical theory for encryption; the strongest and classical point of ECC is based on hardness to compute the discrete logarithm in the set of points of an elliptic curve which have their coordinates in a finite field F_p, where p is a prime or power of prime number. By using the benefits of ECC the new algorithm, we present in this paper is based on another aspect not yet exploited, which is the difficulty to find the exact walk in the Pizer graph having as vertices elliptic curves and as edges the isogenies. Our algorithm matches to the coefficients DC of an image in the JPEG compression process a set of isogenies in the graph of Pizer chosen according to a secret key. This algorithm has been clearly proved to be comparable to a proved existing methods like ECC-DLP, AES and RSA [4]. The remaining of this paper is organized as follows. In Sect. 2 and 3, we recall some necessary properties of elliptic curves and graph of Pizer. Section 4 presents the proposed approach. Performance evaluation and comparative results are given in detail in Sect. 5. Finally, some conclusions are made.

II. ELLIPTIC CURVE CRYPTOGRAPHY

I. *Definitions*

We call elliptic curve [5] defined over the finite field F_p a non-singular curve writed in the Weierstrass form

$E : y^2 = x^3 + ax + b.$

Let denote by $\Delta(E)$ the discriminant of E and defined as

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27\, b_6^2 + 9\, b_2 b_4 b_6.$$

And by $j(E)$ the *(j-invariant)* of E defined as

$$j(E) = \frac{c_4^3}{\Delta}.$$

II. *Isogeny*

Let E and E' two elliptic curves defined over a finite field F_p. One can define an isogeny between E and E', an application φ such as for a point $P \in E$ we associate an image $\varphi(P) = Q \in E'$. We can gather all the isogenies between E and E' in a set denoted by $Hom(E, E')$. The dimension of the kernel of the isogeny φ between E and E 'is called the degree of φ. Let $\varphi : E \rightarrow E'$ and let d the degree of φ, then there is a unique isogeny denoted by $\hat{\varphi}$ between E' and E such as $\hat{\varphi} \circ \varphi = [d]_E$, where $[d]_E$ is an isogeny defined by

$$[d]_E : E \rightarrow E$$
$$P \rightarrow mP.$$

III. RAMANUJAN GRAPH

We begin by defining the family of graphs. Let p and l be two distinct prime numbers. Define the graph $G(p, l)$ to have vertex set, V, the set of isomorphism classes of

supersingular elliptic curves over the finite field F_{p^2}. We label vertices with their $j-invariants$, which can be computed directly from the curve equation and are a priori elements of F^2. The number of vertices of $G(p,l)$ is $\lfloor \frac{12}{p} \rfloor + \varepsilon$, where $\varepsilon \in \{0,1,2\}$, depending on the congruence class of $p \equiv 12$. Later, we will impose $p \equiv 1(mod 12)$, in which case $\varepsilon = 0$. Since there are roughly $p/12$ distinct $j-invariants$, we will choose a linear congruential function to map $j-invariants$ from F^2 to F_p. The edge set is as follows: given a supersingular $j-invariant$, j_1, choose an elliptic curve E_1 with $j(E_1) = j_1$ in the manner described in the next paragraph and a subgroup $H_1 \subseteq E_1$ of order $l \neq p$. Connect j_1 to $j_2 := j(E_2)$ where E_2 is the elliptic curve E_1/H_1. A priori, since there are $l+1$ subgroups of order l this gives a directed $(l+1)$- regular graph. However, if we assume that $p \equiv 1(mod 12)$, then the graph can be made into an undirected graph as follows: for each subgroup $H_1 \subseteq E_1$ of order l, there is a canonical choice of subgroup $H_2 \subseteq E_2$ (of order l) such that $E_2/H_2 \cong E_1$. Thus, we can identify the edge associated to H_1 with the edge associated to H_2 [3].

IV. NEW ENCRYPTION SCHEME FOR MULTIMEDIA

The use of expander graphs to produce pseudo-random behavior is well-known to complexity theorists. The idea here is to use expander graphs to produce a new encryption scheme which can be used in the multimedia security. The first input to our scheme is the coefficient DC_0 of the first 8×8 pixel block and this initialization is used to compute the directions for walking around a graph, we associate to DC_0 an elliptic curve E_0, this bloc first coefficient is sent to another position using an and set

$$t(Q) = 2c(Q)a_1 d(Q),$$
$$u(Q) = (d(Q))^2,$$
$$l = \sum_{Q \in (C - \{0_E\})} t(Q),$$
$$\omega = \sum_{Q \in (C - \{0_E\})} (u(Q) + x(Q)t(Q)).$$

Then the curve E/C is given by the equation

$$Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6,$$

Where

$$A_1 = a_1,\ A_2 = a_2,\ A_3 = a_3,$$
$$A_4 = a_4 - 5t,\ A_6 = a_6 - (a_1^2 + 4a_2)t - 7w.$$

From the Weierstrass equation of E/C we can easily determine the $j-invariant$ of E/C. We apply Vélu's isogeny ϕ and the process will ended when the algorithm cover all the DC coefficients of the image. The new encryption scheme is a secret key scheme and the latter is in fact constituted by an ellliptic curve E_0 and a set of isogenies $\phi_0, \phi_1, \phi_2, \ldots, \phi_n$,

$$Key_{Encryption} = (E_0, \phi_0, \phi_1, \phi_2, \ldots, \phi_n).$$

The decryption way is allowed by using the key constituted by E_n and the dual isogenies

$\hat{\phi}_0, \hat{\phi}_1, \hat{\phi}_2, \ldots, \hat{\phi}_n$,

$$Key_{Decryption} = (E_n, \hat{\phi}_0, \hat{\phi}_1, \hat{\phi}_2, \ldots, \hat{\phi}_n).$$

The construction of this scheme is in fact a walking around the Pizer graph, each coefficient is sent to a different position from its original one and so on. We execute a walk on a $k-regular$ expander graph by converting the input block into a new vertex of the graph to a base $(k-1)$ number whose digits then dictate which edge to take at each step. We do not allow backtracking in the walk, so only $k-1$ choices for the next edge are allowed at each step.

I. *Walking into the Graph*

For C a subset of the group of the points on an elliptic curve E, Vélu in [2] gives explicit formulas for determining the equations for the isogeny $E \to E/C$ and the Weierstrass equation of the curve E/C. We give here the formulas when l is an odd prime and in the next section we give those for the formulas when $l = 2$. Let E be given by the equation

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

We define the following two functions in $F_q(E)$. For $Q = (x, y)$ a point on $E\{0_E\}$, define

$$c(Q) = 3x^2 + 2a_2x + a_4a_1y,\ d(Q) = 2ya_1xa_3,$$

formulas for subgroups of order l, and it is clear that this procedure can be done using $O(l)$ elliptic curve operations for each of the $l+1$ groups of order l,

$$E_1 \to E_2 \to \ldots \to E_i \to E_{i+1} \to \ldots \to E_n.$$

II. *Explicit Case* l = 2

In this paragraph we study the explicit case $l = 2$. Here are the steps to compute the encryption scheme when using supersingular elliptic curves and 2-isogenies (i.e. $l = 2$). Since there are 3 edges emanating from each vertex, and no backtracking is allowed in a walk, there are two choices of which edge to follow next from each vertex, and this can be determined by 1 bit as follows. Start at a vertex E_1. Subgroups of E_1 of order 2 are each given by a single two-torsion point on the elliptic curve $E_1 : y_2 = f(x)$. The 3 non-trivial 2-torsion points are $P_i = (x_i, 0)$, where the cubic $f(x)$ factors as

$$(x - x_1)(x - x_2)(x - x_3)$$

over an extension field. As an example, when computing the isogeny φ which corresponds to

taking the quotient by $\langle P_1 \rangle$, both of the other 2-torsion points are mapped to the same 2-torsion point $\phi\langle P_2 \rangle = \phi(P_3)$ on the isogenous elliptic curve, E_2. In turn, the isogeny which corresponds to taking the quotient of E_2 by the subgroup generated by $\phi(P_2)$ is the dual isogeny $\hat{\phi}$ and leads back to E_1. So to choose the next step from E_2, it suffices to choose between the two other 2-torsion subgroups different from $\langle \phi(P_2) \rangle$. An efficient way to determine the 2 new 2-torsion points on E_2 is to keep $\tilde{x_2}$, the x-coordinate of $\phi(P_2)$, and to factor $(x - \tilde{x_2})$ out of the new cubic $f_2(x)$, leaving a quadratic to be factored. The roots of the quadratic can be ordered according to some convention, and one bit suffices to choose between them for the next step in the walk. So if the input bit length is n, then the walk into the graph takes n steps. Using Vélu's formulas [2] one calculates that if E is given by $y^2 = x^3 + a_4x + a_6$ and the 2-torsion point Q is $(\alpha, 0)$ then the elliptic curve $E/\langle Q \rangle$ can be given by the equation

$$y^2 = x^3 - (4a_4 + 15\alpha^2)x + (8a_6 - 14\alpha_3).$$

Furthermore, the equation for the isogeny is

$$(x,y) \mapsto \left(x + \frac{(3\alpha^2 + a_4)}{x - \alpha}, y - \frac{(3\alpha^2 + a_4)y}{(x-\alpha)^2}\right).$$

The formula given here shows the dependence on the 2-torsion point $Q = (\alpha, 0)$. So summa- rizing, each vertex corresponds to an elliptic curve E_i given by an equation $y^2 = f_i(x)$, where $f_i(x)$ is a cubic. To compute the 2-torsion subgroups at each step, factor the cubic $f_i(x)$. At each step, calculate the 2-torsion by keeping the image of the other 2-torsion point (not used to
quotient by), and then factoring the quadratic. After ordering, choose which one to quotient by and apply Vélu's formulas (field operations in F_p or F^2) [7].

III. *Complexity of the new scheme computation*

To compute the complexity of our method we need to enumerate the number of elementary operation cost per block of the walking. After are the essential steps of the method

1. Find the 2-torsion:

a Apply the isogeny from the previous step to one point: 7 field multiplications.

b Factor out the linear factor from the cubic $f_i(x)$: one field inversion.

c Factor the quadratic by completing the square and taking a square root: roughly $(3/2)log2(p)$ field multiplications plus a field inversion if $p \equiv 3(mod4)$. If $p \equiv 3(mod4)$, then one can do this with $2\log_2(p)$ multiplications in a residue ring of $F_p[x]$. The construction of the residue ring requires $\log p$ random bits.

2. Order the 2-torsion.

3. Use Vélu to obtain the equation of the next elliptic curve: 9 field multiplications.

In addition, at the first vertex, the cubic defining the curve must be factored, and at the last step, computing the j-invariant requires several field multiplications and 1 field inversion. An estimate of total cost can be made by estimating a field inversion as 5 field multiplications. To summarize the efficiency of the walking under these assumptions: the cost per bit in terms of
field multiplications is roughly $2\log_2(p)$ [7].

V. RESULTS

In this section we give the results of our algorithm used for the encryption of image. We use MATLAB on a 64-bit Intel Core I7-4500U CPU 2.4Ghz,6G RAM machine to implement our encryption scheme to test its performance for an input bit. Our results are given below. For a
prime p of $192 - bits$ and $l = 2$, the time per step of the walk (which is also the time per input bit) is $2.7 \times 10^5 secs$. For a prime p of 256-bits, the time per input bit is $5.3 \times 10^5 secs$.

Experimental results are given in this section to demonstrate the performance of our proposed method used for image in different purpose: standard use, medical image and satellite image, we used our algorithm to encrypt and decrypt a large number of images. The process of the JPEG compression is depicted in the figure 1 below. Here below we give some results of the implementation of our algorithm to encrypt compressed images.

As the purpose of our scheme is to address the problem of image retrieval in encrypted do- main while preserving the file size and format compliance for JPEG images, here, we first take a partial image encryption technique into account to encrypt JPEG images. The problem is difficult to solve for the traditional cryptography. The most existing partial encryption techniques for JPEG images are mainly based on blocks shuffle, DCT coefficient permutation, and encrypting the signs of DCT coefficients. The proposed encryption in our method in can meet the requirements of format compliance and file size preservation and also to provide valuable information regarding the length of each variable length integer (VLI) code for DCT coefficients. More importantly, the encryption method can make the length of each VLI code remain unchanged before and after encryption. It means that one can still obtain the original length of any VLI code related to DCT coefficients from an encrypted JPEG image. Due to the dependencies of DCT coefficients in each component, their corresponding VLI code length may have similar relationships, which can be exploited to generate feature for image retrieval. As commonly known, a color JPEG image is composed of Y, U, and V components, each of which is partitioned into non-overlapped blocks sized 88.

In each block, there are 64 DCT coefficients namely, one DC and 63 AC coefficients. According to JPEG standard [8], DC and AC coefficients can be transformed into intermediate symbols by utilizing the one-dimensional predictor and the run length coding (RLC), respectively, and then are further Huffman-coded into binary sequences, each of which consists of two parts: the Huffman code and the VLI code. Obviously, the generation of the abovementioned binary sequences is conditioned by the Huffman and VLI coded tables, which are beforehand stored in the JPEG file. In general, the Huffman code of the DC coefficient only contains the information about the length of the VLI code. But the Huff- man code for the AC coefficient also has other information about the number of consecutive zero AC coefficients before the next nonzero AC coefficient in the zigzag sequence. The final JPEG image will be formed by concatenating the JPEG file header and binary sequences of all DCT coefficients of all components. As a matter of fact, the JPEG bit-stream is also a binary sequence and thus converts into a JPEG file when writing to a file byte by byte. Based on the above knowledge about color JPEG image encoding, the procedure of performing the color JPEG image encryption scheme is to encrypt all the DC coefficients in the process In the following figure 3, we studied the effect on the color distribution in the histograms of an image before and after the encryption scheme. We can see that in the case of encryption image the distribution present a random and uniform noise which is essential to stop the various hacking methods.

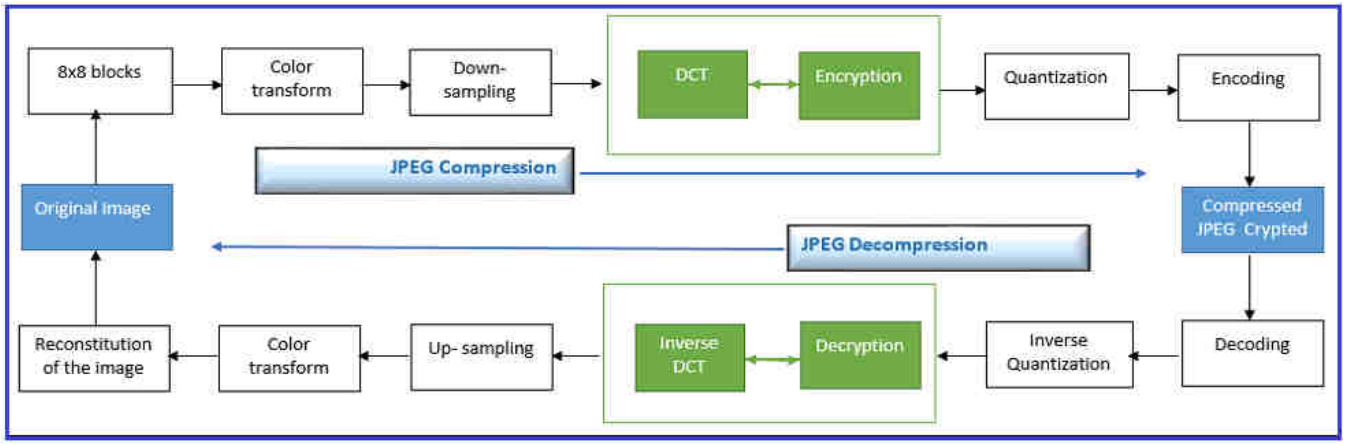

Fig.1: JPEG compression process

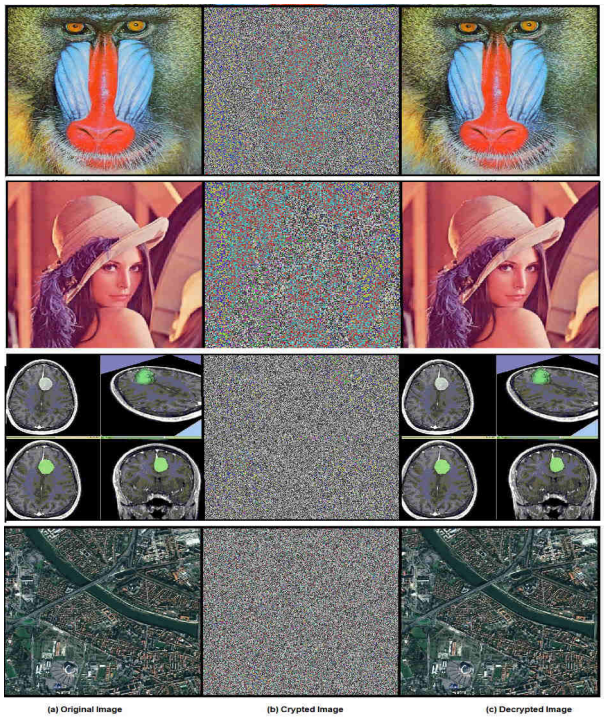

Fig.2:Encryption and Decryption process for 4 types of images

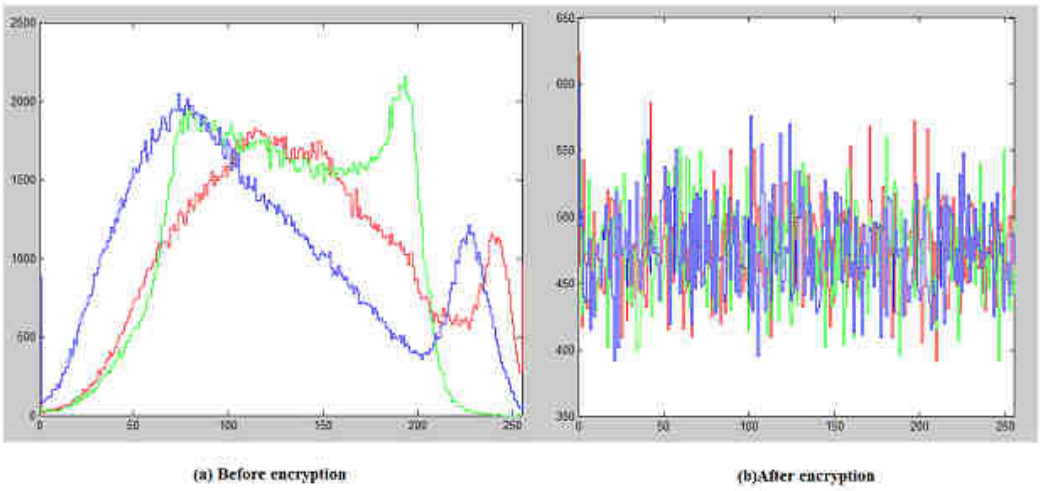

Fig.3: Histogram of encryption (a) and decryption (b) image

I. *Comparison*

To prove the efficiency of a new protocol, this one must be compared to the existing and see the advantages it offers compared to those. The table below published by NIST (National Institute of Standards and Technology) compares different protocols for the same security levels relative to the sizes of keys.

NIST guidlines for public key size		
RSA key size (bits)	ECC key size (bits)	Key size ratio
163	1024	1:6
256	3072	1:12
384	7680	1:20
512	15360	1:30

We can distinguish from this table that small ECC key size provides a very good level of security, this is a huge advantage for implementations of this method compared to hardware constraints such as memory size and real time.

In our study we compared over time encryption for large library of images our method ECC- Graph to other that are most popular as AES, RSA, and the classical ECC-DLP protocol based on the discret logarithm problem (DLP).We obtained the following results in Figure 4.

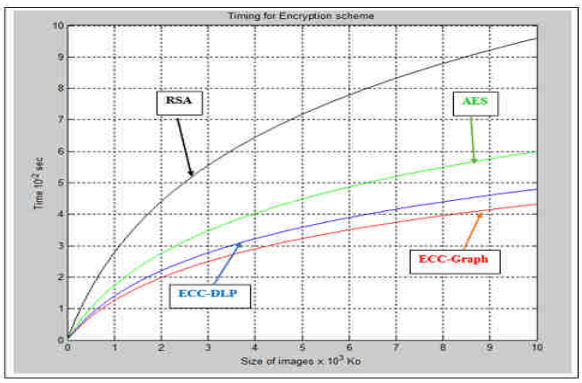

Fig.4: Comparison of protocols

VI. CONCLUSION

In this paper we give an efficient new encryption scheme to encrypt compressed image, this protocol was compared to other existent and the results proved that it is faster and it can be a good candidate to the hardware implementation. We can easily extend this method to video decoder which is the subject of other works that are submitted to be publish.

REFERENCES

[1] Jean-Pierre Deschamps, "Implement Finite-Field Arithmetic in Specific Hardware (FPGA and ASIC)," McGraw- Hill, (2009).

[2] J. Ve´lu , "Isognies entre courbes elliptiques," C. R. Acad. Sc. Paris 273, (1971).

[3] W. Li, , "A Survey of Ramanujan Graphs," in R. Pellikaan, M. Perret, and S.G Vladut 'eds.), Arithmetic, Geom- etry, and Coding Theory, Proc. Confat CIRM, Luminy, France, de Gruyter, Berlin, (1996).

[4] Alfred Menezes, Paul van Oorschot, and Scott Vanstone , "Handbook of Applied Cryptography," CRC Press, (1996).

[5] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen and Frederik Ver- cauteren, "Handbook of Elliptic and Hyperelliptic Curve Cryptography," Dis. Math.Its App. 1st Edition, (2005).

[6] Yang Yang, Bin B. Zhu, Shipeng Li and Nenghai Yu, "Efficient and Syntax-Compliant JPEG 2000 Encryption Preserving Original Fine Granularity of Scalability," EURASIP J.Inf. Sec. (2007).

[7] Denis X. Charles, Kristin E. Lauter and Eyal Z. Goren, "Cryptographic Hash Functions from Expander Graphs," J. of Crypt. 22, Issue 1, (2009).

[8] Hang Cheng, Xinpeng Zhang, Jiang Yu and Fengyong Li3, "Markov process-based retrieval for encrypted JPEG images," EURASIP J.Inf. Sec. 1 (2016).