Malaysian Journal of Computing and Applied Mathematics 2020, Vol 3(1): 52-62
©Universiti Sultan Zainal Abidin
(Online)

MALAYSIAN JOURNAL OF COMPUTING AND APPLIED MATHEMATICS

A New Approach to Verifying and Sharing a Secret QR Code using Elliptic Curves

***Hichem Bouchakour Errahmani**[a,c]**, Hind Ikni**[b]*

[a]EEDIS Laboratory, Djillali Liabes University of Sidi Bel Abbes, Algeria
[b,c]Computer Science Department, Belhadj Bouchaib Center, University of Ain Temouchent, Algeria

[*]Corresponding author: b_hichem@hotmail.fr

Received: 11/12/2019, Accepted: 03/04/2020
http://dx.doi.org/10.37231/myjcam.2020.3.1.44

Abstract

One of the modern applications of cryptography is the sharing of secrets in occurrence keys. Indeed, the need to establish a shared secret key in a multi-user system clearly remains a major problem of trust between users. Therefore, one solution is to share this secret key between users seamlessly. New technologies embedded systems such as sensor networks provide an ideal platform for sharing secrets. In addition, elliptic curves offer an adequate solution for reducing the size of keys, which is suitable for embedded systems. In this article, we propose an approach for sharing a secret leaked in a QR code adapted for a multiuser system, where each user has the ability to verify its share by an access structure. The system allows a recovery without loss of data in this case the QR code used.

Keywords: elliptic curve cryptography, discrete logarithm problem, image secret sharing, verifiable secret sharing.

INTRODUCTION

Classical cryptography treats the notions of encryption, decryption, hashing using secret keys whose owners are the actors of the cryptosystem. Those keys represent the security basis of the entire system according to Kerckhoffs principles. On the other hand, the question that could arises in our mind, is how to protect such an important key? Hence, the notion of threshold secret sharing, where the key is distributed over a group of participants in such a way that none of them possesses an information about the secret, but some candidates representing the access structure collaborate at its reconstitution. Several works have contributed to improve secret sharing since the first approach of Adi Shamir, such as verifiable approaches and proactive ones. However, the particularity of contemporary methods lies in the use of elliptic curves, for the reason that they revolutionized cryptosystems security by providing solutions to constraints caused by key size and operations complexity. In this paper, we propose a method of securing visual cryptographic keys by multi secrets sharing scheme with self-selecting of private ones, based on ECDLP. The scheme takes as input an image matrix which represents the secret to share on a server–client network without information loss. In our method, we give the participants the capability to verify their received shares without secret reconstruction, to prove the validity of the dealer, shadows, and even candidates. The rest of the paper is structured as follows: Section II illustrates preliminaries techniques for a good comprehension of the subject. Section III presents related works for sharing secrets using elliptic curves. Section VI describes steps of the proposed approach. Section V discuses results. Finally, section IV concludes and resumes the paper.

PRELIMINARIES

In this section, we describe briefly the basic techniques used for secret sharing with elliptic curves.

A. Elliptic Curve

An elliptic curve Eover a finite field $\mathbb{F}p$ is a set of pairs 2 resolving the equation Y $(X, Y) \in \mathbb{F}p$+ A X +B $(modp)$ union a particular element called point at infinity noted $\mathcal{O}$ (with A, $B \in$ $\mathbb{F}p$ and 4A 23= X32+ 27$B \neq$ 0 $(modp)$). We should mention some operations properties over ($\mathbb{F}$) (Errahmani & Faraoun, 2018):

a) Closure: $\forall$ P, $Q \in$, if$P + Q =$ R then $R \in E$;
b) Associativity: $\forall$ P, Q, $R \in E$, $+ Q + R = P + (Q + R)$;
c) Identity element: $\forall P \in$, $P + \mathcal{O} = \mathcal{O} + P = P$;
d) Inverse element: $\forall(x, y)$ $\in$ E, $\exists - P(x, -y) \in$ E;
e) Commutativity: $\forall P$, $Q \in$: $P + Q = Q + P$;

We infer that $E(\mathbb{F}p)$ forms an abelian group. The addition operation in $E(\mathbb{F}p)$ is defined as follows:

For each $P\left(x_{p,}y_p\right), Q\left(x_{q,}y_q\right), R(x_r, y_r)$ and $P + Q = R$

$$x_R = \gamma^2 - x_P - x_Q \ (mod\ p)$$

And $$y_R = \gamma(x_P - x_R) - y_P \ (mod\ p)$$

Such that:

$$Y = \{ \begin{matrix} (y_Q - y_P)\left(x_Q - x_P\right)^{-1}(mod\ p) & ifP \neq Q \\ (3x_P^2 + A)(2y_P)^{-1}(mod\ \ p) & else \end{matrix}$$

The inverse of R is obtained by $-y_R$ $(mod\ p)$.

Given a large prime number p, finding the integer n such that $Q = n \cdot P$ where P, $Q \in$ ($\mathbb{F}p$), is a very hard problem to solve. This problem is called the Elliptic Curve Discrete Logarithm Problem (ECDLP), which makes a good tool for cryptographer.

B. Threshold secret sharing of Shamir

A threshold secret sharing scheme consists to split a secret key and distribute it among n participants in such a way its reconstitution requires only a qualified group of them.

In its paper, Shamir (1979) describes the conditions of a threshold (k, n) sharing system:

- Knowledge of any k or more pieces of the secret, makes it easily computable
- Knowledge of any$k - 1$ or fewer pieces of the secret leaves it completely undetermined.

To share a secret S among n persons with a threshold k, we define a random $k - 1$ polynomial

$$f(x) = a_0 + a_1{}^x + \cdots + a_{k-1}x^{k-1}$$

in which $a_0 = S$ and $a_1, \cdots, a_{k-1} \in \mathbb{R}$. To determine the different shares, we compute n points $(i, f(i))$.

For secret reconstruction, we use Lagrange interpolation for k given points:

$$P_n(x) = \sum_{i=0}^{n} y_i \prod_{\substack{k=1 \\ k \neq i}}^{k=n} \frac{(x - x_k)}{(x_i - x_k)}$$

RELATED WORKS

The first threshold secret sharing scheme was invented in 1979; we owe it to Shamir (1979). Also called $(t,\ n)$ scheme, his approach is based on Lagrange Polynomial Interpolation, where a secret can be distributed over n participants, and reconstructed by at least t of them.

In the same year, a geometric approach was published by Blakley (1979), who represented the secret by an intersection point of hyper plans, in such a way that each candidate receives one hyper plan equation. Several techniques of sharing secret have followed, adding some options to main ideas. A notion of sharing multi secrets was treated in different approaches. Based on Shamir's scheme and Elliptic Curve, Hua & Aimin (2010) and Binu & Sreekumar (2017) have both published a method where a set of secrets are shared by Shamir's polynomial coefficients using elliptic curves bilinear pairing and a cryptographic hash function. Moreover, to study key management for MANETs, Dahshan & Irvine (2011) put forward a new scheme for sharing a matrix of secrets among mobile nodes using Lagrange Polynomial Interpolation and ECDLP. His method is divided in two main parts, an offline initialization phase where a central authority distributes pairs of long term public/private keys for each node, and an online phase in which the node with the largest identity number considered as a dealer, generates session keys using his own long term private key, then collects public session keys to reconstruct secrets by interpolation.

Furthermore, Kumar et al. (2017) proposed a scheme for MANETs based on Shamir’s approach; however, he adopted it with bivariate polynomial which allows scalability of his system.

For another type of networks system, Al-Adhami et al. (2016) designed a threshold quorum system allowing a secure distribution of logistics information on RFID Tags, where the shares are stored encrypted using El Gamal ECC scheme, which provides security and privacy during package transmission. Thus, according to the authors, the quorum system maintains information security against several RFID attacks.

In order to have more efficiency, a verification option technique was proposed. In 1991, Pedersen (1991) build a signed threshold sharing scheme assigning to each candidate additional information allowing him to verify the validity of his own share using Discrete Logarithm Problem (DLP).

After that, Han et al. (2003) constructed a sharing cryptosystem based on Pedersen's theory using Elliptic Curve Signature Algorithm (ECSA) and Elliptic Curve Encryption System (ECES) based on ECDLP, the author claims that the scheme resists to attacks but requires safe transmission channels.

In the other hand, Nisha (2016) have propounded a different verifiable multi-secret sharing scheme where he overcomes channels security weaknesses by using Double Knapsack algorithm to secure transmissions.

In another side, different schemes are built with self-selecting secret key option based on ECDLP, where each participant chooses a private key by himself for the sharing operation. Caimei's (2009) scheme uses Diffie-Hellman elliptic key exchange algorithm to generate the private key point coordinate and exploits a cryptographic hashing function to secure them.

SCHEME DESCRIPTION

Our proposed scheme treats a secret sharing method on a distributed system, where secrets are represented by each pixel of a given image. Two servers are used for the network communication as shown in Figure 1, one as a Dealer for sharing parameters initialization system, publishing them and distributing the shares. The second server, called Combiner, is used only for secrets reconstruction computation where the threshold participants collaborate by connecting to it.

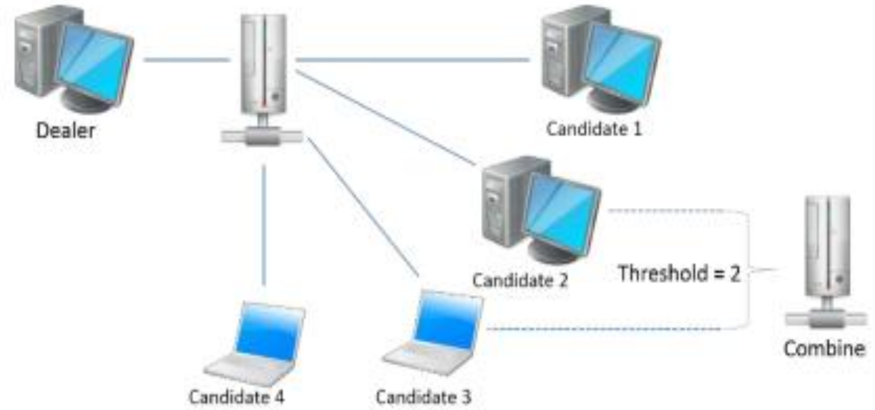

Figure 1. Network architecture

A. Sharing system initialization

All mathematic notations used in the scheme are shown in Table 1. It's the role of the Dealer to initialize the settings for the sharing system. Since all cryptographic arithmetic operations require an elliptic curve over a finite field, the Dealer chooses first a big prime p and an appropriate cryptographic elliptic curve

$$E(\mathbb{F}p\ ):\ y^2 = x^3 + ax + b\ (mod\ p)$$

Where a, $b \in \mathbb{F}p$, he selects a base point generator (x , yG) such that $\#E \cdot G = O$.

Besides, an image of size $T = L \times \mathrm{C}$ is required to represent the matrix of secrets M, where each pixel is considered as a unique secret to share. Finally, the Dealer publishes the parameters < p, E, G, L, C >.

B. Shares distribution

In the proposed scheme, each candidate u_i is identified by a unique number $nonce$ which is generated once a client connected to the server. u_i generates his own private sharing keys in matrix form, using published parameters, where each element s_i is randomly chosen over $\mathbb{F}p$.

$$S^i = \begin{pmatrix} S_{11}^i \dots S_{1C}^i \\ . \\ . \\ . \\ S_{L1}^i \dots S_{LC}^i \end{pmatrix} \tag{1}$$

Table 1: Mathematical Notations

Symbol	Description
p	Prime number
$\mathbb{F}p$	Finite field
E	Elliptic curve $y^2 = x^3 + ax + b\ (mod\ p)$
O	Point at infinity
$\# E$	Number points
G	Base point
U	Set of all participants
$u_i \in U$	A unique participant
$n = \lvert U \rvert$	Number of participants

k	Threshold
T	Size of the secret matrix
M	The secret matrix
S^i	Private key of participant u_i
L	Lines of a matrix
C	Columns of a matrix

then calculates his public keys by ECDLP using G to generate T public points P_{lc}^{i}:

$$S^i \cdot G = \begin{pmatrix} s_{11}^{i} \cdot G & \cdots & s_{1C}^{i} \cdot G \\ \vdots & \ddots & \vdots \\ s_{L1}^{i} \cdot G & \cdots & s_{LC}^{i} \cdot G \end{pmatrix} = P^i = \begin{pmatrix} P_{11}^{i} & \cdots & P_{1C}^{i} \\ \vdots & \ddots & \vdots \\ P_{L1}^{i} & \cdots & P_{LC}^{i} \end{pmatrix} \quad (2)$$

After collecting all public key matrices Pi, the Dealer prepare the shares in several steps :

- **Step 1** He verifies the distinction of all public keys collected from each other's. For each $P^i = P^j$ replies to u_i and u_j asking for other matrices, where the specific candidates generate an other private keys matrix Si to compute different public matrix Pi. The Dealer iterates this procedure until collecting n different matrices.
- **Step 2** He chooses his private key $r \in \mathbb{F}p$ to generate a private matrix of points Q^i:

$$r \cdot P^i = \begin{pmatrix} r \cdot P_{11}^{i} & \cdots & r \cdot P_{1C}^{i} \\ \vdots & \ddots & \vdots \\ r \cdot P_{L1}^{i} & \cdots & r \cdot P_{LC}^{i} \end{pmatrix} = Q^i = \begin{pmatrix} Q_{11}^{i} & \cdots & Q_{1C}^{i} \\ \vdots & \ddots & \vdots \\ Q_{L1}^{i} & \cdots & Q_{LC}^{i} \end{pmatrix} \quad (3)$$

  Where each point Q_{lc}^{i} has coordinates $(X_{lc}^{i}\ Y_{lc}^{i})$.
- **Step 3** The secret matrix M is obtained by converting a given image pixels to elements over $\mathbb{F}p$:

$$M = \begin{pmatrix} M_{11} & \cdots & M_{1C} \\ \vdots & \ddots & \vdots \\ M_{L1} & \cdots & M_{LC} \end{pmatrix} \quad (4)$$

- **Step 4** For each secret element M_{lc} of the matrix, the Dealer randomly generates a k degree polynomial according to Shamir's scheme:

$$f_{lc}\ (x) = \sum_{i=0}^{k-1} a_{i,lc} \cdot X^i\ (mod\ p) \quad (5)$$

  Where $a0,lc = M_{lc}$ and $a_{i,lc}$ with $1 \leq i \leq -1$ randomly chosen over $\mathbb{F}p$ to obtain a matrix of polynomials :

$$F = \begin{pmatrix} f_{11} & \cdots & f_{1C} \\ \vdots & \ddots & \vdots \\ f_{L1} & \cdots & f_{LC} \end{pmatrix} \tag{6}$$

- **Step 5** To compute the shares of each participant, the Dealer determines the polynomial image of each X_{lc}^{i} coordinate of Q_{lc}^{i} by the adequate polynomial F_{lc}, to generate n shares matrices I^{i} also called shadows:

$$I^{i} = \begin{pmatrix} f_{11}(X_{11}^{i}) & \cdots & f_{1C}(X_{1C}^{i}) \\ \vdots & \ddots & \vdots \\ f_{L1}(X_{L1}^{i}) & \cdots & f_{LC}(X_{LC}^{i}) \end{pmatrix} = \begin{pmatrix} I_{11}^{i} & \cdots & I_{1C}^{i} \\ \vdots & \ddots & \vdots \\ I_{L1}^{i} & \cdots & I_{LC}^{i} \end{pmatrix} \tag{7}$$

- **Step 6** Finally, the Dealer publishes a public key point R generated by ECDLP to exchange private points matrix:

$$R = r\ G\ (mod\ p)$$

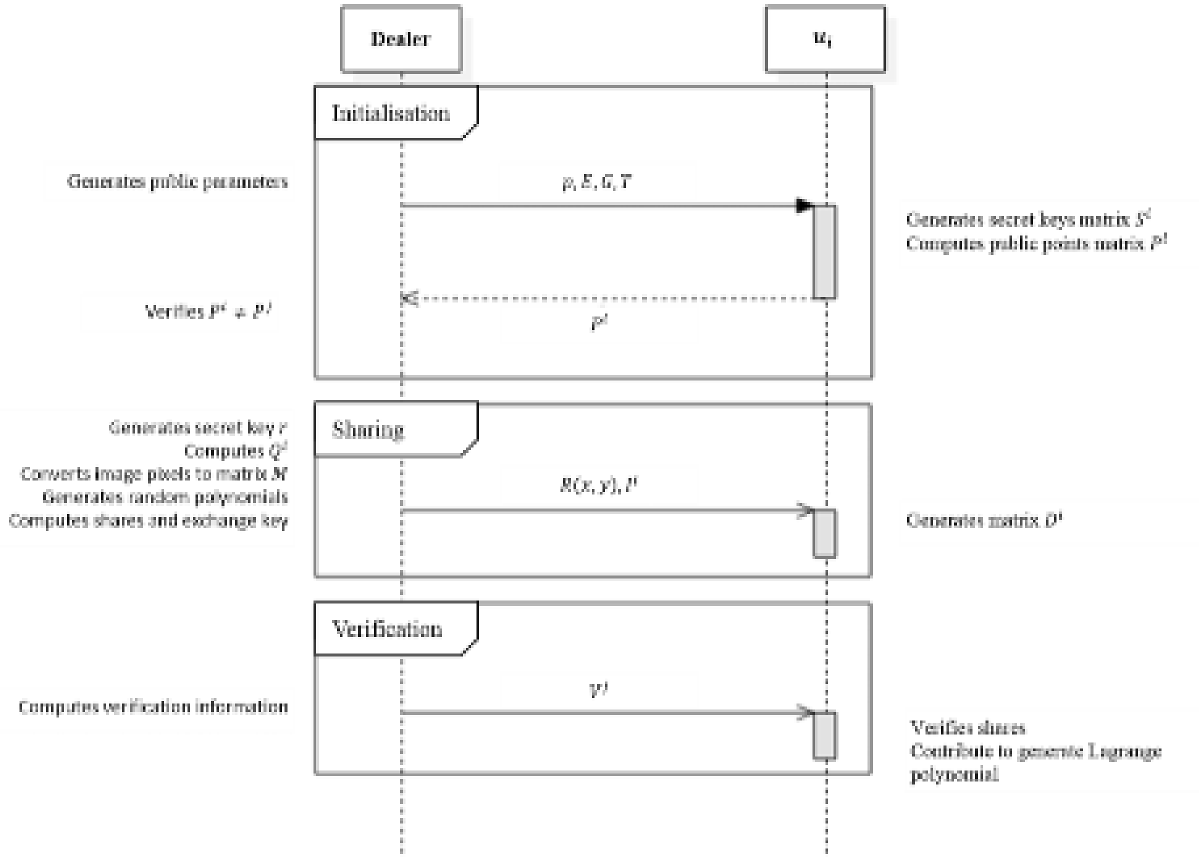
Dealer
u_i
Initialisation
Generates public parameters
p, E, G, T
Generates secret keys matrix S^i
Computes public points matrix P^i
Verifies $P^i \neq P^j$
P^i
Sharing
Generates secret key r
Computes Q^i
Converts image pixels to matrix M
Generates random polynomials
Computes shares and exchange key
$R(x, y), I^i$
Generates matrix D^i
Verification
Computes verification information
V^i
Verifies shares
Contribute to generate Lagrange polynomial

Figure 2. Approach sequence diagram

C. Secrets reconstitution

For secrets reconstruction, k participants uj are required to collaborate in order to construct Lagrange polynomial using Ii matrices and the public point R.

- **Step 1** At first, each candidate uj computes the matrix of points for interpolation using private keys matrix S^j.

$$D^j = S^j \cdot R = \begin{pmatrix} D^j_{11} & \cdots & D^j_{1C} \\ \vdots & \ddots & \vdots \\ D^j_{L1} & \cdots & D^j_{LC} \end{pmatrix} \tag{9}$$

- **Step 2** the Combiner construct a Lagrange polynomial for each secret of the matrix M using D^j_{lc}abscissa.

$$P_n(x) = \sum_{i=1}^{k} I^i_{lc} \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{(x - X^j_{lc})}{(X^i_{lc} - X^j_{lc})} \tag{10}$$

D. Non interactive verification of shares

In our approach, each candidate has independently the capability to verify the validity of his shadow at any time, even without collaborating to reconstruct the main secret matrix, using additional information computed by the Dealer and broadcasted to all participants.

According to every polynomial coefficient aj for each secret element M_{lc} with $0 \leq j \leq k - 1$, the Dealer computes with ECDLP k points v^j_{lc} :

$$v^j_{lc} = a^j_{lc} \text{ G (mod p)} \tag{11}$$

Then regroups all v^i_{lc}points corresponding to each secret in a matrix V^j, k matrices will be broadcasted:

$$V^j = \begin{pmatrix} v^i_{11} & \cdots & v^i_{1C} \\ \vdots & \ddots & \vdots \\ v^i_{L1} & \cdots & v^i_{LC} \end{pmatrix} \tag{12}$$

So, each candidate will be able to check the validity of his matrix shares by the formula:

$$I^i_{lc} \cdot G = \sum_{j=0}^{k-1} (X^i_{lc})^j \cdot v^j_{lc} \ (mod\ p) \tag{13}$$

If it returns true, the share is correct and can fit for the recovery formula. If not, the participant publishes a notification warning.

E. Correctness

In this subsection, we give the proofs to the correctness of key exchange equation for the sharing operation and the verification formula.

1. *Key exchange proof* : Candidate u_j computes at the beginning the public point P using his private key S by ECDLP (2) that he sends to the Dealer publicly, this last at his turn computes the private points Q also by ECDLP using his own private key r (3), which coordinates have been exploited in Shamir's polynomial (7).

$$Q_{lc}^{j} = r \cdot P_{lc}^{j} = r \cdot S_{lc}^{j} \cdot G = S_{lc}^{j} \cdot R = D_{lc}^{j} \tag{14}$$

so, $k$participant u_j can recover the secrets using matrices D^j (10) coordinates.

2. *Verification proof*: Any participant ui can verify the intercepted share by ECDLP according to the formula:

$$\begin{aligned} I_{lc}^{i} \cdot G = f_{lc}\left(X_{lc}^{i}\right) \cdot G \ (mod\ p) \\ = \left(\sum_{j=0}^{k-1} a_{j,lc} \cdot \left(X_{lc}^{i}\right)^{j} (mod\ p)\right) \cdot G \\ = \sum_{j=0}^{k-1} a_{j,lc} \cdot G \cdot \left(X_{lc}^{i}\right)^{j} (mod\ p) \\ = \sum_{j=0}^{k-1} v_{lc}^{j} \cdot \left(X_{lc}^{i}\right)^{j} (mod\ p) \end{aligned} \tag{15}$$

RESULTS AND DISCUSSION

In this section, we demonstrate the feasibility of the proposed method by exposing experimental results in timing, non-loss information after recovery and security efficiency.

A. Non-loss information

To prove the scheme efficiency with non-loss information, we tested it on a QR digital image of 33 × 33 px Figure 3, which gives after conversion a secret matrix of big values with the same size, each pixel (element of the matrix) is represented in the same bit length as the curve field chosen.

To ensure that the shadow does not reveal any information about the original secret, we present the greyscale histogram of both, the main image secret and the shadows Figure 4 were we can observe the distinction of frequencies for the same ranges. Results are obtained from a sharing with a threshold equal to 3 using a cryptographic elliptic curve over 192 bits prime field (NIST P-192). To prove the scheme validity, we use a QR code reader to extract the secret from the reconstructed image so we get the original plain text hidden inside.

B. Timing results

Table 2 represents the different timing measures computed during 4 tests to evaluate the performance of our application, incrementing each time the threshold value. From these results, we conclude that keys calculation and verification operations are computationally more expensive than Shamir's sharing and Lagrange interpolation algorithm, this is due to the complicated process of ECDLP with a large prime (192 bits) and for a matrix of 33 × 33 of big bit length values.

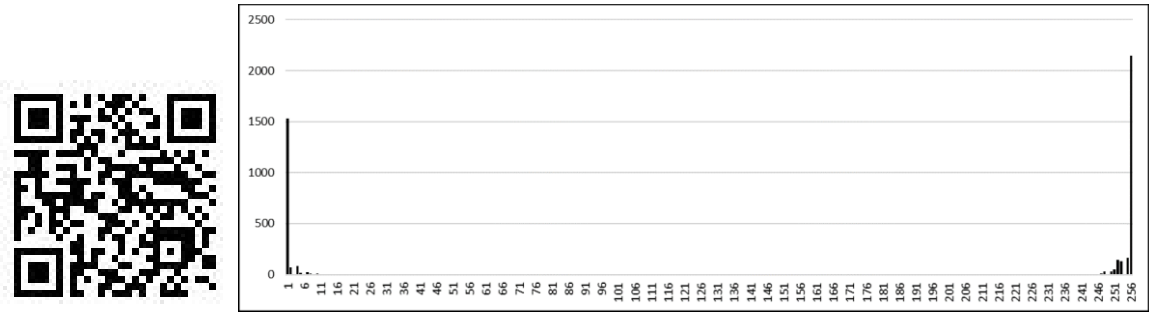

Figure 3. Original secret image shared and its histogram

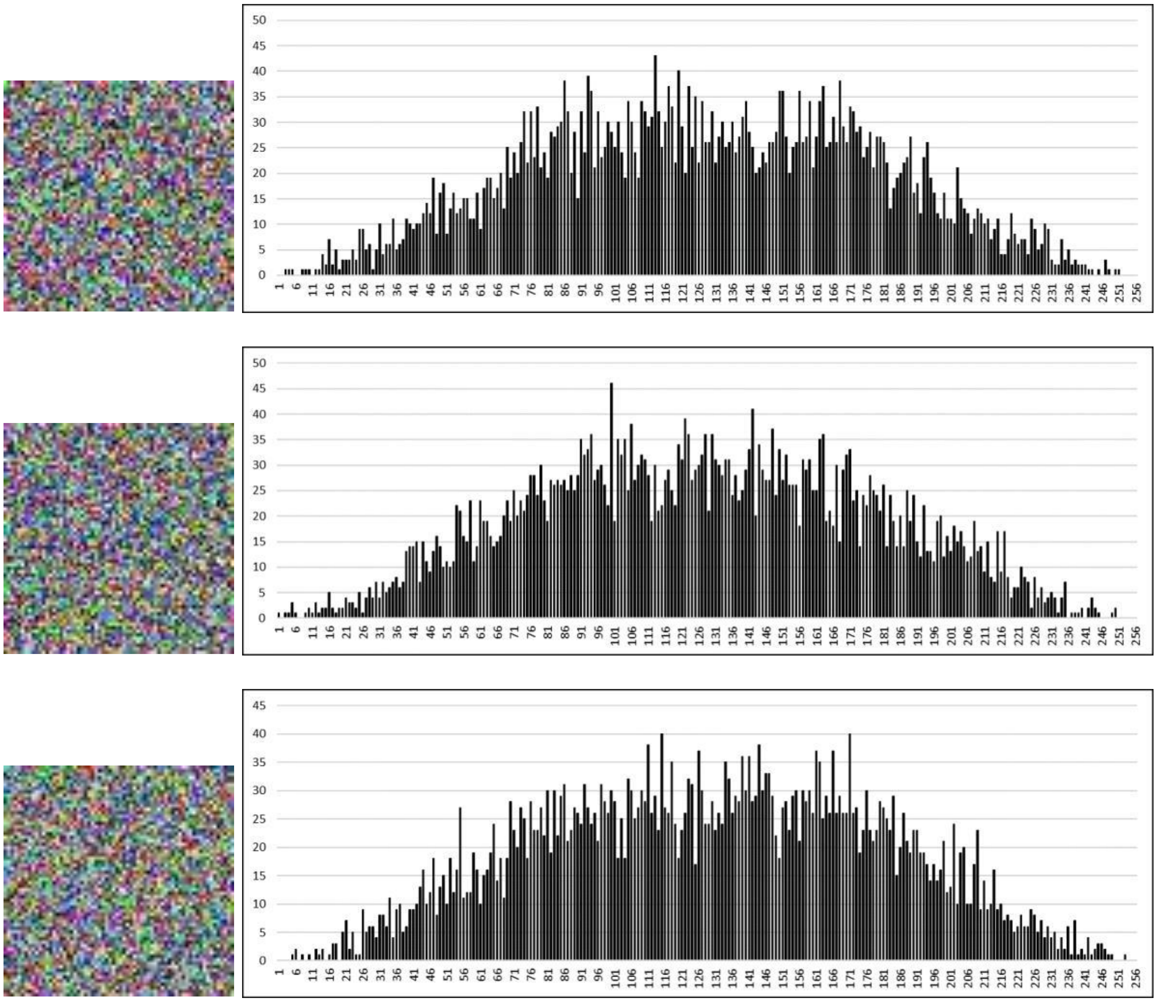

Figure 4. Shares (shadows) obtained and their histogram

Table 2. Proposed Scheme Timing Results in ms for 33×33 Matrix

Threshold	Average computations				Reconstitution
	Generation Verification information V	***Points matrices ECDLP***	***Shamir's sharing***	***Verification***	
2	8037	7022	4	19835	184
3	14514	7027	**13**	39775	312
4	21619	6923	15	65343	431
5	28266	7037	18	99543	635

Table 3. Performance and Security Comparison

Scheme	**Secure initial distribution keys**	**Secure combining channel**	**Share security**	**Malicious shares detection**	**Recovery type**
Proposed	On line and Not required (self-selecting sharing key)	Required	Secured (Meaningless)	Yes	Lossless
Dahshan & Irvine (2011)	Off line	Required	Secured (Refreshed))	Yes	Lossless
Kumar et al.	Not mentioned	Not mentioned	Secured	Yes	Lossless

(2017)			(Refreshed)		
Al-Adhami et al. (2016)	On line and Not required	Required	Secured (Encrypted)	Yes	Lossless
Nisha (2016)	On line and Not required (self-selecting sharing key)	Public (Double Knapsack)	Secured	Yes	Lossless

C. Security efficiency

From the shadows histogram, we conclude that the scheme is not sensitive to the threshold value, whether shares are generated with k = 2 or k = 5, we still obtain histograms with no information about the original image. Before talking about security aspect, we must elucidate an important notion about the proposed architecture. Communications with the Dealer does not require a high security channel, he is considered as the unique distant person possessing the secret, and all parameters sent or received by him are either public, broadcasted or transferred no plain information. On the other hand, contribution to reconstruct the secret requires a server combiner in a local network with high security channels.

In a secret sharing system, we have two categories of attacks, from outside or inside the system. For insider attacks, the scheme allows each candidate to verify the integrity of his shadow, even the combiner is in ability to verify shares of each one of them, which revealed any malicious information in the system. Intercepting the whole shadows requires an attacker knowing the exact timing of shares transmission, because participants are independent and there is no interaction between them. Hence, an intruder cannot reconstruct the secret even if he intercepts some shadows because he does not possess the secret keys.

D. Comparison

The proposed approach is compared in Table 3 with some typical existing works in term of performance and security. Moreover, in Table 4 we present a comparison with Dahshan & Irvine (2011) scheme in term of verification timing, since the structure of secrets in both works are similar. For e.g. the results of this test on an image size matrix 24 × 16px with a threshold of 5 participants and elliptic curve field of 192bits length are as follows; ECDLP matrix points computations are measured to an average of 2615ms, while the shadows matrix calculations run into just 4ms and for the recovery operation takes 385ms. For the verification we measure the timing of the matrices generation by the Dealer which runs in 10113ms, and the verifying operation by the candidates, whose average is equal to 35526ms, which is 2000ms less than Dahshan & Irvine (2011) scheme value for the same parameters.

CONCLUSION

In this paper, we proposed a verifiable image self-selecting secret sharing scheme for any server-client network like distributed systems, based on Shamir's secret sharing and ECDLP. The method takes as main parameters an image that represents our secret and an elliptic curve over a prime finite field. A threshold must also be specified, in order to recover the secret. The method allows also verification of shares validity. The non-loss information is proved by QR secret recovery and grey scale histogram shadows ensure the security efficiency of the sharing. Timing measures demonstrates the complexity of ECDLP algorithm. The results have been proved in comparison section. As a perspective, we propose to develop the scheme with more options like shares refreshing in order to decrease the time validity of each shadow.

Table 4. Verification Timing Comparison in ms

scheme	Matrix	Curve	Threshold	Verification
Dahshan & Irvine (2011)	24 × 16	192 bits	5	37380
		256 bits		67912
Proposed scheme	24 × 16	192 bits	5	35526
		256 bits		64271

References

Al-Adhami A, Ambroze M, Stengel I, and Tomlinson M. (2016). A Quorum System for Distributing RFID Tags. Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress, Toulouse, 2016, pp. 510-517.

Binu V P and Sreekumar A. (2017). Secure and Efficient Secret Sharing Scheme with General Access Structures Based on Elliptic Curve and Pairing. Wireless Personal Communications, 92, 1531--1543.

Blakley G R. (1979). Safeguarding cryptographic keys. Proceedings of the national computer conference, vol 1, pp. 313-317.

Caimei W A. (2009). Self-selecting Sub-secret Keys Sharing Scheme Based on Polynomials over Elliptic Curve. Fifth International Conference on Information Assurance and Security, Xi'an, pp. 734-737.

Dahshan H and Irvine J. (2011). An elliptic curve secret sharing key management scheme for mobile ad hoc networks. Security and Communication Networks, 1405-1419.

Errahmani H B and Faraoun K. (2018). Towards a Hybrid Approach Based on Elliptic Curves and Cellular Automata to Encrypt Images. Journal of Information Security Research.

Han Y A, Yang X, Sun J and Li D. (2003). Verifiable threshold cryptosystems based on elliptic curve. International Conference on Computer Networks and Mobile Computing, Shanghai, China, pp. 334-337.

Hua S A and Aimin W. (2010). A multi-secret sharing scheme with general access structures based on elliptic curve. 3rd International Conference on Advanced Computer Theory and Engineering, Chengdu, pp. V2-629-V2-632.

Kumar N C, Basit A, Singh P, and Venkaiah V C. (2017). Proactive secret sharing for long lived MANETs using Elliptic Curve Cryptography. International Conference on Inventive Computing and Informatics (ICICI), Coimbatore, pp. 312-316.

Nisha P D, Vyavahare P D, Panchal M. (2016). A Novel Verifiable Multi-Secret Sharing Scheme Based on Elliptic Curve Cryptography. The Tenth International Conference on Emerging Security Information, Systems and Technologies, pp. 230-234.

Pedersen T P. (1991). Distributed Provers with Applications to Undeniable Signatures. In: Davies D.W. (eds) Advances in Cryptology — EUROCRYPT ’91. EUROCRYPT 1991. Lecture Notes in Computer Science, vol 547. Springer, Berlin, Heidelberg.

Shamir A. (1979). How to share a secret. Communications of the ACM, 22(11), 612-613.