Extended Proactive Secret Sharing using Matrix Projection Method

Sonali Patil, Nikita Rana, Dhara Patel, Prajol Hodge

Abstract— Proactive Secret Sharing Scheme (PSSS) is a method to periodically renew n secret shares in a (k, n) threshold-based Secret Sharing Scheme without modifying the secret or reconstructing the secret to reproduce new shares. Given enough time, a hacker may be able to compromise enough shares (k or more) to gain the secret. PSSS is a scheme that allows generating new set of shares for the same secret from the old shares without reconstructing the secret. Using PSSS, all the shares are refreshed so that old shares become useless. Thus, an adversary has to gather at least k shares between two executions of PSSS. The secret remains confidential if fewer than k shares were compromised from the start of one PSSS to the end of the next PSSS. In this paper proactive secret sharing scheme for images is proposed based on matrix projection method. The proposed scheme provides the extended capabilities of enrolling and disenrolling of shareholders in the existing scheme. Also in the proposed scheme public information is shared with the participant's shares which makes the scheme more reliable.

Index Terms— Secret Sharing, Visual Cryptography, Proactive Secret Sharing, Extended Capabilities, Image processing

IJSER

1 Introduction

Secret Sharing Schemes (SSS) [1] refers to method for distributing a secret amongst a group of participants, each of whom is allocated a share of the secret.The first secret sharing scheme was proposed by shamir [2] in 1979. The secret can be reconstructed only when a sufficient number of shares are combined together; individual shares are of no use on their own. There are circumstances where an action is required to be executed by a group of people. For example, to transfer money from a bank a manager and a clerk need to cooperate. A ballistic missile should only be launched if three officers authorize the action. Schemes that have a group of participants that can recover a secret are known as Secret Sharing Schemes. Secret sharing has been an active research by mathematicians as object of intrinsic interest in their own right, cryptographers as important cryptographic primitives and security engineers as technique to employ in distributed security applications. There are various kinds of secret sharing schemes like threshold schemes, schemes with general access structure, verifiable secret sharing schemes, proactive secret sharing schemes etc. As per the need of an application the secret sharing scheme should provide the extended capabilities. Here we are focussing on proactive secret sharing:

1.1 Proactive Secret Sharing [3][4][5]

A well-known principle in the analog world is the term reduced trust, meaning that in order to keep a secret, the less knowledge or power each entity has the better. This is the basic philosophy.

The question whom to trust is fundamental for anybody in any situation, and becomes paramount when security is required. There are many examples when even well established trusted entities become malicious. The reasons can be different, but the result at the end is always the same: they are not trusted anymore. One known solution to overcome such a problem is instead of placing your trust just in one trusted party; distribute the trust among a group of entities, especially when the stakes are high. This should be done with the help of proactive secret sharing. It provides facility for Enrollment of shareholder, Disenrollment of Shareholder, Periodically Renewal of Shares to improve the security measures.

Consider the following problems:

- In some situations, there is usually one secret key that provides access to many important files. If such a key is lost (e.g., the person who knows the key becomes unavailable, or the computer which stores the key is destroyed), then all the important files become inaccessible. The question one may ask is how to back up secret information, so that it does not depend on one authority only.
- While performing the encryption procedure, a certain key needs to be stored; as we want to ensure that no single entity is entrusted with too much knowledge or power, the question now, is how to ensure that the key will not be exploited by the authority holding it.

The goal of the pro-active security scheme is to prevent the adversary from learning the secret or from destroying it, In particular any group of k non-faulty shareholders should be able to reconstruct the secret whenever it is necessary. The term proactive means the fact that it's not necessary for a violation of security to occur before secrets are refreshed, the refreshment is done periodically and hence, proactively.

1.2 Features of PSSS:

1. Enrolment of Shareholders: Enrollment of shareholder consist of adding a new person in the k trusted group of shareholders.
2. Disenrollment of Shareholders: Disenrollment of shareholder consist of removing a untrusted person from the k trusted group of shareholders to make secret more secure.
3. Periodically Renewal of Shares: The goal here is to renew the shares without the Dealer's involvement. (as the Dealer might not exist anymore). The shareholders should agree on a new polynomial with the same secret s without revealing the secret, the old polynomial or the new polynomial. At the end of this protocol, each shareholder will obtain a new share on

the new t-1 polynomial. The assumption in this protocol is that each shareholder remembers his/her old share.
4. Recover lost or corrupted shares: It recovers lost or corrupted shares without compromising the secrecy of the shares.

The rest of the paper is organized as follow. Section 2 contains literature survey of few proactive secret sharing schemes. Section 3 covers proposed proactive secret sharing schemes based on matrix projection method.It describes algorithms for added extended capabilities. Section 4 shows implementation results on proposed scheme. Finally in section 5, we summarize the proposed scheme based on algorithms and results.

2 Literature Survey

2.1Shamir's Secret Sharing Scheme

A PSSS based on Shamir [2] secret sharing scheme is explained in [1]. Shamir [7] developed the idea of a (k, n) threshold-based secret sharing technique (k ≤ n). The technique is to construct a polynomial function of order (k − 1) as,

f(x) = d_0+ d_1x + d_2 x^2 + … + d_(k-1) x^(k-1) (mod p),

where the value d_0 is the secret and p is a prime number. The secret shares are the pairs of values (xi, yi) where yi = f(xi), 1 ≤ i ≤ n and 0 < x1 < x2 …< xn ≤ p − 1. The polynomial function f(x) is destroyed after each server Pi possesses a pair of values (xi, yi) so that no single server knows what the secret value d_0 is. In fact, no groups of (k − 1) or fewer secret shares can be used to discover the secret d_0. On the other hand, when k or more secret shares are available, we can set up at least k equations yi = f(xi) with k unknown parameters di's. The unique solution d_0can be solved. Also, a Lagrange interpolation formula [6] is commonly used to solve the secret value d_0 as the following formula,

$$d_0 = \sum_{i=0}^{k} \left(\prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{-x_j}{x_i - x_j} \right) y_i \pmod p$$

where (xi, yj) are any k shares for 1 ≤ i ≤ k. Shamir's SSS is regarded as a perfect SSS because knowing (k − 1) linear equations cannot expose any information about the secret.

We assume an initial stage where a secret s is encoded into n shares using Shamir's secret sharing scheme. Each participant holds his/her share f(i) for some t-1 degree polynomial f(x). After the initialization, at the beginning of each time period, all honest servers/shareholders trigger an update phase in which the servers perform a share renewal protocol.
Each i'th shareholder receives the following shares: (including his own made share Pi(i)) and computes his/her new share by adding his old share- f(i) to the sum of the new n shares. Mathematically speaking:

$$h\ (i) = f\ (i) + \sum_{c=1}^{n} P_c\ (i)$$

2.2 Herzberg's [7] Proactive Secret Sharing scheme

Herzberg [8] proposed the PSS scheme based on the Shamir SSS [2] to address the problem of passive and active attacks. This method periodically renews the shares (without reconstructing the secret) so that it prevents an adversary from gaining the knowledge of the secret before it expires. To counter active adversary attacks, Herzberg et al. combined the ideas of the VSS technique to prevent dishonest participants (or compromised participants by active adversaries) from refusing to change the shares during the renewal process, or launch invalid secret shares.

To periodically update shares is an effective way to protect a secret from being revealed by adversary attacks. Herzberg et al. developed a PSS technique for the Shamir's method. When Shamir's SSS is initialised, at the beginning of every time period, all 'honest' servers can trigger an update phase in which the servers perform a share renewal protocol. The shares computed in period t are denoted by using the superscript t, i.e., (xi, f^t (x_i)), t = 0, 1, ... We know that the secret d_0 at time (t− 1) is,

d_0 = f^((t-1))(0).

The algorithm is to construct a new (k − 1) random polynomial function at each updating phase as,

δ(x) = a_0+ a_1x + a_2 x^2 + … + a_(k-1) x^(k-1) (mod p) (1)

where δ(0) = 0 so that f^t(0) = f^(t-1)(0) + δ(0) = d_0 + 0 = d_0.
Since the δ(x) function does not have a constant term, consequently, any group of k or more servers can still compute d_0 by contributing their new shares. However, a combination of k shares using past and present shares cannot be used to reconstruct the secret. As a result, the secret is protected from being revealed by the passive adversaries.

2.3 Proactive Secret Sharing Scheme using matrix projection [9]

Lie Bai [10] proposed a secret sharing scheme for images. Lie Bai and Zou [9] proposed a secret sharing scheme which supports proactive secret sharing with enrollment, disenrollment, and periodic renewal of shares. There is no need to expose the secret and other shares while providing a new share to new enrolled shareholder. Also he introduced a new, secure and distributed proactive secrete sharing scheme using the matrix projection method. This scheme is different than Hertzberg's scheme. After the shares are updated, any k shares of past and present shares cannot be used to reveal the secret matrix. This method looks after the protection against the passive attacks.
Some other methods are recently published for proactive secret sharing scheme[5] [11][12]. Bai developed a SSS using matrix projection. The idea is based upon the invariance property of matrix projection. This scheme can be used to share multiple secrets. Here, we briefly describe the procedure in two phases:

IJSER

1. Construction of Secret Shares From Secret Matrix S

1. Construct a random m × k matrix A of rank k where m > 2(k - 1) – 1.
2. Choose n linearly independent k×1 random vectors xi.
3. Calculate share vi = (A×xi) (mod p) for 1£ i £ n, where p is a prime number.
4. Compute $ = (A (A'A)-1A') (mod p).
5. Solve R = (S - $) (mod p).
6. Destroy matrix A, xi's, $, S, and
7. Distribute n shares vi to n participants and make matrix R publicly known.

2. Secret Reconstruction

1. Collect k shares from any k participants, say the shares are v1, v2, ..., vk and construct a matrix B =[v1 v2 . . . vk].
2. Calculate the projection matrix $ =(B (B'B)-1B') (mod p).
3. Compute the secret S = ($ + R (mod p)).

EXAMPLE [8]

To demonstrate the method, we show a simple (2, 4) threshold-based example with the prime modulus p = 19 and the secret matrix S,

$$S=\begin{bmatrix}10 & 12 & 4 & 7 & 8\\ 5 & 10 & 9 & 1 & 3\\ 3 & 2 & 1 & 11 & 14\\ 4 & 3 & 8 & 5 & 1\\ 2 & 4 & 2 & 3 & 10\end{bmatrix}$$

IJSER

To construct the shares, we choose a 4 × 2 random matrix A of rank 2 that

$$A=\begin{bmatrix}10 & 1\\ 7 & 2\\ 8 & 4\\ 1 & 1\\ 3 & 5\end{bmatrix}$$

The values of m = 5 and k = 2 satisfy the condition of secret sharing where m > 2k − 3. It is a necessary A Proactive Secret Sharing Scheme in matrix projection method condition for strong protection of the secret matrix S. Choose n = 4 linearly independent vectors as x1, x2, x3, x4

$$\begin{bmatrix}1\\ 17\end{bmatrix}\quad\begin{bmatrix}1\\ 7\end{bmatrix}\quad\begin{bmatrix}1\\ 1\end{bmatrix}\quad\begin{bmatrix}1\\ 9\end{bmatrix}$$

Next we compute vi = Axi for i = 1, 2, 3, 4,

$$v1=\begin{bmatrix}8\\ 3\\ 0\\ 18\\ 12\end{bmatrix}\quad v2=\begin{bmatrix}17\\ 2\\ 17\\ 8\\ 0\end{bmatrix}\quad v3=\begin{bmatrix}11\\ 9\\ 12\\ 2\\ 8\end{bmatrix}\quad v4=\begin{bmatrix}0\\ 6\\ 6\\ 10\\ 10\end{bmatrix}$$

The projection matrix $ is $ = (A (A'A)-1A') (mod 19).=

$$\$=\begin{bmatrix}8 & 8 & 5 & 1 & 14\\ 8 & 14 & 11 & 11 & 5\\ 5 & 11 & 2 & 13 & 14\\ 1 & 11 & 13 & 16 & 1\\ 14 & 5 & 14 & 1 & 0\end{bmatrix}$$

then the remainder matrix R is equal to R = (S – S) (mod 19) =

$$R=(S-\$)(\text{mod}19)=\begin{bmatrix}2 & 4 & 18 & 6 & 13\\ 16 & 15 & 17 & 9 & 17\\ 17 & 10 & 18 & 17 & 0\\ 3 & 11 & 14 & 8 & 0\\ 7 & 18 & 7 & 2 & 10\end{bmatrix}$$

The matrix R is made publicly known. We can destroy A, xi's, S and $, then we distribute four vi shares to our different servers in A. When any two servers' shares are chosen, they can form a matrix B. For example, these two shares are v1 and v2 to form the matrix B as

$$B=[v1\ \ v2]=\begin{bmatrix}8 & 17\\ 3 & 2\\ 0 & 17\\ 18 & 8\\ 12 & 0\end{bmatrix}$$

The projection matrix of B, $ is $ =(B (B'B)-1B') (mod 19)

$$\$=\begin{bmatrix}8 & 8 & 5 & 1 & 14\\ 8 & 14 & 11 & 11 & 5\\ 5 & 11 & 2 & 13 & 14\\ 1 & 11 & 13 & 16 & 1\\ 14 & 5 & 14 & 1 & 0\end{bmatrix}$$

We can validate that tr(S) (mod 19) = 40 (mod 19) = 2 = k. The secret matrix S is obtained by the remainder matrix R and the projection matrix $ as S = (R + $) (mod 19) =

$$S = \begin{bmatrix} 10 & 12 & 4 & 7 & 8 \\ 5 & 10 & 9 & 1 & 3 \\ 3 & 2 & 1 & 11 & 14 \\ 4 & 3 & 8 & 5 & 1 \\ 2 & 4 & 2 & 3 & 10 \end{bmatrix}$$

The reconstructed matrix is the same as the secret matrix, and the shares are 1/m of the size of the secret matrix (for our case, it is 1/5 because m = 5). This matrix projection method is not a perfect SSS, but it is a multiple-secret sharing scheme and has a strong protection on the secrets.

3 Proposed scheme

3.1 Image Secret Sharing

The proposed scheme is implemented to share the secret images. The [10] is modified using Thein and Lins [6] method to use for images. Thien and Lin [6] proposed a (k, n) threshold-based image SSS by cleverly using Shamir's SSS [2] to generate image shares. The essential idea is to use a polynomial function of order (k − 1) to construct n image shares from an l × l pixels secret image (denoted as I) as,

$$Sx(i, j) = I(ik + 1, j) + I(ik + 2, j)x \ldots +I(ik + k, j)x^{k-1} \pmod p$$

where 0 ≤ i ≤ (l/ k) and 1 ≤ j ≤ l. This method reduces the size of image shares to become 1/k of the size of the secret image. Any k image shares are able to reconstruct every pixel value in the secret image. An example of (2, 4) image secret share construction process where k = 2 and n = 4.According to the technique, a first order polynomial function can be created as,

$$Sx(i, j) = (110 + 112x) \pmod{251}$$

where 110 and 112 are the first two pixel values in the Lena image. For our four participants, we can randomly pick four x values, and substitute them into the polynomial function by setting p value to be 251 which is the largest prime number less than 255 (maximum gray image value). Four shares are computed as (1, 222), (2, 83), (3, 195) and (4, 56). They become the first pixel in four image shares. The second pixel is computed in the same manner by constructing another first order polynomial function using next two pixels in the Lena image. This process continues until all pixels are encoded. And the size of each image share is half (1/2) size of the original image. None of the image shares appear to reveal information about the secret image. However, the pixel values in a natural image are not random because the neighboring pixels often have equal or close values. It is evident that the first two pixel values (110 and 112) are very close to each other. That creates the possibility that one image secret share may be used to recover the secret image by assuming the neighboring pixels have the same values in the first order polynomial function.Since Thien and Lin's method reduces the size of image shares to become 1/k of the size of the secret image,.The matrix of pixel values of images is considered to be the secret and used for image secret sharing.

3.2 Enrolment of Shareholders

1. Store random m × k matrix A of rank k where m > 2(k - 1) – 1 in persistant memory which was generated at the time of construction of n shares.
2. Again choose one more linearly independent k×1 random vector xe.
3. Calculate share vi+1 = (A×xe) (mod p) , where p is a prime number.
4. Distribute newly generated shares vi+1 to n+1'th participant along with matrix R which is publicly known.

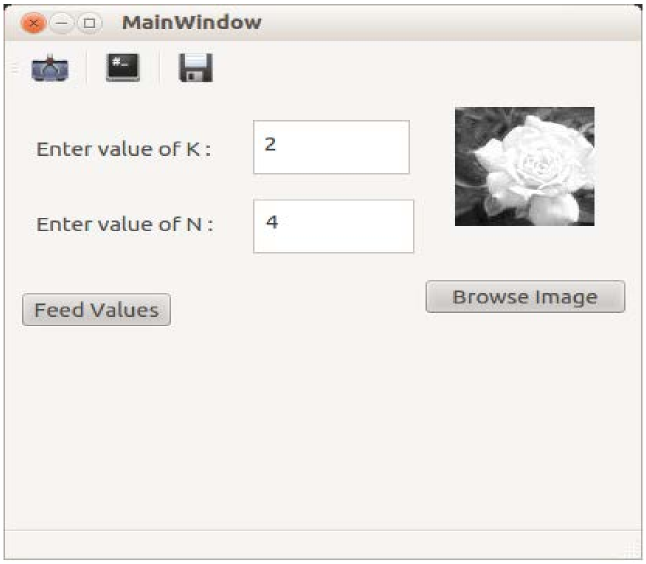
3.3 Disenrollment of Shareholders

The dealer will discard the share of shareholder who is not more trustworty by not considerng his/her share as a part of the seret sharing scheme.

3.4 Avoiding Single Point Failure

In the existing scheme the Remainder matrix R is made public. However, matrix R can become single-point-failure if it is corrupted or lost. To overcome this problem, the proposed method uses Thien and Lin's image SSS [9] to secretly share the matrix R as a Gi =g1(i),g2(i),….g(m/k)n (i) for g(i)t (j) = I(tk+1, j)+. . .+I(tk+k−1, j)rk−1t mod 251 where 1 ≤ t ≤[m/k] and 1 ≤ j ≤ m . Each image share Shi is the combination of vi and Gi.. (1)

4. Result

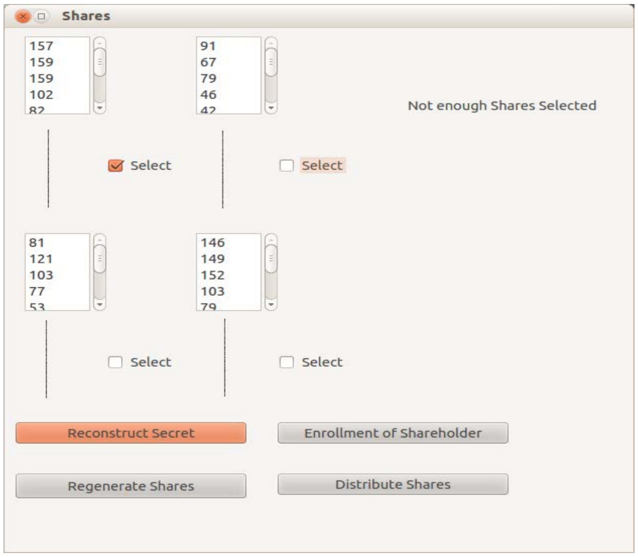


Enter value of K : 2

Enter value of N : 4

Fig1.Main Window (Input Window)

IJSER



157
159
159
102
82

91
67
79
46
42

Not enough Shares Selected

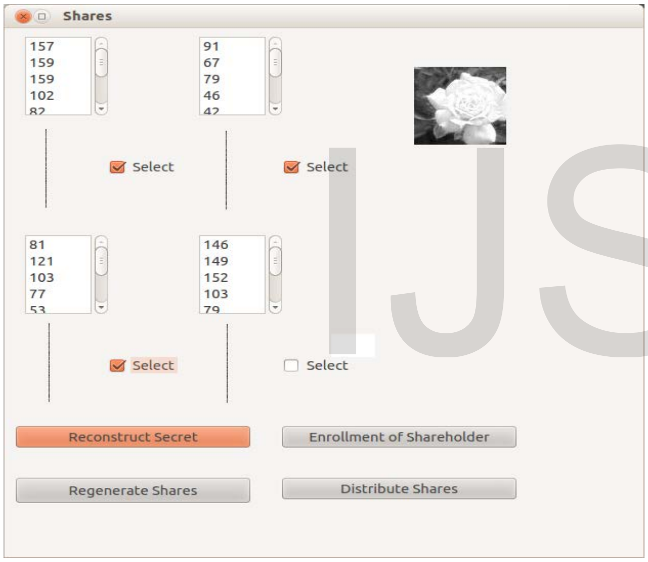
☑ Select ☐ Select

81
121
103
77
53

146
149
152
103
79

☐ Select ☐ Select

Fig2.Constructed Shares



157
159
159
102
82

91
67
79
46
42

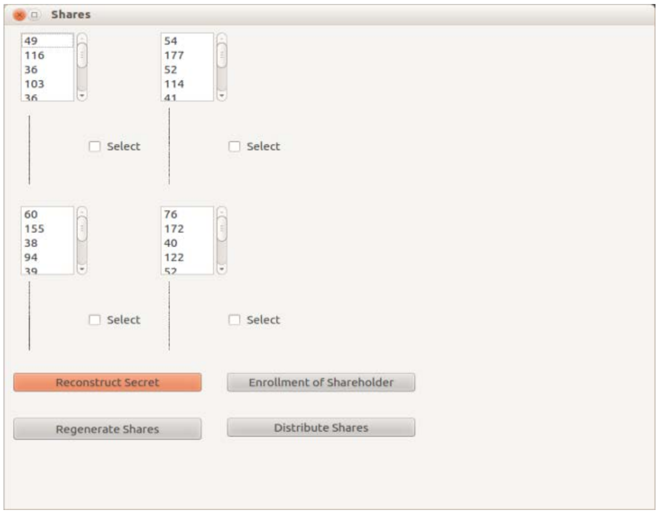
☑ Select ☑ Select

81
121
103
77
53

146
149
152
103
79

☑ Select ☐ Select

Fig3.Reconstructed Secret



49
116
36
103
36

54
177
52
114
41

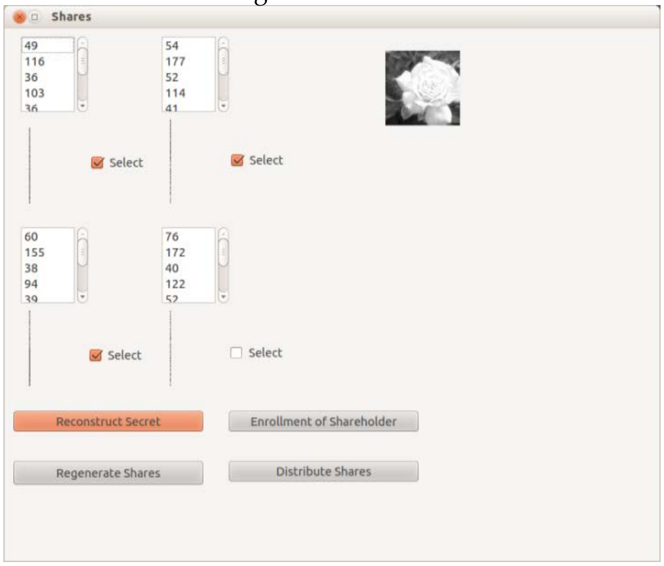
☐ Select ☐ Select

60
155
38
94
39

76
172
40
122
52

☐ Select ☐ Select

Fig4.Renewed Shares



49
116
36
103
36

54
177
52
114
41

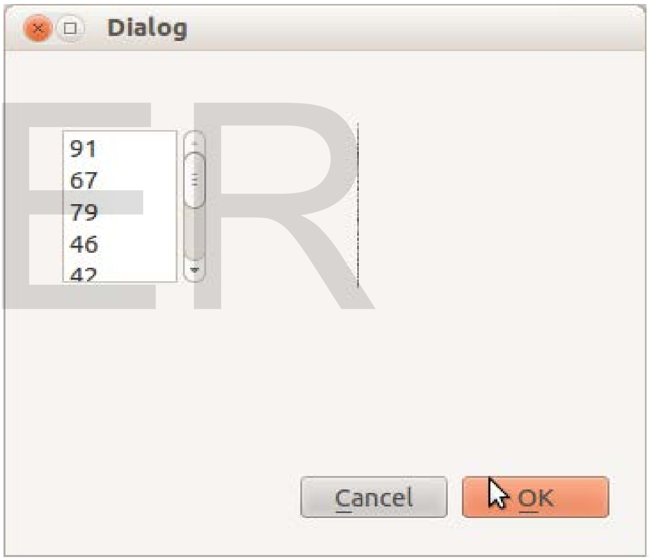
☑ Select ☑ Select

60
155
38
94
39

76
172
40
122
52

☑ Select ☐ Select

Fig5.Reconstructed Secret using Renewed shares



91
67
79
46
42

Fig6. Enrolled Dialog for new enrolled shareholder

IJSER

5. Conclusion

The proposed scheme is having strong mathematical base as it is based on matrix projection method. The proposed scheme is implemented to share the secret images. The scheme adds the extended capabilities like enrolling and dis-enrolling of the shareholders in the existing proactive secret sharing scheme. Also the public information is shared with the participants shares which makes the scheme more reliable. In future the scheme can be modified for better time complexity without Dealers interference and to handle active attacks in near future. Along with this cheater identification using verifiable secret sharing can be added in proactive secret sharing.

REFERENCES

[1] R. Stinson, “Cryptography: Theory and Practice”, CRC Press, Boca Raton 1995.

[2] Shamir, A., “How to Share a Secret”, Communications of the ACM, vol.22, no.11, 1979.

[3] Sonali Patil and Prashant Deshmukh. “An Explication of Multifarious Secret Sharing Schemes.” International Journal of Computer Applications 46(19):5-10, May 2012

[4] Sonali Patil. Nikita Rana. *Dhara Patel*. Prajol Hodge. “Analyzing Proactive *Secret Sharing* Schemes”, International Journal of Engineering Research & Technology (IJERT),ISSN: 2278-0181,Vol. 1 Issue 7, September – 2012.

[5] Sonali Patil, Prashant Deshmukh , “Analyzing Relation in Application Semantics and Extended Capabilities for Secret Sharing Schemes”, , International Journal of Computer Science Issues, IJCSI, Mauritious, Volume 9, Issue 3, May 2012.

[6] C.-C. Thien and J.-C. Lin, “Secret image sharing,” Computers & Graphics, vol. 26, no. 5, pp. 765–770, 2002.

[7] Ben-Or, M., Goldwasser, S. and Wigderson, A. (1988) ‘Completeness theorems for non-cryptographic faulttolerant distributed computation’, Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing, 2–4 May, Chicago, Illinois, pp.1–10.

[8] Herzberg, A., Jarecki, S., Krawczyk, H. and Yung, M. (1995) ‘Proactive secret sharing or: how to cope with perpetual leakage’, in Don Coppersmith (Ed.): Advances in Cryptology – Crypto ’95, August, Santa Barbara, CA, pp.339–352.

[9] Bai, L. and Zou, X. (2009), Proactive Secret Sharing Scheme in matrix projection method, Int. J. Security and Networks, Vol. 4, No. 4, pp.201–209.

[10] Lie Bai ,“A Reliable (k, n) Image Secret Sharing Scheme”, 2006

[11] Yike Yu “A Proactive Secret Sharing Scheme Based on Elliptic Curve Cryptography”, Education Technology and Computer Science, 2009. ETCS '09.

[12] Ling Ma, Inst. of Inf. Security & Secure Broadcasting & Telev., Commun. Univ. of China, Beijing, China Shouxun Liu ; Yongbin Wang ” A DRM model based on proactive secret sharing scheme for P2P networks” Cognitive Informatics (ICCI), 2010 9th IEEE International Conference

[13] Zhengjun Cao, Olivier Markowitch, “Two Optimum Secret Sharing Schemes Revisited”, International Seminar on Future Information Technology and Management Engineering, 2008 IEEE, p. 157-160.

Sonali Patil is pursuing PhD from Amravati University. Her research interest include Secret Sharing, Information Security. She has published several papers in good International Journals. Currently she is working as an Assistant Professor at Pimpri Chinchwad College of Engineering, Pune.

Nikita Rana has completed Diploma in Computer Engg from MSBTE. Currently pursuing Bachelors of Computer Engineering from Pune University

Dhara Patel has completed Diploma in Information Technology from MSBTE. Currently pursuing Bachelors of Computer Engineering from Pune University

Prajol Hodge currently pursuing Bachelors of Computer Engineering from Pune University

IJSER