Hindawi Publishing Corporation
Chinese Journal of Engineering
Volume 2014, Article ID 736750, 7 pages
http://dx.doi.org/10.1155/2014/736750

Research Article

SSDLP: Sharing Secret Data between Leader and Participant

Hazem Al-Najjar and Nadia Al-Rousan

College of Badr, Department of Computer, Taibah University, Medina, Saudi Arabia

Correspondence should be addressed to Hazem Al-Najjar; hazem_najjar@yahoo.com

Received 30 September 2013; Accepted 7 November 2013; Published 14 January 2014

Academic Editors: Z. Shi and S. Simani

This paper investigates the problem of sharing the secret document containing a secret data between leader and participant(s) depending on specific conditions and rules. The participant(s) can retrieve part of the secret document but will not be able to retrieve any secret data without the leader. At the same time, the leader may have a little information about the secret document but cannot retrieve the secret data and the secret document without cooperating with participant(s). To evaluate the proposed model and the system efficiency, four tests are suggested, which are concatenation and sharing data test, leader visual test, information entropy analysis, and correlation analysis. Results show that the proposed model is efficient in sharing the data between the leader and participant(s) and the model can achieve our concept of the data sharing between leader and participant(s). However, by analyzing the proposed model using numerical tests and visual tests, the results show that the visual tests will not give attackers useful information about the original data, while the numerical tests show that the entropy attacks are not possible and the correlation between the adjacent pixels will not give useful information. Finally, the results show that the proposed model is strong against different types of attacks.

1. Introduction

The secret sharing mechanism is a mechanism used in the large network to share the secret key between participants in the network, in which each participant has his own shadow. The purpose of secret sharing is to secure the key between different participants, to allow the authorized participants to retrieve the secret information, and to recover the secret key if some shadows are lost or distorted. Therefore, the key could be retrieved if and only if a specific number of participants collaborated together by using their shadows. In 1979, Shamir [1] and Blakley [2] introduced the prototype of the secret sharing named as (t, k)-threshold secret sharing system. The problem statement introduced by Shamir in his work is the following.

> *"Eleven scientists are working on a secret project. They wish to lockup the document in a cabinet so that the cabinet can be opened if and only if six or more of the scientists are present. What is the smallest number of locks needed? What is the smallest number of keys to the locks each scientist must carry?"*

In this paper, we try to reformulate the problem to a new problem called leader and participant sharing puzzle as follows.

Eleven scientists are working on a secret project containing a secret data. One of them is a team leader and the rest are the team members. They wish to lockup the document in a cabinet so that the cabinet can be opened if and only if at least one leader and five participants are present. At the same time, the team leader or any five members can retrieve part of the secret project but will never retrieve the secret data.

The dealer of this system has two parts of information: the secret document and the secret data in the document. The solution could be described as two-level cabinet, one for participants as a first level and another one for leader as a second level (one inside another one). The participants can access the first cabinet that contains partial document which describes part of the information not the whole information, where the leader cannot access either document or the secret

data but it may have a little information about the document. In addition, neither leader nor participant(s) will ever retrieve the secret data in the document alone. The participants need to collaborate with leader to retrieve the whole secret document and the secret data in the document and vice versa.

In this scheme, a dealer can encode and divide secret document into two parts: the participant part and the leade part. The dealer then distributes the k shadows of the participant part to the involved participants. So, any t out of k shadows authorized participants and, with the leader part, the document can be retrieved with the secret data.

The proposed system could be found in many of our social life. Assume that we have a store with two doors: iron door and glass door, one behind the other one. If we assume that the glass door is a leader and the iron door is a participant(s), then the leader and the participant(s) should be existing at the same time to open the two doors and to access the store resources. With only the participant(s) information, the participant(s) can see what is inside the store through the glass door and will not have a permission to access the store without the leader part, where the leader cannot access the whole information about the store and it may access a little information only.

The rest of this paper is organized as follows. Related work is discussed in Section 2. In Section 3, we explain our proposed model. The experiment results and discussion are shown in Section 4. Finally, our conclusions are drawn in Section 5.

2. Related Work

Many researchers in the data sharing field focused on sharing the secret images between the participants in the network [3–6]. As a second level of their research Naor and Shamir [3] introduced a new (t, k)-threshold visual secret sharing scheme, in which the image is encrypted into k transparencies called shares and at least t of k shares need to be collaborated together to retrieve or to decrypt the image. Thien and Lin [4] proposed a secret image sharing scheme. In the proposed scheme, a dealer generates n shadows from the secret image for all participants in the network. At least t of k participants can cooperate to recover the lossless secret image. Based on Thien and Lin's scheme, Wang and Shyu [5] introduced a scalable secret image sharing scheme that is depending on the priority of the participants. So, if the participant has his own permission to access the whole information at least t shadows will be given. If the participant has lower permission we can give him $t - 1$ shadows and at least he needs to cooperate with only one more participant to retrieve the data. The proposed system assumed three sharing modes, which are the multisecret, the priority, and the progressive modes, which allow the dealer to assign different priority shadows to the participants.

Lin and Chan [6] proposed a verifiable secret image sharing scheme to resist dishonest participants and to satisfy the requirements of lossless and camouflage. After running some experiments, the results indicate that the proposed scheme can share a large secret capacity according to the threshold t. Yang et al. [7] proposed a fast secret image sharing based on Haar wavelet transform and Shamir's method. The proposed model decreased the computation time for sharing and retrieving that data by reducing the secret image to its quarter size by using discrete Haar wavelet transform. Chang et al. [8] proposed a new lossless sharing method to share the image among different users on the network by adopting the Sudoku puzzle in generating the image shadows. Bhattacharjee et al. [9] proposed a simple secret image sharing scheme based on bitwise operations and by using matrix addition and subtraction processes to share generation and reconstruction processes, respectively. On another side, Anbarasi and Kannan [10] proposed reversible image sharing approach for color image that revealed the secret image without loss and preserved the cover image. After some experiments, the proposed model indicates that the generated shadows are meaningful with better PSNR value compared with the previous methods.

This paper aims to design a new concept in the data sharing by assuming two types of users: leader and participant. The dealer can share the secret document with the secret data between the participant(s) and the leader, in which the participant(s) can retrieve part of the secret document but will not be able to retrieve any secret data without the leader. At the same time, the leader may have a little information about the secret document but cannot retrieve the secret data and the secret document without cooperating with participant(s).

The following subsections are dedicated to explain Shamir's (t, k)-threshold sharing mechanism [1] and the finite field and the benefits of using the finite field in the hiding and sharing models.

2.1. Shamir Data Sharing (t, k). To share a secret s, a dealer determines a prime m and generates a $(t - 1)$-degree polynomial $F(x)$ as (1). Choosing any prime numbers will not always guarantee retrieving the $F(x)$ coefficients, so we need to specify a monic irreducible (primitive) polynomial of degree n for calculations in GF (2^n) as shown in [1, 11]. Consider

$$P(X) = \left(s + a_1 x + \cdots + a_{t-1} x^{t-1}\right), \tag{1}$$

$$F(x) = P(x) \bmod m. \tag{2}$$

The coefficients $a_1, a_2, \ldots, a_{t-1}$ are integer numbers within $[0, m - 1]$. The dealer then can derive k shadows by substituting the x numbers in (2). Then the shadows will be distributed to the involved participants. At least t participants should collaborate to retrieve the secret data by using the langrage interpolation polynomial in finite field. On the other hand, if the calculations are not in the finite field, the participants will not always guarantee to retrieve all coefficients of the $F(x)$, since the calculations in the standard arithmetic could find more than one solution for $P(x)$, whereas if the calculations are in the finite field only one solution of $P(x)$ could be found [11].

The irreducible polynomial could be found for most degrees. For example, there are eight different irreducible polynomials of degree 8. In Table 1, all the primitive polynomials from 2 up to 8 degree are listed.

(a) (b)

(c) (d)

Figure 1: The four 256 × 256 test images: (a) peppers; (b) montage, (c) Lena, and (d) cameraman.

Table 1: The possible primitive polynomials for different degrees.

n degree	Primitive polynomial
2	7
3	11
4	19
5	37, 61, 55
6	67, 103, 109
7	137, 143, 157, 247, 191, 213, 131, 203, 229
8	285, 361, 487, 299, 357, 351, 451, 355

2.2. Data Hiding. The secret data would be hidden within the sharing data by using the secret data as a coefficients of the (t, k) model instead of the random numbers. So, the dealer will create shadows using the secret data and send each shadow to the corresponding participant. Only k participants or more could collaborate to retrieve the hiding data using the langrage interpolation. Moreover, if the calculations are in the simple arithmetic the retrieving will not always grantee to retrieve the secret data since different solutions could be found for $P(x)$, whereas in the case of finite field using the primitive polynomial will retrieve only one solution for $P(x)$ [11].

3. Proposed Model

In this section, the proposed sharing model and retrieving model will be discussed, in which the sharing model is divided into three core phases, which are startup phase; to create a leader and the participant, hiding phase to hide the secret data within the participant data, and sharing phase to share the participant data between the participants, where, to retrieve the original data and the secret information, the reverse calculations will be applied.

3.1. Proposed Sharing Model. The proposed sharing model is divided into three phases which are startup, hiding, and sharing phases as shown in the detailed subsections.

3.1.1. Startup Phase. The original data will be divided into two parts: leader part and participant part, in which the generated parts have smaller size than the original data and could describe part of the original data. The proposed model will divide the original data using the following:

$$\text{Participant} = \frac{\text{Data}}{16}, \tag{3}$$

$$\text{Leader} = \text{Data mod } 16. \tag{4}$$

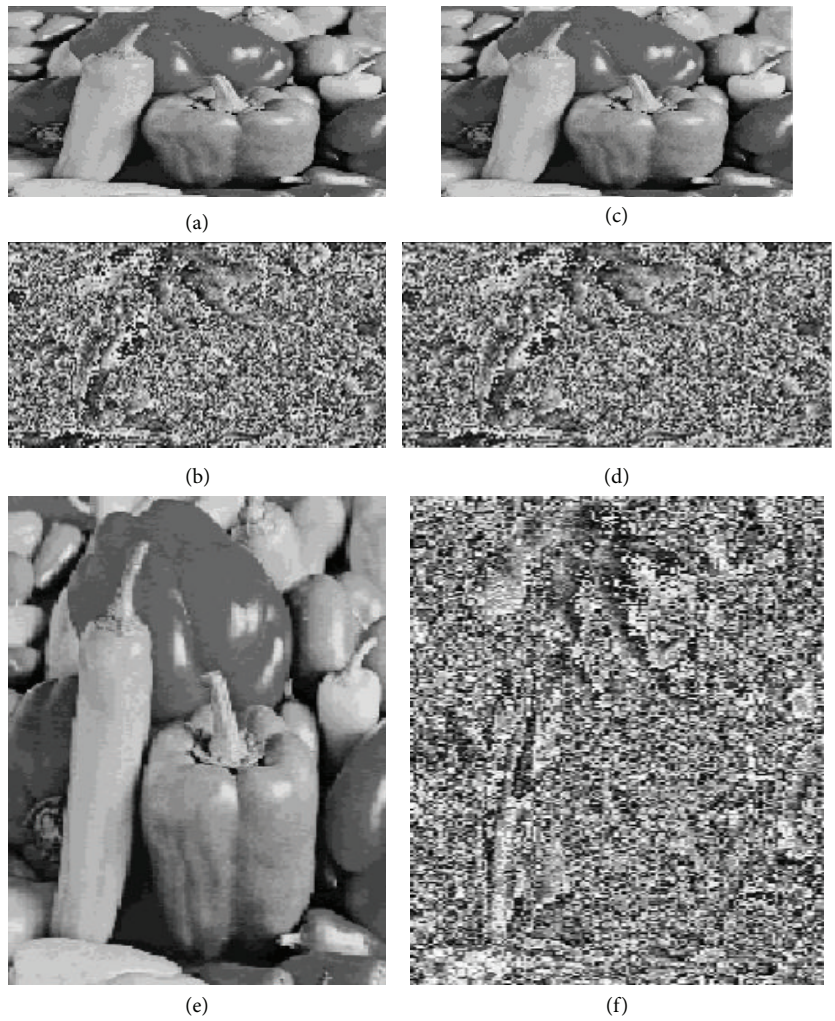

Figure 2: Peppers image using the proposed model.

The participant and the leader parts have the same size of the original image, where each block contains 4 bits only. Therefore, each adjacent block will be concatenated to create one block with 8 bits each as shown in (5). The concatenation will be within the same row or column or diagonal adjacent. Each type of concatenation will create new image characteristics:

$$\begin{aligned} \text{Participant}_C &= +_{\text{Type},2}\ \text{Participant}, \\ \text{Leader}_C &= +_{\text{Type},2}\ \text{Leader}, \end{aligned} \tag{5}$$

where + means the concatenation between adjacent blocks, type = {row, column, diagonal} adjacent, and 2 is the number of concatenated blocks within the same type. Assume that the size of the original data is equal to $M \times N$, so, by using three types: row, column, and diagonal adjacent, the data size will be $M \times N/2$, $M/2 \times N$, and $M/2 \times N$, respectively.

3.1.2. Data Hiding Phase. Before sharing the secret data, a linear independence relationship between the leader and the secret data will be created. The simple method to create a linear independence relationship is to use XOR operation between two sides as shown in the following:

$$\begin{aligned} \text{Sec}_L &= \text{Sec} \oplus \text{Leader}_C, \\ \text{Leader}_S &= \text{Leader}_C \oplus \text{Participant}_C. \end{aligned} \tag{6}$$

Creating the linear independence between the participant and leader and between secret data and leader will increase the randomness of the transmitted data, which will add a new protection level on the transmitted data. Moreover, the modified secret data (Sec_L) will use a Shamir model to hide the data as shown in the next phase.

3.1.3. Sharing Phase. The dealer will share the two parts: leader and participant, to the corresponding users on the network. The leader data will be transmitted to the leader using different media: CD, video tape, USB flash, and so forth, where the participant data will be shared using the Shamir

model in (7) by considering the (2, k)-threshold model. Consider

$$\begin{aligned}&\text{Participant}_S(x)\\&= \text{Participant}_C + \text{Sec}_L x \,(\text{mod } 285) \quad \text{in the GF}\left(2^8\right),\end{aligned} \tag{7}$$

where all the calculations will be in the finite field 2 with the degree 8 GF (2^8). In this model, the primitive polynomial (285) for the 8 bits data is used. Moreover, to retrieve the participant data at least two participants need to be collaborated with each other.

Lemma 1. *The dealer can share the original data between the users by using (t, k) threshold in a finite field by choosing one of the primitive polynomials [11].*

Proof. The dealer can divide the data into two parts using (3)–(6); then the participant part can be shared between the participants using the Shamir model in the finite field by using one of the primitive polynomials in the GF [11]. □

3.2. Retrieving Model. The original data will be retrieved by using the reverse order of the sharing process. So, the leader and the participant need to be collaborated with each other to retrieve the data and the secret information. First, the participants need to be collaborated with each other to retrieve the participant part by using the langrage interpolation in a finite field. Afterwards, the leader and the participant will be collaborated with each other to retrieve the secret data and the original data using (8)–(12). The sharing participant part (Participant_C) and the sharing leader part will be used to solve the linear independence relationship and to retrieve the original leader part (Leader_C) in (8) and to retrieve the secret data in (9). Moreover, to retrieve the original data the splitting method for the leader and the participant parts will be used to retrieve the original image size depending on the type of concatenation in (10) and (11). Finally, the participant and the leader will be combined in (12) to retrieve the original data:

$$\text{Leader}_C = \text{Leader}_S \oplus \text{Participant}_C, \tag{8}$$

$$\text{Sec} = \text{Sec}_L \oplus \text{Leader}_C, \tag{9}$$

$$\text{Participant} = \text{Splitting}_{\text{type},2}\text{Participant}_C, \tag{10}$$

$$\text{Leader} = \text{Splitting}_{\text{type},2}\text{Leader}_C, \tag{11}$$

$$\text{Image} = 16 * \text{Participant} + \text{Leader}. \tag{12}$$

All the calculations in (8)–(12) will be in the normal arithmetic and only the participants will use the calculations in the finite field to retrieve the participant part.

Lemma 2. *The participants can retrieve part of the original data using the langrage interpolation in the finite field [11].*

Proof. The data is divided into two parts: participant and leader; since the participant will use (3), only part of the original data will be described. To share the participant part the dealerwill use (7), and the participant will use the langrage interpolation in GF (2^8) to retrieve the original coefficients and participant part as shown by authors in [11]. □

Lemma 3. *The participant can retrieve the original data and the secret data if and only if leader and participant are used.*

Proof. The linear independence relationship between the leader and the participant and between the leader and the secret data can be solved only if the two parts are used. So, the participant will not be able to retrieve the original data and the secret data without other parts from another side. □

Theorem 4. *The participant can retrieve the original data and the secret data using the langrage interpolation in the finite field if and only if leader data is used.*

Proof. Proofed in the above discussion. □

4. Experimental Results and Analysis

To evaluate the performance of the proposed model different types of images are used. Figure 1 shows grayscale test images with 256 × 256 pixels.

4.1. Concatenation and Sharing Data Test. Due to the page limit, the peppers image is used only in this test. Using the proposed model, the data will be divided into two parts: leader and participant. The leader part will be sent to the desired person using any media such as CD, video tape, and internet, where the participant part will be shared between the participants on the network. Figures 2(a), 2(b), 2(c), 2(d), 2(e), and 2(f) show the participant part and leader part for the peppers image using different concatenation types: row, column, and diagonal, respectively. The resulted participant images will be sent to the participants using (2) (Figure 3), where the primitive polynomial is equal to 285 and the concentration type is the row concentration. The results show that the images are not visually meaningful to the users on the network.

4.2. Leader Visual Test. The visual test is used to validate if the leader part will give any useful information about the original image. In this test, four images are used: peppers, Lena, montage, and cameraman with row concatenation type. To increase a randomization in the image, we can use a random concatenation or a distance concatenation (using the faraway rows) instead of the three mentioned methods. The Figures (Figures 4 and 2(f)) are partially useful for the user but they may give little information about the original images. Overall, the leader image will not be useful to retrieve the original image completely and the secret data.

4.3. Information Entropy Analysis. The entropy could be defined depending on the field of science. In the data transmission and information theory, the entropy is defined as a measure of the loss of information in a transmitted signal, whereas, in the statistical mechanics, it is defined as a measure of the randomness of the microscopic constituents of a

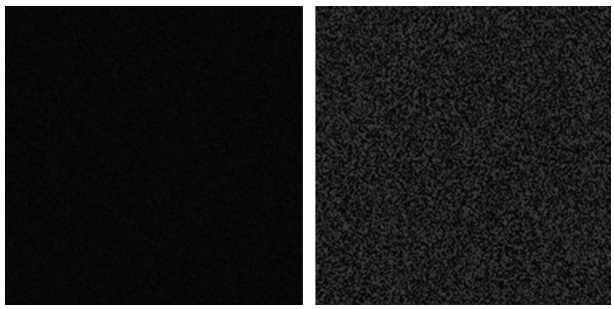

Figure 3: Two shares for the participant part using (2).

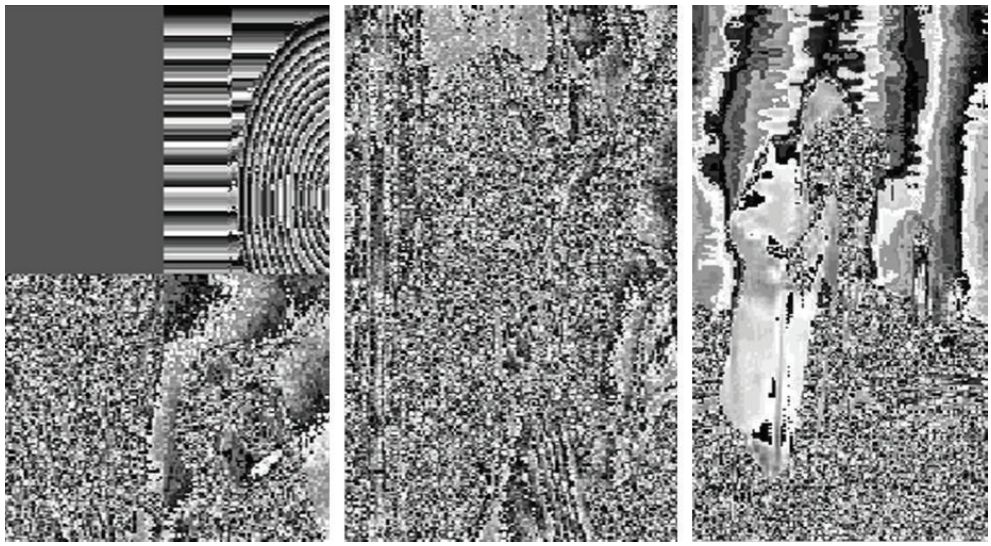

Figure 4: Leader visual test.

thermodynamic system. In this part, we are interested in the randomness of leader and participant images, where the true random variable should generate 2^8 symbols with equal probability and the entropy value equals 8. To check the randomness of the image the following is used:

$$H(s) = \sum_{s} P(S_i) \log \frac{1}{P(S_i)}, \tag{13}$$

where $P(S_i)$ represents the probability of symbol S_i; in our tests the average entropy of the leader images (Table 2) for Lena, peppers, and cameraman are close to the optimal value, so the entropy attack is not possible. Where the average entropy for montage image, indicates that the result is not randomized properly compared with the previous tested images.

In Table 3 the participant's entropy is shown, in which the results indicate that the pixels have a lower entropy compared with the original data.

4.4. Correlation Analysis. It is known that some algorithms were broken by using correlations analysis between the adjacent pixels, so the correlation coefficient will be calculated for all possible cases. To find a correlation between the adjacent pixels the correlation coefficient is calculated by using the following formula:

Table 2: The information entropy for the leader part.

Image	Leader_R	Leader_C	Leader_D	Average
Lena	7.9592	7.9202	7.9646	*7.9480*
Peppers	7.9349	7.9045	7.9483	*7.9292*
Montage	6.4283	6.5454	6.7207	*6.5648*
Cameraman	7.2078	7.2691	7.4107	*7.2959*

$$r = \frac{\text{Cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}},$$

$$D(x) = \frac{1}{M}\sum_{i=1}^{M}(x - \overline{x})^2, \tag{14}$$

$$\text{Con}(x, y) = \frac{1}{M}\sum_{i=1}^{M}(x - \overline{x})(y - \overline{y}),$$

where M is the total number of randomized pairs and x and y are the two vectors that contain x values and y values of the pair in the tested image, respectively.

Table 3: The information entropy for the participant part.

Image	$Part_R$	$Part_C$	$Part_D$	Average
Lena	5.3331	5.0588	5.4728	*5.2882*
Peppers	5.2263	5.1187	5.4652	*5.2701*
Montage	4.5669	4.4087	4.8000	*4.5919*
Cameraman	4.4983	4.4841	4.7128	*4.5651*

Table 4: Correlation coefficients of adjacent pixels.

Name	Leader	Vertical	Horizontal	Diagonal
Lena (0.9060–0.9609)	Row	0.1855	0.1482	0.0986
	Column	0.1215	0.1183	0.0717
	Diagonal	0.0702	0.0908	0.0959
Montage (0.9069–0.9737)	Row	0.4253	0.2808	0.2561
	Column	0.3141	0.4792	0.2476
	Diagonal	0.2443	0.4286	0.1823
Cameraman (0.9198–0.9535)	Row	0.4947	0.4531	0.4145
	Column	0.4536	0.5314	0.4856
	Diagonal	0.4726	0.5007	0.4522
Peppers (0.9147–0.9567)	Row	0.1612	0.1404	0.0793
	Column	0.1757	0.1702	0.0399
	Diagonal	0.0604	0.2041	0.1352

Table 4 shows the correlation coefficients between two adjacent pixels of the leader part using row, column, and diagonal concatenation in all possible cases which are vertically, horizontally, and diagonally adjacent. The test used four images: Lena, montage, cameraman, and peppers, to show the improvement on the correlation coefficients of each image. The correlation coefficients are written below each image name as a range between the smallest value and the largest value. The results revealed that using the correlation coefficients on the leader image is not helpful and our proposed method randomized the pixels in a very efficient way.

5. Conclusion

This paper addressed the problem of leader and participant sharing puzzle. The puzzle defined how the leader and the participant(s) can share the secret information with the secret data on the network. The puzzle assumes the following conditions to share the data: the participant(s) can retrieve part of the secret document but will not be able to retrieve any secret data without the leader. At the same time, the leader may have a little information about the secret document but cannot retrieve the secret data and the secret document without cooperating with participant(s).

After evaluating the proposed system by using four tests which are concatenation and sharing data test, leader visual test, information entropy analysis, and correlation analysis, the results indicate that proposed model is efficient in sharing the data between the leader and the participant(s). However, after analyzing the proposed model using numerical tests and visual tests, the tests indicate that the proposed model is strong against different types of attacks and useful to be used on the internet. Finally, in our future work we will address the problem of multilevel leaders that applied in the huge networks.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[2] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of the AFIPS National Computer Conference (NCC '79)*, vol. 48, pp. 313–317, 1979.

[3] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology—Eurocrypt*, vol. 94, pp. 1–12, Springer, Berlin, Germany, 2005.

[4] C.-C. Thien and J.-C. Lin, "Secret image sharing," *Computers and Graphics*, vol. 26, no. 5, pp. 765–770, 2002.

[5] R.-Z. Wang and S.-J. Shyu, "Scalable secret image sharing," *Signal Processing*, vol. 22, no. 4, pp. 363–373, 2007.

[6] P.-Y. Lin and C.-S. Chan, "A verifiable and recoverable secret image sharing mechanism," in *Proceedings of the 9th IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA '11)*, pp. 288–293, May 2011.

[7] C.-H. T. Yang, Y.-H. Huang, and J.-H. Syue, "Reversible secret image sharing based on Shamir's scheme with discrete haar wavelet transform," in *Proceedings of the 2nd Annual Conference on Electrical and Control Engineering (ICECE '11)*, pp. 1250–1253, September 2011.

[8] C.-C. Chang, P.-Y. Lin, Z. H. Wang, and M. C. Li, "A sudoku-based secret image sharing scheme with reversibility," *Journal of Communications*, vol. 5, no. 1, pp. 5–12, 2010.

[9] T. Bhattacharjee, J. P. Singh, and A. Nag, "A lossless secret Image sharing scheme based on pixel partitioning," *International Journal of Electronics Communication and Computer Technology*, vol. 2, no. 1, 2012.

[10] L. Jani Anbarasi and S. Kannan, "Secured secret color image sharing with steganography," in *Proceedings of the IEEE International Conference on Recent Trends in Information Technology (ICRTIT '12)*, pp. 44–48, 2012.

[11] M. Huang and V. Rego, "Polynomial evaluation in secret sharing schemes," https://www.cs.purdue.edu/research/PaCS/polyeval.