Iranian Journal of Operations Research
Vol. 13, No. 1, 2022, pp. 149-163

Establishing secure communication based on the design of a visual secret sharing scheme

A. Salehi, N. Javadian[1,*]

***T**oday, a high volume of multimedia information is transmitted in computer networks, such as the internet, that the requirement for achieving high security level against unauthorized access. the visual secret sharing scheme is a cryptographic system without requiring a secret key that is able to encrypt information in a multi - user computer network. in this research, a visual secret sharing scheme including two strategies for binary communications and multiple relationships were considered. in binary communications, an entity plays a role in the role of the server and an entity in the role of the client 's service in this strategy using a network - based visual secret sharing scheme (2 , 2) a secure approach to establish double relations where the provider entity is sending confidential information after authentication of the client 's service. then, two main phases of registration and verification are performed on the basis of the visual secret sharing scheme based on random networks. in tuple communication (n , n) an entity plays a role in the role of the server and several entities in the role of the service, and then two main phases of registration and verification are executed.*

***Keywords**: security, communication, computer networks, visual secret sharing, random networks.*

Manuscript was received on 07/03/2023, revised on 03/14/2023 and accepted for publication on 04/01/2023.

1. Introduction

How to solve the security problem in the process of information transmission has become an important challenge. Image encryption is one of the important means to ensure the security and confidentiality of image information.the visual secret sharing scheme is designed to design a non - key encryption system for use in multi - user computer networks [1]. Secret Sharing (SS) is considered to be one of the most important primitives for protecting confidentiality of multimedia data. Image encryption is an effective method to protect private images by converting them into meaningless. the visual secret sharing scheme is specifically used to encrypt digital images [2]. in this technique, a digital image is partitioned into a number of different contributions during the implementation of the encryption operation. each share of the generated share does not provide information from the main image. during the decoding operations, the main image can be reconstructed by having the share of them. in figure 1, the encryption process is shown schematically, in figure 2, the process of decoding the visual secret sharing scheme.

[1] Department of Industrial Engineering, Mazandaran University of Science & Technology, Babol, Iran, Email: nijavadian@ustmb.ac.ir..

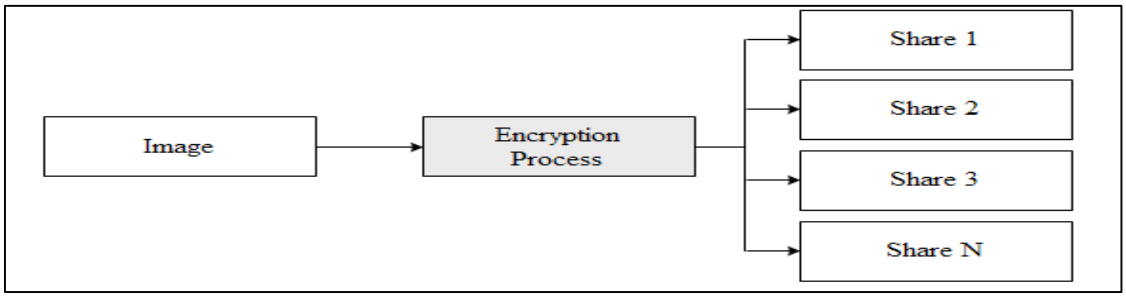

Fig. 1. the process of encryption scheme of visual secret [3]

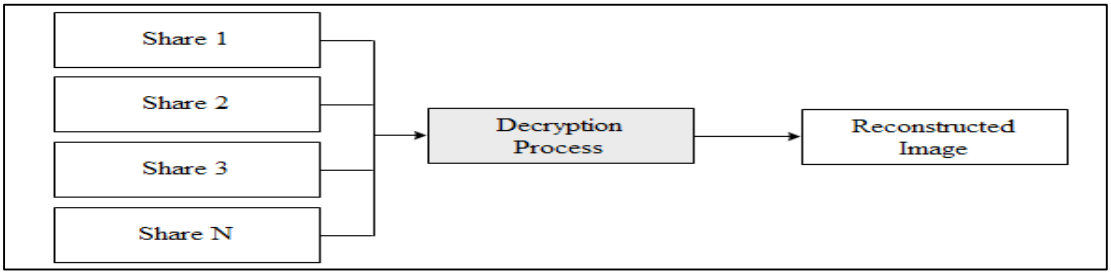

Fig. 2. the decoding process of the visual secret sharing scheme [3]

In general, the visual secret sharing scheme is partitioned into two categories of random networks and visual cryptography [4]. in the visual secret sharing scheme, we need a book to perform encryption operations required to perform encryption operations. however, in scheme of visual secret sharing scheme based on random networks in order to perform encryption operations, no code is required. also, in the visual secret sharing scheme, there is a problem for the spread of pixels, but in the visual secret sharing scheme based on random networks there is no problem to spread the pixels. therefore, a visual secret sharing scheme based on random networks has better performance than the visual secret sharing scheme because of the lack of instruction manual and lack of difficulty in creating the pixels. the only common point is the visual secret sharing scheme based on visual cryptography and the visual secret sharing scheme based on random networks that do not require a secret key to perform encryption and decryption operations. in this research, the scheme of visual secret sharing based on random networks has been considered in order to establish secure communications. in the proposed method, a visual secret sharing scheme based on random networks is used to share the different share of users in order to secure connections in computer networks. In the proposed method, the problem of key management is missing because the visual secret sharing scheme based on random networks is a cryptographic system without requiring a secret key.

2. Research assumptions

Primary and primary answers to research questions are called research hypotheses. according to the questions, the research hypotheses are stated as follows. the validity of the research hypotheses must be examined on the basis of the evaluations done.

- **I**n the visual secret sharing scheme based on random networks, the generated share of the security level is high.
- **I**n the visual secret sharing scheme based on random networks, the reconstructed image is of high visual quality.

3. Design of the proposed method

In order to design the proposed method, two strategies are considered. in the first strategy, binary

communications are considered as the main constraints and in the second strategy, multiple connections are considered as the main components .in the first strategy, double communication is considered in computer networks. in this strategy, using scheme based on random networks, a secure approach is designed to establish double relations. in the registration phase, the entity 's existence must be identified by the provider entity and receive a security code. for this purpose, first, the entity 's entity is sending a request message to the provider entity. then, the server entity of a binary image is randomly selected from the data pool.

Algorithm 5

// Encryption Process

1. Generate R_1 as a random grid, $T(R_1)= {}^1/_2$
   for (each pixel $R_1[i,j]$, $1 \le i \le w$, $1 \le j \le h$) do
   $R_1[i,j]$= random_pixel(0,1)
2. for (each pixel $B[i,j]$, $1 \le i \le w$, $1 \le j \le h$) do
   if ($B[i,j]=0$) $R_2[i,j]=R_1[i,j]$
   else $R_2[i,j]=\overline{R_1[i,j]}$
3. output (R_1 , R_2)

Fig. 3. a binary image encryption algorithm by two random networks

In the authentication phase, the provider entity demands a security code to send information to the service provider. the provider entity must transmit the second random network to the provider entity. the provider calls the first random network and the binary image. using the first and second random network, the binary image is reconstructed.

Algorithm6

// Decryption Process

1. Receive R_1 as a random grid, $T(R_1)= {}^1/_2$
2. Receive R_2 as a random grid, $T(R_2)= {}^1/_2$
3. Receive B as a binary image
4. for (each pixel $B'[i,j]$, $1 \le i \le w$, $1 \le j \le h$) do
   $B'[i,j]=R_1[i,j] \oplus R_2[i,j]$
5. output (B')

Fig. 4. algorithm of decoding a binary image by two random networks

In the second strategy, multiple connections are considered in computer networks. suppose that in multiple connections a single entity in the role of service provider and m entity is considered to be in the role of the service. in the registration phase, the entity of all services must be identified by the provider entity and each service provider should receive a security code. for this purpose, at first all services are sent to the server. then, the server entity of a binary image is randomly selected from the data pool.

Algorithm 7

// Encryption Process

1. for ($1 \le k \le n-1$) do
   Generate R_k as a random grid, $T(R_k)= {}^1/_2$
2. for (each pixel B[i,j], $1 \le i \le w$, $1 \le j \le h$) do
   $A_1[i,j]=R_1[i,j]$
   for ($2 \le k \le n-1$) do
   {
   $A_k[i,j]=R_k[i,j]$ XOR $A_{k-1}[i,j]$
   }
   $R_n=B[i,j]$ XOR $A_{n-1}[i,j]$
3. output (R_1 , R_2 , , , , , R_n)

Fig. 5. a binary image encryption algorithm by n random networks

In the authentication phase, the provider entity demands a security code to send information to the service provider. in this stage, all service providers must send their security code to the server.

Algorithm 8

// Decryption Process

1. Receive R_i as a random grid, $i=1,2,\ldots,n$
2. Receive B as a binary image
3. for (each pixel B′[i,j], $1 \le i \le w$, $1 \le j \le h$) do
   $B'[i,j]=R_1[i,j] \oplus R_2[i,j] \oplus \ldots \oplus R_n[i,j]$
4. output (B′)

Fig. 6. algorithm for decoding a binary image by n random networks

Table 1. proposed method parameters

Meaning	Variable	Row
Binary image	B	۱
Reconstruction image	$B^{'}$	۲
Random network i	R_i	۳
The length of the binary image in pixels	W	۴
The width of the binary image in pixels	H	۵
Number of connections	M	۶
The number of random networks	N	۷
Average brightness intensity of random network	T(R)	۸
Indicates the XOR operator	$\oplus$	۹

4. Encryption system

In the first strategy, a visual secret sharing scheme based on random networks (2 , 2) was proposed to encrypt the binary images . to improve the visual quality of the reconstructed image, the xor operation is used in the decoding phase. in table 2, the xor operation is shown on two random networks.

In the second strategy, a visual secret sharing scheme based on random networks (n , n) was proposed to encrypt the binary images . in table 3, the xor operation is shown on three random networks.

Table 2. XOR operation on two random networks

$r_i \in R_i$	$r_j \in R_i$	$r_i \oplus r_j$
0	0	0
0	1	1
1	0	1
1	1	0

Table 3. XOR operation on three random networks

$r_i \in R_i$	$r_k \in R_k$	$r_j \in R_i$	$r_i \oplus r_j \oplus r_k$
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

5. Evaluation criteria

In order to evaluate the encryption system, two criteria of security level and visual quality should be considered. from the point of view of security level, it should be proved that each of the random networks alone provides information of the image. and from the point of view of visual quality, the results of random network decoding should be in order to detect the desired image by the human visual system. to prove the criteria for evaluating the level of safety and visual quality, relations 1 and 2 must be proved. in these relations, the variable r represents the random network, the variable b (0) represents pixels in the original image that have a value of zero and the variable b (1) represents pixels in the original image with a value of 1 .

$$T(R) = \frac{1}{2} \tag{1}$$

$$T\left(B'\left(B(0)\right)\right) > T\left(B'\left(B(1)\right)\right) \tag{2}$$

6. Implementation of strategies

In order to implement the first strategy, a binary image is considered as the input of the algorithm. the binary image is transformed into two random networks. each of the random networks alone provides information from the original image to the attackers. two random networks are decoded in the authentication phase and a reconstruction image is generated. in figure 7, the results of the implementation of the encryption system are shown in the first strategy.

In order to implement the second strategy, a binary image is considered as the input of the algorithm. the binary image is converted to n random networks in the registration phase. in fig. 8, the results of the implementation of the encryption system are shown in the second strategy with three stochastic networks. in figure 9, the results of the implementation of the encryption system are shown in the second strategy with four random networks. the reconstructed image in both strategies is exactly the same in terms of visual quality.

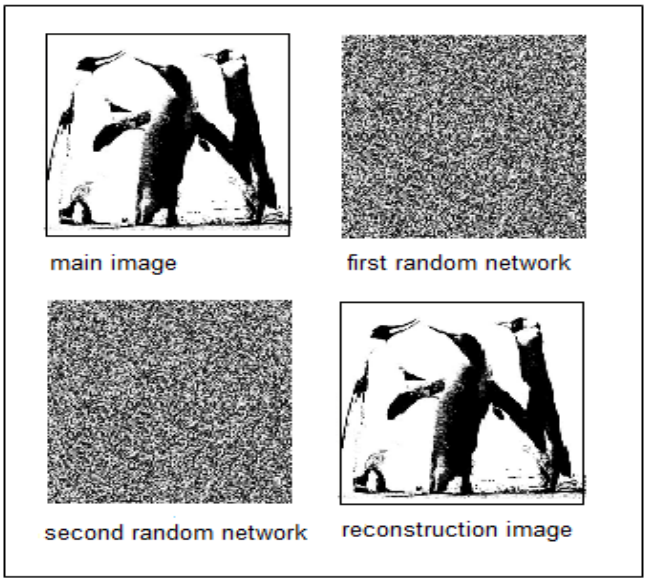

Fig. 7. Implementation results of the encryption system in strategy first

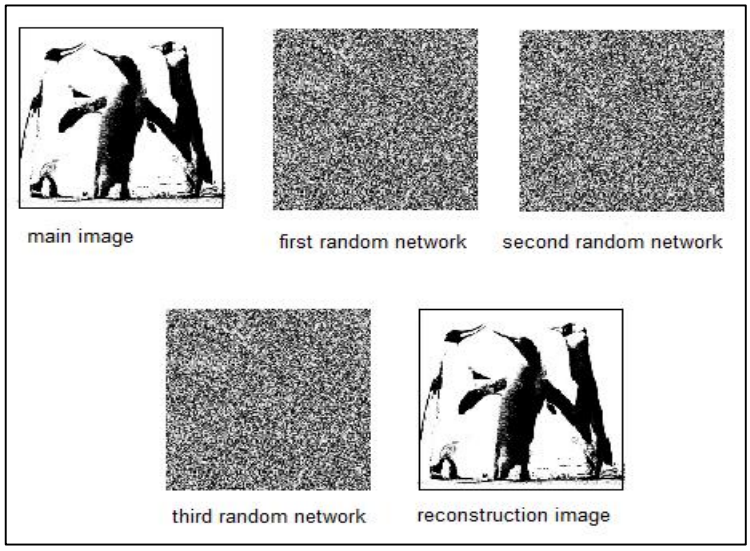

Fig. 8. results of implementation of encryption system in second strategy with three random networks

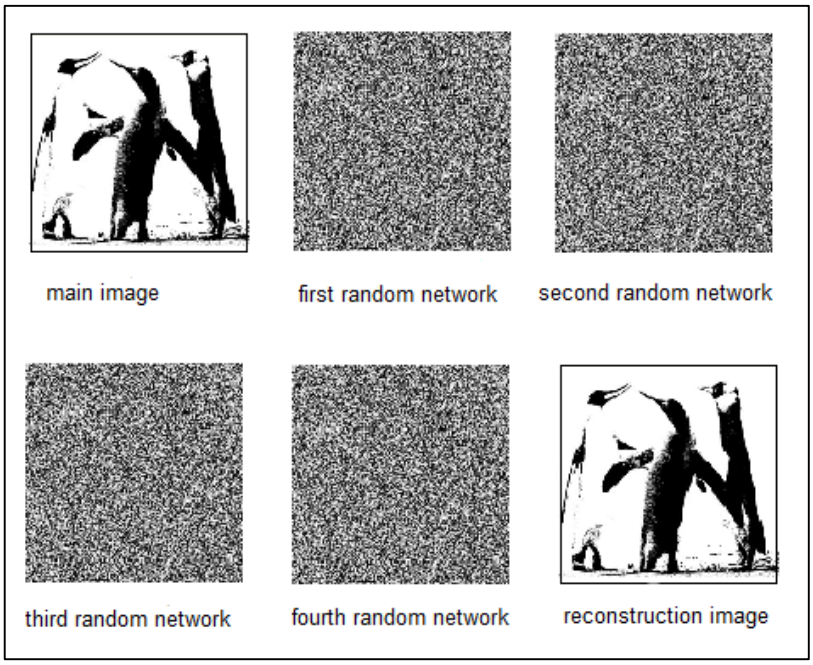

Fig. 9. results of implementation of encryption system in second strategy with four stochastic networks

7. Security level assessment

In the first strategy, a visual secret sharing scheme based on random networks (2 , 2) is designed to establish secure connections . from the point of view of the security level criterion, it should be proved that the average intensity of the light intensity of both random networks is 0.5. based on the proposed algorithm in figure 3, the first random network (r _ 1) is generated in a completely randomized process. each pixel in the first random network is based on a random process of milk or value line. thus, the average intensity of the first random network is 0.5. accordingly, the relationship no. 3 always exists.

$$T(R_1) = \frac{1}{2} \tag{3}$$

Also, based on the algorithm presented in figure 3, the relationship no. 4 and 5 is established.

$$T(R_2[B(0)]) = T(R_1[B(0)]) = \frac{1}{2} \tag{4}$$

$$T(R_2[B(1)]) = T\left(\overline{R_1[B(1)]}\right) = \frac{1}{2} \tag{5}$$

Based on equation 6, equation 7 is shown.

$$R_2 = R_2[B(1)] \cup R_2[B(0)] \tag{6}$$

$$T(R_2) = \frac{1}{2} \tag{7}$$

In the second strategy, a visual secret sharing scheme based on random networks (n , n) is designed to establish secure connections . from the point of view of the security level criterion, it must be proved that the average of the average intensity of the random network n is 0.5. based on the proposed algorithm in figure 5, the number of n - 1 random networks are valued completely by the milk or line process. thus, equation 8 always exists.

$$T(R_1) = T(R_2) = \cdots = T(R_{n-1}) = \frac{1}{2} \tag{8}$$

Assume that the variable a _ (n - 1) represents the result of the operation on n - 1 random network. otherwise, equation 9 is established.

$$T(A_{n-1}) = T(R_1 \oplus R_2 \oplus \ldots \oplus R_{n-1}) = \frac{1}{2} \tag{9}$$

Also, based on the proposed algorithm in figure 5, the number of numbers 10 and 11 will be established.

$$T(R_n[B(0)]) = T(A_{n-1}[B(0)]) = \frac{1}{2} \tag{10}$$

$$T(R_n[B(1)]) = T\left(\overline{A_{n-1}[B(1)]}\right) = \frac{1}{2} \tag{11}$$

On the basis of equation 12, equation 13 is shown.

$$R_n = R_n[B(1)] \cup R_n[B(0)] \tag{12}$$

$$T(R_n) = \frac{1}{2} \tag{13}$$

8. Visual quality assessment

Table 4. Possible modes for generating the reconstructed image in the strategy first

$b \in B$	$r_k \in R_1$	$r_j \in R_2$	$b' \in B'$
0	0	0	0
	1	1	0
1	0	1	1
	1	0	1

Table 5. results of the visual quality of the reconstructed image in the first strategy

Value	Characteristic
1	$T\left(B'(B(0))\right)$
0	$T\left(B'(B(1))\right)$
$T\left(B'(B(0))\right) > T\left(B'(B(1))\right)$	

Table 6. possible scenarios for the generation of reconstructed image in the second strategy with three random networks

$b \in B$	$r_k \in R_1$	$r_j \in R_2$	$r_i \in R_3$	$b' \in B'$
0	0	0	0	0
	0	1	1	0
	1	0	1	0
	1	1	0	0
1	0	0	1	1
	0	1	0	1
	1	0	0	1
	1	1	1	1

In this stage, the use of the Xor operator instead of operator or improves the visual quality of the reconstructed image.

Table 7. results of the visual quality of the reconstructed image in the second strategy with three random networks

Value	Characteristic
1	$T\left(B'(B(0))\right)$
0	$T\left(B'(B(1))\right)$
$T\left(B'(B(0))\right) > T\left(B'(B(1))\right)$	

Table 8. possible scenarios for the generation of reconstructed image in the second strategy with four random networks

$b \in B$	$r_k \in R_1$	$r_j \in R_2$	$r_i \in R_3$	$r_p \in R_4$	$b' \in B'$
0	0	0	0	0	0
	0	0	1	1	0
	0	1	0	1	0
	0	1	1	0	0
	1	0	0	1	0
	1	0	1	0	0
	1	1	0	0	0
	1	1	1	1	0

1	0	0	0	1	1
	0	0	1	0	1
	0	1	0	0	1
	0	1	1	1	1
	1	0	0	0	1
	1	0	1	1	1
	1	1	0	1	1
	1	1	1	0	1

According to tables 4, 6, and 8, the reconstructed image in terms of visual quality is exactly the same as the original binary image.

Table 9. Visual quality results of the reconstructed image in the second strategy with four random grids

value	Characteristic
1	$T\left(B'(B(0))\right)$
0	$T\left(B'(B(1))\right)$
$T\left(B'(B(0))\right) > T\left(B'(B(1))\right)$	

9. Resistance to attacks

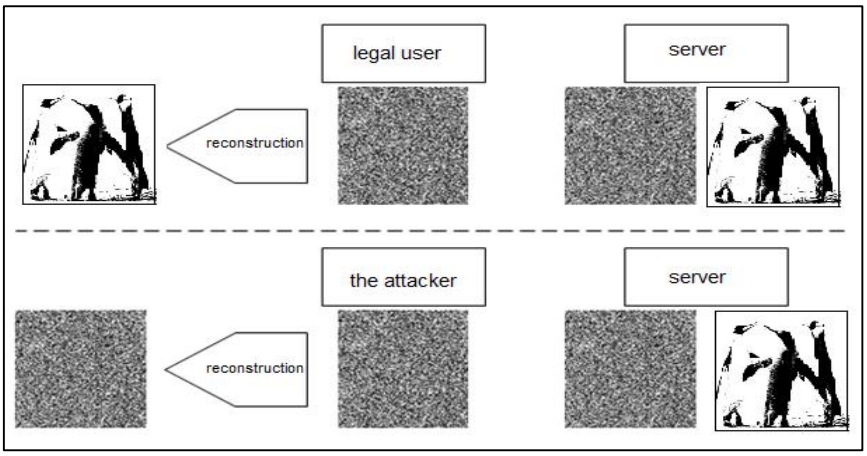

fig. 10. the resistance scheme of the visual secret sharing scheme based on random networks (2 , 2) against attacks

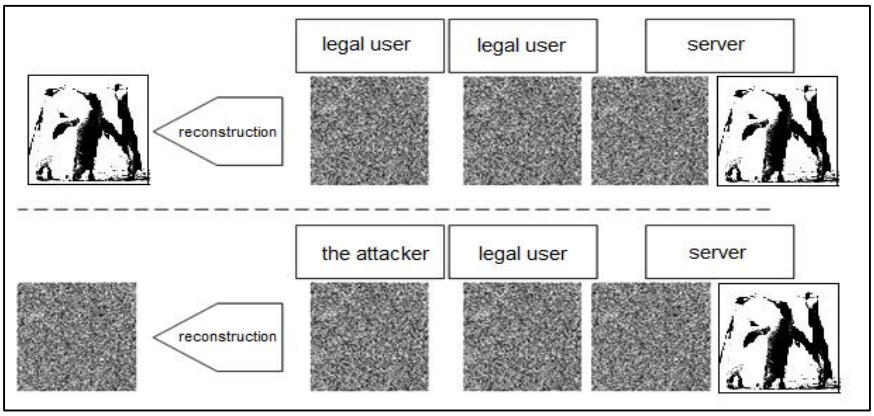

Fig. 11. the resistance scheme of the visual secret sharing scheme based on random networks (3 , 3) against attacks

In this section, the resistance of encryption system against attacks is shown. in order to evaluate the robustness of attacks, encryption algorithms are evaluated. assume that an attacker intends to generate a random network and introduce itself as a legitimate user. in the following, the system robustness against the attack will be investigated.

Scheme based on random networks (2 , 2)

In the first strategy, the entity 's existence must send a second random network to the provider entity. therefore, if the attacker wants to introduce himself as a legitimate user, it should be able to produce a second random network. the only way to generate a second random network for the attacker is to guess all of the pixels of the second random network. suppose that the attacker generates a random network and sends for the authentication phase to the client. the client 's service is based on the received random network and the first random network is trying to reproduce the image. however, given that the second random network is incorrectly generated, it is not possible to reconstruct the image for the client. therefore, the attacker identity is not verified. in figure 4 - 4, the resistance scheme for the visual secret sharing scheme based on random networks (2 , 2) is shown in response to attacks.

Scheme based on random networks (3 , 3)

In the second strategy and in the visual secret sharing scheme based on random networks (3 , 3) , the first receiver must send the second random network to the provider entity and the second service provider shall transmit the third random network to the provider entity . so, if the attacker wants to introduce himself as a legitimate user, it should be able to introduce himself as a legitimate recipient. in fact, the only way to solve the attacker is to generate the second random network or third random network. suppose that the attacker generates a random network and sends for the authentication phase to the client. the client 's service is based on the received random network and the first random network is trying to reproduce the image. however, considering that the received random network is incorrectly generated, it is not possible to reconstruct the image for the client. therefore, the attacker identity is not verified. in figure 4 - 5, the resistance of the

visual secret sharing scheme based on random networks (3 , 3) is shown in the presence of attacks.

10. Contrast analysis

Suppose that variable b represents the original image and variable b ^ ' variable representing the reconstruction image. then, the contrast of the image is calculated based on the relationship no. 14. the numerical value of one means that the reconstructed image is exactly the same as the original image.

$$\propto = \frac{T\left(B'\left(B(0)\right)\right) - T\left(B'\left(B(1)\right)\right)}{1 + T\left(B'\left(B(1)\right)\right)} \qquad (۱۴)$$

Table 10. analyze contrast scheme of proposed visual secret

Contrast value	Characteristic
1	visual secret sharing (2،2) scheme
1	visual secret sharing (3،3) scheme
1	visual secret sharing (4،4) scheme

11. Method comparison

In the proposed method, all encryption systems have the highest contrast.

In this section, the proposed visual secret sharing scheme is compared with other algorithms from the point of contrast criterion. in table 4 - 8, the results of the proposed method are compared with other methods based on contrast criteria. as shown in the table, all encryption systems have the highest contrast in the proposed method. in fact, in the proposed visual secret sharing scheme, the reconstructed images are exactly the same as the original images. therefore, from point of view point of contrast, the proposed visual secret sharing scheme has better performance than other algorithms.

Table 11. comparison of the proposed method with other methods based on contrast criteria

Contrast amount	Decoding operator	parameter	Type of encryption scheme	Algorithm
$\propto = \frac{1}{2}$	OR	n=2	visual secret sharing (n,n) scheme	The first algorithm [5]
$\propto = \frac{1}{5}$	OR	n=2	visual secret sharing (n,n) scheme	The second algorithm [5]
$\propto = \frac{1}{4}$	OR	n=2	visual secret sharing (n,n) scheme	The third algorithm [5]

$\propto = \frac{1}{4}$	OR	n=3	visual secret sharing (n,n) scheme	The fourth algorithm [6]
$\propto = 1$	XOR	n=2	visual secret sharing (n,n) scheme	The proposed algorithm
$\propto = 1$	XOR	n=3	visual secret sharing (n,n) scheme	The proposed algorithm
$\propto = 1$	XOR	n=4	visual secret sharing (n,n) scheme	The proposed algorithm

In this section, the proposed visual secret sharing scheme is compared with other algorithms in point of view of the problem of spreading pixels. the problem of spreading pixels occurs when the reconstructed image has larger dimensions than the original image. in table 4 - 9, the results of comparison of the proposed method with other methods are shown in point of view of the problem of spreading pixels. as it is known, the pixel expansion rate in all the proposed algorithms is equal to 1. in other words, there is no problem for spreading the pixels. the reason for this is that all algorithms are based on random network sharing scheme. it was noted that algorithms in the visual secret sharing scheme based on visual cryptography have the problem of spreading pixel. the pixel expansion rate of this algorithm is 2 or 4**.**

The sensitive Analyses

- ## Operator OR

The output of this operator is 1 if both variables are variables or one of the parties 1. this operator is done between two binary numbers and the single single single house is together. the operator or, if the output of 1 / 1, if all of the home is 0, then the result will be 0.

- ## Operator Xor

The xor operation is performed between two binary numbers and one single single home is xor operation with the xor. the output of this operator is one that is only one of the parties.

Table 12. comparison of the proposed method with other methods from point of view point of problem development

Expantion rate	parameter	Type of encryption	Algorithm
1	n=2	visual secret sharing (n,n) scheme	The first algorithm [5]
1	n=2	visual secret sharing (n,n) scheme	The second algorithm [5]
1	n=2	visual secret sharing (n,n) scheme	The third algorithm [5]
1	n=3	visual secret sharing (n,n) scheme	The fourth algorithm [6]

1	n=2	visual secret sharing (n,n) scheme	The proposed algorithm
1	n=3	visual secret sharing (n,n) scheme	The proposed algorithm
1	n=4	visual secret sharing (n,n) scheme	The proposed algorithm

In [7] , published in 2020 , a secure communication system based on a semantic visual secret sharing scheme is presented . in this system, a visual secret sharing scheme (2 , 2) is proposed in which two random networks are located in two colored images . in table 13, the results of the proposed method are shown by the method presented in article 7. as it is clear, the proposed algorithms in the proposed communication system from point of view of contrast criteria are better than the algorithm presented in article 7. the pixel expansion rate in both methods is equal to 1.

Table 13. comparison of the proposed method with the proposed method in [7]

Contrast measure	rate of expansion	parameter	Type of encryption	Algorithm
$\propto = 1$	1	n=2	visual secret sharing (n,n) scheme	The proposed algorithm
$\propto = 1$	1	n=3	visual secret sharing (n,n) scheme	The proposed algorithm
$\propto = 1$	1	n=4	visual secret sharing (n,n) scheme	The proposed algorithm
$\propto = \frac{1}{2}$	1	n=2	visual secret sharing (n,n) scheme	[23] Method

12. Conclusion

In 2008, Liu et al. [6] presented a novel image secret sharing scheme based on combination theory. in this research, a network - based visual secret sharing scheme is designed to establish secure connections in computer networks. in order to design the proposed method, mathematical relations and algorithm were used. the proposed method is designed so that there is no need for key management to establish secure connections between network entities. in order to design the proposed method, two strategies were considered. in the first strategy, binary communications were considered as the main predictors and in the second strategy, multiple relationships were considered as the main predictors. a network - based visual - secret sharing scheme for secure connections in computer networks was implemented and evaluated. in order to implement the proposed method, matlab software was used. security and visual quality measures were used to evaluate the encryption system. also, the rate of resistance to attacks was investigated. both strategies have favorable performance at the point of view of security level. the security level of the visual secret sharing scheme based on random networks is proved to establish binary and binary relations based on mathematical relations. in other words, the contrast of the reconstructed image in the first and second strategy is equal to one which indicates the desired performance of the proposed method. finally, it was shown that the proposed visual secret sharing scheme

outperforms other algorithms in terms of image contrast. the reason for this is to use the xor operator in the decoding phase. therefore, the proposed visual secret sharing scheme is better in comparison with other methods. in both strategies the contrast rate of the reconstructed image is equal to one which is improved compared to other algorithms. the contrast rate of reconstructed images in both strategies is improved compared to other methods.

Refrences

[1]	Yang, C.N. Laih, C.S. (2000), "New colored visual secret sharing schemes", Designs, Codes and cryptography, 20(3), 325-336.
[2]	Patil, S.M. Purushothama, B.R. (2021), "Pixel co-ordinate-based secret image sharing scheme with constant size shadow images", Computers & Electrical Engineering, https://doi.org/10.1016/j.compeleceng.2020.106937.
[3]	Sarosh, P. Parah, S.A. Bhat, G.M. (2021), "Utilization of secret sharing technology for secure communication: a state-of-the-art review", Multimedia Tools and Applications, 80(1), 517-541.
[4]	Fu, Z. X. Yu, B. (2013), "Visual cryptography and random grids schemes", International Workshop on Digital Watermarking, Berlin, Heidelberg, 109-122.
[5]	Kafri, O. Keren, E. (1987), "Encryption of pictures and shapes by random grids", Optics letters, 12(6), 377-379.
[6]	Shyu, S. J. (2009), "Image encryption by multiple random grids", Pattern Recognition, 42(7), 1582-1596.
[7]	Blesswin, J. Raj, C. Sukumaran, R. (2020), "Enhanced semantic visual secret sharing scheme for the secure image communication", Multimedia Tools and Applications, 79(23), 17057-17079.
[8]	Hua-Kun Wang, G-Bao Xu, D-Huan Jiang (2023), “Quantum grayscale image encryption and secret sharing schemes based on Rubik’s cube”, Statistical Mechanics And Its Applications, 128482
[9]	Suraj Kumar Sahoo, A. Adhikari, S. Dutta (2022), “Practical Attacks On A Class Of Secret Image Sharing Schemes Based On Chinese Reminder Theorem”, Computers And Electrical Engineering, 107924
[10]	Dong Ming Huo, Z. Zhu, X. Zhou, L. Wei, X. Bai, C. Han (2022), “A Flexible And Visually Meaningful Multi-Image Compression Encryption And Hiding Scheme Based On 2D Compressive Sensing”, Heliyon, e14072
[11]	Xue-Hang Qian, G-Bao Xu, H-Kun Wang, D-Huan Jiang (2022), “Threshold Secret Sharing Scheme Of Quantum Images Based On Least Significant Bit Theory”, Statistical Mechanics And Its Applications, 128248
[12]	Zhihua Gan, S. Song, L. Zhou, D. Han, J. Fu, X. Chai (2022), “Exploiting Compressed Sensing And Polynomial-Based Progressive Secret Image Sharing For Visually Secure Image Selection Encryption With Authentication”, Journal Of King Saud University-Computer And Information Sciences, 9252-9272