(k, m) Secret Image Sharing Scheme with Cheater Detection Using RSA Cryptosystem

Harshita Pathak[1], Anjulata Yadav[2], Manish Panchal[3], Prakash vyavahare[4]
[1]*PG student, Department of ETC, SGSITS, Indore, 45200, India*
[2,3]*Associate Professor, Department of ETC, SGSITS, Indore, 45200, India*
[4]*Retired Professor, Department of ETC, SGSITS, Indore, 45200, India*

Abstract **- Secret sharing schemes are mainly used in cryptography with the purpose of keeping the secret safe. (k, n) threshold secret image sharing technique involves the distribution of secret image among n participants that is called shadow images that satisfy the following conditions:**
(a) The complete image information will not be received when less than k shadow images.
(b) Again, construct the complete image any k or more than k shadow images are required.
This scheme is mainly used in applications where single trusted entity is not available. Secret image sharing schemes have been applied to the military, e-commerce and communication fields. In this paper we propose (k, m) secret image sharing scheme with cheater detection using RSA cryptosystem.

Index Terms **- Secret image sharing, RSA cryptosystem, Cheater Detection, Encryption, Decryption.**

I.INTRODUCTION

In this era, people completely depend on internet for performing online transaction, data exchange by an individual or within an organization, e-commercing, digital data storage, cloud computing and computer networks. Therefore, security of data stored, and data transmission has become a point of concern for making integrity of data. Cryptography is the major tool used for securing of data transmission and data storage over such computer networks and data storage devices. In cryptography system complex encryption and decryption algorithm is used for hiding the secret data. For securing the confidential data, firstly introduced a secret sharing technique by Shamir [1] and Blakley [2] in 1979. Shamir's technique is formed on Lagrange interpolation polynomial whereas Blakley's technique is formed on the principle of hyperplan geometry. In the Shamir's (k, n) threshold-based secret share technique the secret sharing information S is split among "n" participants in such a manner that any k or more than k participants can again construct the secret but less than k participants does not get any information about secret [1]. Both the techniques have some limitations are as follows:

1. At a time only, single secret can be splitted.
2. After reconstructing the secret there is no use of participant's shares.
3. There is no way to detect cheater.

In 2002, Thien and Lin [3] proposed the extension of Shamir's polynomial approach in the form of (k, n) threshold based secret image sharing method.
(k, n) secret image sharing technique can be categories in to two strategies that is given below:

a. Polynomial based scheme [5-7]
b. Visual cryptography scheme [8-10]

Lossless recovery is important for the transmission and storage of data. In the polynomial based secret image sharing technique reconstructed the original image without loss with decrease the shadow size.
Visual cryptography was invented by Naor and Shamir in 1994[4]. In which the secret image is divided among two or more than two shares and at the time of reconstruction, the shares are stacked on one another, and secret image will appear without any complex computation. Visual cryptography scheme is executed by human visual approach without any calculation. In the secret share technique, the cheating problem was firstly presented in 1989 by Tompa and Woll [10]. They consider the situation that at the time of reconstruction the secret, some dishonest participants forged the fake shares. In this manner, the cheater gets back the secret and honest participants get the fake secret. In 2018 Liu-Sun-Yang has proposed the (k, n) secret image share strategy is able to detect the cheater [12].

The rest of the paper is arranged as follows: In the part 2. Some preliminaries in which Shamir's (k, n) secret share technique, Thien-Lin's secret image share technique, Liu-Sun-Yang (k, n) Secret image share technique able to reveal the cheater are introduced. In part 3. Describe the RSA cryptosystem. In part 4. Proposed (k, m) image secret sharing scheme using RSA cryptosystem is being presented. In part 5. Comparability among the proposed scheme and the other schemes. Finally, the conclusion comprised in part 6.

II. PRELIMINARIES

[1] Shamir's (k, n) secret share technique: In this technique the secret sharing information S is split among "n" shares using in such a manner that at the time of reconstruct the secret any k or more than k secret shares are required but less than k secret shares do not get any information of the secret [1]. A secret sharing scheme has two phases:

A. Share distribution Phase:

1. Construct the polynomial function of the order of $(k-1)^{th}$ degree by,

$f(x) = b_0 + b_1x + b_2x^2 + \ldots\ldots\ldots + b_{k-1}\, x^{k-1} \pmod p$

where b_0 is the secret and p are the prime number. The secret shares are in the form of pair values (x_i, y_i) whereas,

$y_i = f(x_i)$, $1 \le i \le n$ and $0 < x_1 < x_2 \ldots\ldots < x_n \le p-1$.

2. Shareholder holds the pair value of (x_i, y_i) and there is single shareholder does not get the secret value b_0. Even though less than k shares cannot find the secret b_0.

B. Reconstruction Phase:

1. At the time of reconstruct the secret the k or more than k shares are required and then find the secret b_0 by using Lagrange interpolation method.

[2] Thien-Lin's secret image share technique: Thien and Lin have proposed [3] a (k, n) threshold-based image secret share technique by using the concept of Shamir's secret share technique [1]. Utilize the idea of polynomial function of order (k-1) to make n image shadows from m × m pixels secret image (it is denoted by I).

$St (a, b) = I (ak+1, b) + I (ak+1, b)\, x + \ldots..+ I (ak+1, b)\, x^{k-1} \pmod p \ldots\ldots\ldots (1)$

where, $0 \le i \le [m/k]$ and $1 \le j \le m$. This technique reduces the size of image shadow will become 1/k original size of the secret image. Any k image shadows are required to reconstruct each pixel value in the secret image.

Take an example of (2, 4) image secret sharing technique is shown in figure 1. Where n = 4, k = 2

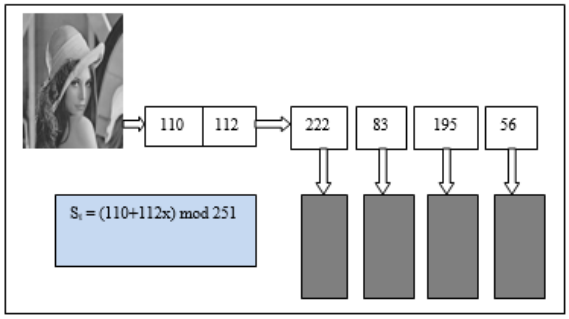

Fig 1. Secret Sharing method for Lena image

1. Create first order polynomial function by using first two-pixel values of Lena image that is,
   St (a, b) = (110 + 112x) (mod 251)…….(2)
   For generating four shares randomly choose the x values into the polynomial function and 251 is the largest prime number but less than 255 (which is the highest gray value of image).
2. After computing the 4 shares we get, (1, 222) (2, 83) (3, 195) (4, 56) it shows that first pixel of image is converted into 4 image shadows. This operation continues until all the pixels are encrypted.
3. This operation shows size of each image shadow is half of the original image size. Therefore, Thien Lin's scheme reduces image shadow size will become 1/k of the secret image size.
4. It is possible that a secret image can be recovered from less than k image shadow because of the adjacent pixel values is close to each other. To reduce this security issue Thien and Lin advised that to permutate the order of pixel before the image shares are calculated.

[3] Liu-Sun-Yang (k, n) Secret image share scheme able to reveal cheater:

The Liu-Sun-Yang's procedure contains following steps,

a. The Shadow formation step
b. The image reconstruction and cheating detection step [12].

(A) The Shadow formation step:

1. Taking the secret image SI as a input and n image-shadows Sh_1, Sh_2, . . . ,Sh_n as a output.
2. Distributer divides the secret Image SI into l non-intersecting 2k – 2 pixel blocks, PB_1, PB_2,……, PB_l.
3. In every pixel blocks PB_i, i ∈ [1, l], there are 2k – 2 confidential pixels are available that is, $b_{i,0}$, $b_{i,1}$, . . . , $b_{i,k-1}$ and $c_{i,2}$, $c_{i,3}$, . . . , $c_{i,k-1}$ ∈ GF(251) then by using this confidential pixels distributer creates k − 1th degree of polynomial function, $f_i(x) = b_{i,0} + b_{i,1} x +, . . . ,+ b_{i,\,k-1} x^{k-1}$ ∈ GF(251).
4. The distributer will generate another (k-1)th degree polynomial function $g_i(x)$ by choosing random integer re and computes two pixels $c_{i,0}$, $c_{i,1}$ which assure that , $r_e b_{i,0} + c_{i,0} = 0$, $r_e b_{i,1} + c_{i,1} = 0$ over GF(251) and create $g_i(x) = c_{i,0} + c_{i,1}x +, . . . ,+ c_{i,\,k-1}x^{k-1}$.
5. For every pixel block PB_i, i ∈ [1, t], the distributer calculates the part of image shadows $u_{i,j} = \{ p_{i,j}, q_{i,j} \}$, $p_{i,j} = f_i(j)$, $q_{i,j} = g_i(j)$, j = 1, 2, . . . , n for all participant P_j. The image shadow Sh_j for P_j is $Sh_j = u_{1,j} \| u_{2,j},\| . . . .\| u_{l,j}$.

(B) Image Reconstruction and Cheater Detection step:

1. Take out $u_{i,j} = (p_{i,j}, q_{i,j})$, i = 1, 2, . . . , l, j = 1, 2, . . . , k from Sh_1 , Sh_2. . . , Sh_k.

2. For every set of $u_{i,1}, u_{i,2},\ldots, u_{i,k} \in [_{1,\,l],}$ again construct $f_i(x)$ and $g_i(x)$ from $p_{i,1}, p_{i,2}, . . . , p_{i,k}$ and $q_{i,1}, q_{i,2},\ldots, q_{i,k}$ with the help of Lagrange interpolation respectively.

3. Let $b_{i,0}$, $b_{i,1}$ and $c_{i,0}$, $ci_{,1}$be the coefficients of $x_0$and x in the polynomial function $f_i(x)$ and $g_i(x)$ respectively. For detecting the cheater there is exist a common integer re which satisfies the equation that, $r_e b_{i,0} + c_{i,0} = 0$ and $reb_{i,1} + c_{i,1} = 0$, It shows the recovery of 2k-2 pixel blocks $PB_i = \{b_{i,0}, b_{i,1}, . . . ,b_{i,k-1}, c_{i,2}, c_{i,3}, . . . , c_{i,k-1}\}$ and the secret image $S_I = PB_1 \| PB_2 \|, . . . , \| PB_l$.

III. DESCRIPTION OF RSA CRYPTOSYSTEM

RSA Cryptosystem: Security is important when information is being exchanged between participants through unsecure network therefore the strong encryption algorithm prevent this information from getting hacked or cracked. The first public key cryptosystem is the RSA CRYPTOSYSTEM, and it is created by Ron, Rivest, Adi Shamir and Leonard Adleman in 1977 [16]. In which the user creates and publishes the public key based on two large prime numbers. User utilizes the public key for encrypt a plaintext or images and private key is used for decrypt ciphertext or images.

(A) The generation of RSA's keys are as shown below:

1. User should be select two distinct large prime numbers "p" and "q" to form R=p*q.
2. Discover the Euler's phi-function by this formula φ(R) = (p-1) (q-1).
3. Select two positive integers e and d in such a way that d is the inverse of e modulo φ(R).
4. Then declare the pair (e, R) belongs to the public key and holds the (d, R) as a secret that belongs to the private key.

(B) The encryption and decryption method for the RSA Cryptosystem is explained below:

1. For encrypting the plaintext that could be a message or an image, the sender translates the letters and images into their numerical function and pixel number then form the plaintext block "M".
2. Encryption algorithm is used by the sender using public key (e, R) that is, $E(M)=C=M^e \bmod (R)$ here, "C" is the corresponding ciphertext to M.
3. For Decrypting the ciphertext block C, the decryption algorithm is applied on each block using private key (d, R) that is, $D(C) =M= C^d \bmod (R)$.

IV. PROPOSED SCHEME

The proposed scheme called as "(k, m) image secret sharing scheme with cheater detection by using RSA cryptosystem". This scheme is the expansion of Liu-sun-yang scheme is the secret image sharing which is based on polynomial [12]. In our proposed scheme RSA cryptosystem used for encrypting and decrypting the secret image.

To encrypt and decrypt the secret image we need the strong algorithm and also concern about the problem of cheater detection during the reconstruction time because cheaters can put the forged image shadows so the result will be the sincere participants recover the forgery image and cheater are able to reconstruct the secret image. The proposed scheme is extended from Liu-sun-yang secret image sharing scheme which is based on polynomial. More security is important therefore in our scheme RSA algorithm is used.

This scheme consists of three stages:

(A) Share generation stage:

1. First Dealer "D" divides image I in to l non – intersecting 2k-2 pixel blocks B_1, B_2, B_3..…. B_l. Our secret pixels are $S_i = M_{i,0}, M_{i,1}, M_{i,2}$,….. $M_{i,k-1}$.
2. We have already discussed in the previous section about RSA algorithm. Now Dealer will apply RSA algorithm on the secret pixel S_i. Dealer will encrypt every 2k-2 secret pixel blocks by applying $C_i = M_i^e$ mod R.
3. After encrypting the secret pixels dealer will get another encrypted pixel that is, $a'_{i,0}$, $a'_{i,1}$, $a'_{i,2}$, ……, $a'_{i,k-1}$.
4. Using this encrypted pixel $a'_{i,0}$, $a'_{i,1}$, $a'_{i,2}$, ……, $a'_{i,k-1}$. dealer will make polynomial of degree (k-1)th that is $f_i(x) = a'_{i,0} + a'_{i,1}x + a'_{i,2}x^2 + \ldots + a'_{i,k-1}x^{k-1} \in GF(251)$
5. The dealer will choose random integer r_1 and compute another pixel $b'_{i,0}$, $b'_{i,1}$, $b'_{i,2}$……., $b'_{i,k-1}$ which satisfy,
   $a'_{i,0} + r_1 b'_{i,0} = 0 \pmod{251}$
   $a'_{i,1} + r_1 b'_{i,1} = 0 \pmod{251}$
   .
   .
   $a'_{i,k} + r_1 b'_{i,k-1} = 0 \pmod{251}$ here, another polynomial is, $g_i(x)$ will create by $b'_{i,0}$, $b'_{i,1}$,……,$b'_{i,k-1}$.
6. For every block B_i, $i \in [1,l]$, dealer will compute the sub shares to put the, share's identification ID_x that is, x=1,2,….n for each participants p_j on every polynomial of $f_i(x)$ and $g_i(x)$ and creates the sub shares, $t_{ix} = [u_{ix}, v_{ix}]$, $u_{ix} = f_i(x)$, $v_{ix} = g_i(x)$, x = 1,2,….n, for each participants pj, the secret $s_i = t_{ix}$. The dealer distributes the image shadows to the participants that is, $t_{ix} = [u_{ix}, v_{ix}]$ up to n participants.

(B) Image reconstruction stage:

1. Extract $t_{ix} = [u_{ix}, v_{ix}]$, i= 1,2,….,l, x=1,2,…..,k from s'_1, s'_2, s'_3……,s'_k.
2. For each and every group of $t_{i,1}$, $t_{i,2}$,….., $t_{i,k,\ i} \in [1,l]$ from u_{ix} and v_{ix} using Lagrange interpolation method respectively.
3. Dealers share the secret shadow with n participants and any k or more than k participants are required to reconstruct the image secret that is called (k, m) image secret sharing scheme. Here from the share $[u_{ix}, v_{ix}]$ only k shares are required out of n and apply Lagrange interpolation method then will get $f_i(x)$ and $g_i(x)$.
4. After getting $f_i(x)$ and $g_i(x)$ apply decryption method by using private key (d, R) on both the polynomial then will get original secret image pixels that is ,
   $M_i = C_i^d \bmod R$, $C_i = \{a'_{i,0}, a'_{i,1}x,\ldots,a'_{i,k-1}x^{k-1}\}$ and $\{b'_{i,0}, b'_{i,1}x,\ldots,b'_{i,k-1}x^{k-1}\}$
   $M_i = a_{i,0}, a_{i,1}x,\ldots, a_{i,k-1}x^{k-1}$

(C) Cheater detection: if any participants submit forged secret pixel at the time of reconstruction then dealer will apply the Lagrange interpolation on the shares that is $t_{ix} = [u_{ix}, v_{ix}]$ and we will get the get $f_i(x)$ and gi(x) and dealer use the integer r1 and satisfy the $a_{i,0}+r_1b_{i,0}=0 \pmod{251}$ $a_{i,1}+r_1b_{i,1}=0 \pmod{251}$ then there is no cheater but if any participants submit forged pixel shares then this condition will not satisfied then dealer will get to know there is cheater exist. Our scheme recognizes the cheating problem.

V. AN EXAMPLE FOR (K, M) IMAGE SECRET SHARING SCHEME USING RSA CRYPTOSYSTEM

1. 1.In this example, Let (k, m) = (2, 3) and the secret image I is divided in to l blocks where each block includes 2k-2 = 2*2-2 = 2 secret pixels.
2. Assume the 1st block B1 consist of the 2 pixels (57, 68) = (a_{i0}, a_{i1}), dealer will apply RSA encryption algorithm on these two pixels.
3. Dealer select two prime numbers, p=11, q=17 and form R=p*q= 11*17=187 and discover the Euler's phi function $\varphi(R) = (p-1)*(q-1) = 10*16=160$.
4. Chooses two positive integer e and d in such a way that d is an inverse of e modulo φ(R),
   e, $1<e<\varphi(R)=\gcd(e, \varphi(R))=1$
   gcd (7,160) =1
   $d*e=1 \bmod \varphi(R)$,
   $23*7=1 \bmod 160$
   (e, R) = (7,187) will be their public key and
   (d, R) = (23,187) will be their private key.
5. Dealers use the public key to encrypt the image's secret pixel that is (57, 68)
   $C = M_e \bmod R$
   $C_1 = (57)7 \bmod 187$
   $C_1 = 150 = (a'_{i,0})$
   $C_2 = (68)7 \bmod 187$
   $C_2 = 51 = (a'_{i,2})$

6. After encrypting secret pixel, dealer will make polynomial of (k-1)th degree , $f_i(x)= 150+51x$; $a'_{i,0} + a'_{i,1}x$……eq. (1)
   Then dealer pick a random integer $r_1=9$ and calculates two pixels and will generate another polynomial gi (x) of degree (k-1)th that is,
   $a'_{i,0} + r_1b'_{i,0} = 0 \pmod{251}$; $150+9*67=0 \pmod{251}$
   $a'_{i,1} + r_1b'_{i,1} = 0 \pmod{251}$; $51+9*78=0 \pmod{251}$
   here we got, $b_{i,0} = 67$, $b'_{i,1} = 78$ and make $g_i(x)= 67+78x$; $b'_{i,0} + b'_{i,1}x$…….eq(2)
   put the value of x=1,2,3,…..n (that is user's identification $ID_1=1$, $ID_1=2$, $ID_3=3$) on eq(1) and eq(2) then will get:
   f(1)=201, f(2)=252, f(3)=303 ; g(1)=145, g(2)=223, g(3)=301, then the dealer distribute the secret shadows to the participants,
   first participant shadow $t_1= (u_1,v_1) = (201,145)$
   second participant shadow $t_2= (u_2,v_2) = (252,223)$
   third participant shadow $t_3= (u_3,v_3) = (303,301)$

(B) Image reconstruction stage:

1. At the time of reconstruction stage participants shares their secret shadows to the dealer that is ti then dealer will apply Lagrange interpolation method on every secret shadow which is provided by the participants.
2. Here we can proof the (k, m) threshold secret sharing scheme:
   m=3, k=2 so any 2 or more than 2 participants are required to reconstruct the secret pixels. Here we take two shares that is (201,252), (145,223) split this in to (ID_1,u_1) (ID_2,u_2), (ID_1,v_1) (ID_2,v_2); (1,201) (2,252), (1,145) (2,223)
3. Now apply Lagrange's interpolation on (1, 201) (x_0, y_0), (2, 252) (x_1 , y_1)
   $f(x) = (\frac{x-x1}{x0-x1}) * y_0 + (\frac{x-x0}{x0-x1}) * y_1$ will get, $f(x) = 150+51x$…….eq(3) similarly, apply Lagrange's interpolation on (1, 145) (x_0, y_0) (2, 223) (x_1 , y_1) then will get $g(x) = 67+78x$…....eq(4)
4. Then apply decryption method on eq (3) and eq (4)
   $f(x)=150+51x$; $M_i = C^d_i \bmod R$.
   $(150)^{23} \bmod 187= 57$
   $(51)^{23} \bmod 187=68$
   Here, 57, 68 are the reconstructed secret pixels.

(C) Cheating Detection:

There is m=3 participants and k= 2 participants are required to reconstruct the secret but if one of them submit forged secret shares to the dealer. Assume first share and second share submit forged secret $t_1^*= (300,200)$, $t_2^*= (150,100)$ as a result two polynomials are $f^*(x) = 450-150x$ and $g^*(x) = 300-100x$, dealer already have been chosen $r_1 = 9$ so a_1^* and b_1^* are not satisfying the below condition:
$450\ r_1 +300=0 \pmod{251}$
$150\ r_1-100=0 \pmod{251}$,
now we can say that the cheating is successfully detected.
Note: Proposed scheme satisfy the feature of (k, m) threshold, such that any k or more than k participants can recover the secret image and less than k participants get no information about the secret image.
There is m=3 participants and k= 2 participants are required to reconstruct the secret but if one of them submit forged secret shares to the dealer. Assume first share and second share submit forged secret $t_1^*= (300,200)$, $t_2^*=(150,100)$ as a result two polynomials are $f^*(x)=450-150x$ and $g^*(x)=300-100x$, dealer already have been chosen $r_1 = 9$ so a_1^* and b_1^* are not satisfying the below condition:
$450\ r_1 +300=0 \pmod{251}$
$150\ r_1-100=0 \pmod{251}$,
now we can say that the cheating is successfully detected.
Note: Proposed scheme satisfy the feature of (k, m) threshold, such that any k or more than k participants can recover the secret image and less than k participants get no information about the secret image.

VI. TABLE

Parameter	Thien-Lin [3]	Liu-sun-yang[11]	Lin-wang[12]	Zhaoetal [13]
Secret image	N	N	n	n
Cheating prevention	No	yes	no	yes
Distortion free recovery	No	yes	no	no
Encrypted shadow size	$\frac{m*n}{k}$	m*n	$\frac{m*n}{k}$	$\frac{m*n}{k}$
Probability of brute force attack	Low	low	low	low	very low

VI. CONCLUSION

Our scheme is based on Liu-Sun-Yang (k, n) secret image share scheme which is capable of cheating detection [11]. This paper proposes (k, m) secret image sharing scheme with cheater detection using RSA cryptosystem. The RSA algorithm has been applied in image encryption for giving the better security. Decrypted image completely different from original image, therefore no one can find out the original image without knowing the private key. Therefore, this approach has secure and strong strategy to encrypt the images using RSA cryptosystem. Proposed scheme has capability to detect the cheating behavior by using Lagrange interpolation from up to k-1 cheaters. The proposed scheme has been proved mathematically.

REFERENCE

[1] A. Shamir, "How to share a secret," Communication of the ACM, vol. 22, pp.612-613, 1979.

[2] G.Blakley, "Safeguarding cryptographic keys," Proc. of the AFIPS 1979 National Computer Conference, vol. 48, pp. 313-317, 1979.

[3] C.C.Thien, J.C. Lin,"Secret image sharing," Computer Graphics, vol. 26, pp.765–770, 2002.

[4] Naor M, Shamir, "A Visual cryptography. In Advances in Cryptology - EUROCRYPT'94. Berlin 1994.

[5] C.N. Yang, Y.Y. Chu,"A general (k, n) scalable secret image sharing scheme with smooth scalability," J. Syst. Software, vol. 84, pp.1726–1733, 2011.

[6] Y.X. Liu, C.Y. Yang, P.H. Yeh,"Reducing shadow size in smooth scalable secret image sharing," Secure. Communication. Network, vol.7, pp.2237–2244, 2014.

[7] Y.X. Liu, "Scalable secret image sharing scheme with essential shadows, "Signal Processing Image Communication, vol. 58, pp.49–55, 2017.

[8] R.Z. Wang, "Region incrementing visual cryptography," IEEE Signal Proc. Lett, vol.16, pp. 659-662, 2009.

[9] C.N. Yang, H.W. Shih, C.C. Wu, L. Har, "k out of n region incrementing scheme in visual cryptography," IEEE Trans. Circ. Syst. Video Technol, vol. 22, pp.799–809, 2012.

[10] C.N. Yang, Y.C Lin, C.C. Wu, "Region in region incrementing visual cryptography scheme," in Proc. IWDW2012, LNCS, vol. 7809, pp. 449–463, 2013.

[11] M. Tompa, H. Woll, "How to share a secret with cheaters," J. Cryptol, vol. 1, pp. 133–138, 1989.

[12] Y.Liu, Q.Sun, C.Yang, "(k, n) secret image sharing scheme capable of cheating detection," Journal on Wireless Communication Network, vol. 72, pp.1-6, 2018.

[13] Y.Y. Lin, R.Z. Wang, "Scalable secret image sharing with smaller shadow images," IEEE Signal Process Lett, vol.17, pp.316-319,2010.

[14] R.Zhao, J.J.Zhao, F.Dai, F.Q. Zhao, "A new image sharing scheme to identify cheaters cheaters," Comput Stand Interfaces, vol.31, pp.252–7,2009.

[15] G. Gong, L. Harn, "Public-key cryptosystems based on cubic finite field extensions," IEEE Trans Inf Theory, vol.45, pp.2601-5,1999.

[16] Hashim, Hayder, Mohamed Al-Sabti, Karrar, "A new approach for image encryption in the modified RSA cryptosystem using MATLAB," Global Journal of Pure and Applied Mathematics, vol.12, pp. 3631-3640,2016.

[17] C. Lv, M. Yu, Y. Liu, "A secret image sharing scheme based on Lagrange interpolating polynomial," J. Huazhong Univ. Sci. Tech, vol.33, pp.285-288 ,2005.

[18] G. Ulutas, M.Ulutas, V.V. Nabiyev, "Secret imag sharing scheme with adaptive authentication strength," Pattern Recognition letters, vol.34, pp. 283-291,2013.

[19] C.N.Yang, S.M, Huang, "Constructions and properties of k out of n scalable secret image sharing," Optics Communications, vol.283, pp. 1750–1762,2010.

[20] B. Chen, W. Lu, J. Huang, J. Weng and Y. Zhou, "Secret sharing based reversible data hiding in encrypted images with multiple data-hiders," in IEEE Transactions on Dependable and Secure Computing, vol.01, pp.1-1, 2020.

[21] Jingju Yan, Lei Sun, Jinrui Liu, Xuehu Yan. Fake and dishonest participant location scheme in secret image sharing[J]. Mathematical Biosciences and Engineering, vol.18(3), pp. 2473-2495, 2021.