IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

Image Secret Sharing using IWT (Integer Wavelet Transform) Algorithm

Mrs. P. Elakkiya[1], Akshaya. D[2], Keerthi Kiran K. A[3], Mahisha. S[4]
Assistant Professor, Department of Computer Science and Engineering[1]
Students, Department of Computer Science and Engineering[2,3,4]
Anjalai Ammal Mahalingam Engineering College, Kovilvenni, Tiruvarur, Tamil Nadu, India

Abstract: *Because of the importance of digital images and their extensive application to digital watermarking, block chain, access control, identity authentication, distributive storage in the cloud and so on ,image secret sharing(ISS) is attracting ever-increasing attention .Share authentication is an important issue in its practical application. However, most ISS schemes with share authentication ability require a dealer to participate in the authentication. To design an ISS for a(k ,n)-threshold with separate share authentication abilities of both dealer participatory authentication and dealer non participatory authentication .the advantage of polynomial-based ISS and visual secret sharing(VSS) are skilfully fused to achieve these two authentication abilities Without sending a share by using a screening operation. In addition, the designed scheme has the characteristics of low decryption (authentication) complexity, lossless decryption and no pixel expansion .Experiments and theoretical analyses are performed to show the effectiveness of the designed scheme.*

Keywords: Image secret sharing, lossless recovery share authentication, no pixel expansion

I. INTRODUCTION

Recently, secret image sharing has become a key technology used to keep confidentiality in the field of information security and protection. Shamir [1] first proposed a concept of secret data sharing called a (r, m) threshold scheme. Thien and Lin [2,3] developed a secret image sharing method based on this (r, m) threshold scheme. Their method permutes a secret image first to de-correlate pixels and then incorporates the (r, m) threshold scheme to process the image pixelwise or pattern-wise in the spatial domain sequentially, hence, it may not be suitable for real time progressive transmission. A reversible integer-to-integer (ITI) wavelet transform maps an integer-valued image to integer-valued transform coefficients and provides the exact (lossless) reconstruction of the original image [4 - 8]. This multi-resolution representation can be fast computed with only integer addition and bit-shift operations. Most of the signal energy is concentrated in the low frequency bands and the transform coefficients therein are expected to be better magnitude-ordered as we move downward in the multi-resolution pyramid in the same spatial orientation [4,5,8]. The smooth (scaling) coefficients have the same range of values as that of the input image and the detail (wavelet) coefficients have smaller absolute values than the input image. Instead of using permutation to de-correlate pixels [2] prior to applying the (r, m) threshold scheme, we first apply ITI wavelet transform and then process transform coefficients with a combination procedure to decorrelate pixels (coefficients) and increase security, enabling the real time progressive transmission.

II PRELIMINARY

In this section, some preliminary work is illustrated, including image feature analysis RG-VSS for the (2, 2) threshold and original polynomial-based ISS schemes. To achieve lossless decryption and avoid auxiliary encryption in the designed scheme, the feature of an image is analysed; RG-VSS for the (2, 2) threshold is used to encrypt each binary authentication pixel into two random bits; traditional polynomial-based ISS schemes are the foundation of our scheme. By using a screening operation, our scheme realizes the independent public sharing authentication ability. In conventional ISS for the (k, n) threshold, a secret image S2 is encrypted into n shares SC1, SC2,⋯ SCn , and the image S2' is decrypted from t ($k \leq t \leq n$,$t \in Z+$) shares.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

A. The Feature Analyses of a Digital Image

A digital image is a specific data format, but there are some specific features about it that should be taken into account when designing an ISS scheme.

1. The value of each pixel in an image is associated with its adjoining ones to form texture, structure, edges and so on. In particular, in a local region of an image, the grayscale value of one pixel resembles its adjoining pixels.
2. An image includes generous pixels with a large amount of data; therefore, the efficiency is of sovereign significance.
3. An image has its specific coding method to store the image file. In particular, for a grayscale image, its pixel values range from 0 to 255. Thus, the value of each output share pixel and the value of the input secret pixel should also range from 0 to 255.
4. Using one byte represents the value of each grayscale pixel, an ISS technique is easily extended to an SS technique. The value of one binary pixel is represented by one bit, and the value of one grayscale pixel is represented by one byte. An ISS technique can process an image absolutely including each grayscale pixel, e.g., one byte; ordinary data is composed of byte. This is why we say that ISS technique can be easily extended to SS technique. In general, VSS is applied to key management covered by a binary image. It is not be suitable for data security, simply because ordinary data are not visual data. However, in some special cases, VSS may be suitable for data security, such as XOR-based VSS. XOR-based VSS with the feature of lossless recovery may process ordinary data because XOR-based VSS can process one binary pixel represented by one bit. Of course, whether XOR-based VSS belongs to the field of classic VSS is another issue.

B. Random Grid-Based VSS (RG-VSS)

RG-VSS is close to probabilistic VSS [38], [39]. The RG encryption procedure in RG-VSS replaces the codebook (basic matrix) design in probabilistic VSS. Thus, in this paper, only RG-VSS is used as an example. In RG-VSS [24], [40], '0' denotes a white pixel and '1' denotes a black pixel. The encrypting and decrypting phases of a typical (2, 2) RG-VSS are presented as follows. Encrypting Step 1: Using a coin flipping function to encrypt 1 RG S1C1 pseudorandomly. Encrypting Step 2: Using Eq. (1) to calculate S1C2. Decrypting phase: S1 = S1C1 ⊗ S1C2 as Eq. (2), where ⊗ indicates stacking (Boolean OR) decryption.

$$S_1C_2(h,w)=\begin{cases} S_1C_1(h,w) & if\ S_1(h,w)=0 \\ \overline{S_1C_1(h,w)} & if\ S_1(h,w)=1 \end{cases} \quad (1)$$

$$S_1'(h,w)=S_1C_1(h,w)\otimes S_1C_2(h,w)$$
$$=\begin{cases} S_1C_1(h,w)\otimes S_1C_1(h,w) & if\ S_1(h,w)=0 \\ S_1C_1(h,w)\otimes \overline{S_1C_1(h,w)}=1 & if\ S_1(h,w)=1 \end{cases} \quad (2)$$

AS0 (resp., AS1) is a white (resp., black) area of S1, a.k.a., AS0 = {(h, w)|S1(h, w) = 0, 1 ≤ h ≤ H, 1 ≤ w ≤ W} (resp., AS1 = {(h, w)|S1(h, w) = 1, 1 ≤ h ≤ H, 1 ≤ w ≤ W}). For any pixel s1 of S1, the probability that the pixel color is white or transparent (0) is represented by P(s = 0), and the probability that the pixel color is black or opaque (1) is represented by P(s = 1). P(S = 0) = 1 − P(S = 1) = 1 − 1 HW H i=1 W j=1 S(h, w), 1 ≤ h ≤ H, 1 ≤ w ≤ W. Definition 1 (Contrast): The image quality of the decrypting secret image S1' in VSS is in general evaluated by contrast, denoted by α, as follows [24]:

$$\alpha=\frac{P_0-P_1}{1+P_1}=\frac{P(S_1'[AS0]=0)-P(S_1'[AS1]=0)}{1+P(S_1'[AS1]=0)} \quad (3)$$

In which P1 denotes the error decrypting probability of the black area of S1 and P0 denotes the correct decrypting probability of the white area of S1.

The contrast will to some degree determine how well human eyes may recognize the decrypted binary secret image. For clarity corresponding to different contrast values, please refer to [41].

C. Polynomial-Based ISS Scheme

To encrypt a grayscale secret image, denoted by S2, the primitive of Shamir's polynomial-based ISS method is used to encrypt the secret pixel value s2 into n corresponding pixels distributed to corresponding n shares. The designed scheme

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

uses part of the thought of the primitive of Shamir's polynomial-based ISS scheme. The primitive scheme is presented below.

III. ALGORITHM

Shamir's Polynomial-Based ISS

Input: A grayscale secret image S2 with size of H × W, and the threshold parameters (k, n)

Output: n shares S2C1, S2C2,⋯ S2Cn

Step 1: P = 251 is selected. For each position (h, w) ∈ {(h, w)|1 ≤ h ≤ H, 1 ≤ w ≤ W} , repeat Steps 2-4

Step 2: For s2 = S2(h, w), if s2 ≥ P, set s2 = P − 1. To encrypt s2 into pieces s2c1,s2c2,⋯s2cn, a k − 1 degree polynomial is constructed as follows. f (x) = (a0 + a1x +⋯+ ak−1xk−1) mod P (4) in which a0 = s2, and ai is random, for i = 1, 2,⋯ k − 1.

Step 3: s2c1 = f (1),⋯ ,s2ci = f (i),⋯ ,s2cn = f (n). (5) where i is in general served as an order label or an identifying index for the i-th participant.

Step 4: Assign s2c1,s2c2,⋯s2cn to S2C1(h,w), S2C2(h,w), ⋯ S2Cn(h, w).

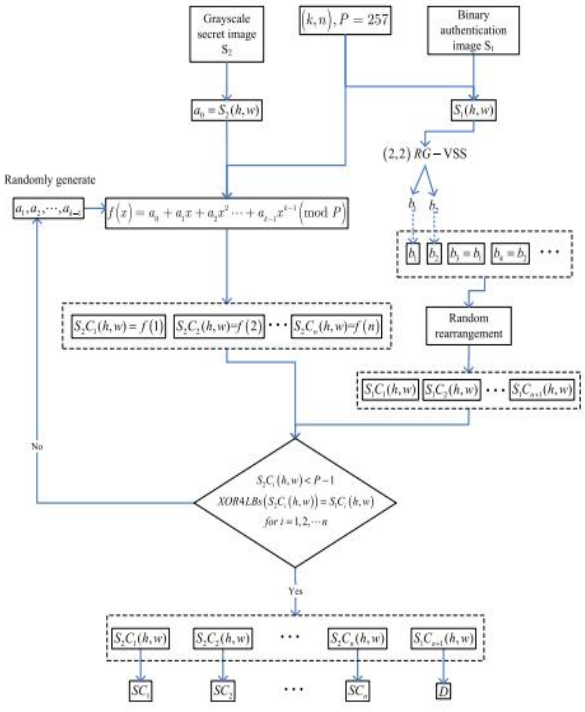
Step 5: Output the n shares S2C1, S2C2, ⋯ S2Cn.

In the decrypting phase, as long as given any k pairs of the n pairs {(i,s2ci)} n i=1, the coefficients of f (i) can be solved by Lagrange interpolation and then set s2 = f (0). With any less than k shares, the secret s2 cannot be universally solved.

IV. THE DESIGNED ISS WITH SEPARATE COMMON SHARE AUTHENTICATION ABILITY

A. The Designed Scheme

The idea of the designed ISS for the (k, n)-threshold with separate share authentication abilities of both dealer participatory authentication and dealer non participatory authentication, denoted by ISS Common Authentication for short, is illustrated. The detailed encrypting algorithm is in **Algorithm 1**, and its corresponding decrypting method is in **Algorithm 2**.



Regarding Algorithm 1, we note the following

1. A binary authentication image S1 is input by the dealer and known among all the participants. The dealer can

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

replace it by setting an authentication password converted into a binary image such as "HIT" as well, which refrains from storing an image.

2. Selecting the prime number P = 257 in step 1, the sharing pixel in the range of[0, 255]and lossless decryption is realized by using screening operation in Step 4 S2Ci (h, w) < P − 1.
3. The purpose of Step 3 is to use the polynomial to realize the characteristics of no pixel expansion and the (k, n) threshold.
4. Step 4 is designed to meet the requirements of XOR4LBs (S2Ci (h, w)) = S1Ci (h, w) to realize share authentication with only XOR4LBs(S2Ci(h ,w)).
   Design idea of the designed image secret sharing with common share authentication ability.
5. The performance is enhanced by utilizing the randomness of b1, b2,⋯ bn+1.
6. Because grayscale a1, a2,⋯ , ak−1 are random, when n − k is small we screen the random values in order to satisfy S2Ci (h, w) < P − 1 and XOR4LBs (S2Ci (h, w)) = S1Ci (h, w), for i = 1, 2,⋯ n in Step 4. In this way, S2 can be losslessly decrypted and common share authentication ability is realized.

Regarding Algorithm 2, we note the following.

1) Before sending the corresponding share, the XOR4LBs(SCij) can be easily obtained.

2) In Step 1 for case 1, the dealer collects shares to check whether S 1 is recognized as S1 by HVS to complete authentication. Thus, our method based on XORing and stacking operations could realize separate share authentication for the dealer participatory case; for case 2, each received XOR4LBs(SCiq) is authenticated by the participant to check whether S1' is recognized as S1 by HVS. Thus, our method based on XORing and stacking operations realizes any two shares' authentication ability by two participants themselves for the case of dealer non participatory authentication.

B. Security Analysis and Proof

Here, we show the security analysis and performance proof of the designed ISSCommonAuthen. In the following, we assume that both the authentication image S1 and the grayscale secret image S2 are natural images, which are independent on each other, namely, they have no correlation.

Algorithm 1 The Designed Image Secret Sharing With Common Share Authentication Ability (ISSCommon Authen)

Input: A binary authentication image S1 with a size of H × W; a grayscale secret image S2 with a size of H×W; threshold parameters (k, n), where 2 ≤ k ≤ n.

Output: Share SCi , i = 1, 2,⋯ n, and a binary authentication share D.

Step 1: Select P = 257. For (h, w) ∈ {(h, w)|1 ≤ h ≤ H, 1 ≤ w ≤ W} , repeat Steps 2-5.

Step 2: Employ (2, 2) RG-VSS to encrypt S1(h, w) to two temporary bits, denoted by b1 and b2. Compute b3 = b1, b4 = b2,⋯ if (n + 1 mod 2) = 0, bn+1 = b2 else bn+1 = b1. Rearrange randomly b1, b2,⋯ bn+1 to S1C1(h, w), S1C2(h, w),⋯ S1Cn+1(h, w).

Step 3: Construct a following k − 1 degree polynomial. f (x) = (a0 + a1x +⋯+ ak−1xk−1) mod P (6) where a0 = S2(h, w), and ai is random, for i = 1, 2,⋯ k − 1. Compute S2Ci (h, w) = f (i), for i = 1, 2,⋯ n.

Step 4: Let XOR4LBs(a) represent the XORing result of the four lower bits of a. If S2Ci (h, w) < P − 1 and XOR4LBs (S2Ci (h, w)) = S1Ci (h, w), for i = 1, 2,⋯ n, go to Step 5; otherwise, go to Step 3.

Step 5: Assign S2Ci (h, w) to SCi (h, w), for i = 1, 2,⋯ n. Set D(h, w) = S1Cn+1(h, w).

Step 6: Output the n gray scale shares SC1, SC2,⋯ SCn, and a binary authentication share D for the dealer. We assume that the collected k gray scale pixels are denoted by sci1 ,sci2 ,⋯scik in the decryption phase corresponding to SCi1 (h, w), SCi2 (h, w),⋯ SCik (h, w). s2 and s1 mean S2(h, w) and S1(h, w), respectively.

Lemma 1: s2 and sci can range from 0 to 255 for i = 1, 2,⋯ n. Proof: Due to P = 257, s2 can range from 0 to 255. S2Ci (h, w) < P − 1, sci can range from 0 to 255 for i = 1, 2,⋯ n.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

Theorem 1: Stacking any two of S1C1, S1C2,⋯ S1Cn+1, the binary secret image S1 is decrypted with contrast.

$$\alpha = \begin{cases} \dfrac{\frac{1}{2} - \frac{C^2_{\frac{n+1}{2}}}{C^2_{n+1}}}{1 + \frac{C^2_{\frac{n+1}{2}}}{C^2_{n+1}}} & when\ n+1\ is\ even \\ \dfrac{\frac{1}{2}\left(1 - \frac{C^2_{\frac{n}{2}} + C^2_{\frac{n+2}{2}}}{C^2_{n+1}}\right)}{1 + \frac{1}{2}\frac{C^2_{\frac{n}{2}} + C^2_{\frac{n+2}{2}}}{C^2_{n+1}}} & when\ n+1\ is\ odd. \end{cases}$$

Proof: According to Eqs. (1) and (2), if the value of a secret pixel s1 is 1 (black), the decrypted bit b1 ⊗ b2 = 1 is always black; If the value of a secret pixel is 0, the decrypted.

Algorithm 2

The Decryption and Authentication in the Designed Image Secret Sharing With Common Share Authentication Ability

Input: Any k grayscale shares SCi1 , SCi2 ,⋯ SCik , a binary authentication share D and a binary authentication image S1.

Output: Decrypted grayscale secret image S 2 with a size of H×W and authenticating result of SCij , for j = 1, 2,⋯ , k.

Step 1: The authentication can be divided into two cases.

Case 1: dealer participatory authentication. For j = 1, 2,⋯ , k, compute XOR4LBs(SCij), and stack XOR4LBs(SCij) and D to obtain the decrypted binary authentication image S1'. If S1' is recognized as S1 by HVS, pass the authentication and go to Step 2; otherwise, a fake share is identified, denoted by i ∗ j , and immediately broadcast the fake one to the other participants.

Case 2: dealer nonparticipatory authentication. For the i p-th participant, prior to share SCi p with the iq-th participant for q = {1, 2,⋯ , k}\p, send XOR4LBs(SCi p) and XOR4LBs(SCiq) to each other first, and stack XOR4LBs(SCi p) and XOR4LBs(SCiq) to obtain the decrypted binary authentication image S1'. Here, q means any one of {1, 2,⋯ , k} except p. If S1' is recognized as S1 by HVS, pass the authentication, send their shares to each other and go to Step 2; otherwise, a fake share is identified, denoted by i ∗ j , and immediately broadcast the fake one to the other participants with S1 and XOR4LBs(SCi p).

Step 2: For each position (h, w) ∈ {(h, w)|1 ≤ h ≤ H, 1 ≤ w ≤ W}, repeat Steps 3-4.

Step 3: Solve Eq. (7) to obtain a0 by Lagrange interpolation.

f (i1) = (a0 + ai1 +⋯+ ak−1i1 k−1) mod P

f (i2) = (a0 + ai2 +⋯+ ak−1i2 k−1) mod P

⋯

f (ik−1) = (a0 + aik−1 +⋯+ ak−1ik−1 k−1) mod P

f (ik) = (a0 + aik +⋯+ ak−1ik k−1) mod P (7)

Step 4: Compute S2'(h, w) = a0.

Step 5: Decrypted grayscale secret image S 2 with a size of H×W and authenticating result of SCij for j = 1, 2,⋯ , k.

bit b1 ⊗ b2 has a 0.5 chance to be white or black since b1 is random. In Step 2 of Algorithm 1, we have b3 = b1, b4 = b2,⋯ . When stacking any two bits of b1, b2,⋯ , bn+1, if the value of a secret pixel is 0, we have P0 = 1 2 ; if the value of a secret pixel s1 is 1 (black), we assume that C2 x = 0 when x < 2, we have

$$P_1 = \begin{cases} \dfrac{C^2_{\frac{n+1}{2}}}{C^2_{n+1}} & when\ n+1\ is\ even \\ \dfrac{1}{2}\dfrac{C^2_{\frac{n}{2}} + C^2_{\frac{n+2}{2}}}{C^2_{n+1}} & when\ n+1\ is\ odd \end{cases}$$

Finally, based on definition 1, the theorem is satisfied.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

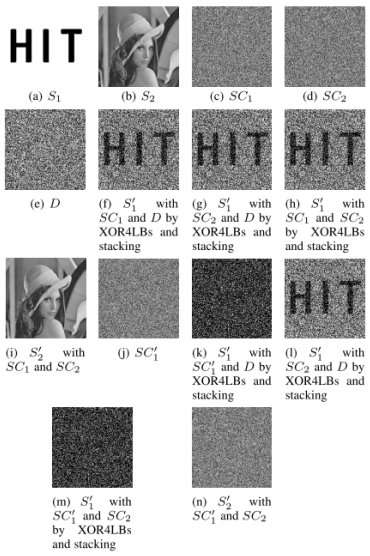
Theorem 2: Using S1 and any two of D and SC1, SC2,⋯ SCn , we will authenticate whether SCi is fake, for i = 1, 2,⋯ n.
Proof: In Step 4 of **Algorithm 1**, XOR4LBs (S2Ci (h, w)) = S1Ci (h, w), for i = 1, 2,⋯ n. According to theorem 1, stacking any two of D and SC1, SC2,⋯ SCn , the binary secret image S1 is visually decrypted. As a result, using S1 and any two of D and SC1, SC2,⋯ SCn , we will authenticate whether SCi is fake, for i = 1, 2,⋯ n. **Theorem 3:** Our designed scheme is a valid ISS approach for the (k, n) threshold with lossless decryption when n − k is limited.
Proof: From Lagrange interpolation and Eq. (7), we can determine a0 and ai uniquely for i = 1, 2,⋯ k−1. According to Lemma 1, s2 = a0 < P; hence, s2 can be losslessly decrypted with sci1 ,sci2 ,⋯scik . If in Eq. (7) only k − 1 equations are constructed, we have P solutions rather than a unique one to Eq. (7). As a result, the secret image S2 cannot be decrypted with k − 1 or fewer shares.
According to the definition of a (k, n)-threshold, the mentioned conditions are satisfied.
In general, grayscale a1, a2,⋯ , ak−1 are random; thus, the number of possible random values are 256k−1. To satisfy S2Ci (h, w) < P − 1 and XOR4LBs (S2Ci (h, w)) = S1Ci (h, w), for i= 1, 2,⋯ n, NA will decrease to
256 k−1 × (256 /257 × 1/2)n= (1/2) n × 256n+k−1/257n , where NA indicates the number of available random values of a1, a2,⋯ , ak−1 satisfying
S2Ci (h, w) < P − 1 and XOR4LBs (S2Ci (h, w)) = S1Ci (h, w), for i = 1, 2,⋯ n.
NA is related to security and encrypting efficiency. A larger NA will result in higher encrypting efficiency and security because the number of brute-force attacks will be higher. We require NA ≥ 2 since if NA = 1, a unique random value is repeatedly used, which is not secure. NA ≥ 4 is suggested for an acceptable performance. Moreover, n−k/ n ≤ 1/2 is suggested for an acceptable performance.

V. EXPERIMENTAL RESULTS

In this section, experiments are performed to verify the effectiveness of the designed ISSCommon Authen. Then, parameters will be discussed. Finally, feature comparisons with related schemes are performed to clarify the advantages of our scheme. We assume that there is no noise in each share because we mainly focus on share authentication rather than robustness.

A. Image Illustration:

In the experiments, since there is no pixel expansion in the designed ISS, the illustrated test images have the same size of256 × 256.
Fig. 6 displays the results of the designed ISS CommonAuthen, where k = 2, n = 2, a binary authentication image S1is demonstrated in Fig. 6 (a) and a gray scale secret image S2is presented in Fig. 6 (b). Figs. 6 (c-d) indicate the output of2 grayscale shares SC1 and SC2. Fig. 6 (e) shows the output



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

Fig. 6. Results of the designed ISSCommonAuthen, where k = 2 and n = 2. (a) A binary authentication image S1; (b) a grayscale secret image S2; (c)−(d) two grayscale shares SC1 and SC2; (e) the binary authentication share D preserved by the dealer; (f) the decrypted binary authentication image S 1 with SC1 and D by XOR4LBs and stacking; (g) the decrypted binary authentication image S 1 with SC2 and D by XOR4LBs and stacking; (h) the decrypted binary authentication image S 1 with SC1 and SC2; (i) the decrypted grayscale secret image S 2 with SC1 and SC2; (j) a fake share SC 1; (k) the decrypted binary authentication image S 1 with SC 1 and D by XOR4LBs and stacking; (l) the decrypted binary authentication image S 1 with SC2 and D by XOR4LBs and stacking; (m) the decrypted binary authentication image S 1 with SC 1 and SC2; (n) the decrypted grayscale secret image S 2 with SC 1 and SC2612authentication share D preserved by the dealer. Figs. 6 (f-h) show the decrypted binary authentication images S 1 with any two of SC1, SC2 and D by XOR4LBs and stacking, respectively, where the authentication image is well visually recognized, and thus, the corresponding share is authenticated. Fig. 6 (i) shows the grayscale secret image decrypted with the 2 shares based on Lagrange interpolation, where the secret image is losslessly decrypted, i.e., Fig. 6 (i) is the same as the adopted secret image in Fig. 6 (b). A randomly generated fake share, SC 1, is demonstrated in Fig. 6 (j), where each grayscale pixel value of the fake share is randomly generated. The decrypted binary authentication images S 1 with any two of SC 1, SC2 and D by XOR4LBs and stacking, respectively, are indicated in Figs. 6 (k-m), where the authentication image is not visually decrypted, and thus, the share SC 1 is fake. Fig. 6 (n) demonstrates the gray scale secret image decrypted

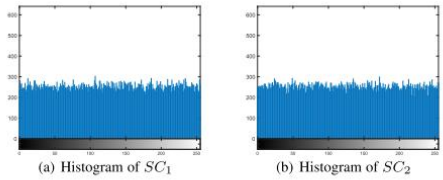

(a) Histogram of SC_1 (b) Histogram of SC_2

Fig. 7. Histograms of shares in Fig. 6.

with SC'1 and SC2 by Lagrange interpolation, which reveals nothing of the secret image; thus, the decryption has failed. We note that the authentication is achieved by using VSS implemented based on probability theory. A binary authentication image with contrast loss may be viewed by stacking and human eyes to some degree in the case of fake or lossy share of a certain ratio. What is the range of tamper tolerant ratio for authentication application is decided by the just recognition point (JRD) of the clarity with regard to contrast in VSS [41]. When average tamper tolerant ratio for authentication application is larger than 0.4, it is hard to recognize the secret image. In addition, Fig. 7 demonstrates share histograms of Figs. 6 (c-d). For each share, the pixel values are uniformly distributed in the range of [0, 255], which to some extent, indicates each share decrypts nothing of the secret image and the security of the designed scheme. In the following, we only illustrate the first share and the decrypted secret image with the first t shares to save space. Fig. 8 displays the results of the designed ISSCommonAuthen, where k = 3, n = 3, the authentication image S1 is demonstrated in Fig. 8 (a) and the grayscale secret image S2 is presented in Fig. 8 (b). Fig. 8 (c) indicates the first share SC1 of the output 3 shares. Fig. 8 (d) shows the output binary authentication share D. Figs. 8 (e-f) show the decrypted binary authentication images S1' with SC1 and D or SC2 by XOR4LBs and stacking, respectively, where the authentication image is well visually recognized, and thus, the corresponding share is authenticated. Figs. 8 (g-h) show the grayscale secret images decrypted with the first 2 or more shares by Lagrange interpolation. From Figs. 8 (g-h), the secret image decrypted with all 3 shares is losslessly decrypted, while nothing of the secret image decrypted with 2 shares is recognized. A generated randomly fake share, SC1', is demonstrated in Fig. 8 (i). The decrypted binary authentication images S1' with SC1' and D or SC2 by XOR4LBs and stacking, respectively, are indicated in Figs. 8 (j-k), where the authentication image is not visually decrypted, and thus, the share SC1 is fake. Figs. 8 (l-m) demonstrate the decrypted secret images S2' with SC1' and some other shares by Lagrange interpolation, which yields no clue about the original secret image; thus, the decryption has failed. Fig. 9 displays the results of the designed ISSCommonAuthen, where k = 3, n = 4, the input binary authentication image S1 is demonstrated in Fig. 9 (a) and the input grayscale secret image S2 is displayed in Fig. 9 (b). Figs. 9 (c) indicates the first share SC1 of the output 4 shares. Figs. 9 (d) shows the

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

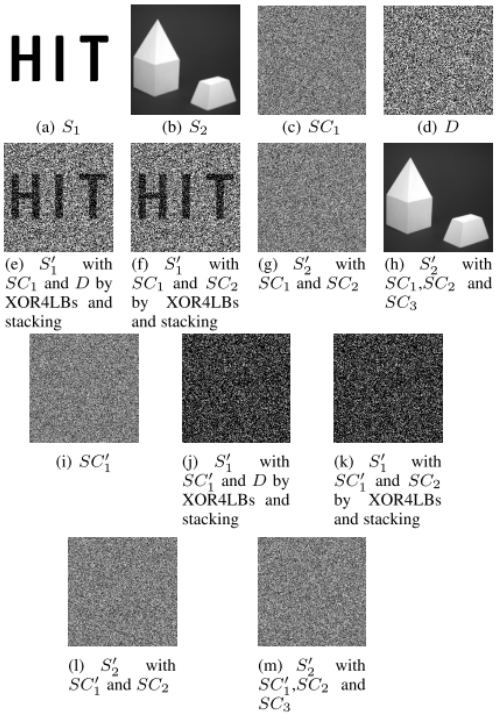


Fig. 8. Experimental results of the designed ISSCommonAuthen, where k = 3 and n = 3. (a) A binary authentication image S1; (b) a grayscale secret image S2; (c) grayscale share SC1; (d) the binary authentication share D; (e) the decrypted binary authentication image S1 with SC1 and D by XOR4LBs and stacking; (f) the decrypted binary authentication image S1 with SC1 and D by XOR4LBs and stacking; (g)− (h) decrypted grayscale secret image S2' with the first two or more shares; (i) a fake share SC1'; (j) the decrypted binary authentication image S1' with SC1' and D by XOR4LBs and stacking; (k) the decrypted binary authentication image S1' with SC1' and D by XOR4LBs and stacking; (l)− (m) decrypted grayscale secret images S2' with SC1' and other one or more shares. output binary authentication share D. Figs. 9 (e-f) show the decrypted binary authentication images S1' with SC1 and D or SC2 by XOR4LBs and stacking, respectively, where the authentication image is well visually recognized, and thus, the corresponding share is authenticated. Fig. 9 (g-i) shows the secret images decrypted with the first 2 or more shares by Lagrange interpolation. From Figs. 9 (g-i), the secret image decrypted with any 3 or more shares is losslessly decrypted, while nothing of the secret image decrypted with 2 or fewer shares is recognized. A generated randomly fake share, SC1', is demonstrated in Fig. 9 (j). The decrypted binary authentication images S1' with SC1' and D or SC2 by XOR4LBs and stacking, respectively, are indicated in Figs. 9 (k-l), where the authentication image is not visually decrypted and thus, the share SC1' is fake. Figs. 9 (m-o) demonstrate the decrypted secret images S2' with SC1' and other one or more first shares by Lagrange interpolation, which yield no clue about the secret image; thus, the decryption is failed. From the above experiments, we can conclude the following.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

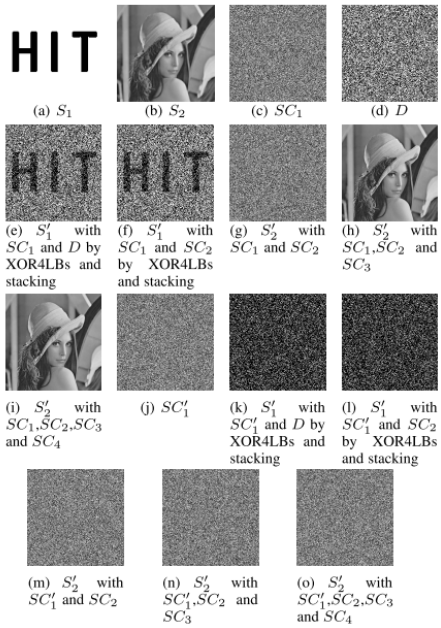
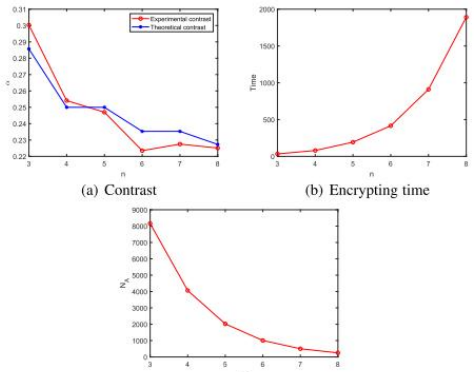


Fig. 9. Additional experimental results of the designed ISSCommonAuthen, where k = 3 and n = 4. (a) A binary authentication image S1; (b) a grayscale secret image S2; (c) the grayscale share SC1; (d) the binary authentication share D; (e) the decrypted binary authentication image S1 with SC1 and D by XOR4LBs and stacking; (f) the decrypted binary authentication image S1 with SC1 and SC2 by XOR4LBs and stacking; (g)− (i) the decrypted grayscale secret image S2' with the first two or more shares; (j) a fake share SC1'; (k) the decrypted binary authentication image S1' with SC1' and D by XOR4LBs and stacking; (l) the decrypted binary authentication image S1' with SC1' and SC2 by XOR4LBs and stacking; (m)− (o) the decrypted grayscale secret images S2' with SC1' and other one or more shares.

1) Each share has no pixel expansion and no cross-interference of the secret image.
2) With fewer than k shares no secret is leaked, which shows the security of the designed ISS.
3) The secret image is losslessly decrypted with any k or more shares.
4) Without sending the share itself, the separate share is visually decrypted to achieve authentication by only XORing and stacking operations, which are only simple operations with low computational complexity.
5) The authentication abilities of both dealer participatory authentication and dealer nonparticipatory authentication are achieved through fusing VSS and polynomial-based ISS.
6) An ISS with separate common share authentication ability for a general (k, n)-threshold is achieved, where $n \geq k \geq 2$.

We note the following. 1) As examples, Fig. 6, Fig. 8 and Fig. 9 are used to validate the effectiveness(characteristics or features) of the designed scheme, where typical thresholds and images are tested. 2) The secret image can be losslessly decrypted by Lagrange interpolation with any k or more shares; thus, any grayscale secret can be input in the designed scheme. 3) Because Definition 1 is given by a statistical result, in VSS the experimental results will be close to the theoretical contrast. Therefore, any binary authentication image can be input in the designed scheme, where close contrast of the decrypted binary authentication image will be obtained. Moreover, the contrast will to some degree determine how well human eyes may recognize the decrypted binary authentication image. For clarity corresponding to different contrast values, please refer to [41]. 4) As a result, we only give some typical experimental results. B. Available Parameters and Quality Discussions We will study the parameters of contrast, encrypting time and NA for k and n given that k and n play important roles in the scheme, where the contrast is that of the decrypted binary authentication image S1 with SC1 and SC2 by XOR4LBs and stacking. Here, x means the x low bits of the share are XORed, where in our designed scheme x = 4. We also intend to study our rationale for setting x = 4. The authentication image and grayscale secret image with a size of 128 × 128 in Fig. 6 are employed in our experiments.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

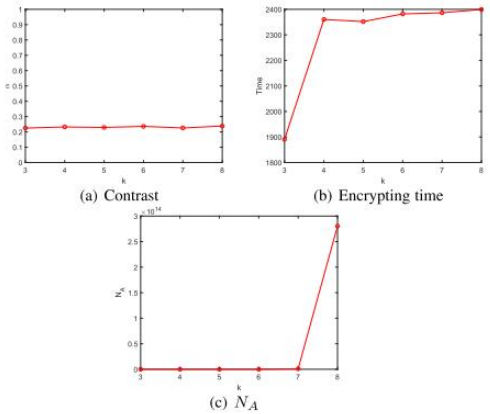


(a) Contrast (b) Encrypting time

(c) N_A

Fig. 10. Contrast, encrypting time and N_A curves for n when $x = 4, k = 3$.

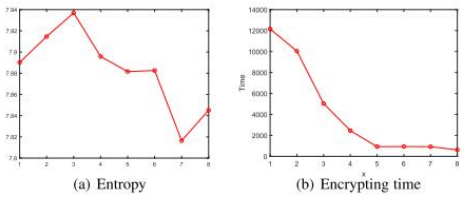
Fig. 10 shows the contrast, encrypting time and NA curves for n when k = 3, where the theoretical contrast is given as well, from which we know the following: 1) The contrast is an approximately monotonically decreasing function of n. The experimental contrast fits with the theoretical analysis, which shows the effectiveness of our analyses. 2) The encrypting time is a monotonically dramatically increasing function of n. As n increases, the screening conditions increase, and thus, the encrypting time increases.



(a) Contrast (b) Encrypting time

(c) N_A

Fig. 11. Contrast, encrypting time and N_A curves for k when $x = 4, n = 8$.



(a) Entropy (b) Encrypting time

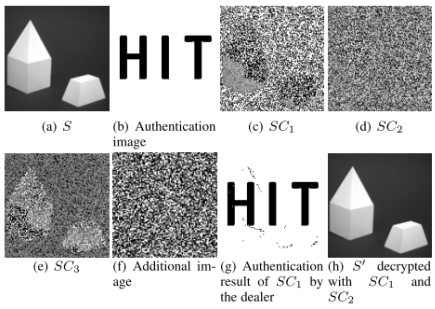
Fig. 12. Entropy, and encrypting time curves for x when $k = 2, n = 6$, $N_A = 16$.

3) NA is a monotonically decreasing function of n. As n increases, the screening conditions increase, and thus, the number of random values decreases. Fig. 11 shows the contrast, encrypting time and NA curves for k when n = 8, from which we know the following: 1) The contrast is nearly the same as k increases. Because S1C1, S1C2,⋯ S1Cn+1 construct a (2, n + 1)-threshold VSS without relations with k. 2) The encrypting time is a monotonically dramatically increasing function of k and slightly increasing when k ≥ 4. As k increases, the screening space increases, and when k ≥ 4, the alternative random values increases. 3) NA is a monotonically increasing function of k and dramatically increasing when k ≥ 7. As

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

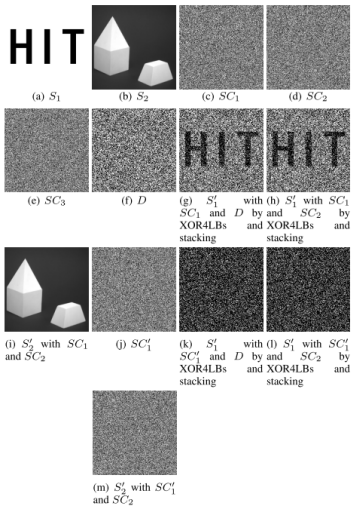
k increases, the number of random values dramatically increases. Fig. 12 intends to convey the rationale for setting x = 4 as follows, where k = 2, n = 6, NA = 16, the entropy is computed by Eq. (8), and the result is that of SC1.

$$H(Y) = -\sum_{y \in Y} Prob(y) \log_2 Prob(y) \qquad (8)$$



(a) S (b) Authentication image (c) SC_1 (d) SC_2
(e) SC_3 (f) Additional image (g) Authentication result of SC_1 by the dealer (h) S' decrypted by with SC_1 and SC_2

Fig. 13. Experiments of Yan et al., where k = 2 and n = 3. (a) A grayscale secret image S; (b) a binary authentication image; (c)− (e) shares SC1, SC2 and SC3; (f) additional binary image preserved by the dealer; (g) the authentication result of SC1 by the dealer; (f) grayscale secret image S1'with SC1 and SC2. 2) 1, 2, 3 and 4 are alternative values of x given that their entropies are larger than 7.88. 3) Considering the encrypting time, x = 4 consumes an acceptable time. 4) In our algorithm, we set x = 4 to balance the security and the encrypting time. C. Comparisons With Related Schemes We will compare the designed ISSCommonAuthen with the related schemes in terms of illustrations and/or features. First, we will compare our method with that of Yan et al. [36] by means of experiments and features where the same secret image as Fig. 13(a) and the (2, 3) threshold will be used. The scheme of Yan et al is chosen for comparison because their scheme has a separate shadow authentication ability for a (k, n) threshold that is also based on a polynomial. Fig. 13 is the experiment of Yan et al., where k = 2 and n = 3, and a grayscale secret image S is in Fig. 13 (a). Fig. 13 (b) is a binary authentication image. Figs. 13 (c-e) shows the three output shares SC1, SC2 and SC3. Fig. 13 (f) displays the binary image preserved by the dealer for authentication. Fig. 13 (g) shows the authentication result of SC1 by the dealer. Fig. 13 (h) shows the secret image decrypted by Lagrange interpolation with the first 2 shadow images. From Fig. 13 (h), the decrypted secret image with any 2 or more shares is lossless. Fig. 14 displays the results of the designed ISSCommonAuthen with the same parameters, where k = 2, n = 3, the input binary authentication image S1 is demonstrated in Fig. 14 (a) and the input grayscale secret image S2 is displayed in Fig. 14 (b). Fig. 14 (c-e) indicate the three shares SC1, SC2 and SC3. Fig. 14 (f) shows the output binary authentication share D. Figs. 14 (g-h) show the decrypted binary authentication images S1 with SC1 and D or SC2 by XOR4LBs and stacking, respectively, where the authentication image is well visually recognized, and thus, the corresponding



(a) S_1 (b) S_2 (c) SC_1 (d) SC_2
(e) SC_3 (f) D (g) S'_1 with SC_1 and D by XOR4LBs and stacking (h) S'_1 with SC_1 and SC_2 by XOR4LBs and stacking
(i) S'_2 with SC_1 and SC_2 (j) SC'_1 (k) S'_1 with SC'_1 and D by XOR4LBs and stacking (l) S'_1 with SC'_1 and SC_2 by XOR4LBs and stacking
(m) S'_2 with SC'_1 and SC_2

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

Fig. 14. Experimental results of the designed ISSCommonAuthen, where k = 2 and n = 3. (a) A binary authentication image S1; (b) a grayscale secret image S2; (c-e) grayscale shares SC1, SC2 and SC3; (f) the binary authentication share D; (g) the decrypted binary authentication image S1' with SC1 and D by XOR4LBs and stacking; (h) the decrypted binary authentication image S1' with SC1 and D by XOR4LBs and stacking; (i) decrypted grayscale secret image S2 with the first two shares; (j) a fake share SC1'; (k) the decrypted binary authentication image S1' with SC1' and D by XOR4LBs and stacking; (l) the decrypted binary authentication image S1' with SC1' and SC2 by XOR4LBs and stacking; (m) decrypted grayscale secret images S2' with SC1' and the other one share. share is authenticated. Figs. 14 (i) shows the grayscale secret images decrypted with the first 2 shares by Lagrange interpolation. From Fig. 14 (i), the secret image decrypted with any 2 or more shares is losslessly decrypted. A generated randomly fake share, SC1', is demonstrated in Fig. 14 (j). The decrypted binary authentication images S1' with SC1' and D or SC2 by XOR4LBs and stacking, respectively, are indicated in Figs. 14 (k-l), where the authentication image is not visually decrypted, and thus, the share SC1' is fake. Fig. 14 (m) demonstrates the decrypted secret images S2 with SC1' and SC2 by Lagrange interpolation, which yields no clue about the secret image; thus, the decryption has failed. According to Figs. 13 and 14, the two schemes are compared as follows. 1) Both schemes have the features of dealer participatory separate shadow image authentication ability,no pixel expansion, lossless decoding, the (k, n) threshold and use of a polynomial. 2) The scheme of Yan et al. can authenticate the shadow image only by the dealer, i.e., dealer participatory authentication, while our method has authentication abilities of both dealer participatory authentication and dealer non participatory authentication. 3) The scheme of Yan et al may have slight information leakage in the shadow image since they only utilize the most significant bit in their scheme; however, because we set x = 4 to balance the security and the efficiency, there is no information leakage in our method. 4) Only the binarization operation is needed for authentication in the scheme of Yan et al., which is slightly lower than ours. Second, we will compare the designed ISSCommonAuthen with Jiang et al.'s work [37].

TABLE I

TIME COMPLEXITY COMPARISON WITH THE RELATED SCHEMES OF LIU *et al.* [35] AND LIU AND CHANG [31]

Scheme	Threshold	Decryption operation	Decryption complexity	Authentication operation	Authentication complexity
Liu *et al.*	(k, n)	Interpolation	$O(k\log^2 k)$	Interpolation	$O(k\log^2 k)$
Liu and Chang	(2, 2)	Matrix turtle shell (MTS), lookup, judge, etc.	Hard to evaluate	MTS, lookup, compare, etc.	Hard to evaluate
Ours	(k, n)	Interpolation	$O(k\log^2 k)$	XOR and OR	$O(k)$

Actually, Jiang et al.'s work is a special case of our scheme when x = 1. According to Fig. 12, Jiang et al.'s scheme needs larger encrypting time than ours. More importantly, because using LSB leads to a smaller value of NA than using 4LBs when value of n − k is larger, their scheme may have failed authentication with a larger value of n − k, and the number of brute-force attacks will be reduced. Third, we will compare the designed ISSCommonAuthen with the related schemes of Liu et al. [35] and Liu and Chang [31] by means of qualitative analyses and time complexity. These schemes are chosen to compare because they also have share authentication ability of ISS. Only qualitative analyses are given rather than a quantitative comparison and illustration because the features are significantly different between theirs and ours, and in addition, only a theoretical proof is performed in Liu et al. [35].

1) In Liu and Chang's scheme, the share authentication ability is chiefly realized based on a turtle shell-based information hiding, among which each share is embedded into a cover image by using information hiding technique. However, it leads to a pixel expansion and high decryption (authentication) complexity. More importantly, their scheme is only suitable for dealer participatory authentication with share sending. By contrast, the designed scheme is suitable for both dealer participatory authentication and dealer nonparticipatory authentication without share sending, which is achieved based on ISS itself rather than information hiding. The authentication is performed based on only XORing and stacking; thus, the designed scheme has low decryption (authentication) complexity and no pixel expansion. Their scheme can achieve tamper detection and location, while ours cannot.

2) Liu et al. embeds an authentication value into a coefficient of the polynomial to extend follow-up improved polynomial-based ISS to achieve share authentication in the field of 251. It can only find the existence of a fake participant when collecting any k or more shares; however, it cannot distinguish which one is fake. Thus, it suffers from lossy decryption, auxiliary encryption, hard fake participant location, and high decryption (authentication) complexity. More

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

importantly, their scheme is only suitable for dealer participatory authentication with share sending. By contrast, the designed scheme is suitable for both dealer participatory authentication and dealer nonparticipatory authentication without share sending. Our scheme can detect each share when collecting the share to achieve separate share authentication ability in the field of 257 with lossless decryption, low encryption and decryption (authentication) complexity, and no auxiliary encryption. 3) Table I shows the theoretical comparison for the time complexity in the stages of the decryption and authentication. Both Liu et al.'s scheme and ours are for the (k, n) threshold, while Liu and Chang's scheme is for the (2, 2) threshold. Since there are many operations in Liu and Chang's scheme and the time complexity analysis is not given in their paper, it is hard for us to evaluate the time complexity. Compared with Liu et al.'s scheme, our scheme has the same decryption complexity and lower authentication complexity. In a word, our scheme has admirable decryption and authentication time complexity compared with related schemes. In summary, compared with the abovementioned schemes, the designed ISSCommonAuthen has the following advantages.

1. Our method is suitable for both dealer participatory authentication and dealer nonparticipatory authentication.
2. The designed ISSCommonAuthen achieves separate share authentication, which can authenticate the share when receiving any other one share.
3. The output share has no pixel expansion, which will save storage.
4. The operation of authentication is simple and no auxiliary encryption is needed, which will save computational power.
5. The secret image are losslessly decrypted.

VI. CONCLUSION

We have created an ISS for a (k, n)-threshold with a separate common share authentication ability that is applicable for both dealer participatory and nonparticipatory authentication in this work. To achieve the extra benefits of distinct share authentication, no pixel expansion, low encryption and decryption (authentication) complexity, lossless decryption, and auxiliary encryption, the developed ISS combines the principles of polynomial and VSS.

The efficiency of the planned method has been demonstrated through experimental illustrations and theoretical studies. To demonstrate the benefits of our programme, we compared its features to those of analogous schemes. In the future, we will primarily concentrate on the following projects. We'll start by expanding our plan to include tamper detection and location. Second, we'll use some other common ISS principles, such as the Chinese remainder theorem-based ISS, to improve our system. Finally, we'll look at the tamper tolerance ratio.

REFERENCES

[1]. A. A. A. El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S. E. Venegas-Andraca, "Secure data encryption based on quantum walks for 5G Internet of Things scenario," IEEE Trans. Netw. Service Manage., vol. 17, no. 1, pp. 118–131, Mar. 2020.

[2]. Y. Zhang, C. Qin, W. Zhang, F. Liu, and X. Luo, "On the faulttolerant performance for a class of robust image steganography," Signal Process., vol. 146, pp. 99–111, May 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S016516841830001X

[3]. X. Zhang, F. Peng, and M. Long, "Robust coverless image steganography based on DCT and LDA topic classification," IEEE Trans. Multimedia, vol. 20, no. 12, pp. 3223–3238, Dec. 2018.

[4]. L. Li, M. S. Hossain, A. A. A. El-Latif, and M. F. Alhamid, "Distortion less secret image sharing scheme for Internet of Things system," Cluster Comput., vol. 22, no. 1, pp. 2293–2307, Nov. 2017, doi: 10.1007/s10586-017-1345-y.

[5]. M. Fukumitsu, S. Hasegawa, J. Iwazaki, M. Sakai, and D. Takahashi, "A proposal of a secure p2p-type storage scheme by using the secret sharing and the blockchain," in Proc. IEEE 31st Int. Conf. Adv. Inf. Netw. Appl. (AINA), Mar. 2017, pp. 803–810.

[6]. Y. Cheng, Z. Fu, and B. Yu, "Improved visual secret sharing scheme for QR code applications," IEEE Trans. Inf. Forensics Security, vol. 13, no. 9, pp. 2393–2403, Sep. 2018.

[7]. A. A. A. El-Latif, B. Abd-El-Atty, M. S. Hossain, M. A. Rahman, A. Alamri, and B. B. Gupta, "Efficient quantum information hiding for remote medical image sharing," IEEE Access, vol. 6, pp. 21075–21083, 2018.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, June 2022
Impact Factor: 6.252

[8]. P. Wang, X. He, Y. Zhang, W. Wen, and M. Li, "A robust and secure image sharing scheme with personal identity information embedded," Comput. Secur., vol. 85, pp. 107–121, Aug. 2019.

[9]. P. V. Chavan, M. Atique, and L. Malik, "Signature based authentication using contrast enhanced hierarchical visual cryptography," in Proc. Electr., Electron. Comput. Sci., 2014, pp. 1–5.

[10]. Y. Li and L. Guo, "Robust image fingerprinting via distortion-resistant sparse coding," IEEE Signal Process. Lett., vol. 25, no. 1, pp. 140–144, Jan. 2018.

[11]. S. Zou, Y. Liang, L. Lai, and S. Shamai, "An information theoretic approach to secret sharing," 2014, arXiv:1404.6474. [Online]. Available: http://arxiv.org/abs/1404.6474

[12]. I. Komargodski, M. Naor, and E. Yogev, "Secret-sharing for NP," J. Cryptol., vol. 30, no. 2, pp. 444–469, Apr. 2017.

[13]. G. Wang, F. Liu, and W. Q. Yan, "Basic visual cryptography using braille," Int. J. Digit. Crime Forensics, vol. 8, no. 3, pp. 85–93, Jul. 2016.

[14]. M. Naor and A. Shamir, "Visual cryptography," in CryptologyEUROCRYPT (Lecture Notes in Computer Science). Perugia, Italy: Springer, 1995, pp. 1–12.

[15]. C.-N. Yang, C.-C. Wu, and Y.-C. Lin, "k out of n region-based progressive visual cryptography," IEEE Trans. Circuits Syst. Video Technol., vol. 29, no. 1, pp. 252–262, Jan. 2019.

[16]. A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[17]. X. Yan, L. Liu, L. Li, and Y. Lu, "Robust secret image sharing resistant to noise in shares," ACM Trans. Multimedia Comput., Commun., Appl., Oct. 2020.

[18]. C. Asmuth and J. Bloom, "A modular approach to key safeguarding," IEEE Trans. Inf. Theory, vol. IT-29, no. 2, pp. 208–210, Mar. 1983.

[19]. X. Yan, Y. Lu, L. Liu, and X. Song, "Reversible image secret sharing," IEEE Trans. Inf. Forensics Security, vol. 15, no. 5, pp. 3848–3858, Oct. 2020.

[20]. Z. Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 383–396, Sep. 2009.

[21]. J. Weir and W. Yan, A comprehensive study of visual cryptography, vol. 5. Berlin, Germany: Springer, 2010, pp. 70–105.

[22]. X. Yan, S. Wang, X. Niu, and C.-N. Yang, "Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality," Digit. Signal Process., vol. 38, pp. 53–65, Mar. 2015.

[23]. Z.-X. Fu and B. Yu, "Visual cryptography and random grids schemes," in Digital-Forensics Watermarking. Auckland, New Zealand: Springer, 2014, pp. 109–122.

[24]. X. Yan, X. Liu, and C.-N. Yang, "An enhanced threshold visual secret sharing based on random grids," J. Real-Time Image Process., vol. 14, no. 1, pp. 61–73, Jan. 2018.

[25]. T. Guo, F. Liu, and C. Wu, "Threshold visual secret sharing by random grids with improved contrast," J. Syst. Softw., vol. 86, no. 8, pp. 2094–2109, Aug. 2013.

[26]. C.-C. Thien and J.-C. Lin, "Secret image sharing," Comput. Graph., vol. 26, no. 5, pp. 765–770, Oct. 2002. Y. Liu, C. Yang, Y. Wang, L. Zhu, and W. Ji, "Cheating identifiable secret sharing scheme using symmetric bivariate polynomial," Inf. Sci., vol. 453, pp. 21–29, Jul. 2018.

[27]. X. Zhou, Y. Lu, X. Yan, Y. Wang, and L. Liu, "Lossless and efficient polynomial-based secret image sharing with reduced shadow size," Symmetry, vol. 10, no. 7, 2018. [Online]. Available: http://www.mdpi.com/2073-8994/10/7/249

[28]. Z. Zhou, C. Yang, Y. Cao, and X. Sun, "Secret image sharing based on encrypted pixels," IEEE Access, vol. 6, p. 15021–15025, 2018.

[29]. C.-C. Lin and W.-H. Tsai, "Secret image sharing with steganography and authentication," J. Syst. Softw., vol. 73, no. 3, pp. 405–414, Nov. 2004.

[30]. Y. Liu and C.-C. Chang, "A turtle shell-based visual secret sharing scheme with reversibility and authentication," Multimedia Tools Appl., vol. 77, no. 19, pp. 25295–25310, Oct. 2018, doi: 10.1007/s11042-018- 5785-z.

[31]. C.-C. Chang, Y.-P. Hsieh, and C.-H. Lin, "Sharing secrets in stego images with authentication," Pattern

Recognit., vol. 41, no. 10, pp. 3130–3137, Oct. 2008. [Online].

[32]. G. Ulutas, M. Ulutas, and V. V. Nabiyev, "Secret image sharing scheme with adaptive authentication strength," Pattern Recognit. Lett., vol. 34, no. 3, pp. 283–291, Feb. 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167865512003479

[33]. P. Li, P. Ma, and X. Su, "Image secret sharing and hiding with authentication," in Proc. 1st Int. Conf. Pervas. Comput., Signal Process. Appl., Sep. 2010, pp. 367–370.

[34]. Y.-X. Liu, Q.-D. Sun, and C.-N. Yang, "(k,n) secret image sharing scheme capable of cheating detection," EURASIP J. Wireless Commun. Netw., vol. 2018, no. 1, p. 72, Apr. 2018, doi: 10.1186/s13638-018-1084- 7.

[35]. X. Yan, Q. Gong, L. Li, G. Yang, Y. Lu, and J. Liu, "Secret image sharing with separate shadow authentication ability," Signal Process., Image Commun., vol. 82, Mar. 2020, Art. no. 115721. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0923596519306940

[36]. Y. Jiang, X. Yan, J. Qi, Y. Lu, and X. Zhou, "Secret image sharing with dealer-participatory and Non-Dealer-Participatory mutual shadow authentication capabilities," Mathematics, vol. 8, no. 2, p. 234, Feb. 2020.

[37]. R. De Prisco and A. De Santis, "On the relation of random grid and deterministic visual cryptography," IEEE Trans. Inf. Forensics Security, vol. 9, no. 4, pp. 653–665, Apr. 2014.

[38]. C.-N. Yang, C.-C. Wu, and D.-S. Wang, "A discussion on the relationship between probabilistic visual cryptography and random grid," Inf. Sci., vol. 278, pp. 141–173, Sep. 2014.

[39]. O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," Opt. Lett., vol. 12, no. 6, pp. 377–379, 1987.

[40]. X. Yan, Y. Lu, H. Huang, L. Liu, and S. Wan, "Clarity corresponding to contrast in visual cryptography," in Proc. 2nd Int. Conf. Young Comput. Sci., Eng., Harbin, China, Aug. 2016, pp. 249–257, 2016, doi: 10.1007/978-981-10-2053-723.