ISSN 2395-1621

Fraud prevention by visual secret sharing multicomponent using Hybrid codebook

[#1]Pranjali Mahajan, [#2]Swati Rupnwar, [#3]Sneha Tekale

[1]pranjalimahajan11@gmail.com
[2]swatirupnawar55@gmail.com
[3]snehatekale007@gmail.com

JSPM's BSIOTR, Wagholi.

ABSTRACT

Visual secret sharing, or the questionable visual cryptography, may be a well-known theme that encrypts a secret image into many unimportant share pictures, sometimes written on transparencies, and decrypts as stacking some or all share pictures by the human sensory system. Additional and additional researches concerning visual secret sharing and its applications are recently planned. sadly, the cheating attack within which malicious participants cheat the honest one by shaping a pretend share image has existed. Since 2006, some cheating hindrance schemes are planned however suffered from one or additional disadvantages as follows: (1) maintaining additional share pictures accustomed verify the integrity of a share image before stacking, (2) introducing additional constituent growth,(3) raising significant computation price, and (4) giving ambiguous cheating detection. During this paper, a multi-factor cheating–preventing theme, aiming at exploiting the hybrid codebook to cover the extra verification pictures into the share pictures, has been planned while not suffering the above-named deficiencies. Two-factor cheating– detection exploits the planning of verification to each share pictures and stacked results to discourage attackers' cheating.The experimental results demonstrate the planned theme is possible.

ARTICLE INFO

Article History

Received:20th October 2015

Received in revised form :

22nd October 2015

Accepted:23rd October, 2015

Published online :

24th October 2015

I. INTRODUCTION

With the progress of engineering and therefore the development of networks, the transmission of digital pictures becomes a daily operation. For the protection of secret pictures transmittad over public networks, trendy cryptosystems like DES, and AES are projected to ensure confidentiality. However these cryptosystems are dear in each coding. Therefore, transmission security, like digital watermarking, and image authentication, becomes imperative in each domain and business.

Visual secret sharing (VSS), initial projected by Nair and Shamir in 1995, encodes a secret image to form many purposeless shares later distributing to participants. Participants decrypt the key by stacking the collected shares and victimization human sensory system with none computation concerned to reconstruct the key image. No extra or difficult computation is needed. A k-out-of-n visual secret sharing theme, additionally referred to as (k,n) VSS, suggests that a secret image is encoded into n shares, and stacking any k or additional shares ðk half dozen no will reconstruct the key image. In (2,2) VSS theme, a secret image is encoded into 2 share pictures Sturmarbeiteilung SB by a codebook.With the colour of a picture element of secret image, Sturmarbeiteilung Associate in Nursingd SB square measure allotted an adaptive sub-block for secret info. the scale of subblocks is two such the scale of the share pictures and reconstructed image is swollen. In the VSS atmosphere, cheating happens once some malicious participants, referred to as cheaters, will fool or cheat honest participants. In 2006, Horng et al. claimed the (k,n) VSS exists the cheating drawback if k < n. Table a pair of shows a codebook of (2,3) VSS theme And Table three shows an example in such some way that a cheating attack is simple to demonstrate.

Participants A and B might cheat the honest participant C by means that of giving a pretend share image. Assume that Participants A and B acquire sub-pixel and , severally. The participants A and B will infer the subpixel of participant C is in line with the (2,3) codebook. Taking the preceding actions, participants A and B will do nothing if they hope the stacked result with participant C is white, or modify their sub-pixel as or if they hope the stacked result with

participant C is black. because the same method, if the participants A and B acquire sub-pixel and , severally. The participants A and B will infer the sub-pixel of participant C is in line with the (2,3) codebook. Then, participants A and B will do nothing if they hope the stacked result with participant C is black, or modify their sub-pixel as if they hope the stacked result with participant C is white. Therefore, the cheating drawback will exist in (k,n) VSS if k < n . principle and Laih planned 2 approaches to find the pretend shares. the primary approach desires the assistance of at rusty authority (TA). TA holds a check share. If stacking the check share with the share of a participant, the verification image is reconstructed to differentiate the participant.

The second approach could be a quite (k,n) VSS theme. Any 2 of them will reveal the verification image accustomed verify the validity of a share image, whereas a minimum of k shares will reconstruct the key image. This approach will work with none facilitate of the TA. In 2006, whereas Prisco and Santis provided a proper definition of cheating, Horng et al.planned 2 schemes to stop VSS from cheating. Within the initial theme, each participant has 2 share pictures: the generic share image and also the verification share image wont to manifest the validity of the generic share images of the opposite participants. Participants should maintain further share pictures. The second theme adopted a (2,n + e) VSS theme during which the dealer generates n + e shares however deliver n share pictures to n participants whereas l shares square measure discarded. sadly, the ambiguous stacked result cannot tell participants if the cheating will happen. Tsai et al. planned a brand new cheating–prevention theme by victimisation the Genetic formula, that is computation-expensive. Hu and Tzeng (2007) planned 3 cheating strategies and a preventive theme. the primary and second cheating strategies aim at the overall VSS theme within which the shares area unit insignificant. The third cheating technique attacks the denotative VSS theme wherever the shares area unit meaty. However, Tsai and Horng gave a proper definition of cheating within the (k,n) VSS theme in terms of authentication, brightness and security condition. They argued that the cheating operation in (n,n) VSS doesn't work. as an example, the slicker has no plan of the opposite share in (2,2) VSS so it's nonsense to pretend a helpful share. moreover, they showed that Hu and Tzeng's initial and second cheating strategies area unit impossible, preventive theme problematic. Unfortunately, the on top of mentioned cheating hindrance schemes suffer from one or additional disadvantages of the following:

(1) further share pictures accustomed verify the integrity of a share image prior to stacking,
(2) extra pixel expansion,
(3) cost increasing, and
(4) uncertainty.

Without removing all the disadvantages mentioned higher than, cheating attacks render VSS useless specified VSS and its applications cannot realistically get off the bottom. This paper proposes a replacement cheating–preventing theme by combining 2 VSS schemes in one. It adopts the hybrid codebooks which square measure skillfully designed to attain the goal that any 2 shares may be wont to reconstruct 2 secret pictures, i.e., the verification and therefore the original secret pictures. the key issue encountered during this paper is the way to style the hybrid codebook. The verification images devoted to attest the validity of the opposite shares. Any 2 shares will reconstruct a definite verification image by suggest that of shifting the generic shares in several locations. With reconstructed unambiguous verification pictures, the validity of shares may be attested so the projected scheme will discover faux shares. The projected theme removes all the disadvantages existing within the connected works.

Firstly, the verification pictures square measure designed to cover within the generic share pictures instead of appending with them to keep up additional verification shares.

Secondly, the computation price in coding is low, up to that of generic VSS scheme while not introducing additional computation cost.

Finally, once the cheating attack happens, the projected theme not solely provides AN ambiguous results of reconstructed secret image however additionally provides the second cheating proof by giving AN ambiguous results of reconstructed verification image. The experimental results and comparison with the present themes within the literature demonstrate the projected scheme will add a higher manner.

II. LITERATURE REVIEW/RELATED WORK

[1]" Visual cryptography, in: Proceedings of Advances in Cryptology:", In this paper we consider a new type of cryptographic scheme, which can decode concealed images without any cryptographic computations. The scheme is perfectly secure and very easy to implement. We extend it into a visual variant of the *k* out of *n* secret sharing problem, in which a dealer provides a transparency to each one of the *n* users; any *k* of them can see the image by stacking their transparencies, but any *k*−1 of them gain no information about it.

[2]" Cheating in visual cryptography, Des. Codes Crypt.", Visual cryptography is an encryption technique to encrypt a secret image into different shares such that stacking a sufficient number of shares reveals the secret image. Most of the previous research work on VC focuses on improving two parameters: pixel expansion and contrast. We considered the cheating problem in the visual cryptography scheme and investigate various cheating prevention schemes. During the reconstruction of the secret, one participant, called cheater, may release a false share. As a result a fake image will be revealed.

[3]" Some new types of visual secret sharing schemes, in: Proceedings of National Computer Symposium", Over the past few years, there is increasing concern over personal information in computer systems has increased interest in data security like Visual Cryptography. Visual cryptography divides secret images into one and morerandom shares and provides secured digital transmission which is used only for one time. The original images can be reuse by using this scheme. It is easy and uncomplicated technique to execute the secret image for shadow images (share of image). In this paper concept of visual cryptography is discussed which is a perfectly secure method of keeping images secret, for feasible use in biometric identification technique and protection such as fingerprint images for the purpose of user authentication along with various visual cryptography schemes as an literature review. This paper not only reviews

how to apply sharing of single secrete image and multiple secrete image on black and white as well as on color images but also a comparative analysis on various visual cryptography schemes is also performed.

III.LIMITATIONS

1) Codebook design of VC is case by case,there is no efficient generic method of generating(k,n) codebooks with minimizing the pixel expantion.

2) To our experience it spends a couple of minute on stacking only two shares.

It is impractical and time consuming to stack 3 OR 4 shares

IV.PROPOSED WORK

Based on a (2,3) VSS scheme, a secret image S is turned into three shares S0, S1, S2 while stacking any two shares can reconstruct the secret image. At the same time, the additional three verification images V0, V1, and V2, used to prevent cheating, are hidden in the above shares by involving (2,2) VSS. Assume that the images S, V0, V1, and V2 are kept secret from all participants by the dealer. Prior to describing the proposed scheme, some definitions are given.

Definition 1. is a (2,2) visual secret sharing function with the input X, an original secret image, and the output Y0 and Y1, two share images. That is , $Y_0 \| Y_1 \leftarrow f_{(2,2)}(X).$ where || is the concatenation operation.

Definition 2. $\bar{f}_{(2,2)} : X \| Y \rightarrow Z$ is a (2,2) visual secret sharing function with the input X, an original secret image, and the input Y, a corresponding share image. The output Z is the other share image. That is, $Z \leftarrow \tilde{f}_{(2,2)}(X \| Y).$.

Definition 3 $f_{(2,3)} : X \rightarrow Y_0 \| Y_1 \| Y_2$ is a (2,3) visual secret sharing function with the input X, an original secret image, and the output Y0, Y1 and Y2, three share images.That is,. $;Y_0 \| Y_1 \| Y_2 \leftarrow f_{(2,3)}(X).$

Definition 4. $\bar{f}_{(2,3)} : X \| Y_0 \rightarrow Y_1 \| Y_2$ is a (2,3) visual secret sharing function with the input X, an original secret image, and the input Y0, a corresponding share image. The output Y1 and Y2 are the other two share images. That is, $Y_1 \| Y_2 \leftarrow f_{(2,3)}(X \| Y_0).$ The proposed cheating-preventing method consists of four phases: hybrid codebook design, decomposition phase, encoding phase, and decoding phase.

Objective:

1)To improve privacy setting of social networking sites, in particular for images posted by using the cheating prevention techniques of VSS without pixel expansion.

2)To develop a novel approach such that access is restricted based on the generated shares and the reconstruction of image at the time of decryption is given to those who has the verifying share.

V. ARCHITECTURE

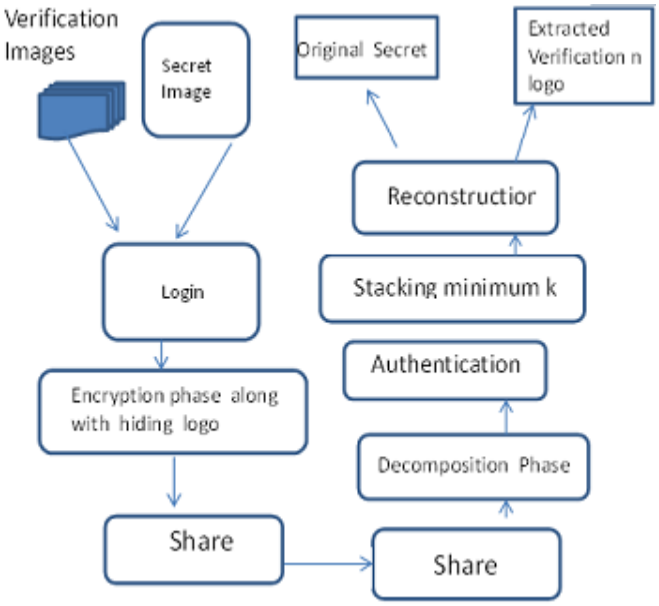

Fig. Architecture diagram

Encoding phase

The encoding phase encompasses some operations including encoding a quarter of secret and hiding a verification logo.

Step (1) Encoding the first quarter of secret

Encode the macro-block S0,0 to generate S00 ;0, S1 0;0; and S2 0;0 of the shareimages S0, S1, and S2 by the (2,3) VSS scheme according to the codebook.

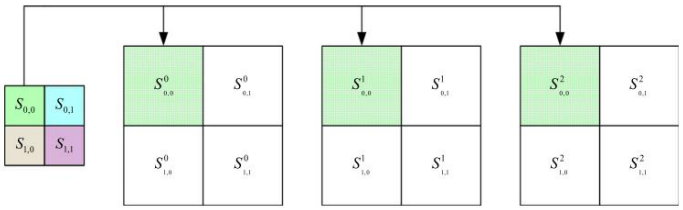

Fig. 1 shows the processes of step 1 in the encoding phase.

Step (2) Hiding the first logo by

Given S00 ;0 and the verification image V0, S10 ;1 of the share image S1 is generatedby the (2,2) VSS scheme according to the codebook . Fig. 2 shows theprocesses.

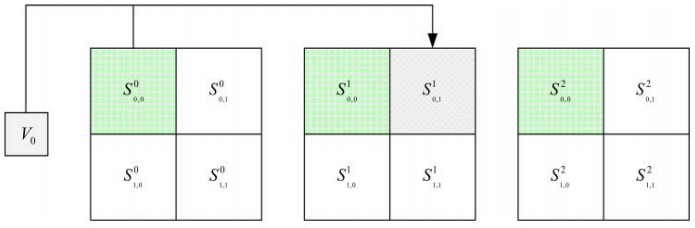

Fig. 2 shows the processes of step 2 in the encoding phase.

Step (3) Encoding the second quarter of secret by Encode the macro-block S0,1 and S1 0;1 to generate S00 ;1 and S20 ;1 of the share image S0 and S2 by the (2,3) VSS scheme according to the codebook. Fig. 3 shows the processes

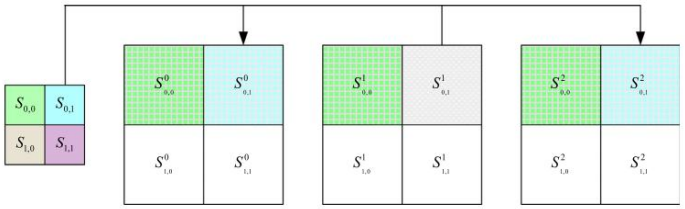

Fig.3 shows the processes of step 3 in the encoding phase.

Step (4) Hiding the second logo by Given S10 ;1 and the verification image V1, S2 1;0 is generated by the (2,2) VSS scheme according to the codebook. Fig. 4 shows the processes

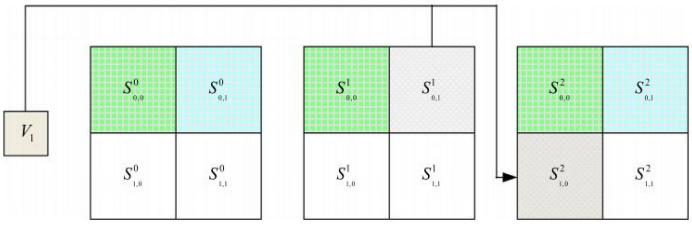

Fig.4 shows the processes of step 4 in the encoding phase.

Step (5) Encoding the third quarter of secret by Encode the macro-block S1,0 and S2 1;0 to generate S01;0 and S11 ;0 of the share image S0 and S1 by the (2,3) VSS scheme according to the codebook in Table 4(a). Fig. 5 shows the processes.

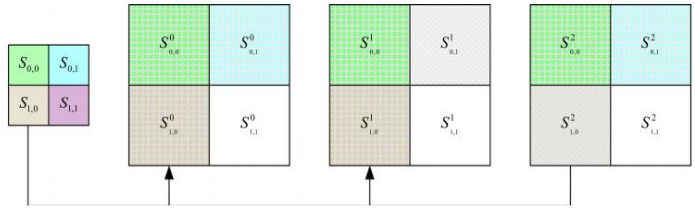

Fig.5 shows the processes of step 5 in the encoding phase.

Step (6) Hiding the third logo by Given S21;0 and the verification image V2, S01;1 is generated by the (2,2) VSS scheme according to the codebook in Table 4(b). Fig. 6 shows the processes.

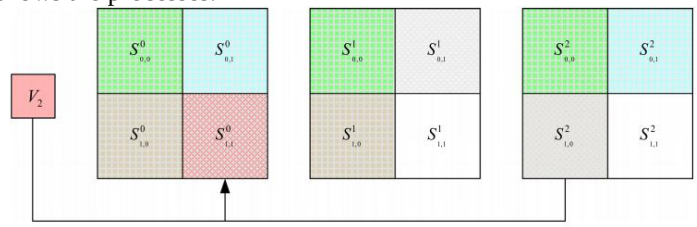

Fig.6 shows the processes of step 6 in the encoding phase.

Step (7) Encoding the last quarter of secret by Encode the macro-block S1,1 and S0 1;1 to generate S11 ;1 and S21 ;1 of the share image S1 and S2 by the (2,3) VSS scheme according to the codebook in Table 4(a). Fig. 7 shows the processes. By concatenating S0i ;j; S1i ;j; and S2i ;j for all i and j (I = 0, 1 and j = 0, 1), we have the share images S0, S1, and S2, distributing to three participants P0, P1, and P2, respectively.

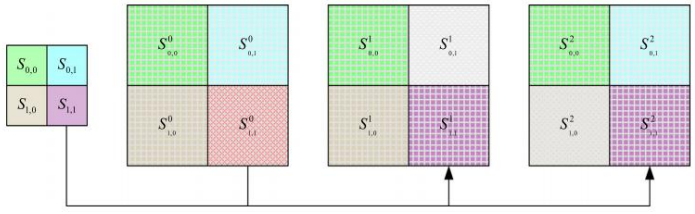

Fig.7 shows the processes of step 7 in the encoding phase.

Decoding phase

If a participant wants to reconstruct the secret image, he has to check the validity of the share images from other participants by reconstructing the verification images. For example, P0 wants to reconstruct the secret image S with P1, he discloses the verification image V0 by stacking the macro-block S00 ;0 of the share S0 and the macro-block S10;1 of the share S1. If the stacked result shows the meaningful or recognizable verification image V0, the P0 reconstructs the secret image S0 by stacking S0 and S1. The P0 checks whether the shape or information of S00;0 in the reconstructed secret image is unambiguous or not. If both S00;0 and the extracted verification image are unambiguous, P0 trusts the correctness of the share S1 and the reconstructed secret. Note that the validation process of verification message is either true or false. Precisely, if partial area of verification message is vague or ambiguous, participants should reject the share intended to stack

VI. ALGORITHMS

Cryptography or **cryptology (encryption and Decryption)** is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analysing protocols that block adversaries;various aspects in information security such as data confidentiality, data integrity, authentication, Image processing and non-repudiationare central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics,computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Encryption is defined as:

$$C=(P\oplus K0)\boxplus K1 \qquad (1)$$

Show the decryption equation, that is, show the equation for P as a function of C, K0 and K1

- C = ciphertext
- P = plaintext
- K = secret key
- K_0 = leftmost 64 bits of secret key
- K_1 = rightmore 64 bits of secret key
- $\oplus$ = bitwise exclusive or (XOR)
- $\boxplus$ = addition mod 264

XORing of Image

$$img3= img1 \oplus img2 \qquad (2)$$

Where,

img1 & img2 is the input image.

img3 is the output image(merge image).

VII. CONCLUSION

In this paper, a new cheating–preventing scheme has been proposed to benefit from a combination of two general VC codebooks. With the hybrid codebook, the verification images are skillfully hidden in the shares to check whether the intended share is fake. In such a way the cheating attack in VSS can be detected. Compared with the related cheating prevention schemes, the present scheme has the following advantages:

(1) participants need no extra share to verify the validity of the other,

(2) the computation cost is low, and

(3) multi-factor cheating detection is involved.

REFRENCES

[1] K. Martin, R. Lukac, K.N. Plataniotis, Efficient encryption of wavelet-based coded color images,Pattern Recogn. 38 (7) (2005) 1111–1115.
[2] T.H. Chen, T.H. Hung, G. Horng, C.M. Chang, Multiple watermarking based on visual secret sharing, Int. J. Innov. Comput., Inform. Control 4 (11) (2008) 3005–3026.
[3] Z.M. Lu, C.H. Liu, H. Wang, Image retrieval and content integrity verification based on multipurpose image watermarking scheme, Int. J. Innov. Comput., Inform. Control 3 (3) (2007) 621–630.
[4] M. Naor, A. Shamir, Visual cryptography, in: Proceedings of Advances in Cryptology: Eurocrypt94,Lecture Notes in Computer Science, vol. 950, pp. 1–12, 1995.
[5] G.B. Horng, T.H. Chen, D.S. Tsai, Cheating in visual cryptography, Des. CodesCrypt. (Feb.2006)219–236.
[6] C.N. Yang, C.S. Laih, Some new types of visual secret sharing schemes, in: Proceedings of National Computer Symposium., vol. 3, pp. 260–268, December,1999.
[7] C.M. Hu, W.G. Tzeng, Cheating prevention in visual cryptography, IEEE Trans. Image Process. 16(1) (2007) 36–45.
[8] D.S. Tsai, T.H. Chen, G. Horng, A cheating prevention scheme for binary visual cryptography withhomogeneous secret images, Pattern Recogn. 40 (8) (2007) 2356–2366.
[9] D.S. Tsai, G. Horng, Cheating in visual cryptography revisited, in: Proceedings of 17th Information Security Conference, pp. 769–771, 2007.
[10] P.A. Eisen, D.R. Stinson, Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels, Des. Codes Crypt. 25 (2002) 15–61.