Cheating Prevention inVisual Cryptography Scheme using Two Factor Hybrid Codebook

Jyoti Rao,
Research scholar of JJTU , Rajasthan , India
jyoti.aswale@gmail.com

Dr. Vikram Patil
Research guide at JJTU , Rajasthan , India & Principal K.B.P. College of Engg.,Satara Maharashtra

Abstract—In today's era of internet security has become integral part of information technology. Its crucial to maintain information security in the era of active users of social networking , and cloud computing. One technique being used maintaining information security is cryptography which deals with study of confidentiality, data security , entity authentication.

The mechanism of visual cryptography is widely used approach which encrypts the secrete image into the many meaningless share images and decrypts as stacking some or all share images by human visual system. There are many methods presented for visual cryptography with their own advantages and disadvantages. Recently new cheating–preventing scheme has been proposed to benefit from a combination of two general VC codebooks. This method resulted into number of advantages such as computation cost is low; multi factor cheating detection is involved etc. However, we identified two research problems such as 1) there is no efficient generic method of generating (k,n) codebooks with minimizing the pixel expansion, 2) it is impractical and time-consuming to stack three or four shares. Therefore in this project our aim is to extend this hybrid codebook based method with goal of overcoming above two listed limitations. We are presenting the efficient approach for codebooks generation with less timing consuming while decryption.
.

Keywords—Contrast;Share;Stacking;Pixel; (key words)

I. INTRODUCTION

Even though the computer technology is advanced and the efforts of computerizing every possible systems available is nowadays current trend. Still using computer to decrypt a secret is not feasible in some situation. In these situations, human visual systems is one of the most convenient and easy to available tool to do checking and secret recovery.

Secret sharing using visual cryptography is different from typical cryptographic secret sharing scheme. VSS allows each participant to keep a portion of secret and provides a way to know at least part of the secret . A large no. of keys are required for the solution but using multiple secrets.

Since its inception visual cryptography has been advanced and had cope for more research for reducing pixel expansion , contrast ,color visual cryptography, etc and even guaranteed as much secure while malicious user's attacks found. But as more work done, it is seen that cheating is possible in VSS causing the generation of fake shares. Thus, many cheating prevention schemes were presented.

This paper consists of the work done in this area of cheating prevention .The proposed work gives rise to the reduction of pixel expansion in two-factor cheating prevention and making use of hybrid code-book design for the encryption process. In next section the future work are discussed, along with the final conclusion.

II. RELATED WORK

A. Basic Visual Cryptography

In 1994, Naor and Shamir proposed the basic model of visual cryptography scheme which can decode concealed image into number of shares without any cryptographic complex computation. When the *k* shares are stacked together, the human eyes do the decryption without any knowledge of cryptography and without performing any computations whatsoever. This is advantage of visual cryptography over the other popular conditionally secure cryptographic schemes. It assumes that the image is a collection of black and white pixels, each pixel is handled individually and it should be taken into account that the white pixel represents the transparent colour. The encryption problem is expressed as a *k* out of *n* secret sharing problem. Given the image, *n* transparencies are generated so that the original image is visible if and only if any *k* of them are stacked together otherwise image remains ambigeous. [1]

The pixel expansion problem that occurred in previous VCS scheme using general access structure was solved by the new algorithm proposed by Lee and Chiu [2]. The extended VC algorithm for GAS which adds a meaningful cover image in each share, does not generate noisy pixels. [2].

B. Literature Survey

Several papers have proposed to solve the cheating problem. First cheating attack detected by Horng et al. proposed two methods to prevent the dishonest participants (referred to as cheaters) collude and want to cheat other participants, which is known as cheating activity(CA). CA can affect unpredictable damage to the participants; therefore, the honest participants accept a fake secret image different from the actual authenticated secret image. They designed two types of cheating prevention techniques, share authentication and blind authentication[3]:

. Share authentication based: By using the verification image authentication process performed against all shares along with malcious share, generated by the cheaters. However, if the

malcious share can pass the authentication, the victim will accept the stacking result.

. Blind authentication(BA) based: With absence of verification image, the cheaters found it difficult to predict the structure of the shares of the other participants is hard.

Later, Hu and Tzeng presented three cheating methods and applied them on attacking existent VC or extended VC schemes. They improved one cheat-preventing scheme. They proposed a generic method that converts a VCS to another VCS that has the property of cheating prevention. The overhead of the conversion is optimal in both contrast degression and pixel expansion. HTCP scheme denotes Hu and Tzengs transformation scheme, which is share authentication based.[4]

Tsai et al. proposed a cheating prevention scheme in 2007, in which shares are generated by Genetic Algorithms. Each qualified subset only disclose the appropriate reconstructed secret image and the others are not known to potential forgers. [5]

In 2010 at Third International Conference on Information and Computing (ICIC), 9.Bin YU, Jin-Yuan LU, Li-Guo Fang presented participants colluding is an important issue of cheater detectable visual cryptography schemes. Intervention of a trusty third party, a co-cheating prevention visual cryptography scheme (CCPVCS) is proposed by authors. Checking effeciency is improved by verifying the truth of several shares simultaneously, with designed special verification shares. However, the number of verification shares which kept by the third party is large .[6]

At Third IEEE International Conference on Computer Science and Information Technology, Qin Chen et al. proposed (n, n) threshold visual cryptography scheme for cheating prevention to improve the generic transformation for cheating prevention scheme (GTCP).
[7]

Horng et al. presented in 2012, the cryptographic analysis of the Hu,Tzeng CPVSS scheme and show that it is not cheating immune. They also outline an improvement that helps to overcome the problem. The proposed an (n, n) VCS for cheating prevention, in which each participant holds his own private verification image, to improve the GTCP. []

Chang et al. proposed in sixth international conference on Genetic and Evolutionary Computing (ICGEC) a verifiable visual cryptography (VC) scheme for checking the validness to the shares engaged in a VC decoding instance. The idea is to stamp a continuous pattern on the shares belonging to the same secret image, and a part of the pattern can be revealed through aligning and stacking half of two shares together. [9]

Cheating is possible in k-out-of-n VC schemes as proved by Horng et al. presented two kinds of the cheating prevention schemes for protecting honest participants. The authors proposed a new authentication based cheating prevention scheme. The scheme is constructed with Naor-Shamir's VC scheme. The scheme presented adopts the black patterns encorporated into verified stacking result. The number of black patterns is used to check whether a share transparency is fake or not. This scheme is effective against cheating without the more expansion for a pixel than previous schemes[10]

The Horng et al revisited some well-known cheating activities and CPVSS schemes, and then categorize cheating activities into meaningful cheating, non-meaningful cheating, and meaningful deterministic cheating. Moreover, authors analyzed the research challenges in CPVSS, and presented a new cheating prevention scheme which is secure authentication based. This scheme is proved to be secure against the meaningful deterministic cheating , does not rely on added transparencies.and has less pixel expansion than previous schemes.[11]

Many of the Visual secret sharing (VSS) presented earlier suffered from pixel expansion , which is denoted by m t as compared with the original secrets.. Random grid (RG) is an approach to solve pixel expansion problem. However, the previous VSS methods using RGs are tied to (2,n),(n,n) and (k,n) schemes. Xiaotian Wu, Wei Sun presented RG-based VSS schemes for general access structures. The proposed algorithms can encrypts one secret image into n random grids while qualified sets can recover the secret visually. Also , a cheat preventing method is presented and is efficient and giving scope for more complex sharing strategies to research furthur.[13]

Chih-Hung Lin et al. proposed a new cheating prevention scheme to benefit from a combination of two general VC codebooks. With the design of hybrid codebook, the verification images are abstracted in the shares to check against the intended share, whether it is fake. Thus, the cheating attacks can be detected. The case of (2,3) is mainly taken into consideration. This scheme has following advantages over the present scheme: (i) participants need no extra share to verify the validity of the other, (ii) the computation cost is low, and (iii) multi-factor cheating detection is involved. There cons for this scheme as follows: the codebook design of VC is case-by-case, there is no efficient generic method of generating (k,n) codebooks with minimizing the pixel expansion. This gives rise to design of two-factor VC scheme with cheating prevention into case by case. Secondly, it spends a couple of minutes on stacking only two transparencies to reveal the secret. If stacking three, tens of minutes are needed.[12]

So, the need of minimizing the pixel expansion and the time taken for the encryption and decryption of shares should be reduced. So, the proposed system is focussing on this issues to be resolved with the efficient cheating detection and prevention process.

III. PROPOSED APPROACH FRAMEWORK AND DESIGN

A. PROBLEM DEFINITION

Different areas work on the sensitive data so that the need of secure data transmission is increasing. Such areas include

the highly secured infrastructures where collaborators will work together but should have mutual authentication, for securing joint account of people belonging to organizations like bank account or defense offices, research laboratory, military offices, investigating offices, various government offices etc. These are some of the applications in which this type of work can be used to provide the security to the data while transmitting through sender to receiver.

For this reason , we need to develop such a system where the response time should be very less and the cheating prevention goal should be preserved.

The two factor cheating prevention visual secrete sharing schemes to benefit from a combination of two general VC codebooks. The resultant method will have advantages such as computation cost is low. The efficient generic method of generating (k,n) codebooks will be encorporated for minimizing the pixel expansion .Therefore this system aim to extend this hybrid codebook based method with goal of implementing less time - consuming process for reconstruction of secret image while decryption. Digital images,printed images, hand painted pictures are used for sharing the secret image process.

The verification image is used to authenticate the validity of the other shares. Any two shares can reconstruct a distinct verification image by means of shifting it in different locations into generic shares. The reconstructed identical verification images which are used for validating shares can be authenticated so that the proposed scheme can detect fake shares. Once the cheating attack found, the proposed scheme not only gives an ambiguous result of reconstructed secret image but also by giving an ambiguous result of reconstructed verification image.

B. EXISTING SYSTEM

The basis for the scheme is on (2,3), a secret image S is converted into three shares S1, S2 and S3. By stacking any two shares can reveal the secret image. concurrently, the aided three verification images are carefully hidden into the shares using the (2,2) scheme. Assume that the verification images and the secret image is kept secret to participants by the dealer.

The scheme has mainly four phases mainly: Hybrid codebook design , decomposition phase, encryption phase and decryption phase.

- Hybrid Codebook Design phase:

The hybrid codebook design phase encompasses the use of (2,3) and the (2,2) codebook design . In that (2,3) is used to generate the three shares S1,S2 and S3 for the participants P1, P2 and P3, respectively. For white pixel there are four cases and for black pixel there are 4! Case. Each pixel is mapped to 2×2 sub-pixel block , called as the codeword.

For (2,2) scheme there are four cases for white pixel and 12 for black pixel. The (2,2) scheme is used to divide the verification image into two parts which are to be hidden into any pair of shares generated by the (2,3) codebook.

- Decomposition phase:

The secret image S is divided into four macro-blocks as $S_{0,0}$, $S_{0,1}$, $S_{1,0}$ and $S_{1,1}$ having the same size for each block. The verification images V1,V2 and V3 are also taken of same size that of the macro-block.

- Encryption phase:

The encoding phase comprises of seven operations which will deal for encoding a quarter i.e. macro-block of secret and hiding the verification logo. The first macro-block is taken as it is in the secret. The first verification logo is hidden into S2 in macro-block $S_{0,1.}$. The next is the encryption of second macro-block of secret by OR-ing with the $S_{0,1}$ of S1 into S1 and S3 share's $S_{0,1}$. The second logo is hidden into $S_{1,0}$ of the S3 share by OR-ing with $S_{0,1}$ of S2 with V2. The next is the encryption of third macro-block of secret by OR-ing with the $S_{1,0}$ into S1 and S2 share. third verification logo is hidden into S1 in macro-block $S_{1,1}$ by OR-ing with $S_{1,0}$ of S3 with V3. The next is the encryption of fourth macro-block of secret by OR-ing with the $S_{1,1.}$ of S1 into S2 and S3 shares . These are the encryption steps performed respectively as mentioned above.

- Decryption phase :

For reconstruction of secret image, the participant has to validate the extracted verification image. The decryption process is performed by stacking any two shares together . The result of stacking is revealed secret along with extracted verification logo.

C. PROPOSED SYSTEM

The proposed system aim to extend the hybrid codebook based method to benefit from a combination of two general VC codebooks with goal of providing efficient generic method of codebooks generation with minimizing the pixel expansion . This system is presenting the efficient approach for codebooks generation with less time consuming operations while decryption.

The proposed scheme also undergoes all the four phases as mentioned in the existing system but the difference is only with the use of the (2,3) and (2,2) random-grid VCS for codebook generation[14].

For reducing the pixel expansion the random-grid VCS scheme is used for the design of (2,3) and (2,2) VCS. The random-grid VCS scheme enables the users to reduce the pixel expansion problem.

The following figure 1 gives the idea of how all the phases are going to be performed stepwise detailing the separation of each components of the system.

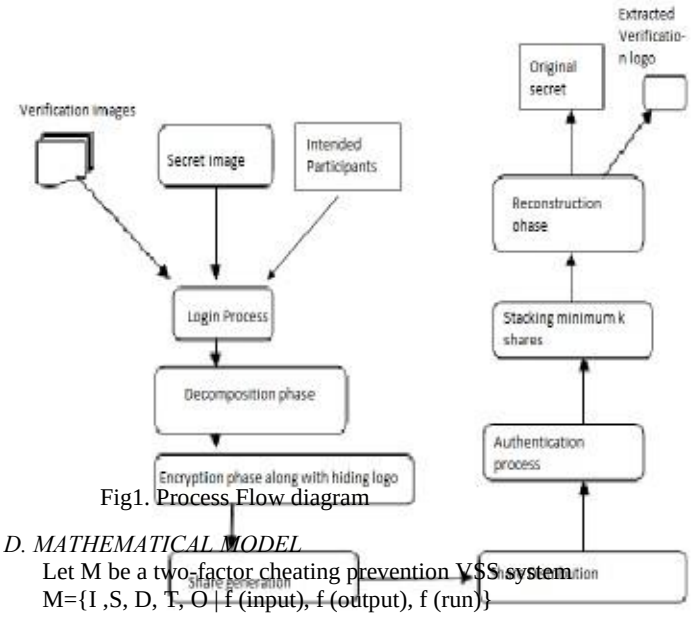

Fig1. Process Flow diagram

D. MATHEMATICAL MODEL

Let M be a two-factor cheating prevention VSS system

M={I ,S, D, T, O | f (input), f (output), f (run)}

Where, I is set of input {S0, V1, V2, V3} where I0 € I is an initial state.

S is set of output {S1,S2,S3} where S0 € S is result of encryption process.

D is set of domains {d1, d2, d3}

T is set of tasks {t1, t2, t3, t4, t5, t6, t7}

O is set of outputs.

M is based on one secret image and three different verification logos, the participants, share creation, stacking shares for participant's authentication.

I) In order to translate the first aspect of M, which is I we must define the M's different inputs. There are two inputs

I= {S0, V1, V2, V3}

S0= Secret image (for enrolment stage)

V1= first verification logo (for enrolment stage)

V2= second verification logo (for enrolment stage)

V3= third verification logo (for enrolment stage)

S={S1,S2,S3}

S1= first share (for authentication stage)

S2= second share (for authentication stage)

S3= third share (for authentication stage)

II) The next aspect of M as it relates to there is D, which stands for domain. A domain is a defined section of a system.

D= {d1, d2, d3}

d1 = User's Registration

d2 = initialization of two-factor cheating prevention system using secret image and three verification logos.

d3 = User's Authentication by stacking any two shares.

III) The third element of M is T for tasks.

t= {t1, t2, t3, t4, t5, t6, t7}

t1 = selection of username and password to sign up.

t2 = putting username name and password to sign in

t3 = decomposition phase of secret image and verification logos.

t4 = generation of shares by encryption process using hybrid codebook design.

t5= storing encrypted template into database.

t6 = decryption process by stacking k shares minimum(k<=2)

t7 = Authentication process for secret with extracted verification image.

IV) The last component of M is O which means Output. An output is defined as the result of an action

O = {o_1, o_2, o3, o_4, o_5, o_6, o_7}.

o_1 = successful accessing of secret share and three verification logos

o_2 = Macro-blocks creation using decomposition phase.

O_3= Successful encryption of secret and hiding logo

O_4 = Successful creation of shares.

o_5 = Successful completion of stacking operations using decryption process

o_6 = Successful Completion of User Authentication

In order for all of these events to fit together, there are several dependencies between

I, S, D, T, & O all of which are within M.

The system M does not only contain components such as actions, domains, and Outputs. The system M may consist of functions.

I) we will first look at the function *step.*

M can consist of a function *step:* $I \times T \rightarrow D$

where , *step* D(n, t) = D_{n+1} denotes the next state of the system after applying action a.

II) M also can have a functions

Outputs of encryption process:

$f_{(2,2)} : S0 \rightarrow S1 \,||\, S2$ is a (2,2) is visual secret sharing function with the input S0, an original secret image, and the output S1 and S2, two share images. Where denotes OR operation.

$$f(2,2) : S0 \,||\, S1 \rightarrow S2$$

is visual secret sharing function with the input S0, an original secret image, and the input S1, a corresponding share image. The output S2 is other share image.

$f_{(2,3)} : S0 \rightarrow S1 \,||\, S2 \,||\, S3$ is a (2,3) is visual secret sharing function with the input X, an original secret image, and the output S1, S2 and S3, three share images.

$$: S0 \,||S1 \rightarrow S2 \,||S3 f(2,3)$$

visual secret sharing function with the input S0, an original secret image, and the input S1, a corresponding share image. The output S2 and S3 are the other two share images.

III) Further, system M can consist of a function *run:* S × T* → I. An example of the *run* function is *run(I,* Ø) = I, where Ø is an empty sequence of tasks.

REFERENCES

[1] M. Naor and A. Shamir, â€œVisual cryptography,â€• in Advances in Cryptology, vol. 950. New York, NY, USA: Springer-Verlag, 1995, pp. 1-12

[2] KH Lee, PL Chiu.: An Extended Visual Cryptography Algorithm for General Access Structures. IEEE Transactions on Information Forensics and Security vol. 7, no. 1, (2012)

[3] Stelvio Cimato,Ching-Nung Yang: Visual Cryptography and Secret Image Sharing, Taylor & Francis Group, 2012 LLC

[4] Hu, C.M., Tzeng W.G.: Cheating prevention in visual cryptography. IEEE Transactions on Image Processing 16(1), 36-45 (2007)

[5] D.S. Tsai, T.H. Chen, and G. Horng. A cheating prevention scheme for binary visual cryptography with homogeneous secret images, Pattern Recognition, Vol. 40 No. 8, 2007, pp. 2356{2366.

[6] Bin YU, Jin-Yuan LU, Li-Guo FANG.: A Co-cheating Prevention Visual Cryptography Scheme. Third International Conference on Information and Computing (ICIC), Vol.4, 157-160 (2010)

[7] Qin Chen, Wen-Fang Pengo Min Zhang, Yi-Ping Chu. : An (n, n) threshold Visual Cryptography Scheme for Cheating prevention. Third IEEE International Conference on Computer Science and Information Technology (ICCSIT), Vol. 8, 587 -592(2010)

[8] Yu-Chi Chen, Student Member, IEEE, Gwoboa Horng, and Du-Shiau Tsai "Comment on Cheating Prevention in Visual Cryptographyâ"• IEEE Transactions on Image Processing, Vol. 21, No. 7, July 2012

[9] Shuo-Fang Hsu ; Yu-Jie Chang ; Ran-Zan Wang ; Yeuan-Kuen Lee ; Shih-Yu Huang, "Verifiable Visual Cryptography"• Sixth International Conference on Genetic and Evolutionary Computing (ICGEC), 2012, 464-467

[10] Y.C.Chen,G. Horng, D.S.Tsai, A new authentication based cheating prevention scheme in Naor-Shamir's visual cryptography, Journal of Visual Communication and Image Representation. 23(8) (2012) 1225-1233
Y.C.Chen,G. Horng, D.S.Tsai, Visual secret sharing with cheating revisited, Digital Signal Processing. 23 (5) (2013) 1449-1504

[11] Chih-Hung Lin et al. : Multi-factor cheating prevention in visual secret sharing by hybrid codebooks. Vis. Commun. Image R. 25 (2014) 1543-1557

[12] Xiaotian Wu, Wei Sun: Random grid-based visual secret sharing for general access structures with cheat-preventing ability, The Journal of Systems and Software 85 (2012) 1119-1134

[13] Ching-Nung Yang, Chih-Cheng Wu, Dao-Shun Wang: A discussion on the relationship between probabilistic visual cryptography and random grid, Information Sciences xxx (2014) xxx-xxx
.

[14]