ISSN:0975-9646

Two-factor Cheating Prevention in Visual Cryptography using hybrid codebook

Sayali Gapate [#1], Prof. Jyoti Rao [*2]

[#] *PG student, Dept. Of Computer Engineering,DYPIET, Pimpri,Savitribai Phule Pune University, Pune, India.*
[*] *Dept. Of Computer Engineering,DYPIET, Pimpri,Savitribai Phule Pune University, Pune, India.*

***Abstract*— To share multimedia and secret images, a variant of cryptographic secret sharing scheme is designed which is popularly known as visual secret sharing or visual cryptography. Several distinguishing shares known as transparencies are used to encrypt a secret image and secret image is decrypted by human visual system by stacking some or all of the shares. More research continued later in the area of visual secret sharing, meanwhile the cheating attack is detected in 2006. The cheating attack occurs when malicious participant cheats the honest ones by forging fake shares. Many cheating prevention schemes were developed since then with few advantages and disadvantages. Extra share and extra pixel expansion were the major issues identified in cheat preventing visual secret sharing schemes. To eliminate or minimize this, a new two factor cheat prevention scheme is proposed. The design of two-factor cheat prevention scheme undergone re-inspection to both stacked results and secret shares.**

***Keywords*— Cheating prevention; visual secret sharing; Hybrid codebook; Stacking; pixel expansion (key words)**

I. Introduction

In 1994, Naor and Shamir Visual cryptography (VC) was by in the Eurocrypt conference. Visual secret sharing scheme soon gain interest of many researchers since it is easy to understand, without any cryptographic knowledge and any costly computations while decryption. The research areas identified in past two decades were general access structure, color image, relative difference and enabling optimum pixel expansion, and multi-secret sharing.

In a traditional (k, n) VSS scheme, the input secret image is encrypted into n shares (transparencies) such that to reveal the secret image , any subset of k ($2 \leq k \leq n$) or more shares are required, no information can be disclosed about the secret if any k-1 or fewer shares are used for decryption process . The decryption process in this VC scheme is performed by superimposition of collected shares with careful alignment, and the secret gets visible then on the superimposed share. The correctness of superimposed shares can be recognized by human eyes itself without any computational aid.

For getting better understanding of VSS, the codebook design pattern is helpful. The concept of codebook design signifies the adaptive sub-blocks for secret information. For example in (2, 2) codebook design two adaptive sub-blocks are designed such that secret is encoded into two shares S1 and S2, with the pixel color of secret image, an adaptive sub-block is designed, such that size of resultant shares and reconstructed secret is also expanded.

The concept of cheating can be defined as when intended malicious or dishonest participants cheat the honest participants by giving fake share. According to (2, 3) scheme it can be explained as: In between three participants, assume that the honest participant C is cheated by A and B by sharing fake share. The participant A and B can infer the pixels of participant C by modifying their sub-pixels by referring to (2, 3) codebook design. Thus, while superimposing three shares, the white pixel may identify as black because of pixel modification took place in third share of participant C. In this way, cheating took place.

II. Related work

A process of collusive cheating ,in 2006 illustrated by Horng et al. involving n + 1 participants in (2, n) VC schemes. They came up with two possible solutions to the problem. For each participant, a dedicated verification share was generated as the first solution such that the participant can inspect the correctness of the shares collected from rest of the participants, is categorized into share authentication based scheme. A (2, n + l) VC scheme, $l \geq 1$, presented as the second solution unlike the traditional (2, n) scheme also known as a 2-out-of-n secret sharing scheme. The scheme presented malicious user's ability to guess the structure of the shares belonging to other participants. The second scheme does not rely on the verifying share is categorized into blind authentication scheme [2]

Hu and Tzeng proposed three methods in 2007, to minimize the disadvantages of the earlier cheating prevention VC schemes. Out of three schemes; two of them were designed for traditional VC schemes, and the third method was designed for the extended VC scheme. To verify the genuineness of shares, extra n verification shares are used by CPVC schemes presented by Hu and Tzeng[3]. A genetic algorithm (GA) having cheating immune ability proposed by Tsai et al.in 2007. Multiple homogeneous secret images was basis of their scheme such that any two shares together can disclose a distinct secret image. With this technique, cheating attacks can be prevented.[4]

Hsu et.al. came up with a new visual cryptography (VC) scheme in 2012, for verifying the validity of the shares involved in a VC decryption process. They used the idea to stamp a continuous pattern on the shares belonging to the same secret image, and a part of the pattern can be reconstructed through arranging the shares in a manner and stacking half of two shares together [5].

Based on Naor-Shamir's VC scheme, Horng researched new authentication based cheating prevention scheme. The scheme employs the black patterns added into the verified stacking result. The black patterns incorporated with verified stacking result are useful to check correctness of a share transparency, whether it is fake or not with less pixel expansion [6].

Horng revisited some well-known cheating activities and CPVSS schemes, and classified cheating activities into meaningful cheating, non-meaningful cheating, and meaningful deterministic cheating. They presented new cheating prevention schemes which was proved to be securing against the meaningful deterministic cheating does not rely on added transparencies with less pixel expansion.[7]

Xiaotian Wu, Wei Sun presented new VSS scheme for general access structures known as random grid-based VSS schemes where the idea of encrypting secret image into n random grids using qualified sets is introduced. Random grid (RG) is a technique designed to eliminate pixel expansion problem. The new RG-based VSS scheme which is authentication-based is introduced to deter the cheating attacks on (2, n) and (t, n) RG [8].

Cheating prevention VC scheme using hybrid codebooks have been presented for efficient pixel expansion considering multiple factors [9].Unlike the previous CPVC schemes using an additional verification share with more pixel expansion [4,5] to resist cheating by malicious participants. The resultant proposed scheme has design of two-factor VC scheme having cheating prevention ability with case by case design incurring less time spend on stacking transparencies. So, the proposed system is focusing on these issues to be resolved with the efficient cheating detection and prevention process.

III. Proposed System

In this paper, proposed scheme combined two VSS schemes in one to have cheat-preventing ability. The hybrid codebook is designed such that with the help of any two shares, the original secret and verification image can be reconstructed. Unlike previous techniques which were dealing with creating separate verification shares and the shares for participating entities using any of the codebooks, the codebook design was the major part which used to encrypt both the secret and to hide the verification shares itself into the generating shares. The hybrid codebook is designed such that the two codebooks (2, 2) and (2, 3) were combined for encryption process. Computer simulations were performed to illustrate the feasibility of proposed system. Instead of keeping extra verification share, the verification images are meant to be hidden in the shares itself. Also, the computation cost for encoding is low, same as it incur for generic VSS schemes without generating additional computation cost. Once the cheating attack is detected, as the proposed scheme gives ambiguous result of reconstructed secret and verification image. Providing the second cheating evidence.

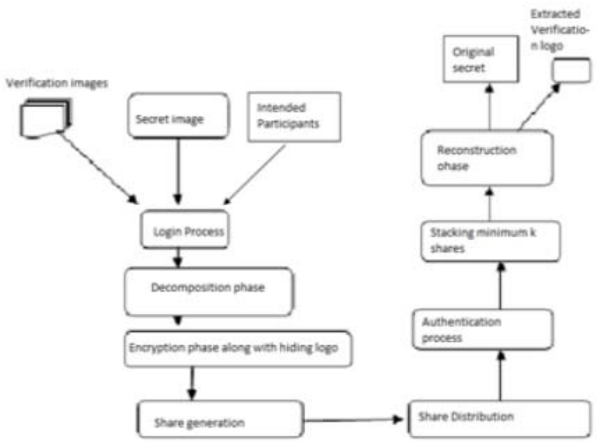


Fig. 1 Workflow diagram

A. *System workflow*

By looking at the above diagram the idea of entire authentication process can be seen, how it undergoes various steps and how the system will transit through the different stages as the encryption and decryption of the shares performed systematically. The following description is the basic idea of the proposed system workflow.

The shares are going to be generated as output of the encryption process which has three verification images and the secret image as input. The generated shares are then distributed to the concerned participants (Here are maximum three participants).

While decryption process, either any two of the generated shares or all the generated shares are meant to be stacked together to generate the resultant reconstructed secret which is going to be validated by checking the extracted verification along with reconstructed secret thus ensuring the double-check while decryption and categorizing the results into cheating and non-cheating cases. If the reconstructed secret is identified as non-cheating case then all the shares are said to be authenticated correct share. If the reconstructed secret is identified to be the cheating case result then it is considered as the concerned share are malicious ones which are being forged by the participant and are successfully tracked as a cheated results.

B. *Construction of Proposed Systems*

The proposed scheme undergoes the mainly the four major phases as a critical part of system:

1) Decomposition phase 2)Hybrid codebook design phase 3)Encryption phase 4)Decryption phase

- **Hybrid codebook design phase**

The (2, 3) codebook

The (2, 3) VSS scheme is chosen to create three shares T1, T1, and T3 for three participants P1, P2, and P3. Four cases for a white secret pixel and 4! cases for a black secret pixel are considered. The code-word is defined as each of the secret pixels is mapped to a 2 ×2 sub-pixel block.

The (2, 2) designed codebook:

In (2, 2) VSS scheme, for white pixel four cases and for black pixel twelve cases are considered.

- **Decomposition phase**

Decomposition phase mainly splits the original secret image S into four macro-blocks-$S_{0,0}$, $S_{0,1}$, $S_{1,0}$ and $S_{1,1}$ of equal size for simplification. The three verification images, V_1, V_2, and V_3 are of the same size as that of a macro-block. Verification image can be chosen from image with relevant message (which is used for spreading meaningful message overall).

The prior assumptions are that participants P_i with share S_i can reveal the secret S while the verification image Vi.

- **Encryption phase**

The encoding phase comprises of seven steps to encode a quarter of secret and hide verification image step by step.

Step (1) Encrypting the first macro-block of secret by

$$S^1_{0,0} \| S^2_{0,0} \| S^3_{0,0} \leftarrow f(2,3)(S_{0,0})$$

Encode the macro-block $S_{0,0}$ to generate $S_{0,0}{}^{1}$, $S_{0,\ 0}{}^{2}$; and $S_{0,0}{}^{3}$ of the share images S_1, S_2, and S_3 according to the (2,3)codebook referring the (2,3) VSS scheme. The superscript digit indicates the containing share number and the subscript indicates the macro-block which has referred. The same indications are applied for each of the following equations coming right away in next steps. $S_{0,0}$ is separated into the three shared images as it is referred as the first macro-blocks of the respective shares.

Here the $S_{0,0}{}^{1}$refers to the first macro-block of share $S_1S_{0,0}{}^{2}$refers to the first macro-block of share S_2 and $S_{0,0}{}^{3}$refers to the first macro-block of share S_3which are when X-ORed results into the creation of the first macro-blocks of $S_{0,0}$ i.e. original secret image.

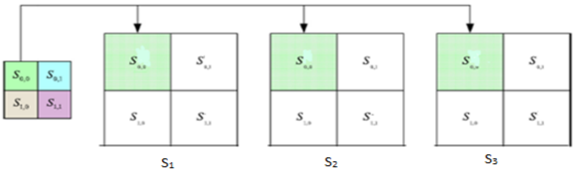


Fig. 2 Step 1 of encryption process

Step (2) Hiding the first verification image by $S^2_{0,1} \leftarrow f(2,2)(S^1_{0,0} \| V_1)$

Given $S_{0,\ 0}{}^{1}$ and the verification image V_1, macro-block$S_{0,\ 1}{}^{2}$ of the share imageS_2 is generated according to the (2, 2) codebook by referring the (2, 2) VSS scheme. The V_1 stands for the first verification image.

The $S_{0,\ 1}{}^{2}$ refers to the second macro-block of the second share S_2 which is resultant of the concatenation of the $S_{0,\ 1}{}^{1}$(second macro-block of the first share S_1) and the first verification image V_1.

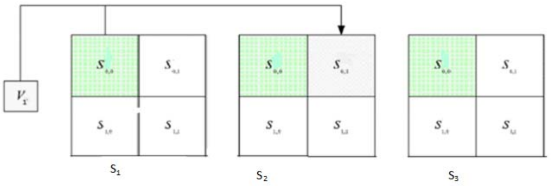


Fig. 3 Step 2 of encryption process

Step (3) Encrypting the second macro-block of secret by $S_{0,\ 0}$.

$$S^1_{0,1} \| S^3_{0,1} \leftarrow f(2,3)\,(S_{0,1} \| S^2_{0,1})$$

Encode the macro-block $S_{0,\ 1}$ and $S_{0,\ 1}{}^{2}$ to generate $S_{0,\ 1}{}^{1}$ and $S_{0,\ 1}{}^{3}$ of the share image S_1 and S_3 according to the codebook in (2, 3) VSS scheme. Here the $S_{0,1}$refers to the second macro-block of original secret image which is when X-ORed with the second macro-block of the share S_2, results into the creation of the first macro-blocks of the shares S_1 and S_3($S_{0,1}{}^{1}$ and $S_{0,1}{}^{3}$, respectively) .

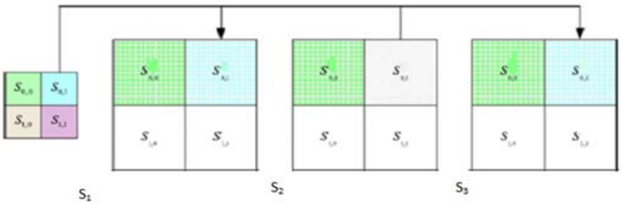


Fig. 4 Step 3 of encryption process

Step (4) Hiding the second verification image by

$$S^3_{1,0} \leftarrow f(2,2)\,(S^2_{0,1} \| V_2)$$

Given $S_{0,\ 1}{}^{2}$ and the verification image V_2, macro-block $S_{1,0}{}^{3}$ is created using (2,2) VSS scheme according to the (2,2)codebook . Here, the second macro-block of the second share is concatenated i.e. X-ORed with the second verification image then the resultant third macro-block of the third share is generated.

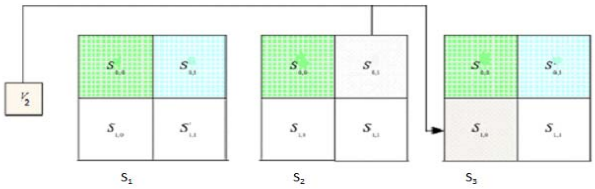


Fig. 5 Step 4 of encryption process

Step (5) Encrypting the third macro-block of secret by

$$S^1_{1,0} \| S^2_{1,0} \leftarrow f(2,3)\,(S_{1,0} \| S^3_{1,0})$$

Encode the macro-block $S_{1,\ 0}$ and $S_{1,\ 0}{}^{3}$ to generate $S0_{1,\ 0}{}^{1}$ and $S_{1,\ 0}{}^{2}$ of the share image S_1 and S_2 according to the (2, 3) codebook in (2, 3) VSS scheme.

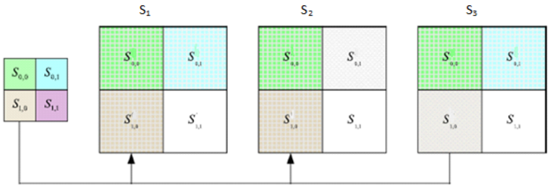


Fig. 6 Step 5 of encryption process

The $S_{1,0}$ of the original secret image S_1 is X-ORed with the third macro-block of the generated share image S_3 results into creation of the third macro-block of first and second share.

Step (6) Hiding the third verification image by

$$S_{1,1}^{1} \leftarrow f(2,2)\,(S_{1,0}^{3} \| V_3)$$

Given $S_{1,0}^3$ and the verification image V_3, $S_{1,1}^1$ is generated according to the (2, 2)codebook with reference to (2, 2) VSS scheme .

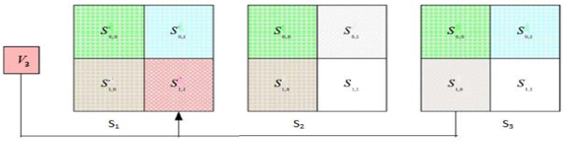


Fig. 7 Step 6 of encryption process

The third verification image is X-ORed with the third macro-block of the secret share S_3 results into the creation of the fourth macro-block of the first generated share S_1.

Step (7) Encoding the last macro-block of secret by

$$S_{1,1}^{3} \| S_{1,1}^{2} \leftarrow f(2,3)\,(S_{1,1} \| S_{1,1}^{1})$$

Encode the macro-block $S_{1,1}$ and $S_{1,1}^1$ to generate $S_{1,1}^3$ and $S_{1,1}^2$ of the share image S_2 and S_3 by the (2,3) VSS scheme according to the (2,3) codebook.

The fourth macro-block of first share S_1 is X-ORed with fourth macro-block of original secret image S which results into the creation of the fourth macro-block of shares S_2 and S_3.

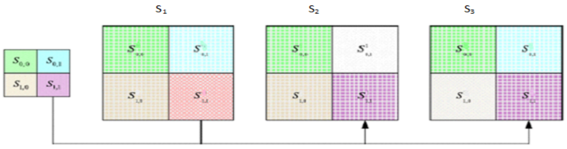


Fig. 8 Step 7 of encryption process

By concatenating $S_{i,j}^1$; $S_{i,j}^2$; and $S_{i,j}^3$ for all Si, j and j (i =0 or 1 and j= 0 or 1), the share images S_1, S_2, and S_3, being distributed to all the three participants P_1, P_2, and P_3, respectively.

- **Decoding phase**

For reconstruction of secret image S , it is mandatory to check the validity of verification images which are extracted as a result of stacking operation (where minimum 2 shares are stacked).These shares are to be taken from the respective participants who owns or claim to own the share of the secret image S.

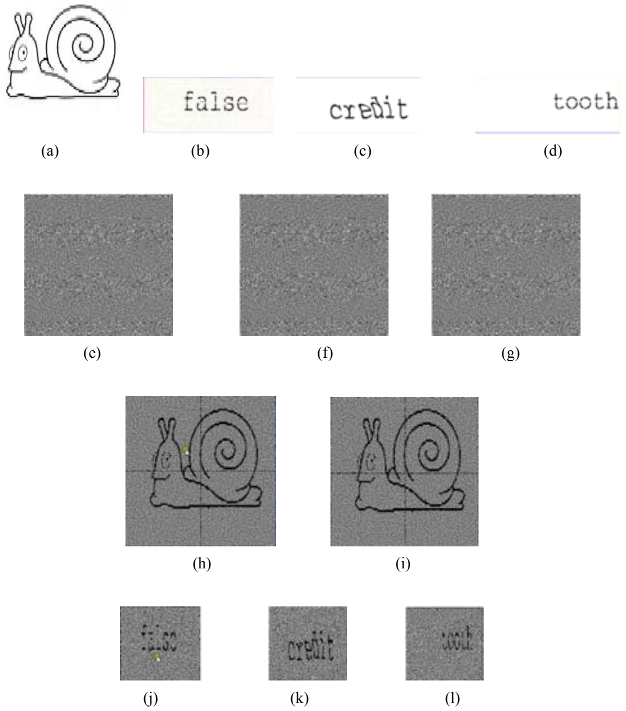
For example, P_1 wants to reconstruct the secret image S along with P_2, he reveals the verification image V_1 by stacking the macro-block $S_{0,0}^1$ of the share $S_1$and the macro-block $S_{0,1}^2$ of the share S_2. If the stacked result of shares reveals the identifiable verification image V_1, the P_1 reconstructs the secret image S by stacking S_1 and S_2. The P_1checks whether the shape or information of $S_{0,0}^1$ in the reconstructed secret image is clear or not. If both $S_{0,0}^1$ and the extracted verification image are clear, P_1 trusts the correctness of the share S_2 and the revealed secret. Note that the validating the correctness of the verification images is dependent on results either true or false. Precisely, if verification image partially unc1ear or uncertain, participants will be rejected for the share intended to stack.

IV. Experimental Results

Main focus of initial development is to implement the system following the encryption algorithm correctly stepwise. The work has been completed for non-cheating case. For other two cheating cases, the work is ongoing and will be completed soon.

Simulation 1: The proposed scheme without cheating

To depict the performance of proposed scheme experiments are conducted. The verification images of size 260 ×180 are shown in Fig. 3(b)–(d). After the encoding operations, the share images S_1, S_2, and S_3 are generated as shown in Fig. 3(e)–(g), respectively. If the participants stack any two shares then, the reconstructed secret image is revealed as shown in Fig. 3(h). Also, Fig. 3(i) presents the result by stacking S_1, S_2, and S_3. The extracted verification image, as shown in Fig. 3(j), can be disclosed by stacking $S_{0,0}^1$ with $S_{0,1}^2$. In the same way, the verification images are extracted, as shown in Fig. 3 (k), can be disclosed by stacking $S_{0,1}^2$ with $S_{1,0}^3$ and the extracted verification images, as shown in Fig. 3(l), can be disclosed by stacking $S_{1,0}^3$ with $S_{1,1}^1$.



(a) (b) (c) (d)

(e) (f) (g)

(h) (i)

(j) (k) (l)

Fig. 9 The proposed scheme does work without cheating

V. DISCUSSION

The proposed two-factor cheating–prevention scheme is evaluated using following factors. The factors are cheating detection, contrast, computation cost and security condition.

1. Two-factor detection

The previous cheat–preventing schemes in the literature were based on considering single factor, i.e., either validating the presence of verification image or identifying the revealed secret and to detect cheating, the ambiguous scheme is used. To have advantages from both techniques with eliminating the disadvantages presented by earlier cheating prevention scheme, the presented scheme in this paper is prove to have effective cheat–detection ability by attributing to both validating verification images if any and identifying the reconstructed secret.

The proposed scheme does provide better results in terms of authenticating the concerned share images and the uncertainty of cheating results. Furthermore, the attackers can be detected either by validating the verification images or identifying the ambiguity of the reconstructed secret.

2. Computation cost

The computation cost of the proposed scheme is estimated to be the better in performance than the previous schemes existing in the literature. For the setup environment we have used the Intel Core 2 duo processors (or succeeding next generations will even boost the performance for e.g. i3, i5, etc.).

3. Contrast

The contrast of the stacked secret can be better understood by having the knowledge the following definitions.

1. Visual contrast.

The contrast α is defined as h-l / n-l , where h denotes the number of existing white sub-pixels in each code-word indicating the white part of the secret image, l denotes the number of white sub-pixels in each code-word indicating the black part of the secret image, and n represents the total number of sub-pixels in a code-word. It is recommended to make α as large as possible. The greater the value of α, the more identifiable the stacked secret will be, is an assumption.

2. Visually identifiable.

The revealed image must be identifiable with the original secret after superimposing share images with regards to, if its contrast is higher than or equal to some threshold value (under normal conditions, it is found to be greater than zero).

In principle, if the reconstructed secret image is identifiable, then α is greater than zero. With the experimental results it will be easy to differentiate the contrast comparing with the previous results.

VI. CONCLUSIONS

In this paper, a two-factor cheating–prevention scheme is proposed to have advantages from both VC codebooks. The design of hybrid codebook enables the hiding verification images skilfully in shares to validate the correctness of intended shares (whether the intended share is fake). This proves whether cheating attack is occurred or not in VSS. In comparison with the related cheating prevention schemes, this scheme has the following advantages: (1) To verify the validity of the shares eliminated the need of maintaining extra share to, (2) low computation cost , and (3) having two-factor cheating detection.

REFERENCES

[1] M. Naor and A. Shamir, “Visual cryptography”, in Advances in Cryptology, vol. 950. New York, NY, USA: Springer-Verlag, 1995, pp. 1-12

[2] Horng, G., Chen, T., & Tsai, D. S. (2006). Cheating in visual cryptography.Designs, Codes and Cryptography, *38*(2), 219-236.

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

[4] 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.

[5] 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

[6] 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

[7] Y.C.Chen,G. Horng, D.S.Tsai, Visual secret sharing with cheating revisited, Digital Signal Processing. 23 (5) (2013) 1449-1504

[8] 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

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