A Block Based (t, n) Visual Cryptography Scheme for Unbounded n and t=2, 3

Sian-Jheng Lin[*] and Wei-Ho Chung[†]
[*†]Research Center for Information Technology Innovation,
Academia Sinica, Taipei, Taiwan.
[*]E-mail: sjlin@citi.sinica.edu.tw
[†]E-mail: whc@citi.sinica.edu.tw

***Abstract*— The (t, n) visual cryptography (VC) is a secret sharing scheme of decomposing a secret image into n transparencies, and the stacking of any t out of n transparencies reveals the secret content. The perfect security condition of VC scheme requires the strict requirement where any t–1 or fewer transparencies cannot extract any information about the secret. For n approaching infinity, previous studies consider the scenario where the probabilistic model is a pixel-to-pixel scheme that encodes each secret pixel to a corresponding pixel in each transparency. In this paper, we extend the pixel-to-pixel scheme to pixel-to-block scheme for the cases t=2 and 3. Given a secret image, the proposed VC scheme generates a transparency through coding each secret image pixel to a m-pixels shadow block on the corresponding position of the transparency. Experiments show that the stacking results reveal better visual quality than the probabilistic model scheme.**

I. Introduction

The visual cryptography (VC) is a kind of secret sharing which admits that the decoding is performed without computations. Given a secret image, the (t, n) VC scheme converts the secret image into n noise-like transparencies, so that we cannot see the secret content from any one transparency. In general, the (t, n) VC scheme possess the property that the secret can be revealed by stacking of arbitrary t out of those n transparencies, but any t–1 or fewer transparencies cannot retrieve any information through visual perception or signal analysis techniques. The basis matrices model of the (t, n) VC scheme is first presented by Naor and Shamir [1]. Later, the extension works, including the probabilistic models [2]-[4], and general access structures [5], [6], had been further studied.

However, the basis matrices model is not suitable for large n, because the size of basis matrices grows very fast. Moreover, the basis matrices cannot properly describe the coding scheme for unbounded n; i.e., $n\rightarrow\infty$. Thus, Lin and Chung [7] proposed the probabilistic model of (t, n) VC scheme for unbounded n. The scheme follows the probabilistic model to generate the unexpanded transparency for the case (t, $n\rightarrow\infty$). Each secret pixel is coded into a pixel in each transparency. To achieve the optimal contrast, the [7] also gives the parameter setup for t = 2 to 6. However, as shown in the experiment of [7], the t = 2 or 3 is suggested in practice, and for $t\geq4$, the contrast is very low so that the stacking result is visually insignificant.

For each transparency generated by the probabilistic VC scheme, each pixel in the transparency is decided by an arbitrary chosen column in the basis matrices. Thus, the stacking result by the probabilistic model is more untidy than the basis matrices model, which uses the whole basis matrix to code a secret pixel. This observation gives the motivation of this paper. In this paper, we extend the pixel-to-pixel scheme to pixel-to-block scheme for the cases t=2 and 3. The extended scheme will expand the size of the transparencies, as contrasted to the scheme [7] with invariant expansion. As shown in experiments, the stacking results of the proposed scheme give better visual quality than the scheme of [7].

The rest of this paper is organized as follows. In Section II, we introduce the formal definitions of VC and the probabilistic model of (t, n) VC scheme for unbounded n [7]. In Section III, we give the major scheme extended from [7]. Section IV shows the experiments. Section V gives the conclusion of this paper.

II. Description of VC scheme

Given a binary secret image S, the (t, n) VC scheme converts each secret pixel $s\in$ {white, black} in S to n blocks at the corresponding positions of n transparencies T_1, T_2,…, T_n, respectively. The basis matrices B_0 and B_1 are a pair of $n\times m$ Boolean matrices, which identify the mapping function turning a secret pixel s into n blocks with size m. Each sub-pixel in a block is opaque or transparent, and we use 0 or 1 to indicate a transparent sub-pixel or opaque sub-pixel in this paper. When two sub-pixels are stacked with matching positions, the representation of the stacking result may be transparent if the two sub-pixels are both transparent. Otherwise, the stacking result is opaque. Let the $\oplus$ denote the stacking operation, we have

$$0\oplus0=0,\ 0\oplus1=1,\ 1\oplus0=1,\ 1\oplus1=1.$$

It can be shown that $\oplus$ is equivalent to the bitwise operation ″OR″.

For the basis matrices B_0 and B_1, each row in the basis matrices corresponds to an encoded block, and the elements in each row represent the sub-pixels. For the s being white or black, the dealer respectively permutes the matrix B_0 or B_1 within uniform probability, and then sends each row of the matrix to each T_i.

The basis matrices are required to meet the conditions described in Definition 1. Let $H(v)$ denote the hamming

weight of a (0, 1)-vector v (i.e. the number of ones in v).

Definition 1: A (t, n) VC scheme with m sub-pixels and contrast $\alpha>0$ can be represented as two $n\times m$ Boolean matrices B_0 and B_1. A valid VC scheme is required to meet the following conditions [1]:

i). Given the stacked v_0 of any t out of the n rows in the matrix B_0, and the stacked v_1 of any t out of the n rows in the matrix B_1, the inequality holds: $H(v_1)-H(v_0)\geq\alpha m$.

ii). For any k-element subset $\{i_1, i_2,\ldots, i_k\}\subseteq\{1, 2,\ldots, n\}$ and $k<t$, the two collections containing m columns obtained from the rows $i_1, i_2,\ldots, i_k$ in B_0 and B_1 are indistinguishable in the sense that the two collections contain the same columns.

The condition (i) defines the contrast requirement. In general, a larger α gives better visual distinguishability in the stacking results. The condition (ii) defines the security requirement. A valid VC must prevent the secret pixels from being revealed by analyzing the probability distribution of the patterns appearing in k transparencies for $k<t$.

In the scenario where n approaches infinity, the size of basis matrices is also infinity, so the construction of basis matrices is impractical. Thus, the [7] employs another framework, called probabilistic model [2], to identify the coding function. Instead of the ordinary method using a row in basis matrices, the probabilistic model only uses one sub-pixel to represent one secret pixel. For the infinite n, the [7] uses a pair of vectors $X=(x_0, x_1,\ldots, x_t)$ and $Y=(y_0, y_1,\ldots, y_t)$ to represent the coding function. Let $E(x_i)$ denote a memoryless binary sequence where the probability of assigning each element to 0 is x_i. The $|y_i|$ is the probability of using the memoryless sequence $E(x_i)$ to encode a secret pixel s, where $y_i>0$ for s=white and $y_i<0$ for s=black. For t = 2 and 3, the [7] gives the parameter setup for optimal contrast:

For t=2, Y=(1/2, –1, 1/2), X=(0, 1/2, 1), α=1/4. (1)

For t=3, Y=(–1/3, 2/3, –2/3, 1/3), X=(0, 1/4, , 3/4, 1), (2)
α=1/16.

Since the stacking result of $t\geq4$ is visually insignificant and the study of $t\geq4$ is only of theoretical interests, so this paper only focus on the two cases t= 2 and 3.

III. The Proposed Algorithm

A. *The case t*=2

In this case, the [7] gives an algorithm to achieve the contrast α=1/4 by using the parameters (1). The algorithm generates a transparency T by using the index table Z. The size of Z is equivalent to the secret image S, and each element $Z[w, h]$ is the index of the used memoryless sequence $E(x_{Z[w, h]})$ to encode the secret pixel $s[w, h]$. For t=2, the Z[w, h] has two possible values 0 and 1, and $P(Z[w, h]=0)=1/2$. Given a secret image S, the dealer reads each secret pixel $S[w, h]$ in S. If $S[w, h]$ is white, the dealer assigns the value $Z[w, h]$ to the transparency $T[w, h]$. Otherwise, if $S[w, h]$ is black, the dealer assigns a random Boolean value to the transparency $T[w, h]$ and $P(T_i[w, h]=0)=1/2$.

To extend the above pixel approach to block approach, we observe that for the white secret pixel, the dealer uses an all-zero sequence or an all-one sequence to encode the white secret pixel, and the two possible cases are determined by the corresponding element in Z. In the block approach, we simultaneously represent the two cases in a block with size two. More precisely, for a white secret pixel, we use [0, 1] or [1, 0] to code the white pixel, and the two cases are determined by the corresponding element in the index table R used in the proposed algorithm. Each element in R is a Boolean integer where $P(R[w, h] = 0) = P(R[w, h] = 1) = 1/2$. For a black secret pixel, we randomly choose [0, 1] or [1, 0] to code the black pixel. The details are described in Algoithm 1:

Algorithm 1. The algorithm of the proposed scheme for t=2.

Input: A binary secret image S and an index table R.
Output: A transparency T.

```
1  for each pixel S[w, h] in S do
2    if S[w, h] = white then
3      if R[w, h] = 0 then
4        T[w, h] = [0, 1]
5      else if R[w, h] = 1 then
6        T[w, h] = [1, 0]
7      end if
8    else if S[w, h] = black then
9      Assign randomly T[w, h] to [0, 1] or [1, 0] where P(T[w,
       h]= [0, 1])=1/2.
10   end if
11 end for
```

For the security of Algorithm 1, we observe that $P(T[w, h] = [0, 1]) = P(T[w, h] = [1, 0]) = 1/2$, regardless of the color of the secret pixel $S[w, h]$. Thus, the owner cannot decode the secret by analyzing the probability distribution of the two patterns [0, 1] and [1, 0] in any one transparency.

B. *The case t*=3

In this case, the [7] gives an algorithm to achieve the contrast α=1/16 by using the parameters (2). Initially, we require the index table Z. By the Y defined in (2), each element of Z is randomly assigned to two possible values {0, 1}, by following the probabilities $P(Z[w, h]=0)=1/3$ and $P(Z[w, h]=1)=2/3$. Given a secret image S, the dealer reads each secret pixel $S[w, h]$ in S. For $S[w, h]$ being white, the dealer next reads the value Z[w, h]. If Z[w, h] = 0, the dealer assigns 0 to the $T[w, h]$; otherwise, if Z[w, h] = 1, the dealer assigns a random Boolean number to the $T[w, h]$, where $P(T[w, h]=0)=3/4$. For $S[w, h]$ being black, the dealer next reads the value Z[w, h]. If Z[w, h] = 0, the dealer assigns 1 to the $T[w, h]$; otherwise, if Z[w, h] = 1, the dealer assigns a random Boolean number to the $T[w, h]$, where $P(T[w, h]=0)=1/4$.

To extend the above pixel approach to block approach, we observe that for the white secret pixel, the [7] uses an all-zero sequence $E(1)$ or an memoryless sequence $E(1/4)$ to encode the white secret pixel, and the two possible cases are determined by the corresponding element in Z. In the block approach, we simultaneously represent the two cases $E(1)$ and $E(1/4)$ in a block with size six. The block is divided into two sub-blocks, where each sub-block denotes one of the two cases $E(1)$ and $E(1/4)$. Since the case of choosing $E(1)$ has a

probability 1/3 and the case of choosing $E(1/4)$ has a probability 2/3, to reflect the probabilities in the block, the case $E(1)$ corresponds to the two-pixel sub-block, and the case $E(1/4)$ corresponds to the four-pixel sub-block. Moreover, to represent the $E(1/4)$ in the four-pixel sub-block, we assign a permutation of [1,1,1,0] to the four-pixel sub-block.

For the black secret pixel, the [7] uses an all-one sequence $E(0)$ or an memoryless sequence $E(3/4)$ to encode the black secret pixel, and the two possible cases are determined by the corresponding element in *Z*. In the block approach, we simultaneously represent the two cases $E(0)$ and $E(3/4)$ in a block with size six. Since the case of choosing $E(0)$ has a probability 1/3 and the case of choosing $E(3/4)$ has a probability 2/3, the case $E(0)$ corresponds to the two-pixel sub-block, and the case $E(3/4)$ corresponds to the four-pixel sub-block. Moreover, we assign a permutation of [0,0,0,1] to the four-pixel sub-block to represent the $E(3/4)$.

To possess the security condition in the proposed method for t=3, we need to uniformly permute the positions of the pixels in the block. Since the pixel permutation in each sub-block is mutually independent for each transparency in encoding, the index table R only needs to record the permutation of two categories of pixels in a block: the first category has four pixels and another category has two pixels. There are $\binom{6}{2}$=15 possible combinations of two sub-sets with two and four elements, so each element of R records a uniform random integer between 0 and 14. The details for the case t=3 are described in Algoithm 2:

Algorithm 2. The algorithm of the proposed scheme for t=3.

Input: A binary secret image S and an index table R.
Output: A transparency T.

1 **for** each pixel $S[w, h]$ in S **do**
2 **if** $S[w, h]$ = white **then**
3 Assign randomly T_0 to a permutation of [1, 1, 1, 0]
4 T_1 = [0, 0]
5 Assign $T[w, h]$ to the permutation of T_0 and T_1 according to $R[w, h]$.
6 **else if** $S[w, h]$ = black **then**
7 Assign randomly T_0 to a permutation of [0, 0, 0, 1]
8 T_1 = [1, 1]
9 Assign $T[w, h]$ to the permutation of T_0 and T_1 according to $R[w, h]$.
10 **end if**
11 **end for**

IV. Experiments

Figure 1 depicts the binary secret image "CITI" used in our experiments. For the first experiment of t=2, because the generated transparencies double the size of image, we shrink the height of the original image to 1/2 shown in Fig. 2(a). Then we apply Algorithm 1 to Fig. 2(a) to generate two transparencies shown in Figs. 2(b-c). Figure 2(d) shows the stacking results. To compare the results with [7], Figure 3 shows the stacking results of [7] for t=2. As compared Fig. 2(d) with Fig. 3, we observe that Fig. 2(d) has better visual quality.

The second experiment for t=3 is shown in Fig. 4. Since the transparencies of the proposed algorithm enlarge the original image to six times, to possess the invariant size property, we shrink the height of image to 1/3 and the width of image to 1/2 shown in Fig. 4(a). Then we apply Algorithm 2 to Fig. 4(a) to generate three transparencies as shown in Figs. 4(b-d). Figures. 4(e-g) show the stacking results of any two transparencies, and Fig.4 (h) shows the stacking of the three transparencies. Figure 5 shows the stacking result of [7] for t=3. As compared Fig. 4(h) with Fig. 5, we observe that Fig. 4(h) show better quality of the word "CITI" than Fig. 5.

Furthermore, we also test another binary secret image shown in Fig. 6. Figure 6(a) is the test image "ACADEMIA SINICA". For the case t=2, Figures 6(b) and 6(c) respectively show the stacking results of [7] and the proposed method. For the case t=3, Figures 6(d) and 6(e) respectively show the stacking results of [7] and the proposed method. Consequently, we can recognize the letters shown in Fig. 6(e), but the letters in Fig. 6(d) are indistinct.

V. Conclusions

We have proposed the block approach of (t, n) VC scheme for unbounded n and t=2, 3. A major drawback of the block approach VC is that the transparencies are much larger than the original image, so we need to shrink the size of secret image to possess the invariant size property. As compared the block approach VC with the probabilistic model VC, the block approach VC gives better visual quality under the same parameter setup. For t=3, the block VC is more practical because the contours shown in Fig. 4(h) and Fig. 6(e) are more clear than Fig. 5 and Fig. 6(d).

Fig. 1. The binary secret image "CITI".

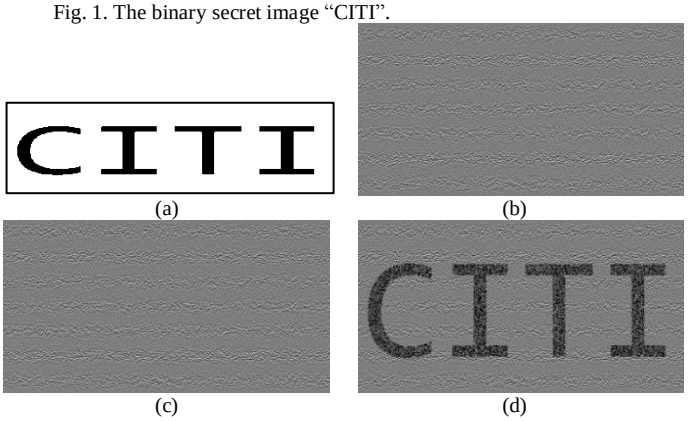


Fig. 2. The results of the proposed scheme for t=2. (a). T_1. (b). T_2. (c). $T_1 \oplus T_2$.

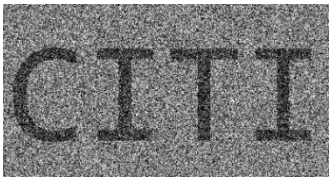
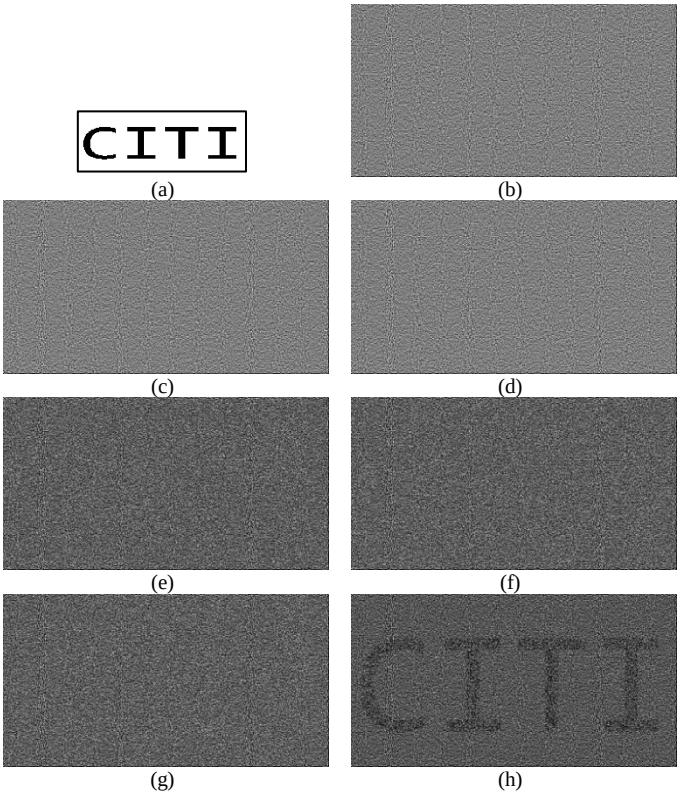


Fig. 3. The stacking result of [7] for t=2.



(a) (b) (c) (d) (e) (f) (g) (h)

Figure 4. The results of the proposed scheme for t=3. (a). T_1. (b). T_2. (c). T_3. (d). $T_1 \oplus T_2$. (e). $T_1 \oplus T_3$. (f). $T_2 \oplus T_3$. (g). $T_1 \oplus T_2 \oplus T_3$.

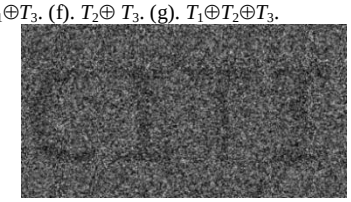
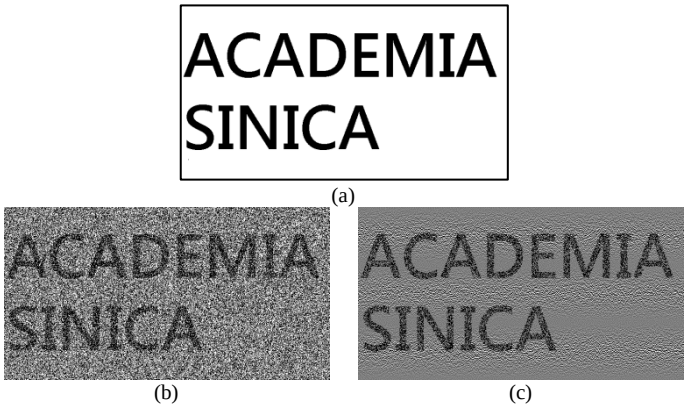
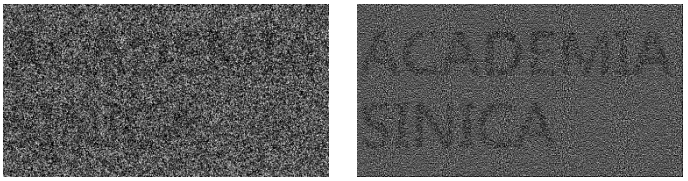


Figure 5. The stacking result of [7] for t=3.



(a) (b) (c)



(d) (e)

Figure 6. The results for another secret image. (a). The test secret image. (b). The stacking result of [7] for t=2. (c). The stacking result of Algorithm 1 for t=2. (d). The stacking result of [7] for t=3. (c). The stacking result of Algorithm 2 for t=3.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptography: EUROCRYPT'94, LNCS, vol. 950, pp. 1–12, 1995.

[2] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," IEICE transactions on fundamentals of electronics, communications and computer sciences, vol. 82, pp. 2172-2177, Oct. 1999.

[3] C. N. Yang, "New visual secret sharing schemes using probabilistic method," Pattern Recognition Letters, vol. 25, pp. 481–494, Mar. 2004.

[4] S. J. Lin, S. K. Chen, and J. C. Lin, "Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion," Journal of Visual Communication and Image Representation, vol. 21, pp. 900–916, Nov. 2010.

[5] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," Information and Computation, vol. 129, no. 2, pp. 86–106, Sep. 1996.

[6] F. Liu, C. Wu, and X. Lin, "Step Construction of Visual Cryptography Schemes," *IEEE Trans. Information Forensics and Security*, vol. 5, no. 1, pp. 27–38, Mar. 2010.

[7] S. J. Lin and W. H. Chung, "A Probabilistic Model of (*t*, *n*) Visual Cryptography Scheme With Dynamic Group," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 197-207, 2012.