EURASIP Journal on
Information Security

RESEARCH Open Access

Improved scheme and evaluation method for progressive visual cryptography

Binh Le Thanh Thai*, Hidema Tanaka and Kohtaro Watanabe

Abstract

Visual cryptography (VC) is a powerful technique with high security and requires no PC or device to reconstruct the secret information. Progressive visual cryptography (PVC) is a variation of the VC scheme in which the quality of the reconstructed image is improved by increasing the number of shared images. The previous study focused directly on maximizing the value of the quality in the completely reconstructed image; thus, there is a difference in the quality of the shared images. In this paper, we focus on the aforementioned issue and propose a new approach based on inductive reasoning. Our basic idea is to maximize the quality of the reconstructed images each time the number of shared images increases. We call this method the *bottom-up approach*. Moreover, hitherto, PVC has been evaluated based on the value of relative difference or by sight. Such evaluation methods are only subjective or difficult to execute without the knowledge of basis matrices. In addition, PVC users cannot easily confirm the effectiveness of their shared images. In this paper, we propose a new information-theoretic evaluation method for PVC, which only uses shared images, to solve the aforementioned problems. Our proposed method can objectively and quantitatively evaluate PVC based on the numerical value, and PVC users can easily confirm the effectiveness of their shared images.

Keywords: Visual cryptography, Progressive visual cryptography, Information-theoretic evaluation method, Shannon-Hartley theorem

1 Introduction

1.1 Background

Visual cryptography (VC) is a secret sharing (SS) scheme [1] in which the secret information is encrypted in the form of digital images, referred to as "shared image." Various VC schemes have been proposed, and they have a common advantage; they do not require any PC or device to reconstruct the secret image and can be executed without electric power supplies [2]. Therefore, VC has many usage and application areas, e.g., pubic services such as temporary authentication cards in disaster areas. Let us imagine that a disaster of the magnitude of "the 2011 Tohoku earthquake and tsunami" occurs in a developing country. The citizens in the disaster area have no electricity or Internet access, and everything they need to prove their identity is lost in the disaster. At that time, VC could be used like the following. One shared image could be distributed to each civilian, who could then take that shared image and stack it with another shared image kept at a special sub-office to prove their identity while protecting personal information and privacy. The other potential usages of VC are considered private usage such as tags for equipment management, privacy protection such as distributed management of medical data (for example, X-ray photographs and CT scan images), etc. The basic idea of VC is simple; thus, various schemes have been proposed. The major schemes are summarized as follows:

Improving Improve the quality of the reconstructed image [3–5].

Progressive Improve the quality of the reconstructed images while increasing the number of shared images [6–10].

*Correspondence: binhbe603501@gmail.com

Department of Computer Science, National Defense Academy of Japan, Hashirimizu, Yokosuka, Japan

© The Author(s) 2022. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

Color Make color images available for use [11–13].

Multiple Reconstruct different secret images by rotating or changing the combinations of the shared images [14–17].

Among the several above-mentioned VC schemes, PVC is versatile and highly practical. In addition, "color" and "multiple" can be realized by applying a "progressive"; hence, in this study, we regard PVC as a basic technology and focus on some weaknesses that were noted in the previous study. The focus of PVC in previous studies was on the application of color images [7], generating shared images without expansion of image size [6], or improving the quality of the completely reconstructed image [9]. In this paper, we are interested in improving the quality of the reconstructed images. Therefore, we emphasize the scheme proposed by Okada and Koga [9], and call it the "basic scheme."

VC was previously exclusively assessed using the "relative difference" or by sight. PVC is also evaluated using similar methods. The evaluation by sight is very subjective and depends on the situation. On the other hand, evaluating based on the value of relative difference necessitates knowledge of basis matrices, making relative comparisons challenging. Therefore, PVC users cannot simply verify the effectiveness of their shared images. As a result, there is an undesirable operating precondition in which users cannot validate the legitimacy of their shared images in advance and must rely on them completely. This problem can be ignored if the same person generates shared images and reconstructs the secret information; however, these problems are considered to be disadvantageous to the user and pose a difficulty in the development of PVC.

1.2 Motivations and contributions

There is a bias in the shared images because the basic scheme solely focused on maximizing the quality of the completely reconstructed image. Furthermore, the quality of certain images that are not reconstructed from all shared images may not be satisfactory. Solving this problem by proposing a novel scheme that can generate all shared images with the same quality is our first motivation. To solve this problem, first, we analyze the cause of such a bias and identify the problems that PVCs face and summarize the requirements for the improvement. Next, we use the idea of "maximizing the quality of the reconstructed image each time the number of shared images rises one" to enhance the method for more effective basis matrices based on the examination of these requirements and limitations. We provide a new parameter based on this concept to ensure the lower bound of black pixels in reconstructed images, hence increasing the quality of all reconstructed images. We refer to our scheme as the "Bottom-up approach" and compare it to the basic scheme. We confirm that using the same conventional evaluation scale, our technique can overcome the aforementioned problems and meet the requirements. This is the first contribution of our study.

As is shown in Section 1.1, in PVC, a general objective evaluation method and the evaluation method from the user side are not employed. Motivated by solving this problem, we propose a new information-theoretic evaluation method. The proposed method uses only shared images; hence, PVC users can easily confirm the effectiveness of their shared images. We also quantified the evaluation value, so PVC may be evaluated objectively and quantitatively in terms of its numerical value. In considering such a method, we focused on the following two facts:

- An ideal shared image should have high randomness.
- The number of black pixels always increases during the reconstruction process.

Through experiments, we confirmed that our proposed method can objectively and quantitatively evaluate PVC. In particular, based on the analysis of the reconstructed images generated from three shared images of the (3, 5)-PVC, we demonstrate the existence of ineffective share images in the basic scheme. Furthermore, the biases between shared images can be estimated numerically, which cannot be confirmed by sight or the relative difference. This is the second contribution of our study.

The remainder of this paper is organized as follows. VC is summarized in Section 2. In Section 3, we describe our proposed VC scheme and the bottom-up approach and compare our scheme with the basic scheme to highlight the advantages of our scheme. In Section 4, we present our second contribution: the information-theoretic evaluation method. Section 5 presents the detailed evaluation results and analysis. In Section 6, we summarize the issues related to the future development of VC. Finally, in Section 7, we present our conclusions.

2 Progressive visual cryptography

2.1 Outline of VC [2]

In this section, we describe the outline of (t, n)-VC for black-white images. Given a secret black-white image, n black-white shared images are generated from this secret image. The ith shared image is distributed to the ith participants securely for each $i \in G = \{1, 2, \ldots, n\}$. In general, one pixel of the secret image is expanded to e_x pixels, and we refer to e_x as the "pixel expansion". We use the "basis matrix" to realize such an expansion. Since OR operation is used in the reconstruction process, a reconstructed pixel will be white if and only if corresponding pixels in all shared images are white, and are black, otherwise. Therefore, we define a white pixel as "0" and a black pixel as "1" and use X_0 and X_1 as the basis matrices for the white and black pixels, respectively. We define the basis matrices as follows:

Definition 1 A pair (X_0, X_1) of $n \times e_x$ Boolean matrices can be defined as the basis matrices of (t, n)-VC if the following two conditions are satisfied:

Conditiona There exists a number $\alpha_k > 0$ such that for any $P \subset G$ and $|P| = k$ $(t \leq k \leq n)$, the following two inequalities hold for some $d_P > 0$:

$$H_w(X_0[P]) + \alpha_k \cdot e_x \leq d_P, \tag{1}$$

$$H_w(X_1[P]) \geq d_P \tag{2}$$

where $X_i[P]$ $(i = 0$ or $1)$ denotes the $|P| \times e_x$ matrix obtained by all the rows of X_i corresponding to P, and $H_w(\cdot)$ denotes the Hamming weight of the OR summation of each column in $X_i[P]$.

Conditionb For $P \subset G$ such that $|P| < t$, $X_1[P]$ can be made identical to $X_0[P]$ by an appropriate permutation with respect to the columns.

Condition a ensures that a secret image can be reconstructed by stacking at least $t(t \leq n)$ shared images. We can actually distinguish white pixels with black pixels in the reconstructed images due to the gap of at least $\alpha_k \cdot e_x$ between the Hamming weights $H_w(X_0[P])$ and $H_w(X_1[P])$.

Condition b guarantees VC security. In a reconstructed image generated from fewer than t shared images, it is impossible to distinguish whether a pixel is black or white in the secret image because such a permuted $X_i[P]$ $(i \in \{0, 1\})$ occurs with the same probability, regardless of whether the pixel is black or white. According to [5] and [10], the following equation can be derived:

$$H_w(X_0[P]) = H_w(X_1[P]) \quad \forall P \subset G, |P| \leq t - 1 \tag{3}$$

The value of α_k in Eq. (2) is defined as the difference between the number of white pixels and the number of black pixels for the stacking of k shared images; this difference is called the "relative difference." There are several definitions and calculation methods for α; herein, we adopt Koga's formula [8], which can be expressed as follows:

$$\alpha_k = \min_{P:P\subset G,|P|=k} \frac{H_w(X_1[P]) - H_w(X_0[P])}{e_x}, \; t \leq k \leq n \tag{4}$$

In general, as the value of α increases or the value of e_x decreases, we can perceive a secret image more clearly on the reconstructed image.

2.2 Basic scheme

In this section, we present the basic scheme proposed by Okada et al. [9], which focused on maximizing the value of α_n. Let $B = \{\boldsymbol{b_1}, \boldsymbol{b_2}, ..., \boldsymbol{b_{2^n-1}}\}$ be a vector set, where $\boldsymbol{b_i}(1 \leq i \leq 2^n - 1)$ denotes an n[bit] binary column vector corresponding to integer i as follows:

$$\boldsymbol{b_i} = (b_{(i,1)}, b_{(i,2)}, \ldots, b_{(i,n)})^\top, \; b_{(i,j)} \in F_2, \; 1 \leq j \leq n \tag{5}$$

For a subset $P \subset G$, we denote $\flat_i^P$ as the OR summation of each column element determined by subset P.

$$\flat_i^P = \bigvee_{j \in P} b_{(i,j)}, \quad P \subset G \tag{6}$$

Basis matrices X_0 and X_1 can be generated from B according to e_x, allowing the overlap choice. We denote S as a multiset of $\boldsymbol{b_i}$s as follows.

$$S = \{\boldsymbol{b}_i^{m(\boldsymbol{b}_i)}, \boldsymbol{b}_j^{m(\boldsymbol{b}_j)}, \ldots\}, \; \sum_{\boldsymbol{b}_i \in S} m(\boldsymbol{b}_i) = e_x, \; m(\boldsymbol{b}_i) \in \mathbb{N}, \tag{7}$$

where $\{\boldsymbol{b_i}, \boldsymbol{b_j}, \ldots\}$ denotes the underlying set and $m(\boldsymbol{b_i})$ denotes the multiplicity of element $\boldsymbol{b_i}$. Let S^p $(p \in \{0, 1\})$ be the multiset corresponding to the basis matrix X_p, and let y_{P,S^p} be the summation of $\flat_i^P$ corresponding to subset P.

$$y_{P,S^p} = \sum_{i:\boldsymbol{b_i} \in S^p} m(\boldsymbol{b_i}) \cdot \flat_i^P \tag{8}$$

Note that the pixel corresponding to vector $\boldsymbol{b_i}$ in the jth shared image is black if $b_{(i,j)}$ is 1, and white, otherwise. For this reason, for $P, Q \subset G$, the pixel corresponding to vector $\boldsymbol{b_i}$ is white when $P \cap Q = \emptyset$ and black when $P \cap Q \neq \emptyset$. With these notations, we summarize the algorithm to find multisets S^p illustrated by Okada et al. [9] in Algorithm 1. Using these multisets, we can derive the basis matrices of the basic scheme. Furthermore, Okada et al. [9] also showed the algorithm to calculate the minimum value of e_x to achieve the maximum α_n in general cases. These algorithms can be easily executed using a mixed-integer linear programming (MILP) solver such as Gurobi [18].

The progressive condition [8] for the basis matrices is as follows:

$$\alpha_t < \alpha_{t+1} < \cdots < \alpha_n \tag{9}$$

The basis matrices of the basic scheme always satisfy this condition and can generate shared images with the maximum value of α_n. However, there may exist some cases where two reconstructed images generated from $k-1$ and $k(t \leq k \leq n-1)$ shared images, respectively, have the same quality even when $\alpha_{k-1} < \alpha_k$ holds. Notably, there may be a significant difference in the value of α between a reconstructed image generated from $k-1$ shared images and that generated from $k+1$ shared images. Therefore, this scheme has two following weaknesses:

Problem1 Large differences in quality among the shared images (we can visually distinguish shared images).

Problem2 The quality of the reconstructed image depends on the combination of the shared images (visibility of the secret image on the reconstructed images differs according to the combination of the shared images).

The aforementioned problems limit the usage of PVC. The following requirements are therefore based on these problems.

Requirement1 Each shared image should be indistinguishable to the sight.

Requirement2 The validity of the shared images should be confirmed (the reconstructed images using any combinations of the shared images have the same amount of visual information).

In this paper, we add a new constraint to maximize the value of α_k continuously throughout the reconstruction process to solve the problems and achieve the stated requirements.

3 Improvement of PVC

3.1 Bottom-up approach

As is shown above, the basic scheme focused on directly maximizing the value of α_n. However, this is not a unique idea for obtaining the maximum value of α_n. In this section, we show a novel approach that is based on inductive reasoning. First, we try to maximize the value of α_k with $k = t$, when the secret image can be recognized. Then, we increase the value of k by one and try to maximize the value of α_k again. We repeat this process until $k = n$, so we can, in theory, obtain the maximum α_n. Note that we must ensure that generated basis matrices always satisfy the progressive condition in Eq. (9). With this consideration, not only the completely reconstructed image but also the reconstructed images that are generated from less than n shared images will have good quality.

To realize this approach, first, we make a small change from Algorithm 1 to maximize the value of α_t in the case $k = t$. We show this result in Algorithm 2. Notably, the last condition of Algorithm 2 is added to ensure that generated basis matrices satisfy the progressive condition. Next, we regard Algorithm 2 as a sub-algorithm MP(k) to calculate the value of α_k. Using this value of α_k, we introduce a new parameter $\beta_k = e_x \times \alpha_k$ and use this parameter to replace some constraints of the Algorithm 2 to maximize the value of α_{k+1}. We summarize this process in Algorithm 3 and call this scheme the "Bottom-up approach." A point to note here is that both the bottom-up approach and the basic scheme aim for a maximum α_n, so there is a non-zero possibility that the same basis matrices will be generated for both schemes. However, compared to the basic scheme, the bottom-up approach always generates reconstructed images generated from k $(t \leq k \leq n-1)$ shared images of higher quality. In the following section, we show an example of this approach.

maximize: $\sum_{P:P\subset G,|P|>0} y_{P,S^1} - \sum_{P:P\subset G,|P|>0} y_{P,S^0}$

subject to: $P, Q \subset G$

$$\sum_{P:P\subset G} y_{P,S^1} = \sum_{P:P\subset G} y_{P,S^0} = e_x$$

$$\forall Q\ s.t\ |Q| < t: \quad \sum_{P:P\cap Q\neq\emptyset} y_{P,S^1} = \sum_{P:P\cap Q\neq\emptyset} y_{P,S^0}$$

$$\forall Q\ s.t\ |Q| \geq t: \quad \sum_{P:P\cap Q\neq\emptyset} y_{P,S^0} \leq \sum_{P:P\cap Q\neq\emptyset} y_{P,S^1}$$

Algorithm 1 Max α_n

maximize: $X \in \mathbb{Z}$

subject to: $P, Q \subset G$

$$\sum_{P:P\subset G} y_{P,S^0} = \sum_{P:P\subset G} y_{P,S^1} = e_x$$

$$\forall Q\ s.t\ |Q| < t: \quad \sum_{P:P\cap Q\neq\emptyset} y_{P,S^0} = \sum_{P:P\cap Q\neq\emptyset} y_{P,S^1}$$

$$\forall Q\ s.t\ |Q| = t: \quad X + \sum_{P:P\cap Q\neq\emptyset} y_{P,S^0} \leq \sum_{P:P\cap Q\neq\emptyset} y_{P,S^1}$$

$$\forall Q\ s.t\ |Q| > t: \quad 1 + \sum_{P:P\cap Q\neq\emptyset} y_{P,S^0} \leq \sum_{P:P\cap Q\neq\emptyset} y_{P,S^1}$$

Algorithm 2 Max α_t

```
Execute MP($t$)
$k = t$
while $k < n$ do
    Execute MP($k$)
    $\beta_k = e_x \times \alpha_k$
    Replace constraint in cases $|Q| = k$ and $|Q| = k + 1$ of MP($k$) as follows.
        $\forall Q \; s.t \; |Q| = k : \; \beta_k + \sum_{P:P\cap Q\neq\emptyset} y_{P,S^0} \leq \sum_{P:P\cap Q\neq\emptyset} y_{P,S^1}$
        $\forall Q \; s.t \; |Q| = k+1 : \; X + \sum_{P:P\cap Q\neq\emptyset} y_{P,S^0} \leq \sum_{P:P\cap Q\neq\emptyset} y_{P,S^1}$
    $k = k + 1$
end while
```

Algorithm 3 Bottom up approach

3.2 Example model

In this section, we describe the example model used in this paper. As is shown in Section 2.2, Okada et al. [9] showed the algorithm to calculate the minimum e_x to achieve the maximum α_n. We use this algorithm to calculate the values of e_x in some cases and show the results in Table 1. From here onwards, let $\{S_1, S_2, \cdots, S_n\}$ be the set of shared images. We denote $R_{[i_1,i_2,\ldots,i_j]}$ as a reconstructed image generated by stacking j shared images $\left\{S_{i_1}, S_{i_2}, \ldots, S_{i_j}\right\}$ and R_j as the label for reconstructed images generated from all combinations of $j(2 \leq j \leq n)$ shared images.

In this paper, we use a (3,5)-PVC for example, and the target secret image is presented in Fig. 1. Since the aspect ratio after coding does not change, we chose e_x as the least square nearest to the theoretical minimum. From Table 1, the optimal value of e_x for (3,5)-PVC is 18; thus, we set $e_x = 16$ and find the basis matrices for the basic and our scheme by using Algorithms 1 and 3. Figures 2 and 3 present examples of the basic and our scheme, respectively. We also show the basis matrices of both schemes in the Appendix.

3.3 Experimental results

In this section, we present the evaluation results of the basic scheme and the bottom-up approach using the conventional evaluation methods.

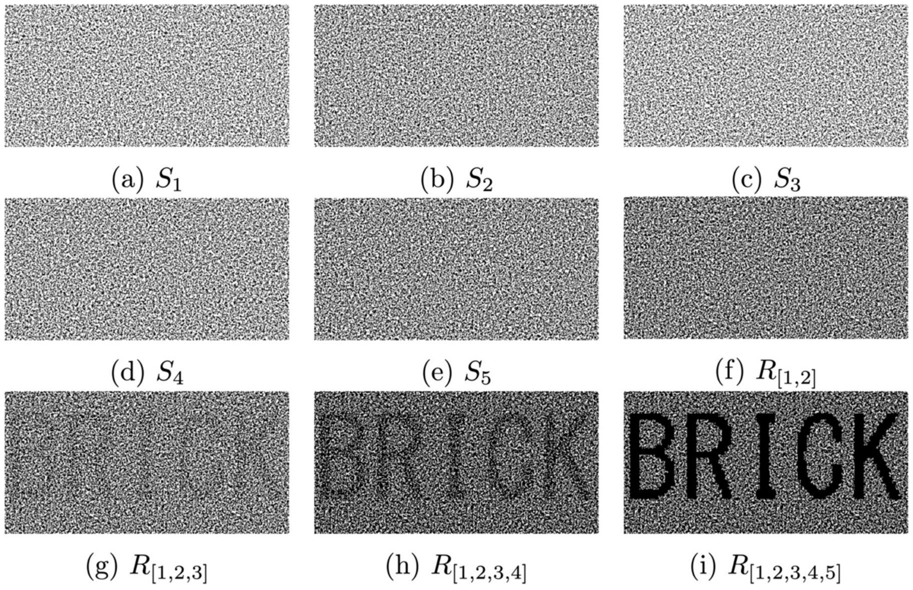
Fig. 1 The secret image

3.3.1 Evaluation by sight

We focus on the Hamming weight of the rows in the basis matrices of the two schemes. In the basic scheme, the Hamming weight of the rows is not the same for all the rows; however, all the rows of the basis matrices have the same Hamming weight in our scheme. This fact leads to the difference in the number of black pixels contained in the e_x pixels when we expand the secret image. Therefore, the quality of the shared images will be different. To confirm this result, let us compare the group of shared images between the two schemes (Figs. 2a–e and 3a–e). Here, we define the row of the basis matrix used to create the shared image S_i as the "basic-row" of S_i. From Fig. 2a (resp. c) and e, we can confirm that S_1 (resp. S_3) and S_5 had different shades of darkness in the basic scheme. S_1 and S_3 were whitish compared to S_5. This indicates there is a significant difference in the quality between the shared images in the group. In fact, the basic-rows of S_1 and S_3 have a Hamming weight of 5, whereas that of S_5 has a Hamming weight of 7. Of course, from the structure of PVC, the shared image leaks no information about the secret image; however, such a large difference in quality can be regarded as obtaining information for distinguishing between the shared images. This result is pointed out in **Problem 1** and reveals that **Requirement 1** is not achieved. On the

Table 1 Minimum e_x to achieve maximum α_n

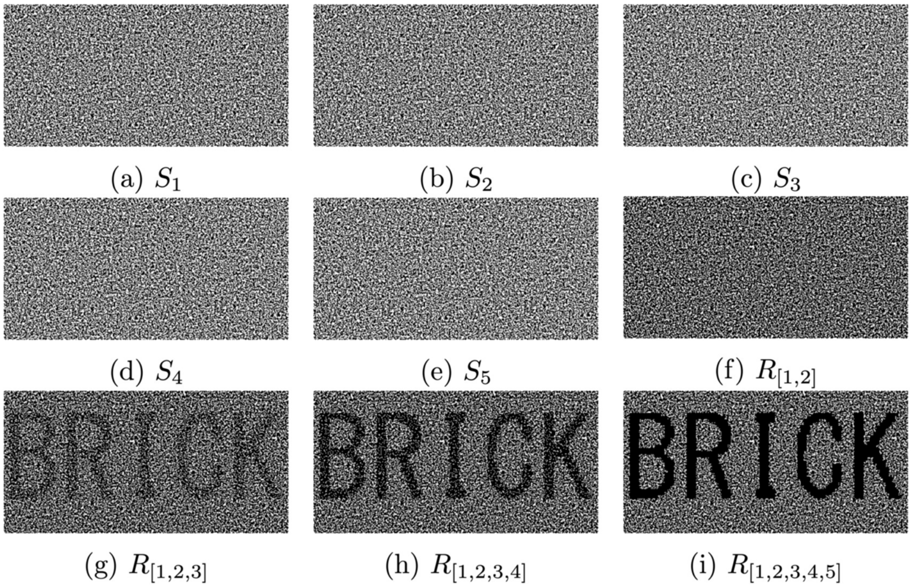
n \ *t*	2	3	4	5	6	7	8	9	10
2	2								
3	3	4							
4	4	6	8						
5	5	18	15	16					
6	6	14	24	30	32				
7	7	16	35	99	70	64			
8	8	35	100	196	128	140	128		
9	9	50	162	576	315	510	315	256	
10	10	33	245	363	650	1155	590	630	512


(a) S_1 (b) S_2 (c) S_3

(d) S_4 (e) S_5 (f) $R_{[1,2]}$

(g) $R_{[1,2,3]}$ (h) $R_{[1,2,3,4]}$ (i) $R_{[1,2,3,4,5]}$

Fig. 2 Example of the (3,5)-PVC generated by the basic scheme


(a) S_1 (b) S_2 (c) S_3

(d) S_4 (e) S_5 (f) $R_{[1,2]}$

(g) $R_{[1,2,3]}$ (h) $R_{[1,2,3,4]}$ (i) $R_{[1,2,3,4,5]}$

Fig. 3 Example of the (3,5)-PVC generated by our scheme

other hand, in our scheme, we cannot distinguish the difference between Fig. 3a–e by sight. In fact, in our scheme, the basic-row of all the shared images has the same Hamming weight of 8. From these results, we conclude that the difference in the Hamming weight of the rows in the basis matrices leads to the difference in the quality of the shared image. Furthermore, we can also conclude that our scheme solves **Problem 1** and achieves **Requirement 1**.

3.3.2 Evaluation by relative difference

First, we consider the reconstructed images R_3 (note that the secret image can be confirmed, and the value of relative difference can be calculated). The basic scheme had $\alpha_3 = 0.0625$, whereas $\alpha_3 = 0.1250$ in our scheme. Here, we introduce a new value called the "intermediate relative difference $\tilde{\alpha}$" for a more detailed comparison. For a reconstructed image $R_{[i_1,i_2,\ldots,i_k]}$ $(t \leq k \leq n)$, we define $\tilde{\alpha}_{R_{[i_1,i_2,\ldots,i_k]}}$ as follows:

$$\tilde{\alpha}_{R_{[i_1,i_2,\ldots,i_k]}} = \frac{H_w(X_1[P]) - H_w(X_0[P])}{e_x}, \quad P=\{i_1,i_2,\ldots,i_k\} \tag{10}$$

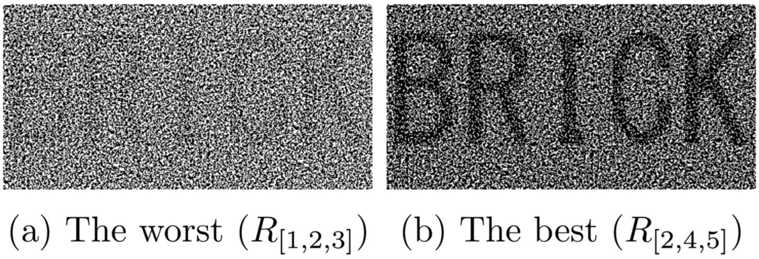
Therefore, Eq. (4) can be rewritten as follows.

$$\alpha_k = \min \tilde{\alpha}_{R_k}, \quad t \leq k \leq n \tag{11}$$

As in the above analysis, in the basic scheme, S_1 and S_3 had the worst quality, whereas S_5 had the best quality. Hence, the reconstructed images containing S_1 or S_3 will consequently have bad quality, and the reconstructed images containing S_5 will have good quality. To confirm this result, we show the best and worst qualities for the R_3 of the basic scheme in Fig. 4. $R_{[2,4,5]}$ had clear secret information with $\tilde{\alpha}_{R_{[2,4,5]}} = 0.1875$, whereas $R_{[1,2,3]}$ had unclear secret information with $\tilde{\alpha}_{R_{[1,2,3]}} = 0.6250$. On the other hand, all R_3s of our scheme had the same $\tilde{\alpha}_4$ value, which was 0.1250. For example, we show two reconstructed images $R_{[1,2,3]}$ and $R_{[1,2,4]}$ in Fig. 5. In both images, the secret image is clear. Similarly, in the case of R_4, the basic scheme had $\alpha_4 = 0.1250$, whereas the value of our scheme was 0.2500. In the basic scheme, $R_{[1,2,3,4]}$ was the worst with $\tilde{\alpha}_{R_{[1,2,3,4]}} = 0.1250$ and $R_{[1,2,4,5]}$ was the best with $\tilde{\alpha}_{R_{[1,2,4,5]}} = 0.2500$. On the other hand, all R_4s of our scheme had the same $\tilde{\alpha}_4$ value, which was 0.2500. These results show the improvement of our approach in the quality of the reconstructed images that are generated from k $(t \leq k \leq n-1)$ shared images. Furthermore, as has been pointed out in **Problem 2**, the quality of a reconstructed image depends on the combination of the shared images in the basic scheme but does not in our scheme.

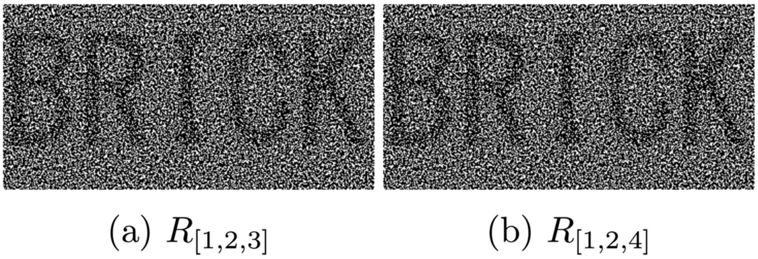
In the case of R_5, both schemes have the same result of $\alpha_5 = 0.3750$. That is, our scheme also achieves the same quality of the completely reconstructed image as the basic scheme. From all the above results, we conclude that our scheme not only achieves a good result in the completely reconstructed image but also in the other reconstructed images that are generated from k $(t \leq k \leq n-1)$ shared images. Furthermore, we also conclude that our scheme can solve **Problem 2** and achieve **Requirement 2**.

Now, let us analyze the relationship between the value of the relative difference and the amount of visual information. Figure 6 shows some R_3s that have the same value for $\tilde{\alpha}_3$ but are generated from different combinations of shared images. We confirmed that although the values of $\tilde{\alpha}_3$ are the same, the clarities of the secret image are different. For example, it is easy to confirm that the clarities of the secret image on $R_{[1,2,3]}$ and $R_{[1,2,4]}$ are different. Furthermore, we also confirmed the existence of some cases where some reconstructed images have the same value for $\tilde{\alpha}$ but are generated from different numbers of shared images (R_3 in a, b, and c and R_4 in d of Fig. 7). These results indicate the limits of evaluation using the relative difference α. We expect that a higher value of α will result in larger visual information. We also expect that the value of α of the reconstructed images will increase with increasing the number of shared images; however, these results show that there is no relationship between α and the amount of visual information in conclusion.



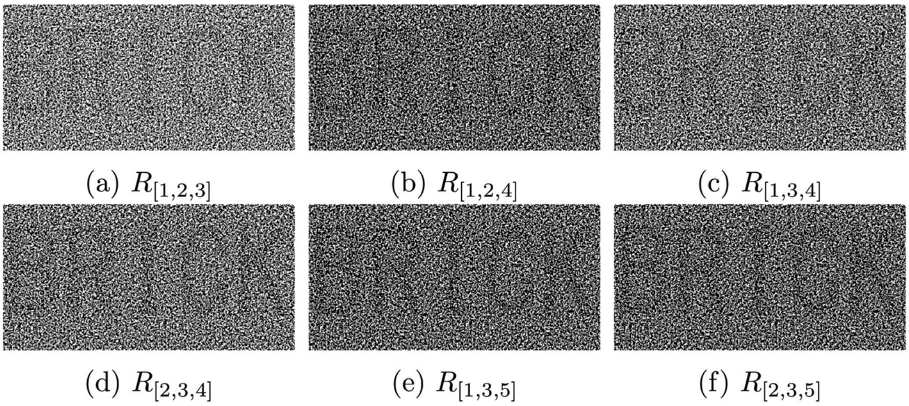
(a) The worst $(R_{[1,2,3]})$ (b) The best $(R_{[2,4,5]})$

Fig. 4 Best and worst qualities of R_3 generated by the basic scheme



(a) $R_{[1,2,3]}$ (b) $R_{[1,2,4]}$

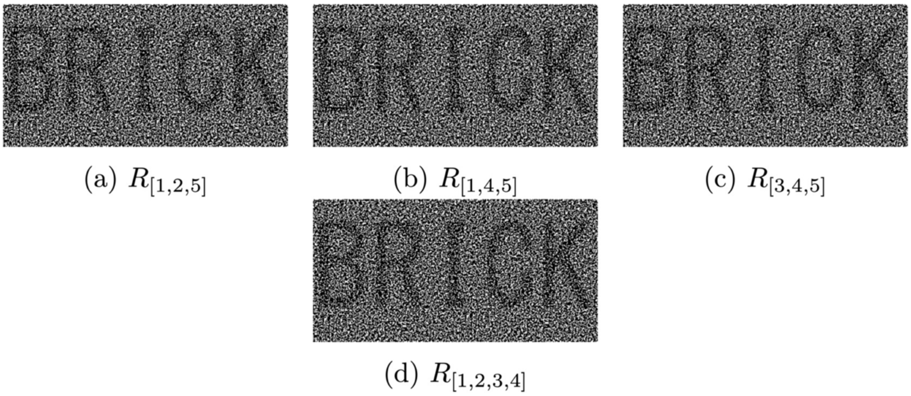
Fig. 5 Two reconstructed images of R_3 generated by our scheme



(a) $R_{[1,2,3]}$ (b) $R_{[1,2,4]}$ (c) $R_{[1,3,4]}$

(d) $R_{[2,3,4]}$ (e) $R_{[1,3,5]}$ (f) $R_{[2,3,5]}$

Fig. 6 Reconstructed images that have the same value of $\tilde{\alpha}_3 = 0.0625$



(a) $R_{[1,2,5]}$ (b) $R_{[1,4,5]}$ (c) $R_{[3,4,5]}$

(d) $R_{[1,2,3,4]}$

Fig. 7 Reconstructed images that have the same value of $\tilde{\alpha} = 0.1250$

4 Information-theoretic evaluation method

As mentioned earlier, the conventional evaluation methods for PVC are not objective or difficult to execute by PVC users. We focused on the feature of PVC that the value of the relative difference increases continuously in the reconstruction process (Eq. (9)). Because the OR operation is used in the reconstruction process, the number of black pixels in a limited space always increases. From the aforementioned facts, we proposed a new evaluation method from the information-theoretic viewpoint, which users can easily execute and can objectively evaluate PVC by a numerical value.

4.1 Preliminary and basic idea

The channel capacity C [bps] on a continuous communication channel can be defined using the Shannon-Hartley theorem. In the frequency range f_1[Hz] $\sim f_2$[Hz], if the noise is additive white Gaussian noise (AWGN), it can be calculated as follows:

$$C = \int_{f_1}^{f_2} \log_2(1 + \frac{S(f)}{N(f)})df \tag{12}$$

where $S(f)$ and $N(f)$ denote the signal power spectrum and noise power spectrum at frequency f [Hz], respectively. This calculation is based on the fact that the condition $S(f) \geq N(f)$ always holds by the AWGN assumption. Because the condition $\alpha_{k+1} \geq \alpha_k$ always holds in PVC (Eq. (9)), we can apply the same assumption if the black pixels are regarded as a signal. This is the basic idea of our proposed evaluation method. If we regard an ideally random shared image as noise and a shared image as a signal, we can apply the Shannon-Hartley theorem to adapt our evaluation method to this type of noise. In this way, an increase in channel capacity denotes an increase in visual information, and a small channel capacity indicates high randomness. Therefore, we can evaluate VC by only using a shared image or a reconstructed image, and **Requirement 2** will be achieved. Moreover, because the noise is ideally random, the increase in visual information caused by comparing or stacking shared images can be quantitatively evaluated.

Let $S(i)$ and $N(i)$ $(i = 0 \sim m)$ be the discrete values of signal power and noise power, respectively, and δ be a constant value of the bandwidth of sampling. The channel capacity for a discrete communication channel can be expressed as follows:

$$C = \sum_{i=0}^{m} (\log_2(1 + \frac{S(i)}{N(i)}))\delta \tag{13}$$

Since index number i is assumed to be a positive integer, it is obvious that the minimum value of δ is one. Hence, we set $\delta = 1$ in this study. In general, the unit for channel capacity is "bit per sec [bps]". However, because the target of the proposed evaluation method is image data, it is appropriate to use "bit per frame [bpf]." For simplicity, we refer to it as only [bit] from here onwards.

4.2 Proposed evaluation method

As mentioned above, the number of black pixels always increases during reconstruction in VC. We observe how the number of black pixels in a limited space called "Mask" increases and calculate the channel capacity by applying Eq. (13). We denote the amount of visual information contained in shared image V as D_V and the number of black pixels in the ith mask of image V as $\#b_V(i)$. If we consider the ideal shared image as noise and the generated image as a signal, we can calculate the amount of visual information as the channel capacity according to Eq. (13). In an ideally random image, the expected value of the black pixels will be approximately half the number of pixels in the mask. In this study, we set the size of the mask as the pixel expansion e_x, resulting in a $\sqrt{e_x} \times \sqrt{e_x}$ [pixel] rectangle. We discuss the details regarding the mask size in Section 6. We move the mask from the bottom-left to the top-right of the image and count the number of black pixels contained in it. Let $\#N$ be half the number of pixels in a mask ($\#N = e_x/2$) and the size of the shared image is width × height [pixel]. Therefore, we have the following:

$$M = (\text{width} - \sqrt{e_x} + 1) \cdot (\text{height} - \sqrt{e_x} + 1) \tag{14}$$

where M denotes the total number of masks in an image.

Let the bottom-left starting point rectangle be the zero-th mask, and the final top-right rectangle be the (M - 1)-th mask. Therefore, we can calculate the amount of visual information of image V using Eq. (13) as follows:

$$D_V = \sum_{i=0}^{M-1} \log_2(1 + \frac{|\#b_V(i) - \#N|}{\#N}) \tag{15}$$

Since D_V depends on the image size, we calculate the average amount of information in the mask unit as follows:

$$C_V = M^{-1} \sum_{i=0}^{M-1} \log_2(1 + \frac{|\#b_V(i) - \#N|}{\#N}) \tag{16}$$

Henceforth, we refer to C_V[bit] as the "amount of information"; this value is obtained using basis matrices and therefore does not depend on the target secret image. However, the amount of information of a reconstructed image is affected by the black-to-white ratio in the secret image (see Section 6.2). Therefore, the amount of information of the reconstructed images may vary based on the secret image.

We summarize our proposed method in the following procedure.

Step 1	Obtain the share image size of (t, n)-PVC
Step 2	Calculate the discrete value of M continuous black pixel numbers
Step 3	Calculate the amount of information in the mask unit by using Eq. (16)

The computational cost of step 2 is M times the count of the black pixels in the mask. For step 3, we need to perform step 2 for each shared image. For example, in the case of (t, n)-VC, there is a total of

$$\sum_{i=1}^{n} \binom{n}{i} = 2^n - 1 \tag{17}$$

combinations of shared images. Hence, a total evaluation of the (t, n)-VC requires a computational cost of $(2^n - 1) \cdot M$.

5 Experimental results

In this section, we present the results of applying the proposed method to the PVC model's examples shown in Section 3.2. Since $e_x = 16$, the mask size was 4 × 4 [pixel] and the resultant generated image size was 360 × 180 [pixel]. Consequently, we obtained $M = 63{,}189$ and $\#N = 8$. Our computer environment was as follows.

CPU	3 GHz 6Core Intel Core i5
Memory	8 GB 2667 MHz DDR4
OS	macOS Catalina 10.15.7
Program	OpenCV 4.4.0 in Python 3.9.0

The average time of calculation for one shared image or reconstructed image was less than 5s.

Table 2 Results of evaluation method with one shared image

	C_{S_1}	C_{S_2}	C_{S_3}	C_{S_4}	C_{S_5}	**Average**	**Standard deviation**
Basic scheme	0.4515	0.3258	0.4514	0.3267	0.2249	0.3560	0.1928
Our scheme	0.1768	0.1780	0.1772	0.1815	0.1797	0.1786	0.0039

5.1 Evaluation of shared images

In this section, we show that the proposed evaluation method can be easily executed using shared images and present the evaluation results. Table 2 presents the amount of information for each shared image in the two schemes. First, let us compare the overall performance of the two schemes using the average and standard deviations for the amount of information. The basic scheme had an average of 0.3560 [bit], whereas, our scheme had 0.1786 [bit]. Compared to the basic scheme, our method had approximately half the amount of information. On the other hand, the standard deviation in our scheme was only approximately 1/60 of the basic scheme (0.0039 and 1.1928). The results show that our bottom-up approach generated more ideally random shared images and successfully generates a group of shared images with a smaller bias as compared to the basic scheme. Notably, these results are the same as those confirmed by sight and the relative difference mentioned in Section 3.2.

Next, for a more detailed analysis, let us compare the best and worst of the two schemes. In the basic scheme, S_5 (Fig. 2e) had the highest randomness with $C_{S_5} = 0.2249$ [bit], whereas S_1 and S_3 (Fig. 2a, c) had the low randomness with $C_{S_1} = 0.4515$ [bit] and $C_{S_3} = 0.4514$ [bit]. Note that we already confirmed by the sight that S_1 and S_3 had the worst quality whereas S_5 had the best quality in the basic scheme. The amount of information for S_1 and S_3 was almost the same, and this value was only approximately 1/2 for S_5. It is also regarded that the difference in the Hamming weight of the basic-row between the shared images led to this result. As mentioned earlier, the Hamming weight of the basic-rows of S_1 and S_3 was small, precisely 5; thus, the number of black pixels in the entire image was also small. Although random shuffle was used during image generation, it is regarded that the value of $|\#b - \#N|$ in Eq. (16) becomes large. Hence, the amount of information also becomes larger. Meanwhile, in our scheme, S_4 had the highest randomness (Fig. 3d) with $C_{S_4} = 0.1815$ [bit], while S_1 had the lowest randomness (Fig. 3a) with $C_{S_1} = 0.1768$ [bit]. The difference was very small (0.0047 [bit]), which could only be confirmed based on the numerical value and cannot be by the sight. This indicates our proposed method can evaluate the detailed value that cannot be otherwise evaluated by sight.

The amount of information could not be evaluated based on the definition of relative difference even the amount of visual information in shared images was evaluated by subjective visual senses in conventional methods. From the above analysis, we conclude that our proposed method can quantitatively evaluate the achievement of **Requirement 1** in a numerical value. Furthermore, our proposed method can execute using only shared images. Therefore, if the PVC provider informs the users of the average value of the amount of information for the shared images, the PVC users can easily calculate the amount of information and confirm the effectiveness of their shared images. This result provides a more reliable and easier-to-use environment for PVC users.

5.2 Evaluation of the reconstructed image

In this section, we demonstrate that our proposed method can also be used to evaluate reconstructed images without any knowledge of basis matrices. First, we consider the reconstructed images generated from (a threshold of) three shared images, where the secret image can be confirmed. The amount of information was not the same for all R_3s in the basic scheme, whereas our scheme had almost the same value for all R_3s. We present the distribution of the amount of information for R_3s in the two schemes shown in Fig. 8. In Fig. 8, the R_3s are arranged on the horizontal axis, and the amount of information they have is represented by a line graph. Since the difference in the quality of shared images leads to a difference in the quality of the reconstructed images, we expect that if a group of ideal images is generated, the graph becomes a horizontal line regardless of the order of the images arranged on the horizontal axis. On the other hand, if the image group has a bias, a zigzag line graph is obtained. The large difference in the amount of information for R_3s of the basic scheme can be confirmed in Fig. 8. The graph of our scheme is nearly linearly parallel to the horizontal axis, whereas that of the basic scheme is zigzag. Consequently, we can confirm that **Problem 2** occurs in the basic scheme but does not in our scheme. Therefore, we conclude that only our scheme achieved **Requirement 2**. This result also shows that we can easily confirm the existence of **Problem 2** and the achievement of **Requirement 2** without any knowledge of basis matrices.

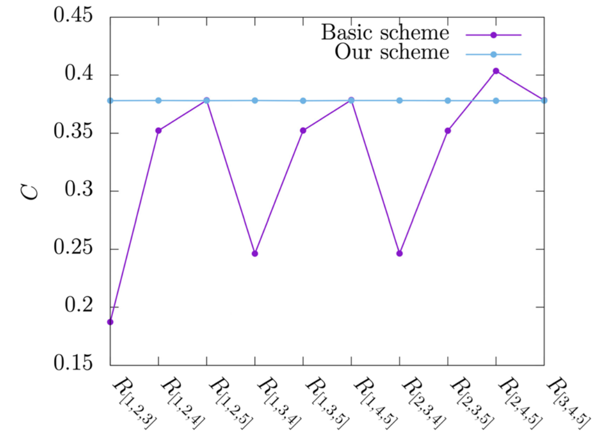


Fig. 8 Amount of information C in R_3 of two schemes

Because the value of the relative difference continuously increases in the PVC, we expect that the amount of information for the reconstructed images also continuously increases. Furthermore, the increase in the amount of information is expected to decrease with an increase in the number of shared images. In the case of a large bias in the shared images, there is a possibility that the randomness increases or does not change when stacking shared images. That is, the amount of information decreases or does not increase, respectively. In the basic scheme, such possibilities are confirmed. We present remarkable examples of the reconstruction process of the basic scheme in Fig. 9 to confirm these results. Figure 9a shows a case where the amount of information decreases because the randomness is improved once. The degree of improvement in randomness can be quantitatively evaluated using the proposed method. Similarly, we also can confirm the case that the amount of information does not increase. In Fig. 9b, S_5 and $R_{[1,5]}$ have the same amount of information. That is, the randomness does not change when we stack S_1 onto S_5. On the other hand, in our proposed scheme, no such cases were found. An example of the reconstruction process of our scheme is presented in Fig. 10. From Fig. 10, we can confirm that the amount of information for the reconstructed images increases continuously and the increase in the amount of information decreases in the process as expected. From the above analysis, we conclude that the proposed method enables more detailed evaluations than the conventional method using the relative difference.

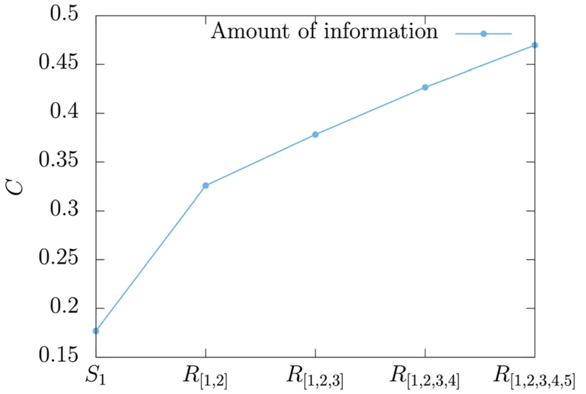
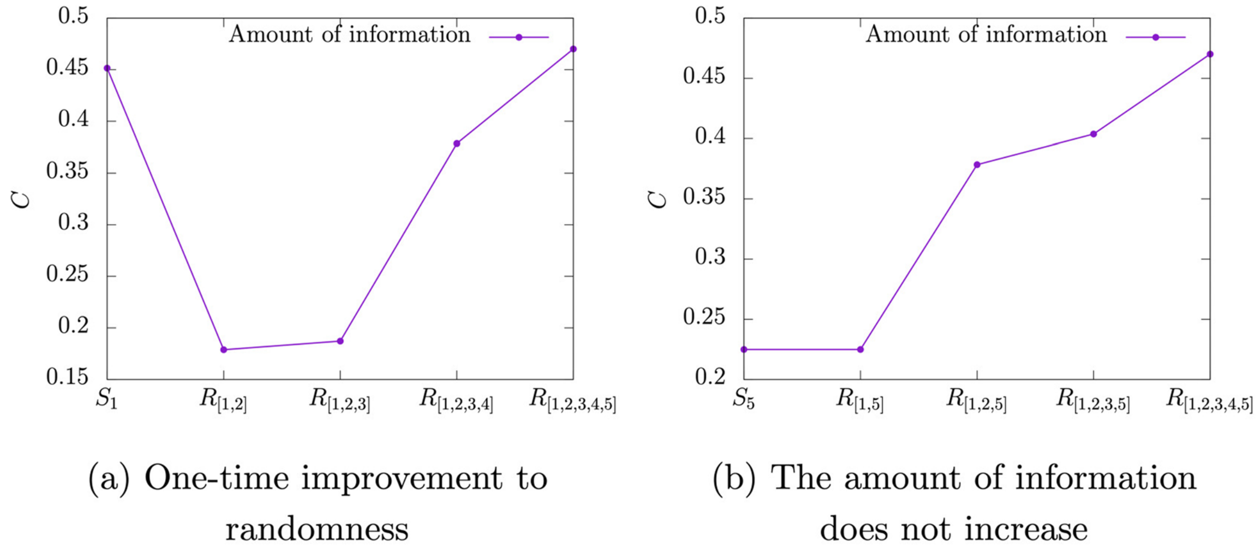


Fig. 10 Example of the stable reconstruction process of our scheme



(a) One-time improvement to randomness

(b) The amount of information does not increase

Fig. 9 Remarkable examples of the reconstruction process in the basic scheme

6 Discussion

6.1 Size of mask

In Section 4.2, we set the mask size to the same value as that of pixel expansion. Therefore, regardless of the value of pixel expansion, the mask size must be determined empirically or experimentally. Our experimental results presented in Section 5 show that a mask size of 4×4 [pixel] is highly effective. Certainly, the setting of mask size to 4×4 [pixel] is appropriate from the condition of $e_x = 16$; however, considering the value of $\#N$ and the range of $\#b$, it is possible that this setting may be optimal for other image sizes and pixel expansions. For example, let us consider the case where the mask size is 3×3 [pixel]. In this case, the value of $\#N$ becomes 4.5; thus, even if the shared image is ideally random, the calculation result of $(\#b - \#N)$ will be non-zero, which leads to unavoidable errors. Therefore, it is not adequate to set the mask size to an odd number of squares. On the other hand, in the case of 2×2 [pixel], the range of $\#b$ is too small. Conversely, in the case of 6×6 [pixel], the range of $\#b$ is large, and it is possible to set detailed values. However, we must examine whether such expressions of detailed values are necessary for evaluation. The value of e_x is sufficiently smaller than the image size; hence, the number of samples is not affected, and the required computational cost does not change (from Eq. (14)). However, the reliability of the calculated evaluation results is significantly different. This issue will be addressed in our future work.

6.2 Validity of AWGN assumption

In view of the fact that the number of black pixels contained in the reconstructed images always increases in the reconstruction process, as mentioned in Section 4.1, we confirmed that the AWGN assumption made in the proposed method is valid. Since the reconstruction process is based on OR operation, this assumption is valid for the entire image; however, it does not apply locally. For example, let us consider two reconstructed images $R_{[1,2,5]}$ and $R_{[1,2,3,4]}$ (Fig. 7a, d) of the basic scheme. These images have the same value $\tilde{\alpha}$, which was 0.1250, and the amount of information is also almost the same, where $C_{R_{[1,2,5]}} = 0.3785$ [bit] and $C_{R_{[1,2,3,4]}} = 0.3786$ [bit]. Theoretically, the following holds.

$$C_{R_{[1,2,5]}} = C_{R_{[1,2]}} + C_{S_5} \tag{18}$$

$$C_{R_{[1,2,3,4]}} = C_{R_{[1,2]}} + C_{R_{[3,4]}} \tag{19}$$

Since $C_{R_{[1,2]}} = 0.1788$ [bit], we can obtain $C_{S_5} = 0.1997$ [bit] and $C_{R_{[3,4]}} = 0.1998$ [bit]. However, the actual values are $C_{S_5} = 0.2248$ [bit] and $C_{R_{[3,4]}} = 0.1809$ [bit]. Therefore, we find that it is inappropriate to directly calculate the sum or difference in the amount of information.

As mentioned above, these differences are a result of the OR operation. We consider the black-to-white ratio in the secret image as for another cause. In general, the white area suppresses the increase in the black pixels in the reconstructed image. However, because the proposed evaluation method focuses only on the increase in the number of black pixels, a larger white area results in a larger error in the calculation of the sum and difference in the amount of information. We expect that if this problem is addressed, more detailed and accurate evaluations can be provided.

6.3 Relationship between basis matrices and security of PVC

During image generation, the rows of the basis matrices are randomly replaced. Naor and Shamir [2] suggested that such a random shuffle guarantees the security of VC. Therefore, under the assumption that random shuffle is secure, the security of VC does not decrease even if all the basis matrices, the value of pixel expansion, and random shuffle are open. However, because random shuffle directly reflects the bias of the Hamming weight and run-length in the basis matrices, there is a possibility of an attack based on such a bias. For instance, if an insecure pseudo-random permutation is used, the initial value can be estimated. Therefore, the bias of Hamming weight of the basis matrices may affect the security of PVC. Specific verification of this is our future work.

7 Conclusion

We demonstrated the problems associated with PVC and described the requirements to improve PVC. We proposed a new improved scheme, the bottom-up approach, which introduces a new parameter to maximize the value of α during the reconstruction process. The experimental results showed that our scheme can solve the aforementioned problems and achieve these requirements of PVC. In addition, we also clarified the problem that the evaluation methods for PVC are subjective or difficult to execute without the knowledge of basis matrices. These problems lead to the fact that PVC users cannot confirm the effectiveness of their shared images. We proposed a new information-theoretic evaluation method that uses only the shared image or the reconstructed images. By experiment, we confirmed that our method can objectively and quantitatively evaluate PVC. Furthermore, the proposed method can achieve a more detailed evaluation, which cannot otherwise be achieved in conventional evaluation methods, by using a numerical value. The proposed method can also confirm the achievement of the aforementioned requirements and can be easily executed by PVC users. We have also highlighted future works for the development of PVC.

Appendix

The basis matrices for (3, 5)-PVC of both schemes mentioned in Section 2.2 are as follows.

The basic scheme:

$$X_0 = \begin{pmatrix} 0,0,0,0,0,0,1,0,1,1,0,0,1,0,0,1 \\ 0,0,0,0,0,0,1,1,1,0,1,1,1,0,0,0 \\ 0,0,0,0,0,0,0,1,1,0,0,1,1,0,0,1 \\ 0,0,0,0,0,0,1,1,1,0,0,0,0,1,1,1 \\ 0,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1 \end{pmatrix}$$

$$X_1 = \begin{pmatrix} 1,1,0,0,0,0,0,0,0,0,0,0,0,1,1,1 \\ 0,0,1,1,0,1,0,0,0,0,0,0,0,1,1,1 \\ 0,0,0,0,1,1,0,0,0,0,0,0,0,1,1,1 \\ 0,0,0,0,0,0,1,1,1,0,0,0,0,1,1,1 \\ 0,0,0,0,0,0,0,0,0,1,1,1,1,1,1,1 \end{pmatrix}$$

Bottom-up approach:

$$X_0 = \begin{pmatrix} 0,0,0,0,0,0,1,1,1,1,1,1,1,1,0,0 \\ 0,0,0,0,0,0,1,1,1,1,1,1,0,0,1,1 \\ 0,0,0,0,0,0,1,1,1,1,0,0,1,1,1,1 \\ 0,0,0,0,0,0,1,1,0,0,1,1,1,1,1,1 \\ 0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1 \end{pmatrix}$$

$$X_1 = \begin{pmatrix} 1,1,0,0,0,0,0,0,0,0,1,1,1,1,1,1 \\ 0,0,1,1,0,0,0,0,0,0,1,1,1,1,1,1 \\ 0,0,0,0,1,1,0,0,0,0,1,1,1,1,1,1 \\ 0,0,0,0,0,0,1,1,0,0,1,1,1,1,1,1 \\ 0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1 \end{pmatrix}$$

Abbreviations

SS: Secret sharing; VC: Visual cryptography; PVC: Progressive visual cryptography; AWGN: Additive white Gaussian noise.

Acknowledgements

Not applicable.

Authors' contributions

KW designed the algorithms of the bottom-up approach, and LTTB and HT designed the algorithm of the information-theoretic evaluation method and carried the experiments. The authors read and approved the final manuscript.

Availability of data and materials

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Competing interests

The authors declare that they have no competing interests.

Received: 16 March 2022 Accepted: 2 December 2022
Published online: 17 December 2022

References

1. A. Shamir, How to share a secret. Commun ACM **22**(11), 612–613 (1979)
2. M. Naor, A. Shamir, in: Santis AD (ed) Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings, Lecture Notes in Computer Science. Visual cryptography, vol 950 (Springer, Berlin, Heidelberg, 1994), pp. 1–12
3. C. Blundo, P. D'Arco, A.D. Santis, D.R. Stinson, Contrast optimal threshold visual cryptography schemes. SIAM J. Discret. Math. **16**(2), 224–261 (2003)
4. T. Hofmeister, M. Krause, H.U. Simon, Contrast-optimal k out of n secret sharing schemes in visual cryptography. Theor. Comput. Sci. **240**(2), 471–485 (2000)
5. M. Iwamoto, A weak security notion for visual secret sharing schemes. IEEE Trans. Inf. Forensics Secur. **7**(2), 372–382 (2012)
6. Y. Hou, Z. Quan, Progressive visual cryptography with unexpanded shares. IEEE Trans. Circuits Syst. Video Technol. **21**(11), 1760–1764 (2011)
7. D. Jin, W. Yan, M.S. Kankanhalli, Progressive color visual cryptography. J. Electron. Imaging **14**(3), 033019 (2005)
8. H. Koga, in: Advances in Cryptology - ASIACRYPT 2002, 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002, Proceedings, Lecture Notes in Computer Science, ed. by Y. Zheng. A general formula of the (t, n)-threshold visual secret sharing scheme, vol 2501 (Springer, Berlin, Heidelberg, 2002), pp. 328–345
9. K. Okada, H. Koga, in: 2017 IEEE Information Theory Workshop, ITW 2017, Kaohsiung, Taiwan, November 6-10, 2017. A construction of the progressive (3, n)-threshold visual cryptography using a BIBD and analysis of its optimality (IEEE, 2017), pp. 249–253
10. S.J. Shyu, M.C. Chen, Optimum pixel expansions for threshold visual secret sharing schemes. IEEE Trans. Inf. Forensics Secur. **6**(3–2), 960–969 (2011)
11. S. Dutta, A. Adhikari, S. Ruj, Maximal contrast color visual secret sharing schemes. Des. Codes Cryptogr. **87**(7), 1699–1711 (2019)
12. C. Yang, C. Laih, New colored visual secret sharing schemes. Des. Codes Cryptogr. **20**(3), 325–336 (2000)
13. S.J. Shyu, Efficient visual secret sharing scheme for color images. Pattern Recognit. **39**(5), 866–880 (2006)
14. G. Ateniese, C. Blundo, A.D. Santis, D.R. Stinson, Extended capabilities for visual cryptography. Theor. Comput. Sci. **250**(1–2), 143–161 (2001)
15. M. Iwamoto, H. Yamamoto, H. Ogawa, Optimal multiple assignments based on integer programming in secret sharing schemes with general access structures. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **90-A**(1), 101–112 (2007)
16. M. Sasaki, Y. Watanabe, Visual secret sharing schemes encrypting multiple images. IEEE Trans. Inf. Forensics Secur. **13**(2), 356–365 (2018)
17. S.J. Shyu, H. Jiang, General constructions for threshold multiple-secret visual cryptographic schemes. IEEE Trans. Inf. Forensics Secur. **8**(5), 733–743 (2013)
18. Gurobi Homepage. https://www.gurobi.com. Accessed 13 Mar 2022

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.