A scalable ideal progressive visual cryptography scheme

LINGFU WANG

School of Computer Science and Information Security, Guilin University of Electronic Technology

JING WANG *

School of Computer Science and Information Security, Guilin University of Electronic Technology

WEIJIA HUANG

School of Computer Science and Information Security, Guilin University of Electronic Technology

Visual cryptography is a kind of image-based secret sharing scheme to share secret image based on the human visual system (HVS). For instance, a (k, n)-visual cryptography scheme (VCS) encrypts a secret image into n shares and distributes them to different participants, the secret image can be recovered by at least k shares. However, most of the existing VCSs are designed for binary images with limited flexibility and scalability. In this paper, a scalable ideal progressive visual cryptography scheme (PVCS) is proposed by scalable basis matrices and random Gaussian noise, which can process non-binarized images directly without pixel expansion. Our proposed basis matrix expansion method greatly improves the flexibility of the scheme and thus the efficiency is improved. In addition, since the visual effect of the VCS is standardized by the HVS and lacks an accurate quantitative index, we measure our scheme by using the peak signal-to-noise ratio (PSNR) and the structural similarity (SSIM), we also propose a method to derive the noise volume according to SSIM. Furthermore, sufficient experiments show that the proposed scheme is visually efficient and superior.

CCS CONCEPTS

• Security and privacy → Cryptography → Information-theoretic techniques

Additional Keywords and Phrases: Progressive visual cryptography, Image secret sharing, Ideal visual secret sharing

1 INTRODUCTION

As the developing of the Internet and smartphones, digital multimedia data is becoming more and more present in people's lives. Protecting digital multimedia data, such as digital images and so on, has become a focus issue. There are many schemes for image encryption, steganography [1] - [2] and cryptographic algorithms [3], but these schemes cannot achieve secret sharing. As one of the most famous image encryption schemes, the visual cryptography scheme (VCS) provides an interesting way to share secret images. Specifically, a (k, n)-VCS encrypts a secret image into n shares and distributes it to n participants. k or more participants were able to recover the secret image by stacking their shares, while less than k participants obtained no information about the secret image. A major advantage of VCS is that it does not require cryptographic knowledge for recovery, so it does not require complex computational effort, only the human vis-

* Corresponding author.
E-mail addresses: wjing@guet.edu.cn

ual system (HVS) is required.

However, there are some drawbacks of traditional VCS. In some scenarios, such as real-time systems or systems with limited network bandwidth, the pixel expansion of traditional VCS inevitably increases storage redundancy. In addition, most of the VCS can only be applied to binary images. In fact, binary images contain less information and are rarely used in daily life. Thus, to improve the performance of VCS, many schemes have been proposed. For color images, Kashyap et al. [4] presented a color VCS which used color decomposition and multilayer halftones technique to construct shares. To avoid the pixel expansion, Purushothaman et al. [5] proposed a VCS based on XOR-operation for General Access Structures, which has a perfect recovery effect and avoids pixel expansion. Shyu et al. [6] designed a (k, n)-VCS based on visual cryptography of random grids (VCRG), which does not require any extra pixel expansion and is suitable for color images.

Although many ideal VCSs that can handle non-binarized images have been proposed, they are inefficient and limited in flexibility. In this paper, we propose an ideal PVCS with strong scalability. Meanwhile, it can be efficiently applied to color images. Our scheme consists of two processes: encryption and recovery. The encryption process uses scalable basis matrices and random Gaussian noise to encrypt the secret image into several shadows. In the recovery process, the secret image can be recovered by modulo addition operation of shadows. With the increasing of shadow number, the visual effect of the recovered image becomes better and better. The contributions of this paper can be summarized as follows:

• We propose the scalable basis matrix PVCS, which makes the VCS more flexible.

• We use the SSIM as the basis for calculating Gaussian noise and quantifying the noise and recovery threshold.

• The effect of the recovered image was progressively improved with the increasing of shadow number, and the scheme can also be directly extended to color images.

2 RELATED WORK

The concept of secret sharing was proposed by Shamir [7] in 1979, specifically, the secret is put into the constant term of the (k-1)-degree polynomial to generate n shares, and the Lagrange interpolation method was used to reconstruct the secret with at least k shares. Since then, many studies have been devoted to improving the performance of the secret sharing scheme [8]. Based on the secret sharing scheme, Naor and Shamir [9] firstly proposed a VCS for sharing the secret binary image. However, the performance of this scheme is normal and has great potential to be improved. For example, it is only suitable for binary images, has pixel expansion, and the quality of the recovered image is poor. Nevertheless, as a completely new method of image encryption, visual cryptography has attracted much attention, and many excellent schemes have been proposed [10] – [12].

For color images, many existing schemes take a similar approach: considering each of the RGB components separately. Kirti et al. [13] proposed a (2, 3)-threshold by placing RGB components into different shares to encode the color image. Luo et al. [14] embedded R, G, and B three-channel values of color images into the (k, n)-threshold structure and proposed the concept of the color transfer visual cryptography. However, their scheme requires a key for encoding and decoding. To solve this flaw, Yang et al. [15] proposed a (k, n)-color transfer visual cryptography without a key, which improved the security and achieved better visual quality.

Meanwhile, some ideal VCSs have been proposed. Ito et al. [16] firstly proposed a scheme without pixel expansion. Kafri et al. [17] firstly proposed a VCS based on random grid (RG). After that, many schemes were

designed based on RG. Liu et al. [18] proposed a (k, n)-threshold scheme based on RG, which has perfect visual quality without pixel expansion, and is also suitable for grayscale or color images.

Additionally, scholars have also put their sights on new VCS, many new schemes, such as extended visual cryptography scheme (EVCS), authentication visual cryptography scheme (AVCS), and progressive visual cryptography scheme (PVCS) have been proposed. The shadows in traditional VCS are noise-like without any information that may arouse adversaries' suspicion. To address this issue, Ateniese et al. [19] embedded cover image into shares to make the shares meaningful and called this scheme EVCS. Liu and Wu [20] proposed (3, 3) and (2, 2)-EVCSs, which realized the threshold access structure. Liu et al. [21] proposed an EVCS using bit-plane compression and Lagrange interpolation formula, which realized that both the secret image and the cover image can be reconstructed losslessly. Since the shadows are distributed to different participants, there may be an adversary who has fake shares. Therefore, it is necessary to add an authentication function to VCS. In the process of reconstruction, if a fake share is detected, the reconstruction process will be terminated immediately. Liu et al. [22] innovatively introduced the turtle shell (TS) reference matrix into VCS to achieve authentication. To solve the shortcomings of the previous schemes that require an authority agency, Yan et al. [23] designed a (k, n)-AVCS based on polynomial. This scheme achieves authority agency participatory authentication and authority agency non-participatory authentication. There is a scheme called PVCS in which the quality of the recovered image progressively upgrades with the increasing of the stacked shadows number. Shivani and Agarwal [24] presented a novel PVCS to generate meaningful shadows, achieving satisfactory recovery results without pixel expansion. Subsequently, Shivani et al. [25] proposed a verifiable PVCS that embedded additional authentication information in each shadow.

3 PRELIMINARY KNOWLEDGE

3.1 Peak signal-to-noise ratio (PSNR).

Peak signal-to-noise ratio (PSNR) is an objective measure for evaluating images and is often used in image compression and other fields to evaluate the quality of images. PSNR defines as:

$$PSNR = 10 \cdot log_{10}\left(\frac{{MAX_I}^2}{MSE}\right), \tag{1}$$

where MAX_I is the maximum pixel value of the image, MSE is the mean square error of two images.

3.2 Structural similarity (SSIM).

Structural similarity (SSIM) is another criterion used to evaluate the degree of similarity between two images. Given two images x and y, the SSIM between the two images can be calculated by this formula.

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{({\mu_x}^2 + {\mu_y}^2 + c_1)({\sigma_x}^2 + {\sigma_y}^2 + c_2)}, \tag{2}$$

where $\mu_x,\ \mu_y$ are the average of *x* and *y* respectively, $\sigma_x,\ \sigma_y$ are the variance of *x* and *y* respectively, σ_{xy} is the covariance of x and y, c_1 and c_2 are constants and $SSIM(x, y) \in [-1, 1]$.

3.3 Hadamard product

The Hadamard product operates on two matrices of the same dimension and produces another matrix, the calculation method is as follows. Suppose there are two matrices $\boldsymbol{A} = (a_{i,j})_{m\times n}$, $\boldsymbol{B} = (b_{i,j})_{m\times n}$, let $\boldsymbol{C} = \boldsymbol{A} \circ \boldsymbol{B} = (c_{i,j})_{m\times n}$, then we have $c_{i,j} = a_{i,j} \times b_{i,j}$, $i \le m,\ j \le n$.

4 PROPOSED SCALABLE IDEAL PROGRESSIVE VISUAL CRYPTOGRAPHY SCHEME

The proposed scalable ideal PVCS consists of three processes: shadows generating process, recovery process, and matrix expansion process.

4.1 Shadows generating

The shadow generation is shown in Figure 1. The steps in this process are as follows: First, we generate the basis matrix set and Gaussian noise matrix set, and then the shadow is generated according to Eq. (3).

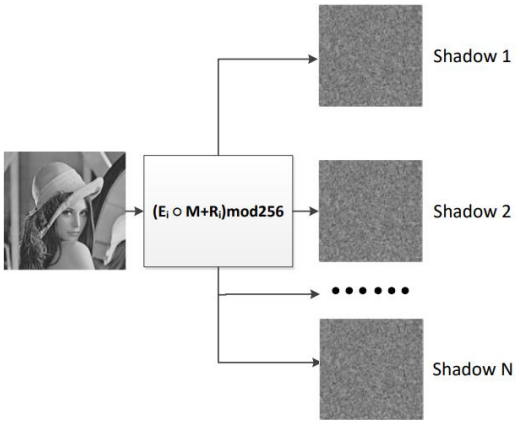


Figure 1: Shadows generating process

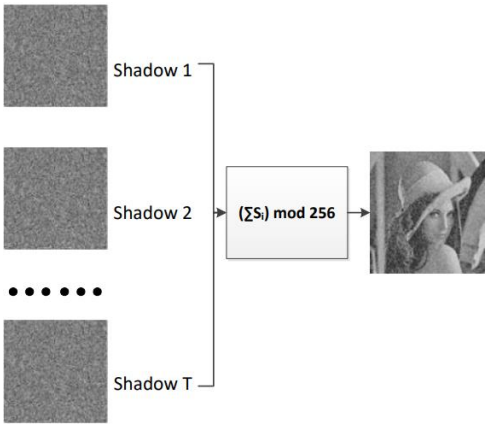


Figure 2: recovering process

The basis matrix set has the following requirements: the basis matrix is 0/1 matrix which has the same dimension as the grayscale matrix corresponding to the secret image, the sum of all basis matrices is a matrix where all elements are 1, the positions of 1 in the basis matrix do not overlap, and the proportion of 1 in each basis matrix is roughly the same as $1/N$, which ensures that each shadow carries substantially the same amount of information. For this, a basis matrix set generation algorithm is presented, as shown in Algorithm1. The algorithm takes the number of shadows and the size of the secret image as input and outputs the basis matrix set through a matrix $\boldsymbol{A}$ whose elements obey a uniform distribution.

ALGORITHM 1: Generate basis matrix set

INPUT: Number of shadows N; Size of secret image $M \times L$.

OUTPUT: A third-order tensor with dimensions of $N \times M \times L$: $\boldsymbol{E} = (e_{l,m,n})_{N\times M\times L}$.

$\boldsymbol{E}$ is initialized as a zero tensor, $k \leftarrow 0$
generate matrix $\boldsymbol{A} = (a_{i,j})_{M\times L}$, where $a_{i,j} \sim U(0,1)$
while $k \neq N$ **do**
  for i from 0 to $M-1$ **do**
    for j from 0 to $L-1$ **do**
      if $(\frac{k}{N} \leq a_{i,j} < \frac{k+1}{N}$ and $0 \leq k \leq N-2)$ or $(\frac{k}{N} \leq a_{i,j} \leq \frac{k+1}{N}$ and $k = N-1)$ **then**
        $e_{k,i,j} = 1$
      end if

9: **end for**
10: **end for**
11: $k \leftarrow k + 1$
12: **end while**
13: **return** $\boldsymbol{E}$

When generating the Gaussian noise matrix set, we need to set the parameters of the Gaussian distribution. In our scheme, we set $\mu = 0$ and derive σ from Eq. (2). The details of this method will be explained in Chapter 5. Here we use σ to represent the parameter. After setting the parameters, we generate N noise matrices of dimension $M \times L$, where the matrix elements obey Gaussian distribution. The set of noise matrices is expressed as $\boldsymbol{R} = \left(r_{l,m,n}\right)_{N\times M\times L}$, where $r_{l,m,n} \sim N(0, \sigma)$.

The formula for generating shadows is as follows.

$$\boldsymbol{S_i} = (\boldsymbol{E_i} \circ \boldsymbol{M} + \boldsymbol{R_i}) \ mod\ 256 \qquad 0 \le i \le N-1\,, \tag{3}$$

where $\boldsymbol{S_i}$ is the shadow matrix, $\boldsymbol{E_i} = (e_{l,m,n})_{M\times L}$ is the basis matrix, $\boldsymbol{M}$ is the grayscale matrix of the secret image, and $\boldsymbol{R_i} = (r_{l,m,n})_{M\times L}$ is the Gaussian noise matrix. After encryption, we obtain the set of shadow matrices $\boldsymbol{S} = \{\boldsymbol{S_i} \mid i \le N-1\}$, then we transform shadow matrices into shadows and distribute them to different participants.

4.2 Recovery

The recovery process is shown in Figure 2. $\boldsymbol{S_i}$ is a shadow matrix, and T is the number of collected shadows. We define a threshold t, The recovering process can be succeeded iff $T > t$. The recovered image matrix $\boldsymbol{M'}$ is calculated as follows:

$$\boldsymbol{M'} = \left(\sum \boldsymbol{S_{i'}}\right) \ mod\ 256 \qquad 0 \le i' \le T-1 \tag{4}$$

where $\boldsymbol{S_{i'}} \subseteq \boldsymbol{S}$ is a collected shadow matrix. There is a principle in VCS that the restricted noise may not significantly impact human recognition of the image. So, the simple modulo operation on the sum of shadows can recover the secret image.

4.3 Basis matrix expansion

When the dimensions of the shadows change, the original basis matrix set cannot be matched. Therefore, we propose a basis matrix expansion method to scale the basis matrix. This method will improve efficiency in most cases.

The basis matrix set has three dimensions, N represents the number of basis matrices, that is, the number of shadows, M and L represent the length and width of the basis matrix, respectively. The algorithm of updating the number of shadows is shown in Algorithm 2, it takes original basis matrices and changed number as input. For $P > 0$, the algorithm randomly generates matrix $\boldsymbol{B}$ whose elements obey a uniform distribution and generates matrix $\boldsymbol{C}$ and $\overline{\boldsymbol{C}}$ based on the matrix $\boldsymbol{B}$. Next, we use the method of Algorithm 1 to generate P matrices. Finally, based on these P matrices, matrix $\boldsymbol{C}$, matrix $\overline{\boldsymbol{C}}$, and the original basis matrices, the algorithm outputs the changed basis matrices with dimension $(N+P) \times M \times L$. For $P < 0$ we directly add the last m matrices from the original basis matrices to the first m basis matrices obtaining the changed basis matrices with dimension $(N+P) \times M \times L$. Furthermore, the other two dimensions of the basis matrices can be increased using the method of Algorithm1, and we can directly delete the rows or columns when decreasing the other two dimensions.

ALGORITHM 2: Update the number of shadows

INPUT: Original basis matrix set $\boldsymbol{E} = (e_{l,m,n})_{N\times M\times L}$; Number of changed shadows P.

OUTPUT: The set of changed basis matrices.

if $P > 0$ **then**
  $k \leftarrow 0$
  generate matrix $\boldsymbol{B} = (b_{i,j})_{M\times L}$, where $b_{i,j}$~$U[\frac{N}{N+P}, 1]$; $\boldsymbol{C} = (c_{i,j})_{M\times L}$ and $\overline{\boldsymbol{C}} = (\bar{c}_{i,j})_{M\times L}$
  generate third-order tensor $\boldsymbol{E}' = (e'_{l,m,p})_{P\times M\times L}$ where $e'_{l,m,p} = 0$
  set the threshold $p = \frac{N}{N+m} \times \frac{m}{N+m} + \frac{N}{N+m}$
  for i from 0 to $M - 1$ **do**
    for j from 0 to $L - 1$ **do**
      if $a_{i,j} > p$ **then**
        set $c_{ij} = 0$
      else
        set $c_{ij} = 1$
      end if
    end for
  end for
  $\boldsymbol{E_i} \leftarrow \boldsymbol{C} \circ \boldsymbol{E_i}$ $(0 \le i \le N - 1)$
  inverse matrix $\boldsymbol{C}$ obtaining matrix $\overline{\boldsymbol{C}}$
  while $k \neq P$ **do**
    for i from 0 to $M - 1$ **do**
      for j from 0 to $L - 1$ **do**
        if ($\frac{N+k}{N+P} \le b_{i,j} < \frac{N+k+1}{N+P}$ and $0 \le k \le P-2$) or ($\frac{N+k}{N+P} \le b_{i,j} \le \frac{N+k+1}{N+P}$ and $k = P - 1$) **then**
          $e'_{k,i,j} = 1$
        end if
      end for
    end for
  end while
  $\boldsymbol{E'_i} \leftarrow \overline{\boldsymbol{C}} \circ \boldsymbol{E'_i}$ $(0 \le i \le P - 1)$
  $\boldsymbol{E} \leftarrow \boldsymbol{E}' \cup \boldsymbol{E}$
  return $\boldsymbol{E}$
end if
else if $P<0$ **then**
  Intercept the set $\{\boldsymbol{E_{N+P}}, \boldsymbol{E_{N+P+1}}, \dots\dots, \boldsymbol{E_{N-1}}\}$ from $\boldsymbol{E}$ and names them as $\boldsymbol{NE_i}(0 \le i \le m - 1)$.
  $\boldsymbol{E_i} \leftarrow \boldsymbol{NE_i} + \boldsymbol{E_i}$ $(0 \le i \le m - 1)$
  return $\boldsymbol{E}$
end if

The matrix expansion method can also be applied to the noise matrix. The noise matrix expansion is simpler

than the basis matrix expansion, because the noise matrix only requires the matrix elements to obey the Gaussian distribution. When the dimension increases, random numbers obeying Gaussian distribution are generated and added to the three dimensions. The dimension of noise matrix decrease only requires the removal of matrix elements in the three dimensions.

5 DERIVATION OF GAUSSIAN DISTRIBUTION PARAMETER

We use PSNR and SSIM to measure the visual effect of the recovered images and use these two indicators for calculating the Gaussian noise. In this chapter, we will derive the parameter σ of the Gaussian distribution based on the SSIM, the same principle is also applied to the derivation based on the PSNR.

We define x as the secret image and y as the recovered image, and the distribution function of y as follows:

$$y = \begin{cases} x + r, & with\ probability\ p = \dfrac{T}{N} \\ r, & with\ probability\ p = \dfrac{N-T}{N} \end{cases} \tag{5}$$

where T represents the number of collected shadows, N represents the number of initially generated shadows, r represents the added Gaussian noise, where $r \sim N(0, T\sigma^2)$. Obviously, x and r are independent. According to Eq. (2), we get

$$\mu_x = \bar{x}, \tag{6}$$

$$\mu_y = \frac{T}{N}\bar{x} + \bar{r}, \tag{7}$$

$${\sigma_x}^2 = D_x, \tag{8}$$

$${\sigma_y}^2 = \frac{NT-T^2}{N^2}\bar{x}^2 + \frac{T}{N}D_x + D_r, \tag{9}$$

$${\sigma_y}^2 = \frac{NT-T^2}{N^2}\bar{x}^2 + \frac{T}{N}D_x + D_r, \tag{10}$$

$$\sigma_{xy} = \frac{T}{N}D_x. \tag{11}$$

Meanwhile $c_1 = 6.5025$, $c_2 = 58.5225$. Thus,

$$SSIM = \frac{(2\bar{x}\cdot\frac{T}{N}\bar{x} + 6.5025)(\frac{2T}{N}D_x + 58.5225)}{(\bar{x}^2 + \frac{T^2}{N^2}\bar{x}^2 + 6.5025)(D_x + \frac{NT-T^2}{N^2}\bar{x}^2 + \frac{T}{N}D_x + D_r + 58.5225)}. \tag{12}$$

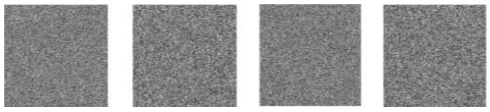
Take image Lena as an example, $\bar{x}$ = 124.0614, D_x = 2290.7816. The information of the secret image can be basically recognized while $SSIM$>0.2. We can get σ = 9.0675 while N = 50, T = 25. Since there will be some difference between the human eye and the actual, in the subsequent experiments, we set σ = 6.

6 PERFORMANCE EVALUATION

The experiments use four images commonly used in the literature as shown in Figure 3. Airplane and Lena have dimensions 512 × 512, Baboon and Sailboat have dimensions 400 × 400. We note that our proposed scheme can be extended to color images by considering each channel separately.

(a).Airplane (b).Baboon (c).Lena (d).Sailboat

Figure 3: The secret images

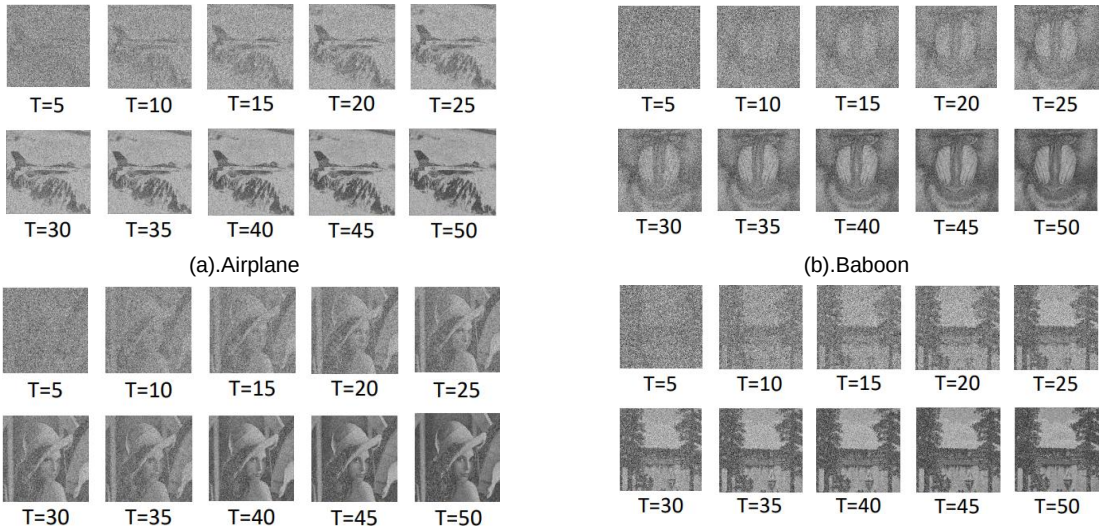


(a).Airplane (b).Baboon (c).Lena (d).Sailboat

Figure 4: The shadows

The shadows are shown in Figure 4. Although four secret images are different, they are all similarly meaningless after encryption, and we cannot obtain any information of the secret image even to an infinitely powerful computer. Therefore, encryption can effectively guarantee the security of the secret image. Besides, the size of the shadow is the same as the secret image, so this scheme is ideal without pixel expansion.

The recovered images are shown in Figure 5. T represents the number of shadows used to recover. Significantly, as T increases, the recovered image becomes clearer, we can get more information from it.

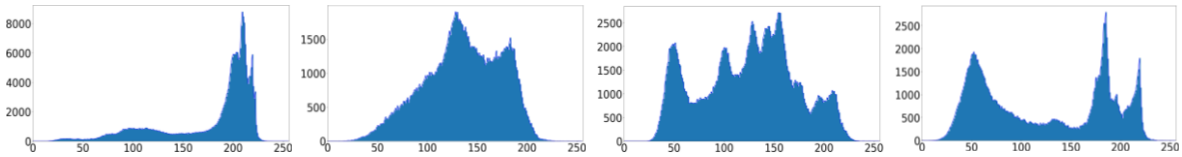


(a).Airplane (b).Baboon

(c).Lena (d).Sailboat

Figure 5: The recovered images

The histogram of the secret image and the recovered images are shown in Figure 6 and Figure 7 respectively. As we can see from Figure 6, the histograms of each four secret images are different. In Figure 7, $T = 1$ represents the histogram of the shadow. We can see that the histograms of all four shadows are similar, most of the pixel values are distributed in the 0 and 255, also proving the security of the secret image. We can also see that as T increases, the pixel distribution of the recovered image is getting closer to the secret image.

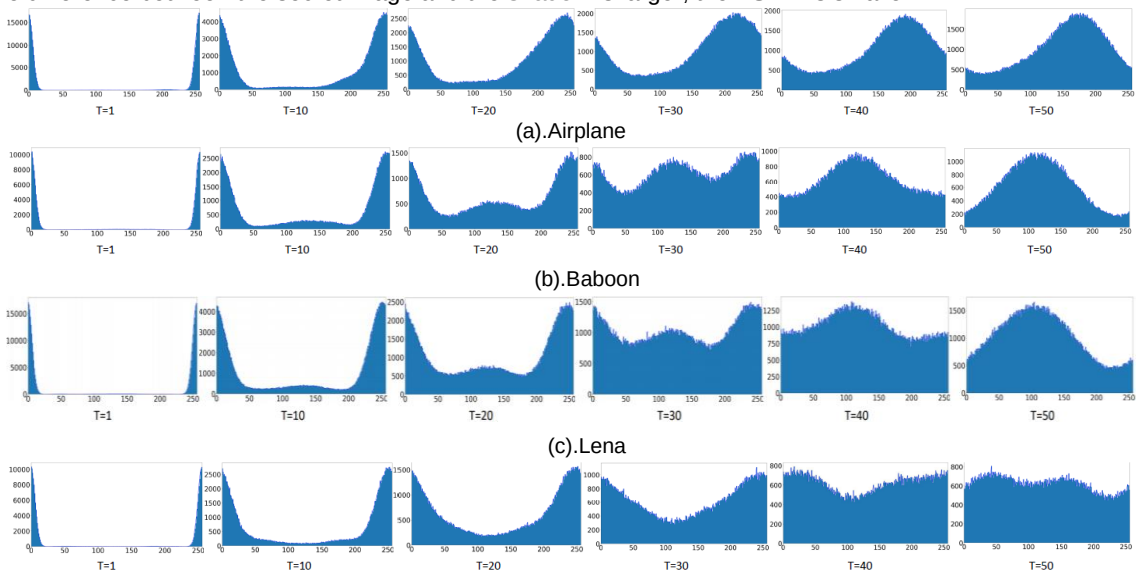


(a).Airplane (b).Baboon (c).Lena (d).Sailboat

Figure 6: Histogram of the secret image

The PSNR of the shadow and the secret image is shown in Figure 8. The reference line represents a boundary that makes HVS unable to recognize the shadow. As σ increases, the *PSNR* rises means that the visual effect of the shadow has become better. The more noise added, the pixel distribution of the shadow will be closer to the pixel distribution of the secret image, since most of the pixel values of the image before adding

Gaussian noise is zero. It can be seen from the comparison of different lines, as N increases, *PSNR* becomes smaller, this is because the more shadows are generated, the less information each shadow carries. Therefore, the difference between the secret image and the shadow is larger, the *PSNR* is smaller.



(a).Airplane

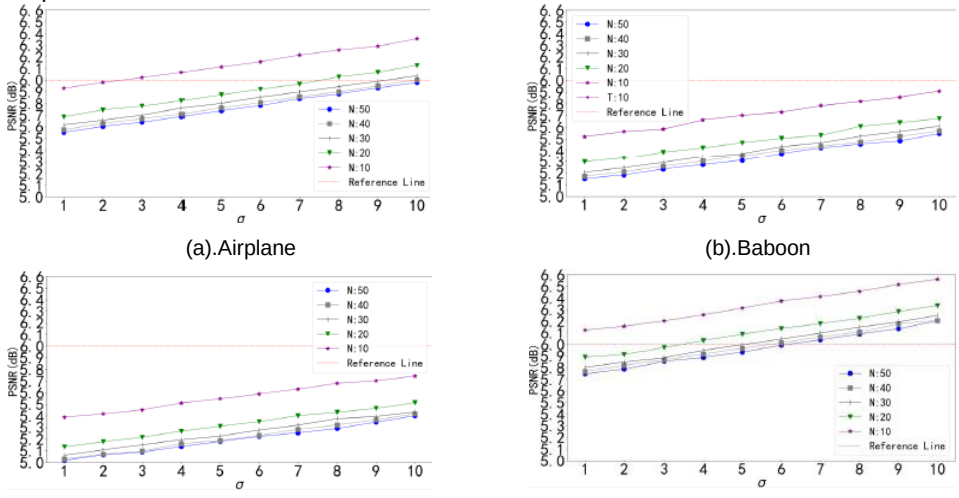
(b).Baboon

(c).Lena

(d).Sailboat

Figure 7: Histogram of the recovered image

The SSIM of the shadow and the secret image is shown in Figure 9. It can be seen that Figure 9 does not show an increasing trend like Figure 8, this is because SSIM captures the structural information of the image in addition to the pixel values, which also reflects that SSIM is more robust than PSNR.



(a).Airplane

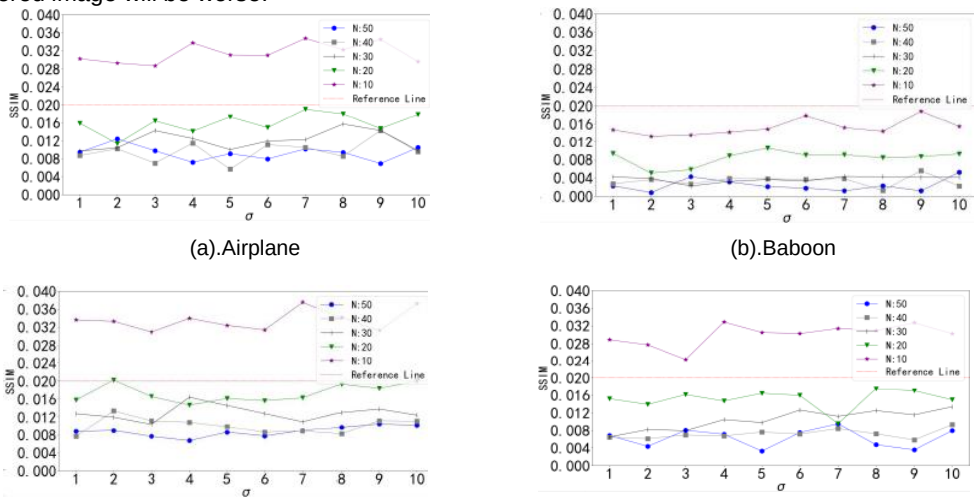
(b).Baboon

(c).Lena

(d).Sailboat

Figure 8: PSNR of the shadow and the secret image

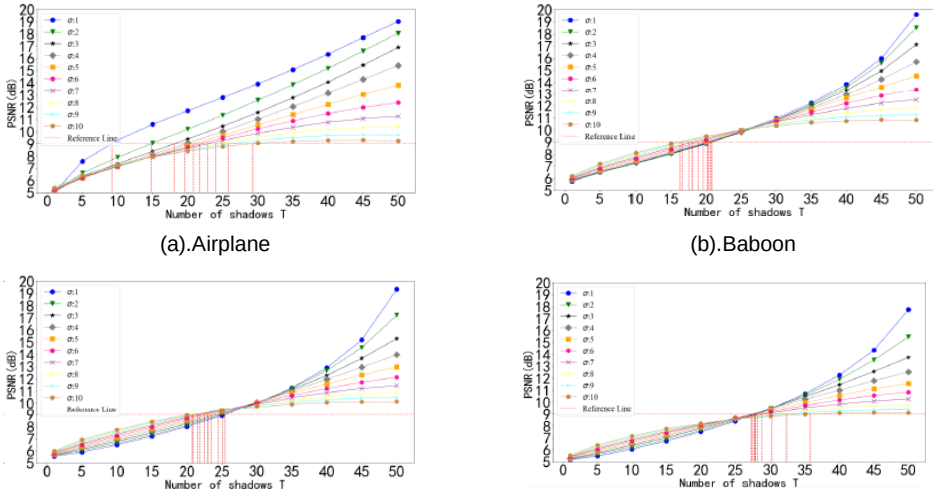
The PSNR of the recovered image and the secret image is shown in Figure 10. The reference line represents the boundary that the recovered image can be identified by HVS. The *PSNR* increases with the growth of T, which indicates that the visual effect of the recovered image becomes better. Comparing different lines, we can see that as σ increases, the PSNR will decrease, indicating that the more noise is added, the visual effect of the recovered image will be worse.



(a).Airplane (b).Baboon

(c).Lena (d).Sailboat

Figure 9: SSIM of the shadow and the secret image

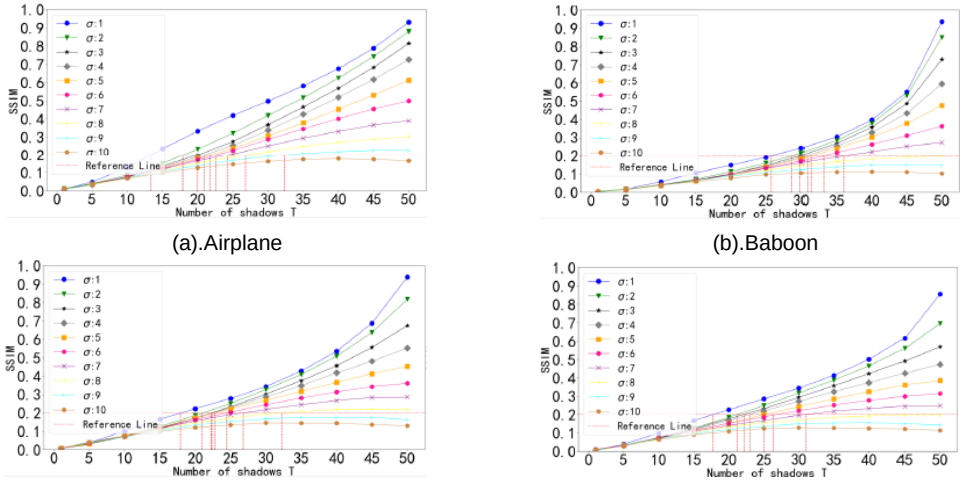


(a).Airplane (b).Baboon

(c).Lena (d).Sailboat

Figure 10: PSNR of the recovered image and the secret image

The SSIM of the recovered image and the secret image is shown in Figure 11. Same as Figure 10, except that the evaluation indicator has been replaced by SSIM, we can also draw the same conclusions as Figure 10.



(a).Airplane (b).Baboon

(c).Lena (d).Sailboat

Figure 11: SSIM of the recovered image and the secret image

7 CONCLUSIONS

In this paper, we propose a scalable ideal PVCS without pixel expansion, it can process non-binarized images and can be directly extended to color images. Our proposed matrix expansion method does not require regenerating the basis matrix to make the scheme more flexible, which can improve operational efficiency. In addition, we derive Gaussian noise based on the SSIM, and experiments have also verified our correctness. Our scheme is simple, flexible, and scalable and can be applied to images of different dimensions to share images securely and efficiently.

ACKNOWLEDGMENTS

This work was supported by the National Science Foundation of China (No.61802083, 61862011), the Natural Science Foundation of Guangxi (2018GXNSFBA281164, 2018GXNSFAA138116).

REFERENCE

[1] Linqiang Ouyang, Jin H. Park, and Harbhinder Kaur, "Performance of Efficient Steganographic Methods for Image and Text," Journal of Advances in Information Technology, 7: 29-33, 2016.

[2] Meenu Kumari, A. Khare, and Pallavi Khare, "JPEG Compression Steganography & Cryptography Using Image-Adaptation Technique," Journal of Advances in Information Technology, 1:141-145, 2010.

[3] Giao N. Pham, Son T. Ngo, Anh N. Bui, Ban Q. Tran, Dinh V. Tran, and Suk-Hwan Lee, "Edges of Interpolating Tetrahedron Based Encryption Algorithm for 3D Printing Model," Journal of Advances in Information Technology, 11:84-90, 2020.

[4] P. Kashyap and A. Renuka. Visual cryptography for color images using multilevel thresholding. In 2019 Third International Conference on Inventive Systems and Control (ICISC), 567–572, 2019.

[5] V. Purushothaman and S. Sreedhar. An improved secret sharing using xor-based visual cryptography. In 2016 Online International Conference on Green Engineering and Technologies (IC-GET), 1–4, 2016.

[6] S. J. Shyu. Visual cryptograms of random grids for general access structures. IEEE Transactions on Circuits and Systems for Video Technology, 23:414–424, 2013.

[7] Adi Shamir. How to share a secret. Commun. ACM, 22:612–613, 1979.

[8] Hui-Chuan Lu, "The Average Information Ratio of Secret-Sharing Schemes for Access Structures Based on Coalescence of Graphs," Journal of Advances in Information Technology, 6:124-129, 2015.

[9] Moni Naor and Adi Shamir. Visual cryptography. In Alfredo De Santis, editor, Advances in Cryptology — EUROCRYPT'94, 1–12, Berlin,

Heidelberg, 1995.

[10] Zhen Wu, Yining Liu, Dong Wang, and Ching-Nung Yang. An efficient essential secret image sharing scheme using derivative polynomial. Symmetry, 11:69-81, 2019.

[11] C. Yang and Y. Yang. On the analysis and design of visual cryptography with error correcting capability. IEEE Transactions on Circuits and Systems for Video Technology, 1–1, 2020.

[12] S. Chougule and P. J. Sapna. Randomized visual cryptography to enhance security. In 2018 IEEE International Conference on Recent Trends in Electronics, Information Communication Technology (RTEICT), 490–494, 2018.

[13] Kirti Dhiman and Singara Singh Kasana. Extended visual cryptography techniques for true color images. Computers & Electrical Engineering, 70:647 – 658, 2018.

[14] Hao Luo, Hua Chen, Yongheng Shang, Zhenfei Zhao, and Yanhua Zhang. Color transfer in visual cryptography. Measurement, 51:81 – 90, 2014.

[15] Ching-Nung Yang, Tzu-Chia Tung, Fu-Heng Wu, and Zhili Zhou. Color transfer visual cryptography with perfect security. Measurement, 95:480 – 493, 2017.

[16] Ryo Ito, Hidenori Kuwakado, and Hatuskazu Tanaka. Image size invariant visual cryptography. IEICE Transactions on Fundamentals of Electronics Communications & Computer Sciences, 82:2172– 2177, 1999.

[17] O Kafri and E Keren. Encryption of pictures and shapes by random grids. Optics Letters, 12(6):377-379, 1987.

[18] Liu X. Yan, X. and CN Yang. An enhanced threshold visual secret sharing based on random grids. Real-Time Image Proc, 14:61 – 73, 2018.

[19] Giuseppe Ateniese, Carlo Blundo, Alfredo De Santis, and Douglas R. Stinson. Extended capabilities for visual cryptography. Theor. Comput. Sci., 250:143–161, 2001.

[20] F. Liu and C. Wu. Embedded extended visual cryptography schemes. IEEE Transactions on Information Forensics and Security, 6:307–322, 2011.

[21] Yining Liu, Qi Zhong, Jian Shen, and Chin-Chen Chang. A novel image protection scheme using bit-plane compression and secret sharing. Journal of the Chinese Institute of Engineers, 40:161–169, 2017.

[22] Chang CC Liu, Y. A turtle shell-based visual secret sharing scheme with reversibility and authentication. Multimed Tools Appl, 77:1–16, 2018.

[23] X. Yan, Y. Lu, C. n. Yang, X. Zhang, and S. Wang. A common method of share authentication in image secret sharing. IEEE Transactions on Circuits and Systems for Video Technology, 1–1, 2020.

[24] Shivendra Shivani and Suneeta Agarwal. Progressive visual cryptography with unexpanded meaningful shares. ACM Trans. Multimedia Comput. Commun. Appl., 12:1-24, 2016.

[25] Shivendra Shivani and Suneeta Agarwal. Vpvc: Verifiable progressive visual cryptography. Pattern Anal. Appl., 21:139–166, 2018