Hindawi
Advances in Multimedia
Volume 2021, Article ID 3287774, 7 pages
https://doi.org/10.1155/2021/3287774

*Research Article*

# A Novel Raster Map Exchange Scheme Based on Visual Cryptography

**Lijing Ren**

*Shijiazhuang Tiedao University, Shijiazhuang 050043, China*

Correspondence should be addressed to Lijing Ren; ren.lijing@foxmail.com

Received 24 May 2021; Revised 4 July 2021; Accepted 22 July 2021; Published 29 July 2021

Academic Editor: Rajesh Kaluri



Raster map is an image that has been discretized in space and brightness, and it is an important carrier of geospatial data. With the rapid development of Internet and big data technologies, preserving the privacy of raster map has become an urgent task. To solve these issues, we propose a novel extended visual cryptography scheme to securely store a raster map into other two meaningful halftone maps in the paper. The scheme avoids the random-looking shares of visual cryptography schemes which are vulnerable and hard to manage. We first apply the halftone and color decomposition methods to transform a color secret map into halftone images. After that, we encode the secret map block by block to avoid pixel expansion. At last, by optimizing the selection of encrypted blocks, we achieve a high-quality secret recovery from generated multiple equal-sized shares. The technique used is to employ a versatile and secure raster map exchange. Experimental results show that, compared with previous work, the proposed scheme significantly improves the performance of recovered raster maps.

## 1. Introduction

A raster map is an image generated from existing paper or film topographic maps. It plays an important role in geographic data, GIS (Geographic Information System), and robot navigation fields. The past decade has seen the rapid development of map service in many fields. As an indispensable carrier of national infrastructure construction and geographic information science, raster maps have become a strategic resource in the national economy and national defense construction. With the rapid development of Internet and big data, it is more convenient now to acquire, replicate, and disseminate raster maps. However, this process increases the risk of data leaks and arises prominently the security issue of raster maps. The application of raster maps has suffered from leak, piracy, and copyright infringement [1].

Much work has been reported recently in these fields of raster map protection including (i) data encryption [2], (ii) digital watermark [3, 4], and (iii) visual cryptography (VC) [5, 6]. When data is encrypted, the raster map is converted into ciphertext as normal text. This method can protect raster maps with curated cryptography. However, once disclosing the encryption key, illegal users could compromise and grab encrypted information. Digital watermarking embeds copyright information into a raster map. Even if a map is abused, the copyright information of a raster map can be identified by the digital watermark. The expansion of information security poses new challenges to traditional cryptography, which requires a lot of effort to store, manage, and distribute keys or watermarks.

The VC is a secret-sharing scheme to encrypt an image into two or more transparencies. The merit of VC lies in the fact that the Human Visual System (HVS) can recover the shared secret just by superimposing multiple shared images. Thus, users can print out shares onto transparencies and reconstruct a secret map even without using any digital device.

Noise shares in VC will cause the suspicion that something is hidden behind them. To conceal the existence of the secret message and increase security, the Extended Visual Cryptography Scheme (EVCS) [7] generates meaningful image shares instead of the random bunch of pixels. However, quite a few issues of EVCS prevent it from widespread applications.

Traditional EVCS suffers from the same problems of (i) *pixel expansion* and (ii) *contrast descent* as VCS. The *expanding* VCS maps a pixel into a block with $m$ subpixels. The *contrast* is the relative difference in a black pixel generated from a secret white pixel. EVCS cannot completely restore the original pixels of secret images. These drawbacks can lead to distortion of shared images, poor portability, and waste of storage space.

To address all the disadvantages listed above, we propose a novel extended visual secret-sharing scheme call F-EVCS (Fittest EVC Scheme) in this paper. This scheme avoids the vulnerability in the random-looking and distinctly different shares which most visual cryptography schemes use. It retains the advantage of traditional visual cryptography, including printable transparencies and computation-free decryption. Our key idea is encrypting a block of pixels as a single unit instead of pixel by pixel so that we can avoid pixel expansion. By optimizing the selection of encrypted blocks, the proposed scheme achieves a high-quality secret recovery from generated multiple equal-sized shares.

The rest of the paper is organized as follows. In Section 2, we first briefly review the existing EVCS. After that, we propose our method in Section 3. Section 4 would offer experimental results and comparisons with previous work. Finally, the conclusions will be presented in Section 5.

## 2. Related Work

Visual cryptography was originally invented and pioneered by Nair and Shamir in 1994. It combines the notions of perfect ciphers and secret sharing in cryptography with that of raster images [8]. From their inception, VCS and EVCS have been an emerging research area in the field of information security [9]. Sharing secrets with high-quality recovery is very achievable and improving on the resultant share size has also been a worthwhile research topic. Attempts to resolve this dilemma have resulted in the development of kinds of VCS and EVCS.

*2.1. Basic EVCS.* In extended visual cryptography, all shares are meaningful as they contain the cover images against the information of the original secret image. In [9], the halftone secret image is first hidden into two other camouflaged halftone images, and then the gray-level value of a pixel is adjusted to fit the pixel values of the secret image and two camouflaged images. After overlaying the two camouflaged halftone images, the secret halftone image can be revealed by using human eyes. In [10], an intelligent preprocessing of halftone images is applied to generate high-quality images from recovered image. Other schemes including EVCS can also benefit from the preprocessing approach. However, these schemes are aimed at gray-level images. It is an essential area of research to apply visual cryptography techniques to color images.

*2.2. Color VCS.* The schemes for processing binary secret images have been extended for processing gray-level and color secret images [11, 12], respectively. In these schemes, the halftoning technique is often used to produce binary images so that the traditional VCS scheme can be adopted. For color secret images, we have to decompose colors into primary colors before the application of halftoning technique.

*2.3. Perfect EVCS.* Perfect reconstruction using a computation-based decryption scheme is very critical in recovering secret information for security concerns. VCS can also be computation-based by disseminating share images combined with watermarking scheme instead of using transparencies [5, 13, 14]. The traditional cryptography-based encryption method cannot hide the secret image, while the watermark-based method fails to conceal the secret message. These methods violate the principle of visual cryptography that exploits human eyes to decrypt secret images.

*2.4. Block-Wise EVCS.* In addition to the pixel-wise operation, the block-wise operation was also widely used [15–18] the construction of new VCS. In the block-wise operation, a block in a shared image corresponds to an equal-sized block in the secret image. The share images are encrypted block by block instead of pixel by pixel in traditional VCS. By such methods, we can eliminate the pixel expansion of VC. However, these methods often have lower contrast due to processing multiple pixels at a time. Paper [16] proposed a novel VCS which improves the pixel expansion and contrast properties compared with many of the known results in the literature. By encrypting an image by pixel blocks, it eliminates pixel expansion.

The current various VCSs often solve shortcoming of VC at the expense of another characteristic and lack a comprehensive solution. As shown in Table 1, compared with the known results including *Basic EVCS*, *Color VCS*, *Perfect EVCS*, and *Block-wise EVCS* in literature, the proposed scheme makes use of the block-wise operation to avoid pixel expansion. The color decomposition and halftone methods are applied to encode gray-level and color raster maps in this paper. In addition, our scheme keeps the security of EVCS and is computation-free and printer-friendly.

## 3. Methods

In this section, we introduce a novel EVCS for color images with no pixel expansion. We make use of VC to partition a raster map into $n$ shares, which can be distributed for safety to corresponding parties. The secret raster map can then be recovered by superimposing share images when enough shares are released.

*3.1. Foundation of Visual Cryptography.* Visual cryptography is a new type of cryptographic scheme, which can decode concealed images without any cryptographic computation. In Naor and Shamir's original ($k$, $n$) (or $k$-out-of-$n$) scheme [6], they split up a secret black ($B$) and white ($W$) image into $n$ shares (known as sheets or shares) and distribute them to

Table 1: Feature comparisons among our proposal and previous schemes.

| Scheme | Size invariant | Quality improvement | Computation-free | Color |
|---|---|---|---|---|
| [9] | × | √ | √ | × |
| [10] | × | √ | √ | × |
| [5] | √ | √ | × | × |
| [13] | √ | √ | × | √ |
| [14] | √ | √ | × | √ |
| [15] | √ | × | √ | √ |
| [16] | √ | × | √ | × |
| [17] | √ | × | √ | √ |
| [18] | √ | × | √ | √ |
| *F-EVCS* | √ | √ | √ | √ |

each one of participants (known as shareholders). The image remains hidden if fewer than $k$ transparencies are stacked together, so the decryption is impossible unless superimposing $k$ or more transparencies together. The encryption problem is expressed as a $k$-out-of-$n$ secret-sharing problem. Each pixel appears within $n$ modified shares.

Visual cryptography is a threshold secret-sharing scheme. It makes use of the HVS to perform the pixel-wise OR logical operation on the superimposed pixels of the shares. This feature allows anyone to use the system without knowledge of cryptography and computation, which makes VCS surpass other cryptography schemes based on keys or watermarks. Thus, the proposed scheme also should be printer-friendly; that is, users can decrypt the secret raster maps without any digital devices.

In implementing visual cryptography schemes, it would be useful to conceal the existence of the secret message, and the shares given to participants in the scheme should not look like a random bunch of pixels [19]. To prevent the attention of the attackers, EVCS encodes the secret into meaningful share images, so this scheme is more suitable for the protection of raster maps.

Figure 1 shows the encryption and decryption procedure of a (2, 2)-EVCS for the black-and-white image. There are usually two participants, $A$ and $B$ in the EVCS, and each of them holds $\text{Share}_1$ and $\text{Share}_2$, respectively (two rows in the middle of Figure 1).

As Figure 1 shows, each secret pixel is expanded to four subpixels in EVCS. For each black or white pixel in the secret image, there are four possible combinations of black and white pixels of the two source images. For example, if the pixel is black in the secret map, black in $\text{Share}_1$ and white in $\text{Share}_2$, the share subpixels will be selected from the second column of Figure 1, that is, the [*B, W, B, B*] and [*W, B, W, B*] blocks. After superimposing the two rows, we get subpixels with four black pixels which corresponds to the secret black pixel.

The difference in the number of black subpixels can help us distinguish black and white pixels in the secret share maps. Note that if there are three black subpixels in the encrypted block, it would be treated by a black pixel, and if there are four black subpixels, it would be treated by a white pixel.

Although EVCS can transmit raster maps by distributing meaningful shares, it is at the expense of reducing *contrast*. EVCS encodes each secret pixel into subpixels as the VCS. The hidden image we encode has black pixels and white pixels. We represent the black pixel of the secret image by all four black subpixels and represent the white pixel with three black subpixels and one white subpixel. Thus, the *contrast* of (2, 2)-EVCS is 1/4. In the VCS, a recovered white pixel is comprised of 2 white and 2 black subpixels, while a black pixel is represented by 4 black subpixels in the recovered image. Thus, the *contrast* of (2, 2)-VCS is 1/2. The *contrast* is further reduced in EVCS.

*3.2. The Encoding Scheme for Gray-Level Raster Map.* In this section, we use a gray-level image to represent raster maps. In raster maps, the space and brightness of an image are discrete. We can treat a raster image as a matrix, where an element corresponds to a point in the image, and the corresponding value corresponds to the gray level of that point. The definition of a raster map is consistent with a gray-level image.

It is fundamental to understand how to handle black-and-white images. Thus, let us start with this method. Although our scheme operates on binary black-and-white images, it can be applied to gray-level images by using a halftoning algorithm to convert the gray-level image into a binary black-and-white image. This allows visual cryptography to encrypt natural and meaningful gray-level images, that is, raster maps.

To eliminate pixel expansion in the traditional EVCS model, we adopt the block-wise operation instead of the pixel-wise encryption. We call the block in the secret image a *secret block*, and the block in the shared image a *share block*. In the traditional pixel-wise operation, they encode secret images pixel by pixel, which expands into a block or maps onto a corresponding pixel. In the block-wise operation, we generate shares block by block, and a share block corresponds to an equal-sized secret block.

In a halftone image, there are not only secret blocks with different numbers of black and white pixels but also the same secret blocks with different arrangements. However, as Figure 1 shows, there are only two permutations, that is, [*B*, *B*, *B*, *B*] and [*B*, *B*, *W*, *B*] for the secret images.

To address limited combinations of pixel blocks, we choose an encryption block $b_e$ from the candidate block $b_i$ that minimizes the global error within a $2 \times 2$ block in (1). $b_m$ is the block to be encrypted in the secret map or share maps. For the secret image, the selection is similar, and the candidate blocks become [[*B, B, B, B*], [*B, B, B, W*]], which is same as the decryption block in Figure 1.

The encoding scheme for gray-level raster maps is shown in Algorithm 1. Our method first converts the secret image and two share images of halftone images. There are many halftone techniques available, where error-diffusion produces superior results, so we adopt it in this paper.

The encrypt_block function in Algorithm 1 selects the most suitable encryption block according to (1). We take the (2, 2)-EVCS as the underlying visual cryptography, so the

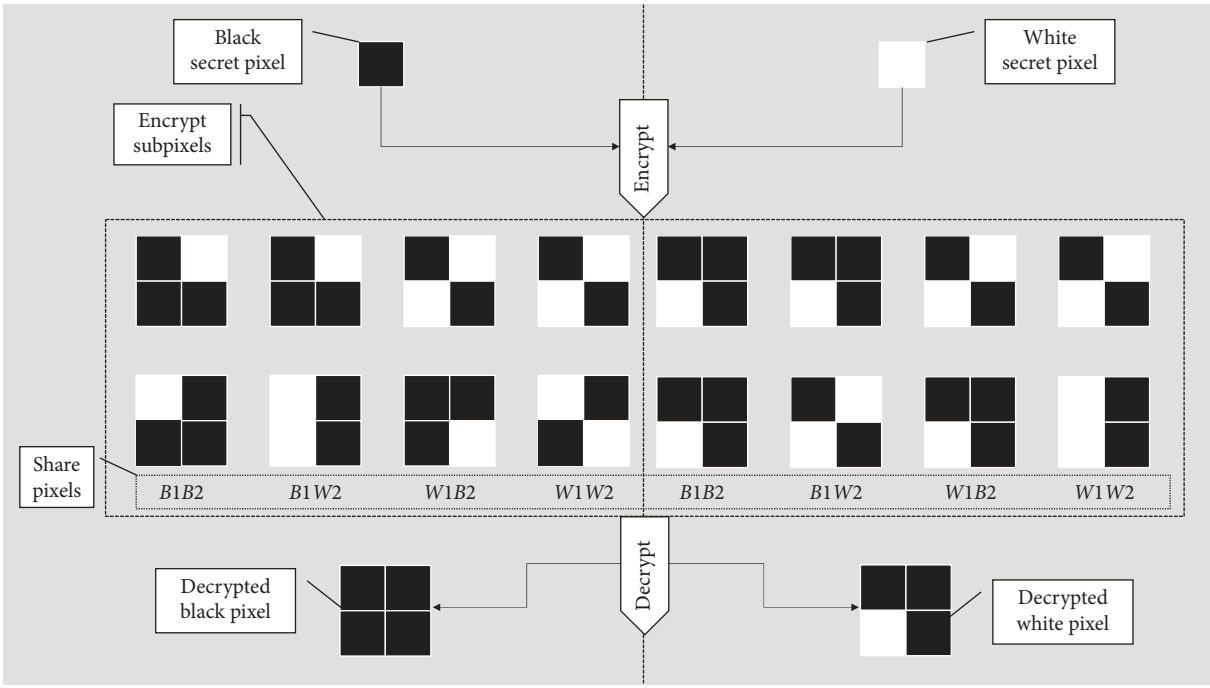



Figure 1: Illustration of a (2, 2)-EVCS for the black-and-white image. The left and right are the encryption and decryption procedure of a black and white secret pixel, respectively. The $B1W2$ denotes that the corresponding pixels in $\text{Share}_1$ and $\text{Share}_2$ are black and white, respectively. The meanings of other symbols are similar.

**Data**: A secret raster map, $I$, and two share raster maps, $I^{s1}$ and $I^{s2}$
**Result**: Two encrypted and meaningful raster maps $S_1$ and $S_2$ for participants, $A$ and $B$, respectively
$I_g \leftarrow$ the gray-level of the secret image $I$;
$I_g^{s1} \leftarrow$ the gray-level of the share image $I^{s1}$;
$I_g^{s2} \leftarrow$ the gray-level of the secret $I^{s2}$;
//**Convert all maps to halftone images**
**for each** $I$ in $\left\{I_g, I_g^{s1}, I_g^{s2}\right\}$ **do**
  $I_{bw} \leftarrow \text{halftone}(I)$;
**end**
//Encrypt all black-and-white images block by block
**for each** $I_{ij}$ in $I_{bw}, I_{bw}^{s1}, I_{bw}^{s2}$ **do**
  $I_{ij} \leftarrow$ non-overlapping blocks of $2 \times 2$ pixels;
**end**
//Select the fittest encrypt block according to secret and cover blocks
**for each** $I_{bw}$ in $\{I_{bw}, I_{bw}^{s1}, I_{bw}^{s2}\}$ **do**
  **for each** $B_{ij}$ in $I_{bw}$ **do**
    $B_{ij}^s \leftarrow \text{encrypt\_block}(B_{ij}), \quad s \in \{S_1, S_2\}$;
  **end**
**end**

Algorithm 1: The algorithm of encoding gray-level raster maps using EVCS.

size of the block is 4. Note other $(k, n)$ schemes can also benefit from the proposed approach if the corresponding $(k, n)$-EVCS is applied. There are four groups of candidate blocks in total, which we can choose randomly in the case of ensuring security.

$$b_e = \min \sum_{i=1}^{n} (b_m - b_i)^2,$$
$$b_i \in \begin{cases} [[B, W, B, B, ], [B, W, B, W]], & \text{for } S_1, \\ [[W, B, B, B], [W, B, W, B]], & \text{for } S_2. \end{cases} \quad (1)$$

Our scheme is also safe, since these candidate groups which are generated from the original $(k, n)$-EVCS satisfy the contrast and security criterion. Each encryption group in a shared image, regardless of its color, is selected from the corresponding candidate groups of a black or white secret pixel. Meaningful share images cannot reveal any information of the secret image individually.

*3.3. Color EVCS.* In this section, we propose a nonexpanding EVCS for color images based on the above gray-level scheme. Most of the methods developed so far work on black-and-white images only, while it is desired to apply visual cryptography techniques to color images including raster maps. The more intuitive and the richer the image information, the higher its application value.

We first decompose color images into monochrome gray-level images and then convert gray-level images into binary images using halftone technology, so the corresponding black-and-white encryption method proposed in the above section can be used to generate corresponding shares.

The two most used color models are RGB (red, green, and blue) and CMY (cyan, magenta, and yellow) [20]. In the RGB color model, which is also called the additive model, each color is produced using a mixture of three primary colors of light. Thus, computer systems generate color images using the RGB model, while most color printers use cyan, magenta, and yellow inks to compose printable colors. To construct a printer-friendly EVCS, we apply the CMY model which is called the subtractive model to represent a raster map. Based on the complementary relationship of RGB and CMY models, we can get CMY channels from RGB channels with the following transformation: $C = 255 - R$, $M = 255 - G$, $Y = 255 - B$. The following describes our invariant color EVCS:

(1) Convert the color image from the RGB model into the CMY model

(2) Apply the halftone transformation to each channel

(3) For each monochrome black-and-white, call the algorithm in Algorithm 1 to generate two meaningful share images

(4) Distribute shares to participants, $A$ and $B$. The final share is formed by combining $C_i$ share with $M_i$ share as well as $Y_i$, where $i \in (0, \ldots, 7)$

Most VCS and EVCS have the property of *perfect black*. The reconstructed image by the proposed scheme also is *perfect black* since stacked blocks associated with black pixels of the secret image are all-black. We can use black for representing important information and white as the background to reduce the side effect of contrast reduction in VCS.

## 4. Experimental Results

Although a lot of effort is being exerted on improving these weaknesses of VCS, the efficient and effective method has yet to be developed. Previous studies focused on the construction of new VCS and lack of application in specific fields. In this paper, we innovatively apply VCS to the privacy protection of raster images. To test the feasibility of the proposed method, we will first compare the performance between the proposed scheme and previous work in the classic images and then evaluate the effectiveness to encode a raster map.

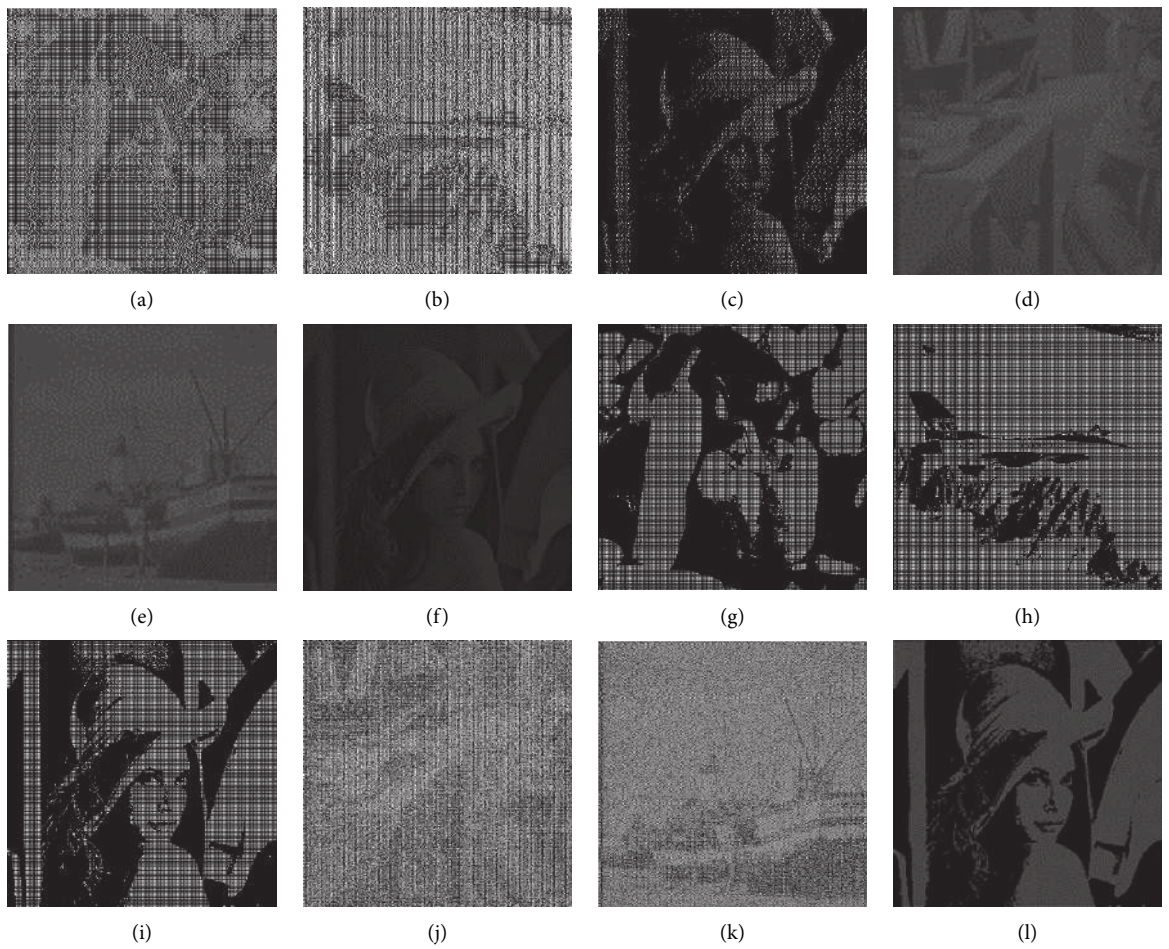
$$\mathrm{PSNR} = 10 \times \log_{10}\left(\frac{\mathrm{MAX}_I^2 \times m \times n}{\sum_{i=0}^{n-1}\sum_{j=0}^{m-1}\left(x(i,j) - y(i,j)\right)^2}\right). \quad (2)$$

An objective way to measure alteration between a secret image and the recovered image is to use PSNR (Peak Signal-to-Noise Ratio). Figure 2 gives the definition of PSNR. The larger the PSNR value, the better the clarity. The PSNR metric is appealed because it is easy to calculate and has clear physical meaning. We offer 1 to $\mathrm{MAX}_I$ for the black-and-images and 255 for the gray-level and color images, respectively.

Figure 2 demonstrates the PSNR comparison of Chen's [18] VCS and our scheme. Because of the randomness of VC encryption, we tested the recovery effect of the Lena image in two sets of sheets (pepper and airplane vs. Barbara and boat). Our method outperforms Chen's method by about 10 in terms of PSNR. VCS uses a probabilistic technique for achieving no pixel expansion. A significant improvement can be observed in the visual quality of the two shares and the reconstructed image in comparison to Chen's methods. For example, in the shares using the cover pepper and airplane, images improved detail in the background is clearly visible in Figures 2(g) and 2(h) versus Figures 2(a) and 2(b). As well, in the recovered secret Lena image, a greater difference between background details is clearly visible in Figure 2(j), in comparison to the result for VCS in Figure 2(c). Similarly, the PSNR values of the stacked secret and cover images show our method achieves a higher quality of recovery.

The reason for the poor image quality of VCS is that it accumulates and diffuses loss of encoding block. However, unlike VCS, EVCS has fewer selectable blocks. For the error-diffusion technology, we can choose all the color blocks with black pixels from zero to four. For VCS, we can only select a block containing two, three, or four black pixels. To make matters worse, we only choose between blocks containing three or four black pixels. Thus, if the error-diffusion technology is still used, the previous errors will accumulate and the subsequent blocks will become darker, as shown in Figures 2(a)–2(c).

To evaluate the performance of the proposed method on raster maps, we select the maps of New York and Paris as cover images and the map of Beijing as the secret image. As shown in Figure 3, the size of images is all the same as the original images. It is obvious that we cannot perceive any clue about Figure 3(c) from any individual cover images in Figures 3(a) and 3(b). When superimposing them altogether, we can easily reconstruct the secret map in Figure 3(c). Due to the multichannel error accumulation, the PSNR values of color map are lower than the gray-level images in Figure 2, but it does not affect the recognition of maps information.

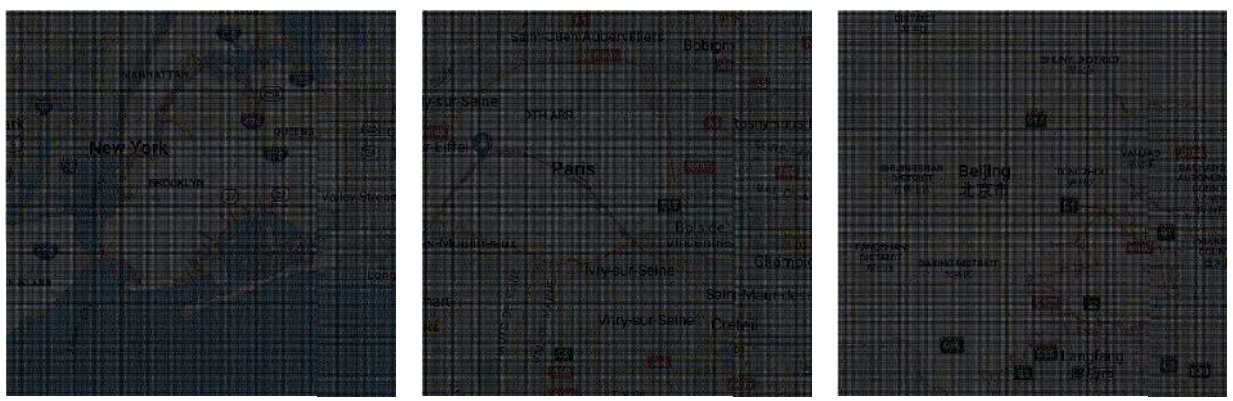


(a) (b) (c) (d)

(e) (f) (g) (h)

(i) (j) (k) (l)

Figure 2: The PSNR comparison of Chen's [18] VCS and our scheme. The first share halftone image ((a) pepper and (d) Barbara), the second halftone image ((b) airplane and (e) boat), and the stacked image ((c, f), Lena) are generated by Chen's [18] VCS. The first share halftone image (g, j), second halftone image (h, k), and the stacked image (i, l) are generated by our scheme. (a) 43.43, (b) 42.43, (c) 41.24, (d) 42.97, (e) 43.65, (f) 42.02, (g) 51.79, (h) 50.94, (i) 51.42, (j) 52.12, (k) 49.63, and (l) 50.29.




(a) (b) (c)

Figure 3: The experimental result and PSNR values of the proposed method on raster maps of (a) New York, (b) Paris, and (c) Beijing cities. The map (c) is superimposed from (a) and (b). (a) 49.62, (b) 49.52, and (c) 49.53.

## 5. Conclusions

The development of Internet technology has brought great challenges to the traditional paper map, which has advantages including macroscopical display, ease of carrying, and printability against limited-computing and untrustworthy networks. In this paper, we focus on security transmission of raster maps and study the computation-free encryption scheme of raster maps. We exploit the perfect ciphers in visual cryptography to split a secret map into two meaningful shares. This method enhances the security of raster maps because we can still store and distribute the map like normal images without regard to the disclosure of confidential information. We can restore the secret map when enough qualified shares are stacked. The proposed method retains the desire features of VC including computation-free and printer-friendly. These characteristics are important for raster maps, since there are many maps that are transmitted between various devices, and many maps must be printed to use. By encrypting an image block by block, we eliminate pixel expansion in traditional EVCS. Based on previous work on color decomposition and halftone, we extend the method to gray-level and color maps. Experimental results have shown that, compared with previous work, the proposed scheme can enhance visual perception.

As future work, we will explore new methods to further improve the quality of the recovered images so that we could apply this method to high-resolution maps.

## Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

## Conflicts of Interest

The author confirms that this article's content has no conflicts of interest.

## References

[1] C. Zhu, "Research progresses in digital watermarking and encryption control for geographical data," *Journal of Geodesy and Geoinformation Science*, vol. 46, no. 10, pp. 411–421, 2017.

[2] W. Jiayao, "Development trends of cartography and geographic information engineering," *Acta Geodaetica et Cartographica Sinica*, vol. 39, no. 2, pp. 115–119, 2010.

[3] W. Sirichotedumrong, T. Chuman, S. Imaizumi, and H. Kiya, "Grayscale-based block scrambling image encryption for social networking services," in *Proceedings of the IEEE International Conference on Multimedia & Expo*, San Diego, CA, USA, July 2018.

[4] Y. Peng, H. Lan, M. Yue, and Y. Xue, "Multipurpose watermarking for vector map protection and authentication," *Multimedia Tools and Applications*, vol. 77, no. 6, pp. 7239–7259, 2018.

[5] A. Rasmi, B. Arunkumar, and V. M. Anees, "A comprehensive review of digital data hiding techniques," *Pattern Recognition and Image Analysis*, vol. 29, no. 4, pp. 639–646, 2019.

[6] L. Fang, Z. Fu, G. Shen, and B. Yu, "Color raster map-sharing algorithm based on visual cryptography," *Journal of Image and Graphics*, vol. 23, no. 1, pp. 123–132, 2018.

[7] M. Naor and A. Shamir, "Visual cryptography," in *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques*, pp. 1–12, Perugia, Italy, May 1994.

[8] J. Weir and W. Yan, "A comprehensive study of visual cryptography," *Transactions on Data Hiding and Multimedia Security V*, vol. 5, pp. 70–105, 2010.

[9] D. Wang, F. Yi, and X. Li, "On general construction for extended visual cryptography schemes," *Pattern Recognition*, vol. 42, no. 11, pp. 3071–3082, 2009.

[10] C.-C. Chang, C.-S. Chan, and W.-L. Tai, "Hiding a halftone secret image in two camouflaged halftone images," *Pattern Recognition and Image Analysis*, vol. 16, no. 3, pp. 486–496, 2006.

[11] N. Askari, H. M. Heys, and C. R. Moloney, "An extended visual cryptography scheme without pixel expansion for halftone images," in *Proceedings of the 2013 26th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, pp. 1–6, Regina, Canada, May 2013.

[12] J. Mohan and R. Rajesh, "Enhancing home security through visual cryptography," *Microprocessors and Microsystems*, vol. 80, p. 103355, 2021.

[13] K. Dhiman and S. S. Kasana, "Extended visual cryptography techniques for true color images," *Computers & Electrical Engineering*, vol. 70, pp. 647–658, 2018.

[14] X. Wu, P. Yao, and A. Na, "Extended XOR-based visual cryptography schemes by integer linear program," *Signal Processing*, vol. 186, 2021.

[15] X. Wu, D. Wong, and Q. Li, "Extended visual cryptography scheme for color images with no pixel expansion," in *Proceedings of the International Conference on Security and Cryptography*, pp. 423–426, University of Piraeus, Athens, Greece, July 2010.

[16] D. Zhang, H. Zhu, S. Liu, and X. Wei, "HP-VCS: a high-quality and printer-friendly visual cryptography scheme," *Journal of Visual Communication and Image Representation*, vol. 78, pp. 103–186, 2021.

[17] Y.-C. Hou, Z.-Y. Quan, C.-F. Tsai, and A.-Y. Tseng, "Block-based progressive visual secret sharing," *Information Science*, vol. 233, pp. 290–304, 2013.

[18] Y.-F. Chen, Y.-K. Chan, C.-C. Huang, M.-H. Tsai, and Y.-P. Chu, "A multiple-level visual secret-sharing scheme without image size expansion," *Information Science*, vol. 177, no. 21, pp. 4696–4710, 2007.

[19] G. R. A. Kang and H.-K. Lee, "Color extended visual cryptography using error diffusion," *IEEE Transactions on Image Processing*, vol. 20, no. 1, pp. 132–145, 2011.

[20] D. Zhang and Z. Gu, "A high-quality authenticatable visual secret sharing scheme using SGX," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 660–709, Article ID 6660709, 2021.