Proceedings of the 3rd International Conference on Mechatronics and Smart Systems
DOI: 10.54254/2755-2721/117/2025.20949

Revolutionary Privacy Protection: Developments of Visual Cryptography for Secure Image Sharing

Shiyu Tang[1,a,*]

[1]*SWJTU-Leeds Joint School, Southwest Jiaotong University, Chengdu, China*
a. luxraaaaay@my.swjtu.edu.cn
**corresponding author*

Abstract: With the development of smart devices and networks, security and privacy protection have become significantly important. Numerous encryption algorithms have been invented to transmit confidential data or to protect user privacy. However, as most of them need complicated computing, sometimes they may not be the best way to encrypt certain types of data. Visual cryptography is a unique approach that is different from other kinds of cryptography as it does not need any mathematical calculation, but only relies on human vision for decryption. It was first proposed by Naor and Shamir. This paper selects two methods of visual cryptography, black-and-white image secret sharing and color image secret sharing. The paper first introduces the concept of the two methods, then summarizes the disadvantages of the two original algorithms and gives several improvements. Finally, provide examples of applications. The simple operations and decryption conditions make visual cryptography quite promising for future applications.

Keywords: visual cryptography, image secret sharing, (k, n) scheme, color image scheme

1. Introduction

In the digital age, the rapid development of smart devices and networks has significantly increased the importance and demand of security and privacy. As a result, cryptography has become a necessary tool for keeping sensitive information safe. Most traditional cryptography algorithms rely on complicated mathematical algorithms, which may not be that suitable for certain applications [1]. When it comes to image secret sharing, visual cryptography (VC) comes out.

VC is a kind of cryptography that deals with exchanged images [2]. It offers an innovative approach that stands apart from conventional methods. Introduced by Naor and Shamir in 1995 [3], it depends on human vision to decrypt secret messages without any use of mathematical computations. This gives VC a great advantage in usability.

With the improvements in visual cryptography, numerous advanced schemes have emerged. Kanwal et al. proposed a new scheme aiming to increase the safety and efficiency of image encryption by combining elliptic curve cryptography (ECC) [4]. The scheme generally uses a chaotic map to generate a new phase of the pixels, then produces a key by ECC. This scheme is safe enough since ECC becomes more complex when the size of the key increases. To improve the quality of the decrypted image, Rong et al. developed an enhanced semantic VC model (ESVC) [5]. It combines artificial intelligence (AI) to compare the quality of the original image and the recovered image. Additionally, due to AI's reinforcement learning (RL), it is safe enough to protect privacy. Moreover,

DOI: 10.54254/2755-2721/117/2025.20949

an extended secret image sharing scheme based on a sharing matrix came out to improve the quality of the recovered image [6]. The scheme slightly changes the cover images by embedding secret pixels, so it can hide the secret pixels more safely.

This paper explores two methods in VC: black-and-white image secret sharing and color image secret sharing, which are both based on pixel decomposition. The black-and-white image secret sharing divides a secret image into n shares and requires a minimum of k shares to decrypt, while the color image secret sharing extends VC to color images, addressing the limitations of earlier methods that were restricted to binary black-and-white images. It decomposes the secret image based on single-color pixels, mostly by cyan (C), magenta (M), and yellow (Y) primaries. This is more suitable for modern life as nowadays most of the images are colorful.

This paper aims to highlight the potential of VC in modern applications, ranging from secure medical communication to biometric systems. Despite the existing defects, by exploring better improvements, VC has the potential to be a promising solution for privacy and security in the modern world.

2. Visual Cryptography for Black and White Images

2.1. Concept

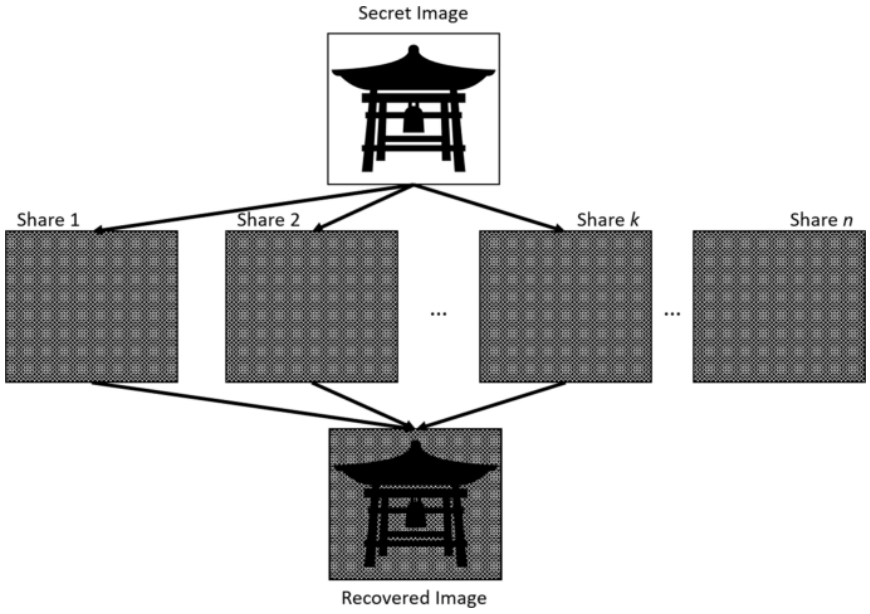

Figure 1: the (k, n) secret sharing concept [3].

The concept of VC, first raised by Naor and Shamir in 1995, can be summarized as dividing a secret image into two secret images. The limitation is that the secret image only consists of black and white pixels, meaning that it is a binary image [3]. This is the original and traditional scheme of VC. Then this concept is extended to a more general idea, k out of n secret sharing scheme, known as (k, n) secret sharing scheme. It gives out that the secret image is divided into n shares and when encrypting, at least k shares are necessary, as shown in Figure 1. The principal means that every share includes a subset of pixels from the secret image. The principle of the scheme results in good security. Because if the number of shares is not enough, decryption will become difficult [7].

DOI: 10.54254/2755-2721/117/2025.20949

2.2. Disadvantages

2.2.1. Contrast Loss

However, there exist several potential defects. First is the contrast loss after decoding. According to Shivani, the image encoded and decoded by the (k, n) scheme, has roughly 50% contrast loss as shown in Figure 2 [8].

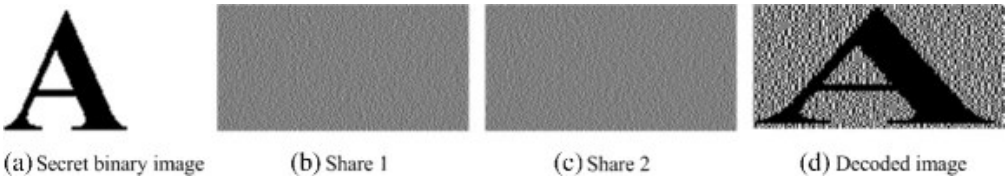

Figure 2: Shivani's example of a (2, 2) secret sharing [8].

To Fix this, Viet D.Q. and Kurosawa K. found a reversing method to deal with the problem [9]. They found that in decryption, the black region was perfectly restored while the white region became gray. As a result, they reversed the black and white regions, then reconstructed them to get perfect images. The method effectively solves the loss of contrast with non-cryptographic operations.

2.2.2. Attack and Cheating

Another two main issues are attack and cheating. To fix the external attack and further develop the (k, n) secret sharing scheme, an XOR-based scheme came out. According to He and Xia, the traditional (k, n) scheme needs a lot of time to process when the value of n is huge while the XOR-based scheme needs less time for encryption and decryption [10]. The principle is that through combinations of the XOR algorithm and the traditional (k, n) scheme, randomly generate new secret keys to apply the XOR algorithm to the secret. This scheme effectively decreases the generating time of the traditional scheme, with the improvement of security as at the end of the algorithm, what is distributed to the participants are the random keys and the final results of the algorithm. That is to say, the original content of the secret will completely be kept mysterious, therefore though some shares are leaked or stolen, the origin secret image keeps safe as the stolen shares themselves have nothing to do with it.

Cheating turns out to be the other issue. One is the participants' collusion defection. It means several participants use their shares to infer others' shares, then change their shares together to other fake shares, leading to the wrong image in decryption. To handle this, an improvement method was raised [11]. Random matrices are generated and used for every pixel in the shares to encrypt. This can prevent the inference to other shares which effectively avoids cheating.

2.3. Applications

The (k, n) secret sharing scheme is used in various fields. QR code application is an example. With the wide use of portable devices, QR codes have become a significant way to transmit messages. As QR codes can be identified by anyone, Cheng et al. used a scheme based on the (k, n) scheme to deal with the QR code, and successfully hide secret messages into it [12]. The success indicates that though the traditional (k, n) secret sharing scheme has problems, after improvement with current technology, it still performs great practicality in secret sharing. The other example is in the fields like medical communication which needs to transfer private images, security and quality are in high demand. A (k, n)-based method, significant VC, combines the Error Abatement Technique with the original scheme. It can decrease the mistakes in decryption in the pixels' aspects and raise the clarity of the secret images [13]. With this technique, for instance, when using online medical services to

DOI: 10.54254/2755-2721/117/2025.20949

transfer images involving patients' privacy, both the security of privacy and the quality of the images will be improved.

3. Visual Cryptography for Color Images

3.1. Concept

Besides the traditional (k, n) secret sharing scheme, since it only applies to black-and-white images, another scheme for color images comes into being. The color image scheme is based on three primary colors: cyan, magenta, and yellow. Under different intensities of different primaries, the compound light will appear to be a different color [14]. This allows color images to be divided into several shares with different single-colors, mostly the primaries, as shown in Figure 3. The concept raised by Hou is seen as the pioneer of the color image VC.

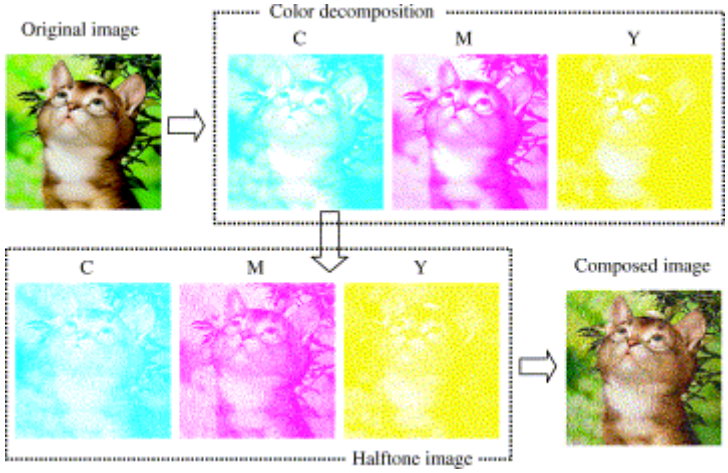

Figure 3: Color decomposition of an image [14].

3.2. Disadvantages and Improvements

Regrettably, Hou's scheme has similar defects to the traditional scheme.

Wu et al. pointed out that Hou's scheme could only hide one message [15]. Therefore based on his scheme, a new improved version came out. The improved scheme generates two secret shares. Besides stacking the two shares to get one message, after horizontally rotating one of the two and then stacking again, the second message comes out. This can improve the efficiency of the cryptography, and decrease the demand for the data.

Another is the low color contrast. Similar to the contrast loss in black-and-white images, the color secret image after decryption is not of the same quality as the origin image. In other words, the image becomes gray and blurred. To solve this, according to Dhiman and Kasana [2], an improved technique is that expand each pixel of the secret image into 5*5 blocks and adjacent blocks fill in different colors to increase the contrast. This technique also solves the above-mentioned low efficiency as it encrypts and decrypts two images at a time, using the logic matrix to determine the block pattern. When decrypting, the red (R), green (G), and blue (B) values of each secret image are dispersed into three sharings, embedding the corresponding color information through a logical matrix. Then every RGB value forms a new color value with the corresponding image. Through OR operation, the RGB values of each sharing can be recombined into the RGB components of the original image. Since the information of each color channel is correctly assigned to the different sharings and all the information can be recovered during the decryption process, there is no color loss.

DOI: 10.54254/2755-2721/117/2025.20949

3.3. Applications

As most images in daily life are colorful, the color image scheme has been widely used. One application is biometrics. Nowadays biometrics plays a significant role in individual privacy. Mohan and Rajesh combined the scheme with the Siamese network and proposed an approach to the facial identification fields [16]. It decomposes the facial image into two shares and stores one of them in the database, and the other in the users' ID card. When identifying, the two shares are collected to decrypt and use the Siamese network to calculate the similarity between the user and the secret image. This method protects the users' privacy well and has high accuracy. In modern life, Alipay, online bank apps, intelligent door locks and so on aspects are all of the high requirements of security, therefore the technique can be of good help.

Another is, that Ibrahim et al. combined the Harris Hawks Optimization (HHO) algorithm with the color image scheme [17]. The HHO calculated every share's probability color level. This operation improves the quality of the recovered image. This technique certainly can be used in the transmission of individual information in portable devices, application programs, and even state secret and military intelligence, resulting in its advantages in high quality and security.

4. Conclusions

VC has been an advantageous method to encrypt secret images as it does not depend on any mathematical calculations but all human visions. This paper mainly introduces two different schemes of VC: the traditional (k, n) secret sharing scheme and the color image secret sharing scheme. Although none of them is perfect, meaning there are still some flaws, such as contrast loss or recovered images, numerous different improved algorithms are proposed.

With the development of technology and smart devices, the simplicity of the VC is destined to play a major role in privacy protection and secret transmission in the future. As long as researchers remain committed to improving their security, image quality, and algorithm streamlining, then VC may finally be widely applied.

References

[1] *Tzeng, W.G. and Hu, C.M. (2002) A New Approach for Visual Cryptography. Designs Codes and Cryptography, 3, 207-227.*

[2] *Dhiman, K. and Kasana, S.S. (2018) Sharing Two True Colour Images Using (3,3)-extended Visual Cryptography Technique. Journal of Modern Optics, 17, 1949-1959.*

[3] *Ibrahim, D.R., Teh, J.S. and Abdullah, R. (2021) An Overview of Visual Cryptography Techniques. Multimedia Tools and Applications, 21-23, 31927-31952.*

[4] *Kanwal, S., Inam, S., Al-Otabi, S., Akbar, J., Siddiqui, N. and Ashiq, M. (2024) An Efficient Image Encryption Algorithm Using 3D-cyclic Chebyshev Map and Elliptic Curve. Scientific Reports, 1, 1-15.*

[5] *Rong, R., Shravage, C. and Mary, G.S. (2024) Enhanced Semantic Visual Cryptography with AI-driven Error Reduction for Improved Two-dimensional Image Quality and Security. Measurement Science and Technology, 10.*

[6] *Li, X.P., Fu, Z.X. and Yu, B. (2024) A Novel Extended Secret Image Sharing Scheme Based on Sharing Matrix. Journal of Visual Communication and Image Presentation, 11.*

[7] *Arumugam, S., Lakshmanan, R. and Nagar, A.K. (2014) On (k, n)*-visual Cryptography Scheme. Designs Codes and Cryptography, 1, 153-162.*

[8] *Shivani, S. (2018) VMVC: Verifiable Multi-tone Visual Cryptography. Multimedia Tools and Applications, 5, 5169-5188.*

[9] *Viet, D.Q. and Kurosawa, K. (2004) Almost Ideal Contrast Visual Cryptography with Reversing. Topics In Cryptography - CT-RSA 2004. San Francisco, USA. (Heidelberg: Springer, 2004), 353-365.*

[10] *Xia, G. and He, C.W. (2021) A (k, n) Threshold Secret Sharing Algorithm Based on the HeterOR Operation. Computer Project, 10, 111-115, 124.*

[11] *Qi, X.D., Jiang, B. and Yin, N.X. (2021) A Visual Password Scheme Against Collusion Deception. Computer Applications And Software, 6, 329-332, 349.*

DOI: 10.54254/2755-2721/117/2025.20949

[12] Cheng, Y.Q., Fu, Z.X. and Yu, B. (2018) Improved Visual Secret Sharing Scheme for QR Code Applications. IEEE Transactions on Information Forensics and Security, 9, 2393-2403.

[13] Mary, G.S. and Kumar, S.M. (2020) Secure Grayscale Image Communication Using Significant Visual Cryptography Scheme in Real Time Applications. Multimedia Tools and Applications, 15-16, 10363-10382.

[14] Hou, Y.C. (2003) Visual Cryptography for Color Images. Pattern Recognition, 7, 1619-1629.

[15] Wu, H.C., Wang, H.C. and Tsai, C.S. (2006) Multiple Image Sharing Based on Colour Visual Cryptography. Imaging Science Journal, 3, 164-177.

[16] Mohan, J. and Rajesh, R. (2021) ENHANCING Home Security Through Visual CRYPTOGRAPHY. Microprocessors and Microsystems, 80.

[17] Ibrahim, D., Sihwail, R., Arrifin, K.A.Z., Abuthawabeh, A. and Mizher, M. (2023) A Novel Color Visual Cryptography Approach Based on Harris Hawks Optimization Algorithm. Symmetry-basel, 7.