An overview of visual cryptography techniques

Article *in* Multimedia Tools and Applications · September 2021

DOI: 10.1007/s11042-021-11229-9

3 authors:

Dyala Rashid Ibrahim
Universiti Sains Malaysia
8 PUBLICATIONS **33** CITATIONS
SEE PROFILE

Je Sen Teh
Universiti Sains Malaysia
42 PUBLICATIONS **714** CITATIONS
SEE PROFILE

Rosni Abdullah
Universiti Sains Malaysia
200 PUBLICATIONS **1,383** CITATIONS
SEE PROFILE

Noname manuscript No.
(will be inserted by the editor)

An Overview of Visual Cryptography Techniques

Dyala R. Ibrahim, Je Sen Teh[0000−0001−5571−4148] **· Rosni Abdullah**[0000−0002−3061−5837]

Received: date / Accepted: date

Abstract Visual cryptography is an encryption technique that decomposes secret images into multiple shares. These shares are digitally or physically overlapped to recover the original image, negating the need for complex mathematical operations or additional hardware. There have been many variations of visual cryptography proposed over the years, each addressing different problems or to fulfill different security requirements. Existing review papers on the area only cover certain types of visual cryptography or lack comparisons between the various schemes. To address this gap, this paper provides broad overview of the area to aid new researchers in identifying research problems or to select suitable visual cryptography methods for their desired applications. For more veteran researchers in the area, our paper provides the most up-to-date coverage of the state-of-the-art[1]. We first provide an introduction to the various categories of visual cryptography techniques, including a discussion on recently proposed schemes. These schemes are then compared in terms of their features, performance metrics, advantages and disadvantages. Compared to prior work, we extend the number of comparison metrics to include signal-to-noise ratio and the type of shares. Over 40 visual cryptography schemes that have been proposed in the past two decades were analyzed and compared. Our findings indicate that existing problems such as pixel expansion, poor quality of recovered image quality, computational and memory complexities still exist, and a optimizing the trade-off between these requirements still requires further investigation. We conclude the paper with a discussion of these open problems and future research directions.

Keywords Confidentiality · Encryption · Information security · Pixel expansion · Secret sharing · Visual cryptography

Dyala R. Ibrahim · Rosni Abdullah
National Advanced IPv6 Centre, Universiti Sains Malaysia

Je Sen Teh(✉)
School of Computer Sciences, Universiti Sains Malaysia
Tel.: +6046534046
E-mail: jesen_teh@usm.my

[1] as of mid-January 2021

1 Introduction

Visual cryptography (VC) was pioneered by Naor and Shamir [1]. VC protects secret visual information in a way that differs from conventional cryptographic methods because it relies the human vision to decrypt secret information without complex mathematical computations nor decryption devices. VC involves splitting a secret image into two noisy images, referred to as shares. The decryption process is performed by superimposing the shares recover the secret image [2]. Each share alone cannot reveal clues about secret image and thus, Naor and Shamir extended this basic idea to a k out of n secret sharing problem ((k, n) scheme), where n is the total number of shares whereas k is the minimum number of shares required to recover the secret. A general depiction of a (k, n) VC scheme is illustrated in Figure 1.

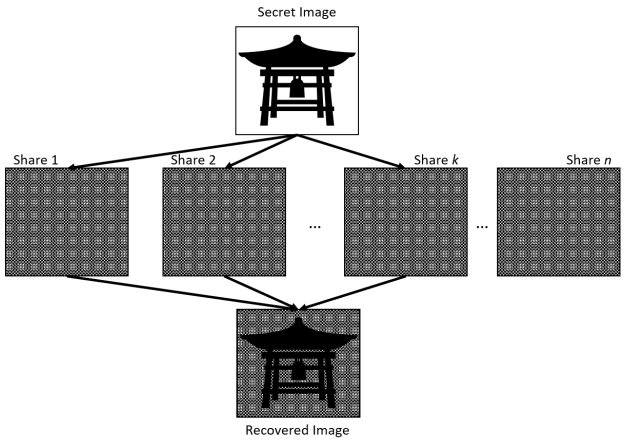

Fig. 1 General process of (k, n) visual cryptography.

VC provides perfect secrecy while having a straightforward decryption process. This perfect security is ensured because an adversary with unlimited computational power has no advantage in extracting pixel information by inspecting fewer than k shares [1]. This is an advantage that VC has over conventional cryptographic schemes that are usually conditionally secure. Due to its unique property, VC has various applications that include securing online transactions [3], digital watermarking [4], authentication [5,6,7], copyright protection for digital images, steganography, electronic cash banking applications [8] and many more.

In the past three years, very few VC survey papers have been published in reputable journals or conferences. Pandey and Som reviewed the applications and usage of VC in areas such as encryption, data hiding, cybercrime and user authentication [6]. Their paper focused solely on the application rather than VC itself. In the following year, Thomas and Gharge published a survey on VC schemes [9]. They covered four main schemes: VC for monochrome, color and halftone images, and also extended VC (which uses meaningful shares rather than noisy shares). The four schemes were compared in terms of two metrics, the number of secret

images and their pixel expansion property. A more thorough survey paper was also published by Punithavathi and Geetha who covered a plethora of VC algorithms [10]. They introduced 17 different VC schemes and compared them in terms of their contrast loss, pixel expansion, number of shares and number of secrets. Chanu and Neelima published a survey paper on secret image sharing schemes which covered steganography, VC, watermarking and other schemes [11]. As they covered a broader range of secret sharing schemes, only 15 different VC schemes were described, ranging from algorithms proposed in 2007 to 2015. No comparison between the schemes was provided. In an overview of visual cryptography schemes by Bhatnagar and Kumar, six types of VC techniques were introduced followed by a brief summary of the properties of 31 schemes proposed between 1994 and 2016 [12]. Critical analysis of those schemes to reveal open problems in VC was not performed.

This paper provides a broad overview of various VC schemes, ranging from classical VC to more advanced schemes such as extended progressive VC. We introduce over 10 different types of VC techniques that have been proposed within the past 20 years which we have categorized based on design goals. We perform a comparison of over 40 individual VC schemes not only in terms of performance metrics, but also their advantages and disadvantages. The number of metrics used for comparison has also been extended (as compared to prior survey papers) to include peak signal-to-noise ratio (PSNR) and the type of shares. The overall aim of this survey is to equip both new and experienced researchers with a strong grasp of the current state-of-the-art of VC and to provide, at a quick glance, the comparison between various VC schemes that have been proposed to date.

This rest of this survey is organized as follows: Section 2 details the performance metrics and parameters for VC schemes. In this section, the very first form of VC is also discussed to provide the reader with some background information. Next, Section 3 introduces the different variants of VC that will be compared in Section 4. Section 5 concludes the paper by highlighting research gaps and future directions in the area.

2 Preliminaries

2.1 Introduction to Visual Cryptography

In Naor and Shamir's VC scheme, which is considered the earliest implementation of VC, the *secret* is a binary image that consists of black and white pixels. In their proposed scheme, each pixel is processed separately. The encryption process splits an input image into two share images or shares that can be printed on transparencies, where black pixels are considered as solid whereas white pixels are considered as transparent. Stacking these transparencies will allow the user to recover the original secret image without any additional computational effort. However, this decryption process is lossy and leads to degraded contrast [13]. In addition, this scheme also involves pixel expansion.

This VC scheme can be generalized as a k out of n secret sharing problem, where n refers to the number of shares that are generated by encrypting the secret image, and that secret image can only be recovered if a minimum of k shares are stacked together. If the number of shares are fewer than k, the secret image cannot

be revealed. Each share is basically a collection of m black and white sub-pixels, which represent a subset of pixels from the original secret image. A share can be represented as a $n \times m$ binary matrix, S where each of the individual pixels $(s_{i,j})_{m \times n} \in S$ is 1 or 0 if and only if the j-th sub-pixel of the i-th share is black or white respectively.

The encryption process is dependent on the parameters discussed in Section 2.1, which include pixel expansion and contrast. Additionally, there are two sets of sub-pixel patterns that are used to represent either white or black pixels in the shares. We denote C_0 as the set of sub-pixel patterns for white pixels whereas C_1 is the set of sub-pixel patterns for a black pixel. C_0 matrices are obtained by permuting the columns of $\begin{bmatrix} 1\,1\,0\,0 \\ 1\,1\,0\,0 \end{bmatrix}$, whereas C_1 is obtained by permuting the columns of $\begin{bmatrix} 1\,1\,0\,0 \\ 0\,0\,1\,1 \end{bmatrix}$.

The hamming weight, $H(V)$ of the OR-ed m-vector V is interpreted as a black pixel if $H(V) \leq d$ and white if $H(V) < d - \alpha m$ for some fixed threshold $1 \leq d \leq m$ and a relative difference $\alpha > 0$. The original VC algorithm can be generalized as a 2-out-of-2 VC scheme, which can also be written as a $(2, 2)$-VC scheme. Due to pixel expansion, each pixel from the secret image will be represented by four pixels in the share image. Selection of the 4-pixel pattern is based on the following rules:

1. If the original pixel is white, one randomly selected 4-pixel pattern is used for both shares.
2. If the original pixel is black, a pair of complementary 4-pixel patterns will be selected for the shares.

Overlapping the shares correctly will align the sub-pixels to reveal the original pixel color. By performing an OR operation of the rows, the matrices from C_1 will lead to a vector of all 1s (black pixel) whereas matrices from C_0 will lead to a vector consisting of two 1s and two 0s (white pixel). Alone, the shares do not give any indication as to whether a particular pixel is black or white. This leads to perfect security because it is impossible to decrypt with fewer than k shares, regardless of the computational capability of an adversary.

2.2 Visual Cryptography Metrics

Before introducing recent VC schemes, we first introduce some relevant metrics that are commonly used to evaluate or describe them. We will discuss each of them individually in this subsection. Table 1 summarizes the different VC schemes that we have reviewed based on these parameters. We will discuss these schemes in detail in Section 3.

Pixel expansion refers to number of sub-pixels m in generated shares that represent a single pixel in an original image. This parameter presents in loss of resolution from an original image to share image in VC procedure. When the shares are overlapped the recovered image will not be of the same quality of original image. The recovered image has less contrast and experiences a loss of resolution as

compared to secret image. This parameter also reflects upon the size of the recovered image, which ideally should be as close as possible to the original secret [14]. Pixel expansion can cause many problems such as image distortion, more storage space, and higher complexity in generating shares. Minimizing pixel expansion has been a central focus in many VC schemes [15].

Contrast is the relative difference between black and white pixels of a binary image [16,17] or the difference in color tones in colored images. It reflects upon the clarity or sharpness of a particular image. For VC schemes, the contrast of recovered (decrypted) images is calculated as a measure of quality. In many cases, the VC encryption and decryption process leads to a loss in contrast.

Security refers to the amount of information about the secret image that can be extracted from share images. The recovered image should not be revealed with less than $k-1$ shares in (k,n) schemes. The security parameter is generally satisfied when the strength of an encryption process (share generation) prevents an intruder from extracting clues about the secret image [18]. The security metric of VC schemes can be measured by calculating correlation coefficients (CC) or performing histogram analysis of the shares [19].

Complexity can be divided into two types: computational and memory complexity. Computational complexity is concerned with the number of total operations (time) required to generate the set of shares n, and to reconstruct the secret image. Memory complexity refers to the amount of storage (memory) required for a VC scheme. Complex VC algorithms have higher computational and memory complexity, which then requires more powerful hardware to implement. This may render certain system unsuitable for fast-paced, real-time decisions. In theory, it is good to have a complex VC algorithm for optimal security but in practice, a complex algorithm may not be suitable for real-life applications that require minimal computational overhead [20].

The **type of shares** of a VC scheme can either be meaningless [21] or meaningful [22]. A meaningless share resembles noise whereas a meaningful share is a discernible image used to embed information from the secret image. Depending on the application, the use of one or the other may be preferred. For example, a meaningless share may rouse the suspicion of an adversary whereas a meaningful share may not.

The **number of secrets** is the number of secret images that are encrypted by a VC method. When there are multiple secrets, the secret images are all encrypted into the same set of shares. Decryption process is performed by overlapping shares that are rotated or flipped to recover various secret images [23,24].

The **accuracy** of a VC scheme measures the quality of a recovered image. Ideally, the recovered image should be an exact replica of the original secret image. The goal of any VC scheme is to maximize accuracy, which can be evaluated by PSNR, mean square error (MSE), and CC metrics [25].

3 Visual Cryptography Variants

In this section, we will cover various VC schemes that can be divided into several categories. In this paper, we formulate two broad categories based on the schemes that have been reviewed: research work on improving schemes for specific type of images, and those that focus on flexibility in terms of shares and secrets. Note that

those that fall under the category of flexibility will also deal with one of the image types. The types of images include binary (black and white), grayscale or color. In terms of flexibility, we cover schemes that involve a varying number of secrets, share flexibility (how shares are generated and can be used to recover images), and the type of shares. The VC categories covered in our paper are as shown in Figure 2.

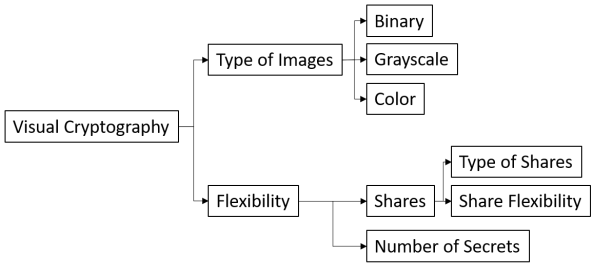

Fig. 2 Visual cryptography techniques covered in this paper.

3.1 VC Schemes: Image Quality

3.1.1 Binary Images

The first type of VC scheme for binary images is pixel-based VC which is based on the pixels in the input image. The VC scheme pioneered by Naor and Shamir falls under this category. The basic model is extended into a visual variant of k-out-of-n or (k, n) secret sharing problem. Generally, given secret images is generated into n shares such that the secret image is disclosed only if any k number of shares are overlapped together (where $k \leq n$). The image cannot be recovered if fewer than k shares are overlapped. Full details regarding this scheme has already been discussed in Section 2.2. The main limitation of pixel-based VC is loss in contrast of the reconstructed image that is directly proportional to the pixel expansion parameter.

Another type of pixel-based VC is the segment-based VC (SBVC) proposed in [26]. This scheme is specifically designed to encrypt secrets that consist of a limited set of symbols, specifically symbols that can be represented by a segment display such as integers from 0 to 9. A depiction of segment-based VC is shown in Figure 3. SBVC has been used to assure the security of biometric templates [27]. The merit of the SBVC scheme over the pixel-based scheme is that it may be easier for the human eye to recognize the representations, such as messages consisting of numbers that can be determined by SBVC using seven segments [28]. Other main advantages of this technique are good quality of recovered image and high contrast of recovered image, but it is computationally expensive.

Random grid VC (RG-based VC) is a pixel-based VC pioneered by Kafri and Keren in [29]. This scheme is a method of implementing VC without pixel expansion. The method uses random black and white images as building blocks for

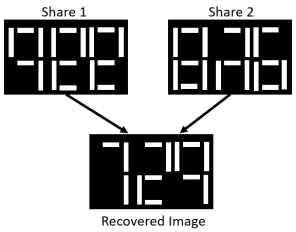

Fig. 3 Segment-based visual cryptography.

sharing secret images. The scheme has no pixel expansion, thus the shares, recovered image and the secret image have the same dimensions [30]. There are also other researchers such as [31] and [32] who have proposed RG-based VC methods. The main advantage for this technique is the good visual quality of both share and recovered images because it removes the problem of pixel expansion [33, 34, 35]. [36] introduced a weighted RG-based VC scheme that allows each share to be assigned a weight based on a participant's importance. Thus, the ability of each share to reveal the secret image varies depending on the participant. This property is similar to the (t, s, k, n) scheme that will be introduced later on. Despite some of its advantages such as size invariance, further investigation on improving the contrast of RG-based VC schemes is still required [37].

[38] proposed a pixel-based size invariant VC (SIVC) scheme which removes the need for the pixel expansion. This leads to smaller shares which are closer to the secret image size. SIVC reduced the number of extra sub-pixels needed to reveal the secret. So, the size of shares will be decreased to be the same size of the secret image which avoids distortion when reconstructing the secret. [39] also proposed a SIVC scheme that reduced the distortion when decrypting the secret image. Their scheme has a wide range of practical applications such as authentication with steganography and cheating prevention schemes. However, there is also a need to improve upon the quality of the recovered image in terms of contrast.

The probabilistic VC schemes proposed in [40] and [41] also aimed to solve the problem of pixel expansion. VC schemes can either be deterministic or probabilistic. For example, Naor and Shamir's scheme performs deterministic pixel expansion. In the probabilistic technique, the frequency of white pixels is used to determine the contrast of reconstructed image. The technique is non-expansible and can be implemented on the conventional VC by using a transfer operation. The probabilistic model has a tuneable feature which allows the participants to determine the ratio of colors for each share. Thus, the recovered image will differ slightly based on the selected ratio, which lends towards the probabilistic nature of the scheme. The RG-based VC scheme proposed in [37] is also a probabilistic scheme. The main advantage of this scheme is that it has no pixel expansion, which then leads to improved quality of the recovered image. However, the contrast of the reconstructed image is similar to pixel-based VC schemes, and as such still needs to be improved.

[42] proposed a probabilistic CVC scheme based on the color-black-and-white (CBW) paradigm introduced by [43]. CBW is a unique concept as it relies on colored shares as a host for black and white pixels of a secret image to reduce pixel expansion. Although their proposed scheme can eliminate pixel expansion entirely,

there exists colored background noise in the recovered images. The scheme proposed by [44] approached the pixel expansion problem from a different perspective by proposing an XOR-based threshold VC scheme with adjustable pixel expansion. Their scheme was able to achieve the same average contrast regardless of the pixel expansion value. However, their scheme cannot eliminate pixel expansion entirely.

3.1.2 Greyscale and Color Images

Grayscale and color images require a pre-processing phase to convert them into binary prior to encryption. Generally, this is done by a pre-processing technique referred to as a halftoning technique. Halftoning is a process to simulate the continuous image tone through use of dots. There are several types of halftoning techniques such as thresholding, error diffusion, random dithering and many more. [45] proposed a novel VC for grayscale images by using error diffusion. Their method embeds a natural secret image into two natural carrier images with high quality at low computational complexity. The secret image is decrypted visually by stacking the two carrier images.

Apart from halftoning technique, Moiré's pattern and gray level relative difference technique can be used to visually encrypt grayscale images. Moiré's pattern is a halftoning technique which works as a randomized share generator for a hidden image, splitting it into two shares which are called pre-shares. Then using a hiding algorithm, the pre-shares are combined with cover images. Its outputs are the final share images which are overlapped to divulge the hidden image [46]. The main limitation for these grayscale schemes is that the pixel expansion problem is not solved, which leads to lower recovered image quality in terms of contrast and clarity. Another grayscale VC scheme based on the absolute moment block truncation coding compression (AMBTC compression) was introduced in [47]. In this scheme, p compressed AMBTC reference images are required for encoding purposes. Thus, each participant is required to hold p shares, which incurs memory costs. This requirement was subsequently eliminated in an improved scheme proposed by [48] which requires only one share per participant.

Color visual cryptography (CVC) has many advantages over binary and grayscale VC because color images are popular and have a wide range of use in many day-to-day applications. It also helps to reduce the risk of alerting someone to the fact that there is information hidden within it. The scheme proposed by Hou in [49] is considered the main starting point for CVC. Their proposal included three VC methods for gray-level and color images based on black-and-white images. The color and grayscale images are transformed into black-and-white format so that conventional VC can be used to encrypt the secret image into many shares. In other words, their methods retain the merits of black-and-white VC while being able to support color and greyscale images.

[50] also introduced one of the earliest color decomposition techniques to be used in CVC. Using this technique, each pixel in an image will be decomposed into three primary colors: cyan, magenta or yellow. However, this method suffers from the same disadvantage as traditional VC with respect to the pixel expansion that occurs. Each pixel is expanded into a 2×2 block where two color pixels are stored along with two transparent (white) pixels. Size-invariant CVC schemes were later proposed in [51] and [52]. Notably, the scheme proposed in [52] emphasized on usability by having one of the shares stored on a smartphone while the other

printed on a PVC transparent surface. In [53], the shares generated from a CVC scheme is further encrypted using a chaos-based encryption algorithm. Although encryption further increases the security of each individual share, this incurs additional computational complexity which is already a problem for other existing CVC schemes in addition to memory complexity [54,55].

3.2 VC Schemes: Flexibility

In this subsection, we discuss various schemes that focus on improving the flexibility of VC in terms of the type and flexibility shares, as well as the number of secrets. Share flexibility refers to alternative ways of how shares are generated and can be used to recover the secret image.

3.2.1 Type of Shares

Extended visual cryptography (EVC) produces meaningful shares from the encryption process. The advantage of meaningful shares as opposed to a random noisy share is that it solves the problem of suspicion. An adversary may suspect that a noisy share contains vital secret information whereas a meaningful share may escape detection [56]. In addition, it is easier to manage meaningful shares as compared to noise-like meaningless shares that visually look very similar. This scheme was pioneered Ateniese et al. in [57]. More recently, [58] introduced an EVC scheme that embeds greyscale images into colored cover images with the goal of maximizing recovered image quality. They achieved a 90% structural similarity between the original and recovered images.

A flip-based EVC scheme was proposed by [59] which allows meaningful shares to be flipped to reveal different secret images. This was an improvement over a prior flip-based scheme proposed by [60] which was limited to meaningless shares. The process of a flip-based EVC scheme is shown in Figure 4. As previously mentioned, the main advantage for this technique is increased security as compared to traditional VC through the construction of meaningful shares [61,62,63,64]. EVC is useful for applications such as copyright protection because the same watermark can be embedded in each meaningful share and recovered when combined with a master share [65]. It also has higher contrast levels than traditional VC. On another hand, the main limitation for EVC is the requirement of high storage capacity during its execution [66].

Apart from EVC, another solution to overcome management problems of meaningless shares is to use tagged shares [67]. Tagged visual cryptography (TVC) schemes embed or stamp a tag image onto existing shares. This tag can be recovered or identified by folding a share in a particular direction (e.g. horizontally). However, when compared to the classical VC schemes, TVC schemes have poor quality of recovered images due to the tags being embedded into the share itself. [68] addressed this problem in their TVC scheme by adopting a probabilistic approach. Their scheme outperformed prior TVC schemes when there are fewer than 5 participants. A typical TVC scheme is depicted in Figure 5.

Natural language letter-based VC (NLLVC) is a technique pioneered by Lin et al. in [69]. In this technique the pixels are replaced by letters, alphabets or numbers in the share images. During the share generation process, shares are

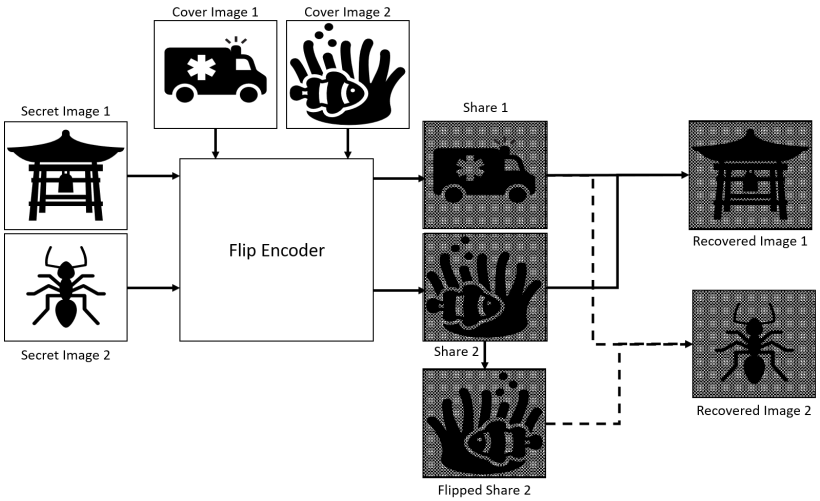

Fig. 4 Flip-based extended visual cryptography (adapted from [59]).

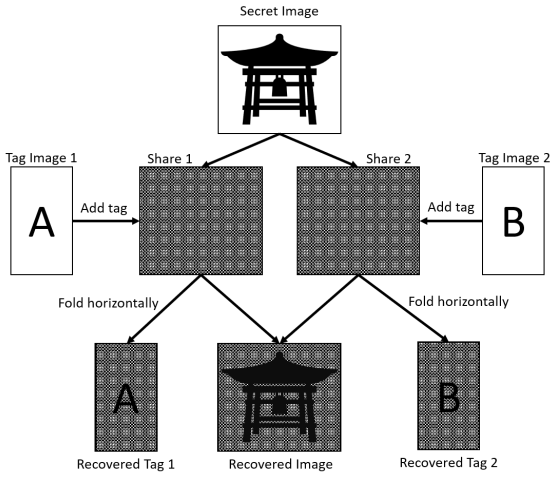

Fig. 5 Tagged visual cryptography.

constructed using meaningful data as a subterfuge to avoid suspicion or detection by adversaries. NLLVC technique uses the overlapping of alphabets in the shares to indicate the difference in contrast. Superimposing different alphabets lead to black pixels whereas superimposing the same alphabets lead to white pixels. Adding more shares will increase the contrast for recovered image. This technique has the same advantages and disadvantages as EVC. A general depiction of NLVC is illustrated in Figure 6.

In most VC schemes, all shares play the same role or have the same level of importance. If certain shares can be made more important than others, VC can also be used to manage the level of access to secret images. For this purpose, [70] introduced a (t, s, k, n) VC scheme for binary images where there are s essential

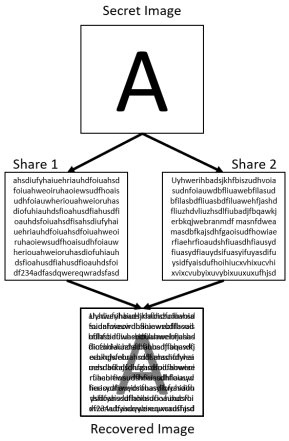

Fig. 6 Natural language letter-based visual cryptography.

shares and the remaining $n - s$ shares are non-essential. To recover the secret image, at least k shares are required, where t of these k shares must be essential shares. More recently, [71] introduced a (t, s, k, n) VC scheme where $t = s$. Their scheme outperformed prior ones in terms of recovered image quality however still suffers from pixel expansion.

3.2.2 Share Flexibility

Next, we discuss VC schemes that generate or utilize shares in different ways. Progressive VC (PVC) achieves higher quality recovered secret image when more shares are used for decryption. In other words, the quality of the recovered image is progressively improved in proportion to the number of shares used for decryption. An example is illustrated in Figure 7. This technique can be used for both color and grayscale images [72]. PVC was first proposed by Fang in [73]. In Fang's scheme, the secret image is encrypted into many shares which have different resolutions. When the shares are overlapped, secret image will be gradually revealed. Thus, the reconstruction process depends on number of shares. The secret image will increase in clarity as the number of overlapped shares increase [74,75]. [76] proposed an extended PVC scheme that embeds the shares into meaningful cover images. Their (k, n) scheme has no pixel expansion, flexibility of choosing various k and n values, supports various secret image sizes and has no residual trace of the cover image in recovered images. Another form of PVC is the block-based PVC proposed by [77]. In this scheme, a secret image is divided into non-overlapping blocks that can each be recovered separately depending on which shares are overlapped. The proposed scheme was susceptible to a cheating attack which was later addressed by [78]. The main advantage of PVC schemes is their single encryption, multiple decryptions paradigm. Secret images are encrypted once, and can be decrypted or reconstructed in a myriad of ways depending on the different combinations of shares. Images of different quality levels can be extracted depending on the application's requirement or the computational resources available. On another

hand, the main disadvantage for PVC is high memory complexity because due to the amount of storage required for the share images.

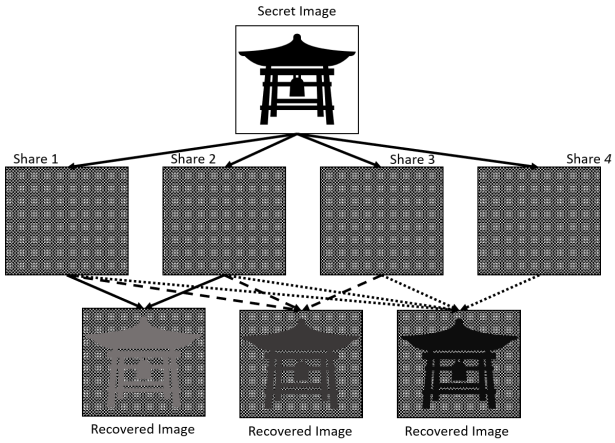

Fig. 7 Progressive visual cryptography.

Hierarchical VC (HVC) is a concept pioneered Chavan and Atique in [79]. The main idea in HVC is to encrypt a secret image in multiple levels (such as in a hierarchy). HVC encrypts the input secret in hierarchical manner whereby secret image is first decomposed into many shares, then each share is further decomposed into more shares. Specific shares are overlapped to obtain a *key* share that is finally combined with the final share to reveal the secret image. The recovery process involves overlapping the *key* share with the share held by a user as shown in Figure 8. HVC is suitable for authentication systems because it is difficult for any intruder to obtain the shares. However, it suffers from high memory complexity. Other researchers have also proposed HVC schemes for applications such as an image cryptosystem [80] and biometric authentication systems [81, 82].

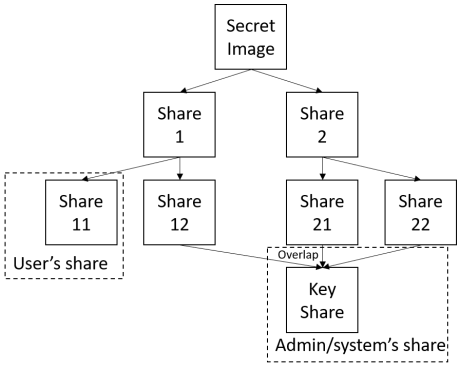

Fig. 8 Hierarchical VC.

VC for general access (GAS) is a scheme pioneered by Ateniese et al. in [83]. They extended the (k, n)-threshold access structure to GAS in the form of $(\Gamma_{Qual}, \Gamma_{Forb}, m)$, where Γ_{Qual} denotes a set of qualified sets, Γ_{Forb} denotes a set of forbidden sets, and m is the pixel expansion parameter. Any qualified set $Q \in \Gamma_{Qual}$ can recover the secret image, whereas any forbidden set $F \in \Gamma_{Forb}$ cannot leak out any secret information. The main purpose of forbidden sets is to prevent an adversary from obtaining information about the secret image from any single share. The advantage of GAS is the ability to grant different levels of access to participants. Given a simple scenario whereby a company comprises of one owner, one supervisor, and two employees, GAS can be used to ensure that employees can never recover the secret by themselves, the supervisor can only recover the secret with an employee, whereas the owner can recover the secret with any one of his colleagues. However, the main drawback of GAS is memory complexity [84]. The ability to assign permission levels to shares have also been previously addressed in the weight-based scheme proposed in [36] and the (t, k, n) scheme in [71].

3.2.3 Number of Secrets

[85] proposed a multiple secret sharing scheme that can hide more than one piece of information within a set of shares, which we refer to as dynamic VC (DVC). The secret image is first encrypted into many shares. The two shares are overlapped top of each other to divulge the first secret image. The shares (which are circular in appearance), can be rotated in specific angles to reveal other shares. The scheme was shown to have good performance in terms of the quality of the recovered image [86]. Another DVC using random grid was proposed in [87]. In this scheme, more secrets can be revealed by overlapping folded shares. Other researchers also proposed DVC scheme for assessing chaotic oscillations [88]. In addition to being able to protect multiple secrets, another advantage of DVC is that its recovered images have high contrast but it suffers from high memory complexity which reduces its effectiveness for real-time applications [89].

Flip-based visual cryptography (FVC) encodes two secret images into share images. FVC was pioneered by Lin et al. in [60]. In FVC, a pair of shares contains pixel information from two secret images. Overlapping the two shares produces the first secret image, whereas flipping one of the shares prior to overlapping them will produce the second secret image. As previously discussed, [59] later improved upon this FVC scheme to support meaningful shares. Apart from being able to support multiple secrets, FVC also has optimal contrast and enhanced security but suffers from the same high memory disadvantage as many VC schemes.

A recursive threshold VC (RTVC) scheme was proposed in [90]. Each share contains at most $\frac{1}{k}$ bits of secrets. The idea is that smaller secrets can be hidden in shares of larger secrets with secret sizes doubling at every step. RTVC can be used to embed invisible watermarks, convey secret keys or encode authentication information when used in network applications. RTVC produces high quality recovered images but at the cost of higher memory complexity.

[91] extended the basic hierarchical VC scheme to not only generate shares in a hierarchical manner but also to support multiple secret images. They managed to increase the number of secrets without increasing pixel expansion. In addition,

their scheme is resistant to share tampering. Another scheme that supports multiple secret images is the one proposed in [92] which embeds both secrets within the same set of shares. When at least 2 shares are combined (either via OR or XOR operations), both secret images are revealed at the same time. The scheme achieves perfect visual quality when the XOR operation is used for recovery.

4 Comparison of Visual Cryptography Schemes

In this section we will perform a comparison of various VC schemes in terms of the VC parameters mentioned in Section 2.1. First, we discuss the importance of the performance metrics that are shown in Table 1, specifically with regards to pixel expansion, number of shares, type of shares and number of secrets. Note that schemes that support meaningful shares can also be used for noise-like or meaningless shares. In addition, we also consider tagged shares as meaningful shares. PSNR values in the table are based on the differences between the original (secret) and recovered image.

One of the most important metrics for VC schemes is pixel expansion because it has a direct impact on the PSNR value. Reducing pixel expansion will lead to an improvement in PSNR [20]. A high PSNR value is desired because it implies that the recovered image is free from noise. Although there are schemes that already minimize or have no pixel expansion, these schemes suffer from disadvantages such as high computational and memory complexity. Thus, newer schemes are still required to fulfill all these requirements simultaneously.

Depending on the application, a higher number of shares can either be an advantage or disadvantage. For example, the scheme in [37] only has 2 shares, which is good for storage capacity (reduced memory requirement) as compared to the scheme in [62] which has 4 shares. However, having more shares leads to more flexibility as more parties can hold on to the shares. The best-case scenario would be to allow the user to specify the exact number of shares that they require without adversely affecting the visual quality of the recovered images.

On another hand, the format of the shares themselves plays an important role in terms of security, whereby meaningful shares are preferred because they can avoid detection [66] as compared to meaningless shares [111]. Meaningful shares or tagged shares also makes the management of shares easier. Thus, deciding on the number or type of share is highly dependent on the application that uses VC. As illustrated in Table 1 most schemes that have a flexible number of shares only support meaningless shares, with the exception of [58] and [76].

The number of secrets parameter is related to the flexibility of a scheme. If a VC scheme can encrypt multiple secret images in a set of shares, it has the potential to be applied in more areas. Traditional VC schemes like the one proposed in [1] generally only encrypt one secret image. In contrast, the scheme in [95] can encrypt multiple secrets but suffers an alignment limitation due to its circular shares. Knowledge of the correct alignment points is vital for successful decryption in addition to knowing how many secrets are hidden within the shares. If too many secrets are concealed, the rotation angle may be too small to successfully extract all the secrets. We note that there seems to be a lack of schemes that can support both a flexible number of shares and multiple secrets. Out of all the schemes covered in Table 1, only the scheme in [108] fulfills this requirement but is limited

Table 1 Analysis of VC schemes according to VC metrics.

ine Ref.	Shares	Secrets	PSNR	Image	Share Type
ine [1]	2	Single	Low	Binary	Meaningless
[49]	2	Single	Low	Color	Meaningless
[93]	2	Single	High	Color	Meaningful
[23]	2	Multiple	High	Color	Meaningful
[62]	4	Multiple	High	Color	Meaningful
[94]	2	Single	High	Color	Meaningful
[95]	2	Multiple	Low	Grayscale	Meaningless
[66]	2	Multiple	High	Color	Meaningful
[96]	2	Single	Low	Grayscale	Meaningless
[81]	2	Single	Low	Binary	Meaningless
[97]	2	Multiple	High	Grayscale	Meaningful
[98]	2	Single	Low	Binary	Random
[37]	2	Single	Low	Grayscale	Random
[50]	2	Single	High	Grayscale	Meaningful
[99]	2	Multiple	Low	Grayscale	Random
[22]	2	Single	High	Color	Meaningful
[100]	2	Single	Low	Binary	Meaningless
[101]	2	Single	Low	Color	Meaningless
[15]	2	Single	Low	Grayscale	Meaningless
[102]	2	Single	Low	Color	Meaningless
[103]	2	Single	Low	Binary	Meaningless
[20]	2	Single	High	Color	Meaningless
[104]	2	Single	High	Color	Meaningless
[105]	2	Single	Low	Binary	Meaningless
[106]	n	Single	Low	Color	Meaningless
[107]	2	Single	Low	Color	Meaningless
[80]	2	Single	Low	Color	Meaningless
[54]	n	Single	High	Color	Meaningless
[108]	n	Multiple	High	Binary	Meaningless
[109]	2	Single	Low	Binary	Meaningless
[110]	2	Single	High	Color	Meaningless
[52]	2	1	-	Color	Meaningless
[48]	n	1	Low	Grayscale	Meaningless
[36]	n	1	-	Binary	Meaningless
[42]	n	2	High	Binary	Meaningless
[59]	2	2	High	Grayscale, Color	Meaningful
[65]	n	1	-	Color	Meaningful
[58]	3	1	High	Grayscale	Meaningful
[68]	2	1	-	Binary	Meaningless
[44]	2	1	-	Binary	Meaningless
[53]	2	1	High	Color	Meaningless
[91]	5	2	-	Grayscale	Meaningless
[71]	n	1	-	Binary	Meaningless
[76]	n	1	High	Binary	Meaningful
[78]	n	1	High	Binary	Meaningless
[92]	3	2	High	Binary	Meaningless
ine					

to binary images. Unfortunately, none of the reviewed VC schemes have both these features in addition to meaningful shares.

In Tables 2 to 4, a comparison of the advantages and disadvantages of the VC schemes is presented. We select several main features that are common to all schemes for comparison purposes, which includes:

- Contrast
- Recovered image quality
- Security
- Computational complexity
- Memory complexity
- Pixel expansion
- Share type/flexibility

We quantify the security of a VC scheme based on correlation coefficients and histogram estimations that shows how well the share creation scheme preserves the confidentiality of the secret image. The security metric can also be measured by the PSNR metric which represents the relationship between an original image and share images. Thus, low PSNR values, low correlation between shares and secret image, and evenly distributed histograms imply higher security and stronger encryption. Certain schemes can achieve good contrast (a large relative difference in color tones) but still have poor recovered image quality due to background noise. Pixel expansion will be listed as an advantage for schemes that achieve low (<2) pixel expansion. Pixel expansion of ≥ 2 is categorized as a disadvantage.

The main issue that seems to affect most schemes is computational complexity and memory complexity, especially when the scheme includes other desirable features. One notable observation is that there is a trade-off between the quality of recovered image and computational/memory complexity. Schemes that achieve a good quality of recovered image suffer from high computational or memory complexity [18,20,104] whereas schemes that are computationally efficient have recovered images that have poor contrast or resolution [46,112]. Apart from decryption quality, schemes that support meaningful shares also generally have complexity issues [59,65,68].

Quite a number of VC schemes have addressed pixel expansion, notably within the past 3 years [36,52,44,59,68]. However, this is at the expense of increased computational or memory complexity. Another interesting point to note is that most of the recently proposed schemes are delving into other functionalities of VC which include assigning permissions, supporting meaningful shares, progressive recovery and multiple secrets rather than improving the performance of the classical schemes.

5 Conclusion and Future Work

5.1 Open Problems and Research Directions

In recent years, a lot of research effort has been dedicated towards VC. Despite the advancements that have been achieved, VC still has some significant drawbacks that prevent its adoption in real life applications. To overcome these issues, one possible research direction would be to examine and improve existing schemes for

Table 2 Comparison of VC schemes.

ine Ref.	Description	Advantage(s)	Disadvantage(s)
ine [104]	(n, n) threshold non-expansible XOR-based VC	Contrast	Memory complexity, pixel expansion
[18]	CVC without pixel expansion with gray wolf optimization	Recovered image quality, pixel expansion	Computational complexity
[20]	CVC using Elliptic Curve Cryptography	Recovered image quality	Memory complexity, pixel expansion
[112]	CVC for banking applications	Computational complexity	Pixel expansion, recovered image quality
[106]	(k, n) CVC	Contrast	Pixel expansion, recovered image quality
[30]	Random grid VC	Contrast	Pixel expansion, recovered image quality
[46]	VC for greyscale images	Computational complexity	Pixel expansion, recovered image quality
[113]	Extended CVC	Meaningful shares	Memory complexity, pixel expansion, recovered image quality
[104]	XOR-based VC	Recovered image quality	Memory complexity, pixel expansion
[114]	(k, n) region incrementing scheme	Contrast	Memory complexity, pixel expansion
[84]	Extended Visual Cryptography General Access Structures	Security	Memory complexity, pixel expansion
[115]	Error filtering schemes for CVC	Security	Pixel expansion, recovered image quality
[33]	Random Grid VC	Recovered image quality	Memory complexity, pixel expansion
[101]	Extended VC using halftoning	Security	Recovered image quality, pixel expansion
[116]	Progressive VC with unexpanded shares	Pixel expansion, progressive recovery	Memory complexity

ine

Table 3 Comparison of VC schemes (cont.).

ine Ref.	Description	Advantage(s)	Disadvantage(s)
ine [24]	VC for multiple secrets without pixel expansion	Pixel expansion, recovered image quality	Memory complexity
[117]	Threshold VC	Security, recovered image quality	Memory complexity, pixel expansion
[66]	Extended CVC Using Error Diffusion	Recovered image quality	Memory complexity, pixel expansion
[61]	CVC with meaningful shares	Contrast	Memory complexity, pixel expansion
[22]	Embedded extended CVC	Recovered image quality	Memory complexity, pixel expansion
[118]	Halftone VC for greyscale images using error diffusion	Quality of recovered image	Memory complexity, pixel expansion
[105]	VC based on DNA microarrays	Security	Computational complexity, pixel expansion
[106]	(k, n) threshold-based VC with multiple decryptions	Computational complexity	Memory complexity, pixel expansion
[80]	Hierarchical VC	Recovered image quality	Memory complexity, pixel expansion
[93]	VC based on derivative polynomials	Quality of recovered image	Computational cost, pixel expansion
[54]	VC with ant colony optimization	Recovered image quality	Memory complexity, pixel expansion
[108]	Random grid VC with multiple secrets	Security	Memory complexity, pixel expansion
[74]	Progressive VC	Contrast	Computational cost, pixel expansion
[110]	VC with homomorphic encryption	Recovered image quality	Memory complexity, pixel expansion
[52]	$(2, 2)$ CVC	Security, pixel expansion	Computational complexity, recovered image quality

ine

Table 4 Comparison of VC schemes (cont.).

ine Ref.	Description	Advantage(s)	Disadvantage(s)
ine [48]	(k, n) threshold CVC	Contrast, security	Computational complexity, pixel expansion, recovered image quality
[36]	Weighted (k, n) threshold VC	Contrast, pixel expansion	Computational complexity, recovered image quality
[42]	Probabilistic VC based on CBW	Contrast, security, contrast	Computational complexity, pixel expansion, recovered image quality
[59]	Flip EVC for grayscale and color images	Meaningful shares, pixel expansion, security, recovered image quality	Computational complexity
[65]	EVC	Meaningful shares, security	Computational complexity, pixel expansion, recovered image quality
[58]	Meaningful shares, recovered image quality, security	Memory complexity, pixel expansion	
[68]	Threshold tagged VC	Contrast, meaningful shares (tags), pixel expansion, recovered image quality, security	Computational complexity
[44]	XOR-based threshold VC	Adjustable pixel expansion, contrast, security	Recovered image quality
[53]	VC with chaotic encryption	Recovered image quality, security	Computational complexity, memory complexity, pixel expansion
[91]	HVC for multiple secrets	Contrast, multiple secrets, security	Memory complexity, pixel expansion, recovered image quality
[71]	(t, s, k, n) VC	Contrast, recovered image quality, security	Memory complexity, pixel expansion
[76]	Progressive EVC	Meaningful shares, progressive recovery, recovered image quality	Memory complexity, pixel expansion
[78]	Block-based progressive VC	Progressive recovery, security	Memory complexity, pixel expansion, recovered image quality
[92]	(2,3) VCS	Contrast, multiple secrets, pixel expansion, recovered image quality (XOR recovery)	Memory complexity
ine			

specific types of images [119] or specific applications. Rather than trying to optimize a trade-off between the various requirements, work can be done to leverage upon the existing advantages of certain VC schemes and apply them to suitable real-life problems that may not be affected by the schemes' disadvantages.

One of the main open problems in VC is pixel expansion which reflects negatively on the quality of reconstructed image. Schemes that address the pixel expansion property are still too inefficient or costly for real-life applications. Minimizing pixel expansion will directly impact the practicality of a VC scheme. A VC scheme that produces shares that are closer to the original image sizes will incur lower transmission and storage costs. To achieve a suitable trade-off in terms of reconstructed image quality, efficiency, and pixel expansion, the use of optimization algorithms can be further explored to be integrated into VC schemes or to select encryption parameters.

Although there are schemes that are able to encrypt multiple secrets, they are either inefficient or are difficult to use [86, 87, 88, 89, 60, 90, 120]. For example, schemes that involve rotating shares may lead to decryption errors when the rotation angles are inaccurate [85]. Schemes that do not need rotation or flipping consists of many shares that lead to higher memory complexity [90, 120]. More research to enhance multiple-secret VC schemes to balance usability and efficiency is still required.

As mentioned in Section 4, recent work in the area focus on other functionalities of VC rather than addressing performance issues of classical schemes. Future research can still consider improving classical schemes by optimizing the trade-off between the various desirable parameters such as pixel expansion, quality of recovered image, computational and memory complexity. Improving these basic requirements will contribute towards other schemes as well as VC's feasibility for real-life applications. In addition, there is also a lack of VC schemes that can support a combination of n shares, multiple secrets, color secret images and meaningful shares. In short, the following research directions can be considered for future work:

1. Leveraging upon specific features of VC schemes for targeted real-life applications
2. Addressing the trade-off between pixel expansion and computational/memory complexity
3. Improving the efficiency of VC schemes that support multiple secrets or progressive recovery
4. Designing efficient VC schemes that support two or more desirable features, including multiple shares, multiple secrets, color images and meaningful shares

5.2 Closing Remarks

This paper has provided an overview of the various categories of VC techniques, their performance metrics, and recently proposed schemes. The merits and demerits of the reviewed VC schemes and their applications were analyzed in detail. Based on the findings, we found that there exists a trade-off between recovered image quality and the computational or memory complexity of the VC schemes. VC schemes that have low complexity lead to lower reconstructed image quality and

vice versa. Other problems within VC that still needs to be addressed includes efficient encryption of multiple secrets and addressing the problem of pixel expansion. Further improvements can be achieved through the use of optimization algorithms or designing schemes for specific real-life applications. Overall, VC has great potential for applications in various areas such as identification and authentication. However, its drawbacks need to be addressed through further research and development before the schemes can be utilized in practice. This survey has highlighted several areas of interest within VC that will hopefully aid future researchers in advancing VC towards practical adoption.

Acknowledgements This is a preprint of an article published in Multimedia Tools and Applications. The final authenticated version is available online at https://doi.org/10.1007/s11042-021-11229-9. This work is supported in part by the Ministry of Education (MOE) Malaysia under the Fundamental Research Grant Scheme (FRGS), project number FRGS/1/2019/ICT05/USM/02/1.

References

1. Naor, M., Shamir, A.: Visual cryptography. In: Advances in Cryptology - EUROCRYPT'94, pp. 1–12. Springer Berlin Heidelberg (1995). DOI 10.1007/bfb0053419
2. Weir, J., Yan, W.: A comprehensive study of visual cryptography. In: Transactions on Data Hiding and Multimedia Security V, pp. 70–105. Springer Berlin Heidelberg (2010). DOI 10.1007/978-3-642-14298-7_5
3. Saturwar, J.H., Chaudhari, D.N.: Review of models, issues and applications of digital watermarking based on visual cryptography. In: 2017 International Conference on Inventive Systems and Control (ICISC). IEEE (2017). DOI 10.1109/icisc.2017.8068588
4. Tuyls, P., Kevenaar, T., Schrijen, G.J., Staring, T., van Dijk, M.: Visual crypto displays enabling secure communications. In: Security in Pervasive Computing, pp. 271–284. Springer Berlin Heidelberg (2004). DOI 10.1007/978-3-540-39881-3_23
5. Haouzia, A., Noumeir, R.: Methods for image authentication: a survey. Multimedia Tools and Applications **39**(1), 1–46 (2007). DOI 10.1007/s11042-007-0154-3
6. Pandey, A., Som, S.: Applications and usage of visual cryptography: A review. In: 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO). IEEE (2016). DOI 10.1109/icrito.2016.7784984
7. Chavan, P.V., Atique, M., Malik, L.: Signature based authentication using contrast enhanced hierarchical visual cryptography. In: 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science. IEEE (2014). DOI 10.1109/sceecs.2014.6804453
8. Roy, S., Venkateswaran, P.: Online payment system using steganography and visual cryptography. In: 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science. IEEE (2014). DOI 10.1109/sceecs.2014.6804449
9. Thomas, S.A., Gharge, S.: Review on various visual cryptography schemes. In: 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC). IEEE (2017). DOI 10.1109/ctceec.2017.8455136
10. Punithavathi, P., Geetha, S.: Visual cryptography: A brief survey. Information Security Journal: A Global Perspective **26**(6), 305–317 (2017). DOI 10.1080/19393555.2017.1386249
11. Chanu, O.B., Neelima, A.: A survey paper on secret image sharing schemes. International Journal of Multimedia Information Retrieval **8**(4), 195–215 (2018). DOI 10.1007/s13735-018-0161-3
12. Bhatnagar, R., Kumar, M.: Visual Cryptography: A literature survey. In: 2018 Second INternational Conference on Electronics, Communication and Aerospace Technology (ICECA). IEEE. DOI 10.1109/ICECA.2018.8474649
13. Bonis, A.D., Santis, A.D.: Randomness in secret sharing and visual cryptography schemes. Theoretical Computer Science **314**(3), 351–374 (2004). DOI 10.1016/j.tcs.2003.12.018

14. Ramya, J., Parvathavarthini, B.: An extensive review on visual cryptography schemes. In: 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT). IEEE (2014). DOI 10.1109/iccicct.2014.6992960
15. Shyu, S.J., Chen, M.C.: Minimizing pixel expansion in visual cryptographic scheme for general access structures. IEEE Transactions on Circuits and Systems for Video Technology **25**(9), 1557–1561 (2015). DOI 10.1109/tcsvt.2015.2389372
16. Naor, M., Shamir, A.: Visual cryptography II: Improving the contrast via the cover base. In: Security Protocols, pp. 197–202. Springer Berlin Heidelberg (1997). DOI 10.1007/3-540-62494-5_18
17. Amitharaja, R., Shaik, A., Thanikaise, V.: Data security through data hiding in images: A review. Journal of Artificial Intelligence **10**(1), 1–21 (2016). DOI 10.3923/jai.2017.1.21
18. Shankar, K., Eswaran, P.: Sharing a secret image with encapsulated shares in visual cryptography. Procedia Computer Science **70**, 462–468 (2015). DOI 10.1016/j.procs.2015.10.080
19. Abraham, A.S., Nair, L.R., Deepa, M.S.: A novel method for evaluation of visual security of images. In: 2017 International Conference on Networks & Advances in Computational Technologies (NetACT). IEEE (2017). DOI 10.1109/netact.2017.8076801
20. Shankar, K., Eswaran, P.: RGB-based secure share creation in visual cryptography using optimal elliptic curve cryptography technique. Journal of Circuits, Systems and Computers **25**(11), 1650,138 (2016). DOI 10.1142/s0218126616501383
21. Yang, C.N., Chen, P.W., Shih, H.W., Kim, C.: Aspect ratio invariant visual cryptography by image filtering and resizing. Personal and Ubiquitous Computing **17**(5), 843–850 (2012). DOI 10.1007/s00779-012-0535-0
22. Deepa, A.K., Bento, B.: Embedded extended visual cryptography scheme for color image using ABC algorithm. In: 2014 12th International Conference on Signal Processing (ICSP). IEEE (2014). DOI 10.1109/icosp.2014.7015084
23. Chen, J., Chen, T.S., Hsu, H.C., Lin, Y.H.: Using multi-ringed shadow image of visual cryptography to hide more secret messages. The Imaging Science Journal **57**(2), 101–108 (2009). DOI 10.1179/174313108x384656
24. R: A novel visual secret sharing scheme for multiple secrets via error diffusion in halftone visual cryptography. In: 2011 International Conference on Recent Trends in Information Technology (ICRTIT). IEEE (2011). DOI 10.1109/icrtit.2011.5972436
25. Shankar, K., Eswaran, P.: A new k out of n secret image sharing scheme in visual cryptography. In: 2016 10th International Conference on Intelligent Systems and Control (ISCO). IEEE (2016). DOI 10.1109/isco.2016.7726969
26. Borchert, B.: Segment-based Visual Cryptography. Tech. Rep. WSI-2007-04, WSI Institute for computer science (2007)
27. Punithavathi, P., Geetha, S.: Cancelable biometric template security using segment-based visual cryptography. In: Advances in Intelligent Systems and Computing, pp. 511–521. Springer Singapore (2016). DOI 10.1007/978-981-10-2104-6_46
28. Chaturvedi, A., Bhat, I.J.: Analysis of schemes proposed for improving the segment based visual cryptography. International Journal of Computer Trends and Technology **30**(1), 26–30 (2015). DOI 10.14445/22312803/ijctt-v30p105
29. Kafri, O., Keren, E.: Encryption of pictures and shapes by random grids. Optics Letters **12**(6), 377 (1987). DOI 10.1364/ol.12.000377
30. Yan, X., Wang, S., Niu, X., Yang, C.N.: Generalized random grids-based threshold visual cryptography with meaningful shares. Signal Processing **109**, 317–333 (2015). DOI 10.1016/j.sigpro.2014.12.002
31. Chao, H.C., Fan, T.Y.: Random-grid based progressive visual secret sharing scheme with adaptive priority. Digital Signal Processing **68**, 69–80 (2017). DOI 10.1016/j.dsp.2017.05.009
32. Chao, H.C., Fan, T.Y.: Generating random grid-based visual secret sharing with multi-level encoding. Signal Processing: Image Communication **57**, 60–67 (2017). DOI 10.1016/j.image.2017.05.005
33. Pang, L., Miao, D., Lian, C.: User-friendly random-grid-based visual secret sharing for general access structures. Security and Communication Networks **9**(10), 966–976 (2015). DOI 10.1002/sec.1392
34. Joshi, A.M., Jadhav, D.M., Kazi, N.A., Suryawanshi, A.N., Katti, J.: Authentication of grayscale forensic image using visual secret sharing. In: 2016 Conference on Emerging Devices and Smart Systems (ICEDSS). IEEE (2016). DOI 10.1109/icedss.2016.7587784

35. Jena, D., Jena, S.K.: A novel visual cryptography scheme. In: 2009 International Conference on Advanced Computer Control. IEEE (2009). DOI 10.1109/icacc.2009.109
36. Yan, X., Liu, F., Yan, W.Q., Yang, G., Lu, Y.: Weighted visual cryptographic scheme with improved image quality **79**(29-30), 21,345–21,360. DOI 10.1007/s11042-020-08970-y
37. Prisco, R.D., Santis, A.D.: On the relation of random grid and deterministic visual cryptography. IEEE Transactions on Information Forensics and Security **9**(4), 653–665 (2014). DOI 10.1109/tifs.2014.2305574
38. Ito R., K.H., Tanaka, H.:). image size invariant visual cryptography. . IEICE transactions on fundamentals of electronics, communications and computer sciences **22**(10), 3830–3841 (1999). DOI 10.1109/tip.2013.2262290
39. Yang, C.N., Chen, T.S.: Reduce shadow size in aspect ratio invariant visual secret sharing schemes using a square block-wise operation. Pattern Recognition **39**(7), 1300–1314 (2006). DOI 10.1016/j.patcog.2006.01.013
40. Yang, C.N.: New visual secret sharing schemes using probabilistic method. Pattern Recognition Letters **25**(4), 481–494 (2004). DOI 10.1016/j.patrec.2003.12.011
41. Yang, C.N., Wu, C.C., Wang, D.S.: A discussion on the relationship between probabilistic visual cryptography and random grid. Information Sciences **278**, 141–173 (2014). DOI 10.1016/j.ins.2014.03.033
42. Wu, X., Yang, C.N.: Probabilistic color visual cryptography schemes for black and white secret images **70**, 102,793. DOI 10.1016/j.jvcir.2020.102793
43. Prisco, R.D., Santis, A.D.: Color visual cryptography schemes for black and white secret images **510**, 62–86. DOI 10.1016/j.tcs.2013.09.005
44. Guo, Y., Jia, X., Chu, Q., Wang, D.: A novel XOR-based threshold visual cryptography with adjustable pixel expansion **10**(4), 1321. DOI 10.3390/app10041321
45. Myodo, E., Takagi, K., Miyaji, S., Takishima, Y.: Halftone visual cryptography embedding a natural grayscale image based on error diffusion technique. In: Multimedia and Expo, 2007 IEEE International Conference on. IEEE (2007). DOI 10.1109/icme.2007.4285100
46. Blesswin, A.J., Visalakshi, P.: An improved grayscale visual secret sharing scheme for visual information security. In: 2013 Fifth International Conference on Advanced Computing (ICoAC). IEEE (2013). DOI 10.1109/icoac.2013.6922012
47. Yang, C.N., Wu, X., Chou, Y.C., Fu, Z.: Constructions of general (k,n) reversible AMBTC-based visual cryptography with two decryption options **48**, 182–194. DOI 10.1016/j.jvcir.2017.06.012
48. Wu, X., Chen, D., Yang, C.N., Yang, Y.Y.: A (k,n) threshold partial reversible AMBTC-based visual cryptography using one reference image **59**, 550–562. DOI 10.1016/j.jvcir.2019.02.008
49. Hou, Y.C.: Visual cryptography for color images. Pattern Recognition **36**(7), 1619–1629 (2003). DOI 10.1016/s0031-3203(02)00258-3
50. Hou, Y.C., Lin, C.F., Chang, C.Y.: Visual cryptography for color images without pixel expansion. Journal of Technology **2**(4), 151 (2001). DOI 10.1049/iet-ifs:20080066
51. Al-Khalid, R.I., Al-Dallah, R.A., Al-Anani, A.M., Barham, R.M., Hajir, S.I.: A secure visual cryptography scheme using private key with invariant share sizes. Journal of Software Engineering and Applications **10**(01), 1–10 (2017). DOI 10.4236/jsea.2017.101001
52. Melgar, M.E.V., Farias, M.C.: A (2,2) XOR-based visual cryptography scheme without pixel expansion **63**, 102,592. DOI 10.1016/j.jvcir.2019.102592
53. Geetha, P., Jayanthi, V.S., Jayanthi, A.N.: Multiple share creation based visual cryptographic scheme using diffusion method with a combination of chaotic maps for multimedia applications **78**(13), 18,503–18,530. DOI 10.1007/s11042-019-7163-x
54. Mary, G.G., Rani, M.M.S.: Application of ant colony optimization for enhancement of visual cryptography images. In: Intelligent Systems Reference Library, pp. 147–163. Springer International Publishing (2018). DOI 10.1007/978-3-319-96002-9_6
55. Fathimal, M., Jansirani: New fool proof examination system through color visual cryptography and signature authentication. In: The International Arab Journal of In-formation Technology, pp. 322–336. Springer Berlin Heidelberg (2019). DOI 10.1007/bfb0052245
56. Dhiman, K., Kasana, S.S.: Extended visual cryptography techniques for true color images. Computers & Electrical Engineering **70**, 647–658 (2018). DOI 10.1016/j.compeleceng.2017.09.017
57. Ateniese, G., Blundo, C., Santis, A.D., Stinson, D.R.: Extended capabilities for visual cryptography. Theoretical Computer Science **250**(1-2), 143–161 (2001). DOI 10.1016/s0304-3975(99)00127-9

58. A, J.B., Raj, C., Sukumaran, R., G, S.M.: Enhanced semantic visual secret sharing scheme for the secure image communication **79**(23-24), 17,057–17,079. DOI 10.1007/s11042-019-7535-2
59. Wang, L., Yan, B., Yang, H.M., Pan, J.S.: Flip extended visual cryptography for grayscale and color cover images **13**(1), 65. DOI 10.3390/sym13010065
60. Lin, S.J., Chen, S.K., Lin, J.C.: Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion. Journal of Visual Communication and Image Representation **21**(8), 900–916 (2010). DOI 10.1016/j.jvcir.2010.08.006
61. Wu, H.C., Wang, H.C., Yu, R.W.: Color visual cryptography scheme using meaningful shares. In: 2008 Eighth International Conference on Intelligent Systems Design and Applications. IEEE (2008). DOI 10.1109/isda.2008.130
62. Kamath, M., Parab, A., Salyankar, A., Dholay, S.: Extended visual cryptography for color images using coding tables. In: 2012 International Conference on Communication, Information & Computing Technology (ICCICT). IEEE (2012). DOI 10.1109/iccict.2012.6398090
63. Sharma, H., Kumar, N., Jha, G.K.: Enhancement of security in visual cryptography system using cover image share embedded security algorithm (CISEA). In: 2011 2nd International Conference on Computer and Communication Technology (ICCCT-2011). IEEE (2011). DOI 10.1109/iccct.2011.6075137
64. Mousavi, S.M., Naghsh, A., Abu-Bakar, S.A.R.: Watermarking techniques used in medical images: a survey. Journal of Digital Imaging **27**(6), 714–729 (2014). DOI 10.1007/s10278-014-9700-5
65. Kukreja, S., Kasana, G., Kasana, S.S.: Extended visual cryptography-based copyright protection scheme for multiple images and owners using LBP–SURF descriptors DOI 10.1007/s00371-020-01883-9
66. Kang, I., Arce, G.R., Lee, H.K.: Color extended visual cryptography using error diffusion. IEEE Transactions on Image Processing **20**(1), 132–145 (2011). DOI 10.1109/tip.2010.2056376
67. Wang, R.Z., Hsu, S.F.: Tagged visual cryptography **18**(11), 627–630. DOI 10.1109/lsp.2011.2166543
68. Chiu, P.L., Lee, K.H.: Threshold visual cryptography schemes with tagged shares **8**, 111,330–111,346. DOI 10.1109/access.2020.3000308
69. Lin, H.C., Yang, C.N., Laih, C.S., Lin, H.T.: Natural language letter based visual cryptography scheme. Journal of Visual Communication and Image Representation **24**(3), 318–331 (2013). DOI 10.1016/j.jvcir.2013.01.003
70. Arumugam, S., Lakshmanan, R., Nagar, A.K.: On (k, n)∗-visual cryptography scheme **71**(1), 153–162. DOI 10.1007/s10623-012-9722-2
71. Li, P., Ma, J., Ma, Q.: (t, k, n) XOR-based visual cryptography scheme with essential shadows **72**, 102,911. DOI 10.1016/j.jvcir.2020.102911
72. Jin, D.: Progressive color visual cryptography. Journal of Electronic Imaging **14**(3), 033,019 (2005). DOI 10.1117/1.1993625
73. Fang, W.P.: Friendly progressive visual secret sharing. Pattern Recognition **41**(4), 1410–1414 (2008). DOI 10.1016/j.patcog.2007.09.004
74. Shivani, S., Agarwal, S.: VPVC: verifiable progressive visual cryptography. Pattern Analysis and Applications **21**(1), 139–166 (2016). DOI 10.1007/s10044-016-0571-x
75. Liu, G.Y., Li, Z.W., Barkaoui, K., Al-Ahmari, A.M.: Robustness of deadlock control for a class of petri nets with unreliable resources. Information Sciences **235**, 259–279 (2013). DOI 10.1016/j.ins.2013.01.003
76. Sridhar, S., Sudha, G.F.: Two in one image secret sharing scheme (TiOISSS) for extended progressive visual cryptography using simple modular arithmetic operations **74**, 102,996. DOI 10.1016/j.jvcir.2020.102996
77. Hou, Y.C., Quan, Z.Y., Tsai, C.F., Tseng, A.Y.: Block-based progressive visual secret sharing **233**, 290–304. DOI 10.1016/j.ins.2013.01.006
78. Yang, C.N., Lin, Y.C., Li, P.: Cheating immune k-out-of-n block-based progressive visual cryptography **55**, 102,660. DOI 10.1016/j.jisa.2020.102660
79. Chavan, P.V., Atique, M.: Design of hierarchical visual cryptography. In: 2012 Nirma University International Conference on Engineering (NUiCONE). IEEE (2012). DOI 10.1109/nuicone.2012.6493182
80. Das, S.S., Sharma, K.D., Chandra, J.K., Bera, J.N.: A hierarchical image cryptosystem based on visual cryptography and vector quantization. In: Advances in Intelligent Systems and Computing, pp. 3–11. Springer Singapore (2018). DOI 10.1007/978-981-13-1540-4_1

81. Chavan, P.V., Atique, M.: Secured approach for authentication using threshold-based hierarchical visual cryptography. International Journal of Information Privacy, Security and Integrity **2**(2), 159 (2015). DOI 10.1504/ijipsi.2015.075440
82. Kumar, M., Verma, H.K., Sikka, G.: A secure lightweight signature based authentication for cloud-IoT crowdsensing environments. Transactions on Emerging Telecommunications Technologies **30**(4), e3292 (2018). DOI 10.1002/ett.3292
83. Ateniese, G., Blundo, C., Santis, A.D., Stinson, D.R.: Visual cryptography for general access structures. Information and Computation **129**(2), 86–106 (1996). DOI 10.1006/inco.1996.0076
84. Lee, K.H., Chiu, P.L.: An extended visual cryptography algorithm for general access structures. IEEE Transactions on Information Forensics and Security **7**(1), 219–229 (2012). DOI 10.1109/tifs.2011.2167611
85. Hsu, H.C., Chen, J., Chen, T.S., Lin, Y.H.: Special type of circular visual cryptography for multiple secret hiding. The Imaging Science Journal **55**(3), 175–179 (2007). DOI 10.1179/174313107x176289
86. Feng, J.B., Wu, H.C., Tsai, C.S., Chang, Y.F., Chu, Y.P.: Visual secret sharing for multiple secrets. Pattern Recognition **41**(12), 3572–3581 (2008). DOI 10.1016/j.patcog.2008.05.031
87. Wang, R.Z.: Random grid-based visual cryptography with identifiable shares. Journal of Electronic Imaging **20**(1), 013,021 (2011). DOI 10.1117/1.3557792
88. Petrauskiene, V., Survila, A., Fedaravicius, A., Ragulskis, M.: Dynamic visual cryptography for optical assessment of chaotic oscillations. Optics & Laser Technology **57**, 129–135 (2014). DOI 10.1016/j.optlastec.2013.10.015
89. Palevicius, P., Ragulskis, M.: Image communication scheme based on dynamic visual cryptography and computer generated holography. Optics Communications **335**, 161–167 (2015). DOI 10.1016/j.optcom.2014.09.041
90. Parakh, A., Kak, S.: A recursive threshold visual cryptography scheme. Cryptologia **26**(1), 68–76 (2009). DOI 10.1080/0161-110291890768
91. Zhao, T., Chi, Y.: Hierarchical visual cryptography for multisecret images based on a modified phase retrieval algorithm **79**(17-18), 12,165–12,181. DOI 10.1007/s11042-020-08632-z
92. Li, P., Ma, J., Yin, L., Ma, Q.: A construction method of (2, 3) visual cryptography scheme **8**, 32,840–32,849. DOI 10.1109/access.2020.2973659
93. Wu, Z., Liu, Y.N., Wang, D., Yang, C.N.: An efficient essential secret image sharing scheme using derivative polynomial. Symmetry **11**(1), 69 (2019). DOI 10.3390/sym11010069
94. Kanakkath, P., Madathil, S., Krishnan, R.: Deterministic extended visual cryptographic schemes for general access structures with OR-AND and XOR-AND operations. Multimedia Tools and Applications **78**(2), 1315–1344 (2018). DOI 10.1007/s11042-018-6158-3
95. Fu, Z., Yu, B.: Research on rotation visual cryptography scheme. In: 2009 International Symposium on Information Engineering and Electronic Commerce. IEEE (2009). DOI 10.1109/ieec.2009.118
96. Hsu, S.F., Chang, Y.J., Wang, R.Z., Lee, Y.K., Huang, S.Y.: Verifiable visual cryptography. In: 2012 Sixth International Conference on Genetic and Evolutionary Computing. IEEE (2012). DOI 10.1109/icgec.2012.150
97. Askari, N., Heys, H.M., Moloney, C.R.: Novel visual cryptography schemes without pixel expansion for halftone images. Canadian Journal of Electrical and Computer Engineering **37**(3), 168–177 (2014). DOI 10.1109/cjece.2014.2333419
98. Lee, K.H., Chiu, P.L.: Image size invariant visual cryptography for general access structures subject to display quality constraints. IEEE Transactions on Image Processing **22**(10), 3830–3841 (2013). DOI 10.1109/tip.2013.2262290
99. Shyu, S.J., Huang, S.Y., Lee, Y.K., Wang, R.Z., Chen, K.: Sharing multiple secrets in visual cryptography. Pattern Recognition **40**(12), 3633–3651 (2007). DOI 10.1016/j.patcog.2007.03.012
100. Jana, B., Chowdhuri, P., auMadhumita Mallick, auShyamal Kumar Mondal: Cheating prevention in visual cryptography using steganographic scheme. In: 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT). IEEE (2014). DOI 10.1109/icicict.2014.6781367
101. Alex, N.S., Anbarasi, L.J.: Enhanced image secret sharing via error diffusion in halftone visual cryptography. In: 2011 3rd International Conference on Electronics Computer Technology. IEEE (2011). DOI 10.1109/icectech.2011.5941725

102. Dahat, A.V., Chavan., P.V.: Secret sharing based visual cryptography scheme us-ing cmy color space. Procedia Computer Science **78**, 550–555 (2016). DOI 10.1016/j.procs.2016.02.101
103. Kumar, H., Srivastava, A.: A secret sharing scheme for secure transmission of color images. In: 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT). IEEE (2014). DOI 10.1109/icicict.2014.6781393
104. Singh, P., Raman, B., Misra, M.: A (n, n) threshold non-expansible XOR based visual cryptography with unique meaningful shares. Signal Processing **142**, 301–319 (2018). DOI 10.1016/j.sigpro.2017.06.015
105. Zhang, X.: A visual cryptography scheme-based DNA microarrays. International Journal of Performability Engineering (2018). DOI 10.23940/ijpe.18.02.p14.334340
106. Wan, S., Lu, Y., Yan, X., Wang, Y., Chang, C.: Visual secret sharing scheme for (k, n) threshold based on QR code with multiple decryptions. Journal of Real-Time Image Processing **14**(1), 25–40 (2017). DOI 10.1007/s11554-017-0678-3
107. Yang, N., Gao, Q., Shi, Y.: Visual-cryptographic image hiding with holographic optical elements. Optics Express **26**(24), 31,995 (2018). DOI 10.1364/oe.26.031995
108. Salama, M.A., Mursi, M.F.M., Aly, M.: Safeguarding images over insecure channel using master key visual cryptopgraphy. Ain Shams Engineering Journal **9**(4), 3001–3013 (2018). DOI 10.1016/j.asej.2018.03.002
109. Hodeish, M.E., Humbe, V.T.: An optimized halftone visual cryptography scheme using error diffusion. Multimedia Tools and Applications **77**(19), 24,937–24,953 (2018). DOI 10.1007/s11042-018-5724-z
110. Shankar, K., Elhoseny, M., Kumar, R.S., Lakshmanaprabu, S.K., Yuan, X.: Secret image sharing scheme with encrypted shadow images using optimal homomorphic encryption technique. Journal of Ambient Intelligence and Humanized Computing (2008). DOI 10.1007/s12652-018-1160-1
111. Lu, J., Yang, Z., Li, L., Yuan, W., Li, L., Chang, C.C.: Multiple schemes for mobile payment authentication using QR code and visual cryptography. Mobile Information Systems **2017**, 1–12 (2017). DOI 10.1155/2017/4356038
112. Premkumar, S., Narayanan, A.E.: Notice of violation of IEEE publication principles - new visual steganography scheme for secure banking application. In: 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET). IEEE (2012). DOI 10.1109/icceet.2012.6203923
113. Askari, N., Heys, H.M., Moloney, C.R.: An extended visual cryptography scheme without pixel expansion for halftone images. In: 2013 26th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE). IEEE (2013). DOI 10.1109/ccece.2013.6567726
114. Yang, C.N., Shih, H.W., Wu, C.C., Harn, L.: k out of n region incrementing scheme in visual cryptography. IEEE Transactions on Circuits and Systems for Video Technology **22**(5), 799–810 (2012). DOI 10.1109/tcsvt.2011.2180952
115. Malar, S., Kumar, J.: Error filtering schemes for color images in visual cryptography. International Journal of Advanced Computer Science and Applications **2**(11) (2011). DOI 10.14569/ijacsa.2011.021112
116. Hou, Y.C., Quan, Z.Y.: Progressive visual cryptography with unexpanded shares. IEEE Transactions on Circuits and Systems for Video Technology **21**(11), 1760–1764 (2011). DOI 10.1109/tcsvt.2011.2106291
117. Chen, Q., Peng, W.F., Zhang, M., Chu, Y.P.: An (n, n) threshold visual cryptography scheme for cheating prevention. In: 2010 3rd International Conference on Computer Science and Information Technology. IEEE (2010). DOI 10.1109/iccsit.2010.5564954
118. Thomas, S.A., Gharge, S.: Halftone visual cryptography for grayscale images using error diffusion and direct binary search. In: 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI). IEEE (2018). DOI 10.1109/icoei.2018.8553863
119. Praun, E., Hoppe, H., Webb, M., Finkelstein, A.: Real-time hatching. In: Proceedings of the 28th annual conference on Computer graphics and interactive techniques - SIGGRAPH '01. ACM Press (2001). DOI 10.1145/383259.383328
120. Kumar, S., Sharma, R.K.: Recursive information hiding of secrets by random grids. Cryptologia **37**(2), 154–161 (2013). DOI 10.1080/01611194.2012.739585