Research Article

Quantitative Weighted Visual Cryptographic \((k, m, n)\) Method

Yewen Wu\(^1\), Shi Zeng\(^1,2,3\), Bin Wu\(^4\), Bin Yang\(^5\), and Xianyi Chen\(^3\)

\(^1\)Institute of Space Weather, Nanjing University of Information Science and Technology, Nanjing, China
\(^2\)College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China
\(^3\)School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, China
\(^4\)School of Computer and Big Data Science, Jiujiang University, Jiujiang, Jiangxi 332005, China
\(^5\)School of Design, Jiangnan University, Wuxi, China

Correspondence should be addressed to Xianyi Chen; 0204622@163.com

Received 19 March 2021; Accepted 11 May 2021; Published 28 May 2021

Academic Editor: Md. Hasanul Kabir

Copyright © 2021 Yewen Wu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The weighted visual cryptographic scheme (WVCS) is a secret sharing technology, where weights are assigned to each shadow (participant) according to its importance. Among WVCS, the random grid-based WVCS (RGWVCS) is a frequently visited subject. It considers the premise of equality of all participants, without taking into account the existence of privileged people in reality. To address this problem of RGWVCS, this paper designs a new model, named as \((k, m, n)\)-RGWVCS (where \(m < k < n\)), in which the secret is encrypted into \(n\) shares and sent to \(k\) participants. In the recovery end, the secret could be reconstructed by minimum \(m\) shares when the privileged join in; otherwise, \(k\) shares are needed. The experimental results show that our method has the advantage of no pixel expansion and no codebook design by means of random grid. Moreover, the contrast of our model increased by 32.85% on average compared with that of other WVCS.

1. Introduction

Visual cryptography scheme (VCS) sometimes also called visual secret sharing was formally proposed by Naor and Shamir at Eurocrypt’94 [1], in which they encrypt a binary secret image into multiple shares, and any qualified share combination can recover the hidden secret in the secret image, while any unqualified share combination cannot obtain any content related to the secret information. Here, the set of combinations that meet the conditions and combinations that do not meet the conditions are called a qualified set and a forbidden set, respectively, and the access structure consists of the pair of the qualified and forbidden sets. The \((k, n)\)-threshold scheme [2, 3] is a typical case of VCS, in which a binary secret image is encrypted into \(n\) shares. Any \(k\) or more shares, when superimposed, can reveal the secret image to the naked eye without any computations, while any \(k−1\) or less shares leak no information about the secret in an information-theoretic sense even with high-performance computing devices and technologies.

As can be seen from the \((k, n)\)-VCS, it encrypts a secret image into visual secret shares so that humans can reconstruct the secret directly with the naked eye without any cryptographic expertise or numerical computation by superposing a qualified visual sharing combination printed on a transparency.

Due to the high security and concealment of VCS, it is essential in the transmission of highly confidential information in a completely hostile channel. More precisely, the problem here is to transmit highly confidential information or authentication information through one or more insecure channels which are under full control of the adversary. Although the emergence of identity authentication technology has made a momentous contribution to keep the identity security, the fwlch or illegal decoding of smartcard and certificate will pose a high safety hazard. Therefore, the visual cryptography technology is combined with the identity authentication to store the shares generated when the identity information is encrypted in the authentication device and the database, respectively. The authentication of the user needs to be decrypted through the superposition of
the stored shares, while the attacker cannot obtain any valuable information of the secret image from the individual share through existing analytical methods, and it is impossible to decrypt by forging user shares. In uncontrolled channels, this problem is difficult to solve, and visual authentication [4] has been the main appropriate security solution up to now.

The loss of contrast and resolution of the secret image enables the VC to achieve security confidentiality, so in general, the quality of the secret recovered image is lower than that of the original secret image. With the gradual maturity of VC technology, efficiency and security have become the focus [5–7]. Scholars have attempted to enhance the contrast and resolution (visibility) of the reconstructed images. To alleviate the pixel expansion in the generated shares, several VCSs without pixel expansion were proposed previously. The VCS based on random grids (RGs) [8, 9] are characterized by no codebook design and no pixel expansion. The follow-up research work of RGVCS mainly focuses on a \((k, n)\) threshold [10] and improves image recovered quality [11]. Many other schemes were proposed to realize diversified visual sharing such as halftone secret images [12], grayscale secret images [13], and color secret images [14]. Moreover, some VC extension methods have also been proposed [11, 15, 16]. In terms of the functionality and security, how to share multiple secrets at one time [17–20] and prevent participants from cheating [21, 22] has become particularly significant in the past few years.

1.1. Related Works. Traditional VCSs mostly devote to optimizing the quality of secret recovered images [23], multilayer secret image encryption [17, 19], application of grayscale images and color images [8], and so on. Kannoja and Kumar [24] proposed a XOR-based \((n, n)\)-VCSXOR visual secret sharing scheme using pixel vectorization. The proposed scheme uses implicit codebook and pixel vectorization technology to directly encode the grayscale secret image without converting to a halftone image, which solves the problems of pixel expansion, contrast loss, clear codebook requirements, and restrictions on the number of participants. Shivani et al. [25–27] proposed a novel PVSS scheme based on an effective preprocessing method and a basic matrix creation algorithm, which has four or more amounts of space efficiency and meaningful shares. Many avoidable encryption restrictions are solved, and the human visual system can easily decrypt without any cryptographic calculations. Besides, Shivani S also proposed a novel multiple secret sharing scheme with unexpanded shares and meaningful shares, which can protect two secret images at once. The experimental results show that all meaningful shares meet the contrast and safety conditions. The secret image can be easily decoded by the human eye without any calculation [28]. However, traditional VCSs can only handle shares of the same weight and ignore the difference in the importance of shares. Therefore, this work considers a weighted VCS with privileged based on random grids, in which secret sharing participant acquires a share with different weights, respectively, according to the importance, and all the eligible participant combinations can recover the secret through the overlay of secret shares. So far, the following VCSs considering the weight difference have been proposed: the privilege-based visual secret sharing model (PVSSM) [29], \((2, n)\)-PVCS [30], random grid-based progressive visual secret sharing scheme with adaptive priority (RGPVSS) [31], and weighted \((k, n)\)-threshold visual cryptography method [32]. In most existing VCSs, each share has the same secret recovery capability. However, in the reality, some participants may enjoy privileges because of their importance or status, e.g., president of company, government official, and so on. Secret image recovery using traditional VCSs cannot highlight their privileges. Therefore, Hou et al. [29] proposed a novel secret sharing mechanism PVSSM that combines the concepts of progressiveness and privilege. In PVSSM, \(n\) participants with different privileges share a secret image. Set a privilege level \((PL) PL_i(1 \leq i \leq n)\) for each participant and create corresponding shares to participants based on the PL. The quality of the recovered secret image depends on the importance of all participants. Therefore, the higher the privilege level, the more secret information contained in the sharing, and the higher ability to recover the secret image. In this scheme, each share assigned to the participant has the same size as the secret image. PVSSM is capable of encrypting binary and halftone images and can clearly recover the secret information hidden in secret images. Compared with other relevant VCSs, the recovery image in this scheme has a superior contrast \((n – 2)/(n – 1)\). Although the method proposed by Hou et al. assigns different weights to different shares, it is only for the \((2, n)\) threshold. Different weights of shares lead to different average optical transmissions, resulting in the ability to visually distinguish shares, i.e., weight leakage.

To address the issue of weight leakage, Yang et al. [30] proposed a new \((2, n)\)-PVCS to solve the critical problems. This solution solves the problem that Hou et al.’s scheme is not a general solution to implement all PVCSs with arbitrary privilege level, i.e., it is the general solution of all \((2, n)\)-PVCS. The scheme also overcomes the problem of shadow whiteness inequality and provides the equal whiteness for each shadow. Unfortunately, the \((2, n)\)-PVCS proposed by Yang et al. requires codebook design. Then, Fan et al. [31] described a random grid-based progressive visual secret sharing scheme (RGPVSS). In this scheme, the priority weighting of each share can be adjusted, and the secret will be recovered gradually with the increase in the number of shares involved in secret recovery. Therefore, as the number of shares superimposed increases, the hidden information in the secret image will be recovered more and vice versa. As a result, each share with different priorities will be generated in this scheme. During secret recovery, the priority weight of the share superimposed determines the extent to which the secret image can be recovered. Each share generated in this scheme has no pixel extension and has the same size as the original secret image. The average light transmission of each share is 1/2, thus preventing the sharing of different priority weights from being discernible. Crucially, for this scheme, codebook design is not indispensable. Tu et al. [32] proposed a weighted \((k, n)\)-threshold nonexpanded visual secret sharing scheme. The secret image can be recovered when the
sum of the participant’s weights is not less than the threshold $k$. Unfortunately, the quality of the secret images recovered by the above scheme is not satisfactory. Yan et al. [33] proposed a weighted visual secret sharing scheme to improve the quality of secret restored images. Compared with other schemes, this scheme is mainly different from the generating mode of last $n \times k$ bits. Yan et al. [34] also proposed a VCS which the value of the last $n \times k$ bits is equal to the first $k$ bits. The contrast of the secret image recovered by this scheme is significantly improved. To the best of our knowledge, this scheme achieves the most satisfactory contrast in RG-based VCSs. However, although the contrast of the secret restored image is improved, the original secret image cannot be restored losslessly. In the military and medical fields, lossless recovery is essential for image transmission and storage [36]. The study of VCSs with lossless recovery capability has very profound implications. Therefore, this paper proposes a weighted VCS with privileged based on random grids, which not only overcomes a series of problems mentioned above but also achieves a lossless recovery of the secret image.

1.2. Our Contributions. In this paper, we propose a novel RGWVC method for a $(k, m, n)$ $(m < k)$ threshold. Compared with the basic WVCs, the proposed RGWVC considers the possible social stratum differences. In combination with the actual situation, the proposed scheme empowers the secret distributor to designate a privileged role among all the participants, in which the privileged has a greater power for secret recovery than the ordinary participant. Assuming that the privileged joins in the secret recovery, only $m$ shares are required, otherwise at least $k$ shares. More precisely, when privileged share participates in secret recovery, a minimum of $m$ participants is required. The innovation of this scheme compared with the preliminary scheme is that it not only assigns different weights to the participants based on their importance but also gives privilege to the significant shareholder in the secret sharing process.

Therefore, the proposed scheme can be better applied to practical models such as management pyramid, and the experimental results and the comparison with the existing schemes are shown that the scheme we designed has several highlights as follows: (1) no codebook design, (2) no pixel expansion, (3) no weight leakage, (4) a weighted VCS, (5) $(k, m, n)$ threshold, considering the existence of privileged role, is more applicable to the reality, and (6) improved image quality compared with relevant WVCs.

1.3. Organization. The rest of this paper is organized as follows. Section 2 reviews preliminaries on the basic WRGVCs. Section 3 presents a generic construction of the designed $(k, m, n)$-RGWVCs and discusses details and feasibility of the scheme. In Section 4, the experimental results are presented and analysed in the form of pictures and data. Besides, the scheme we designed is compared with several relevant VCSs from the aspects of contrast, pixel expansion, codebook design, and so on. Finally, conclusions and research issues are given in Section 5.

2. Preliminaries

In this section, we provide some preliminaries including background, definitions, notations, and conditions that will be used later. For more details about information theory and the definition of secret sharing, see, e.g., [36–38].

2.1. Weighted Random Grid-Based VCS (WRGVC) for a $(k, n)$ Threshold. The weighted random grid-based visual cryptographic scheme (WRGVC) is the basis of the proposed scheme. This method can assign weights to each participant of different importance so that each share has different ability to restore the secret image. Our visual cryptography scheme inherits the advantages of WRGVC and considers the possible privileged role in the reality, which increases the practicality of the scheme and makes it more comprehensive.

Suppose a binary secret image $S$ with a size of $H \times W$, the pixel value denotes $S(s, t)$ ($1 \leq s \leq H, 1 \leq t \leq W$), and the weighted values are $\omega = [\omega_1, \omega_2, \omega_3, \cdots, \omega_k]$ corresponding to participants $\{1, 2, \ldots, n\}$, where $\omega_1 + \omega_2 + \cdots + \omega_k = 1$. So, for each $s = 1, 2, 3 \ldots H; t = 1, 2, 3 \ldots W$, the WRGVC can be summarized as follows:

1. Randomly select $k$ order numbers from $\{1, 2, \ldots, n\}$ according to $\omega = [\omega_1, \omega_2, \omega_3, \cdots, \omega_k]$, denoted as $[i_1, i_2, \ldots, i_k]$, where the probability of selecting the $i$-th order number is $\omega_i, i = 1, 2, \ldots, n$.
2. Generate $b_1, b_2, \ldots, b_n \in \{0, 1\}$ randomly. If $S(s, t) \neq b_{i_1} \oplus b_{i_2} \oplus \cdots \oplus b_{i_k}$, select $p \in \{1, 2, \ldots, k\}$ randomly and update $b_{i_p}$ with $\overline{b_{i_p}}$, such that $S(s, t) = b_{i_1} \oplus b_{i_2} \oplus \cdots \oplus b_{i_k}$.
3. Set $b_{j_1} = b_{j_2} = \cdots = b_{j_k} = b_{j_{n-k}}$, where $\{j_1, j_2, \ldots, j_{n-k}\}$ is the difference set of $\{1, 2, \ldots, n\}$ and $\{i_1, i_2, \ldots, i_k\}$, and $x_q$ is randomly picked up from $\{1, 2, \ldots, k\}$, for $q = 1, 2, \ldots, n - k$.
4. Arrange $b_1, b_2, \ldots, b_n$ in order in the position $(s, t)$ of participant’s matrix $M_1, M_2, \ldots, M_n$.
5. Repeat the Steps 1–4 to fill in the above $n$ matrix $M_1, M_2, \ldots, M_n$, which is the $n$ shares.

2.2. Monte Carlo Method. Monte Carlo method is a numerical simulation method. It takes probabilistic phenomena as its research objective. In equipment effectiveness evaluation, it is often used to determine the efficiency index with random factors, such as the probability of discovery, the probability of hit, and the average number of damaged targets.

The simulation processes are described as follows. (1) Construct a simple and feasible stochastic or probabilistic model to describe the problem. The solution of the proposed problem is bound to some features of the random variables in the model (such as probability, mean value, and variance); (2) Generate a sufficient amount of random numbers according to the different distribution of each random variable in the stochastic or probabilistic model; (3) Design a sampling method suitable for the probabilistic model and random variable distribution; and (4)
According to the established model, the simulation test and calculation are carried out to obtain the random solution of the problem.

2.3. Indispensable Notations and Definitions. In this section, we will introduce some notations and definitions to prepare for the further work. Later, the symbols ⊗ and ⊕ represent the Boolean XOR and OR, while † represents a bitwise complementary operation of any binary bit b. In the visual secret sharing scheme, we generate n secret shares to hide the binary secret image S with size $H \times W$, defined as $\{M_1, M_2, \ldots, M_n\}$. The corresponding secret recovery image $S'$ is reconstructed from any $p (k \leq p \leq n, p \in \mathbb{Z}^+)$ shadows $\{M_{i_1}, M_{i_2}, \ldots, M_{i_p}\}$ by a superposing operation. The white and black areas of the secret image S are denoted as CS0 and CS1, respectively, where $\text{CS0} = \{(s, t) \mid S(s, t) = 0, 1 \leq s \leq H, 1 \leq t \leq W\}$ and $\text{CS1} = \{(s, t) \mid S(s, t) = 1, 1 \leq s \leq H, 1 \leq t \leq W\}$. For any pixel in S, $P(S) = 0$ represents that the probability of pixel color is transparent or white (0), whereas $P(S) = 1$ represents that the probability of pixel color is opaque or black (1). In addition, $P(S) = 0$ is 1 $P(S) = 1$ 1 $P(S) = 0$. Based on above notations, we will give the definition of contrast.

**Definition 1 (contrast).** The contrast can describe the quality of the recovered secret image, denoted as $\alpha$, as follows [34]:

$$\alpha = \frac{P_0 - P_1}{1 + P_1} = \frac{P(S' | \text{CS0}) = 0 - P(S' | \text{CS1}) = 0}{1 + P(S' | \text{CS1}) = 0},$$

(1)

where $P_0$ and $P_1$ denote the correctly and incorrectly revealed probabilities for the white and the black areas of $S'$, respectively, $\alpha \in [-0.5, 1]$, which is proportional to the quality of the secret restored image after superposition. In secret recovery, $\alpha = 0$ means $S'$ has nothing to do with S while $\alpha = 1$ indicates $S'$ is the same as S, a.k.a., S is lossless.

Figure 1 shows the change of contrast under different values of $P_0$ and $P_1$ in formula (1) by using the heatmap. It can be seen from the figure that the contrast is positively correlated with $P_0$ and negatively correlated with $P_1$. When $P_0 = 1$ and $P_1 = 0$, the contrast value is 1, indicating that the image is lossless. Therefore, contrast is a very convincing indicator used to evaluate the quality of $S'$ compared with S, and it is adopted to determine whether the naked eye can recognize the secret in the recovery image in this paper. For the different contrast ranges for different clarity, see [39].

2.4. Feasibility and Safety Conditions. In this part, we will introduce two necessary conditions to verify the feasibility and security of the proposed scheme, in terms of secure encryption and visual decryption.

In the visual cryptography scheme, the ultimate goal is to realize the visualization of secret under the condition of meeting the requirements of the scheme. Therefore, a qualified visual cryptography scheme must meet the following condition in visual recognition:

*Condition 1 (visually recognizable).* The recovery image $S'$ is visually recognizable ($\alpha > 0$) when $p \geq k$, a.k.a., $S'$ can visually recognize the same secret as S with sufficient shadows [1, 32]. In the visual cryptography scheme, the security of encrypted secret is of capital importance. Therefore, a secure visual cryptography scheme must meet the following condition in secret recovery.

*Condition 2 (security).* The secret recovery image $S'$ is visually unrecognizable ($\alpha = 0$) when $p < k$, a.k.a., $S'$ will not give away any information about the secret if there is not enough shadow overlay during the recovery process.

3. The Proposed $(k, m, n)$-RGWVCS

Based on the basic WRGVCS described in the previous section, we designed a new $(k, m, n)$-RGWVCS ($m < k$) that takes privileged role into account, in which the privileged people have a better decryption ability than nonprivileged. In the following section, we will first introduce the construction of $(k, m, n)$-RGWVCS, then analyse the advancement of the scheme, demonstrate its safety and feasibility, and finally analyse the application of the scheme in practice.

3.1. Construction of $(k, m, n)$-RGWVCS. The proposed $(k, m, n)$-RGWVCS ($1 \leq m \leq k < n$), considering the privileged in secret recovery, can be implemented by the combination of binary matrices $\{M_1, \ldots, M_n\}$ and weight of $n$ participants $\{ω_1, ω_2, \ldots, ω_n\}$ (where $ω_1 + ω_2 + \cdots + ω_n = 1$). There are $n$ participants involved in the VCS in all, and the addition of the privileged person allows the secret recovery to be completed with only $m$ participants, rather than at least $k$ participants in the conventional scheme. In this section, we will give a detailed description of the proposed algorithm and analyse its feasibility. Construction 1 shows the proposed $(k, m, n)$-RGWVCS, which satisfies Condition 1 and Condition 2.
**Construction 1.** For every pixel, assign the $n$ sharing matrices using the Monte Carlo method with $[0, 1]$ randomly. If the privileged is not considered, select $k$ or more matrices as the candidate of the secret recovery; otherwise, select $m$ or more shares matrices. Then, flip an element randomly if their superposition of these shares is not equal the secret pixel value. After the above operations, we will get the $n$ secret sharing matrices. The detailed steps are listed as Algorithm 1.

As can be seen from Figure 2, it provides a visual overview of the encryption and decryption secret image into $n$ subpixels and generates $n$ secret sharing matrices, while the right half discusses the different cases of pixel stacking and recovery. The secret sharing matrix and the secret image have the same attributes except the different distribution of pixel values. Different quality secret images can be recovered when the secret sharing matrix meets the quantity requirement.

3.2. Encryption of Single Pixel. After the overall grasp of the shadow encryption architecture in the previous section, this section will analyse the details of the right half of Figure 2. This part is mainly responsible for superimposing $n$ subpixels generated by each single pixel of $S$. In the ordinary VCS schemes, both the original secret and the generated share are data in numerical form, which are finally calculated and decrypted by the computer. In VCS schemes, however, both the original secret and the secret recovered by superposition are visible, i.e., the naked eye can decode directly. All black and white pixels in $S$ are encrypted into corresponding sets of black and white subpixels in secret shares. Therefore, each subpixel set is able to be denoted as a set of matrices $C_b = \{c_{ij}^b\}$ with $b \in \{0, 1\}$, where $b = 1$ represents black pixel and $b = 0$ otherwise and $c_{ij}^b = 1$ represents a black $j$-th strategy in the $i$-th share and $c_{ij}^b = 0$ otherwise.

For the sake of clarity, $(2, 2)$-threshold VCS is taken as an illustrative example where $S$ is encrypted into two shares. All the shares generated are noisy images, and so no secret information could be obtained. Nevertheless, when the generated two shares are superimposed, $S$ can be restored, and its construction method is as follows.

One black-white pixel $e$ is split from original image into two black-white subpixels. If $e$ is black (resp., white), then Strategy 1 or Strategy 2 in the lower (resp., upper) row of Table 1 is randomly selected, and the overlay of all subpixels is entirely black (resp., entirely white). As a result, the initial secret image can be capable of recovering lossless assuming that all shares are superimposed. This structure can be indicated as the sets $C_b^0$ and $C_b^1$ of matrices in Table 1; more specifically, the above encoding and decoding procedures can be indicated as the function $Enc: \{0, 1\} \rightarrow \{0, 1\}^{2 \times 1}$ and $Dec: \{0, 1\}^{2 \times 1} \rightarrow \{0, 1\}$ given by

$$Enc(b) = C_b^b \quad \text{and} \quad Dec(M) = (m_{i1} \oplus m_{i2})$$

for $b \in \{0, 1\}$ and $M = (m_{ij}) \in \{0, 1\}^{2 \times 2}$, respectively. From the function operation, we can see that when the XOR operation result is different from the original secret pixel, we only need to invert the pixel value of any secret sharing matrix. Therefore, in the initial generation of subpixels, we can randomly select the values without considering whether the results of all pixel XOR are correct. If the result of the pixel set XOR is not correct, take the reverse correction.

Pixel expansion refers to the number of subpixels in shares encrypted from a secret pixel. In the example above, each pixel in the secret image is encrypted as a subpixel in each share. Therefore, there is no pixel extension. The degree of pixel expansion is negatively correlated with the actual resolution of the share image. A VCS with the lowest pixel extension indicates that its encryption is optimal.

3.3. Instance of $(k, m, n)$-RGWVCS. Through the above analysis of the shadow encryption system, we can have a sense of the system. In this section, we will demonstrate the detailed process of encryption and decryption using an instance $(3, 2, 4)$-RGWVCS. Thus, we will have a clearer and more specific understanding of the shadow encrypting architecture. In the $(3, 2, 4)$-RGWVCS, the secret image needs to be encrypted into $4$ secret sharing matrices with the same size. During the decryption side, it requires at least $2$ shares to complete the secret recovery when the privileged participate in, whereas at least $3$ shares are required.

For each pixel of $S$, the same position of the $4$ secret sharing matrices, $[M_1, M_2, M_3, M_4]$, is randomly initialized to $0$ or $1$ by the Monte Carlo method, then $M_1 \oplus M_2 \oplus M_3 \oplus M_4$ is calculated, and it is compared with the pixel of $S$. If the comparison result is inconsistent, the random one of the four pixels is reversed. When all pixels of $S$ are handled, $4$ secret sharing matrices in the final form of noise are generated. Next, we will prove the feasibility of the Monte Carlo method (Analysis 1).

**Analysis 1.** In the proposed RGWVCS scheme, step 1 (initialize $n$ zero secret sharing matrices with weight $\omega_i$) satisfies the completely random fairness principle.

**Proof.** In the proposed scheme, we use the Monte Carlo method to achieve secret layering according to the weight, in which 1000 groups of random cast experiments are conducted on four targets with equal probability by the Monte Carlo method. The experimental results are listed in Figure 3.

The unit square plane in Figure 3 is divided into four areas with the same size: $S_1$, $S_2$, $S_3$, and $S_4$, and then 1000 points are scattered on the plane with equal probability. The dots are randomly placed in different regions, and the dots in different regions are assigned different colors. Through experiments and statistics, we can see the projection of 1000 points in the four regions in Figure 3(a) and its statistical results in Figure 3(b). The probability of hitting $S_1, S_2, S_3$, and $S_4$ is $25.9\%$, $24.7\%$, $25.7\%$, and $23.7\%$, respectively. When subtracted from the average, it was $+0.9\%$, $-0.3\%$, $+0.7\%$, and $-1.3\%$, respectively. From the above data analysis, we can draw a conclusion that the hit ratio of these four regions is nearly the same, indicating that in the designed RGWVCS scheme, the Monte Carlo method satisfies the completely random fairness principle.
Input: secret image $Q$ of size $H \times W$, $(k, m, n)$ and $\{\omega_1, \omega_2, \cdots, \omega_n\}$;  
Output: the $n$ secret sharing matrices \{M_1, M_2, \cdots, M_n\}.

(1) Initialize $n$ zero secret sharing matrices $M_i = \{m_i'(s, t) = 0|1 \leq s \leq H, 1 \leq t \leq W\}$ with weight $\omega_i$, ($i = 1, 2, \cdots, n$), i.e., the probability of $M_i$ participates in the secret recovery is $\omega_i$.

(2) For any pixel $m'(s, t)$ in $M_i$, assign $[0, 1]$ randomly to it using the Monte Carlo method.

(3) Assume the $p$-th participant is a privileged person. There are two cases as follows:

(a) If $M_p$ participates the secret recovery, select $j$ secret sharing matrices randomly, i.e., \{M_1, M_2, \cdots, M_j\} (1 \leq i \leq n, m \leq j \leq n);$(b) If $M_p$ is not involved the secret recovery, select $j$ secret sharing matrices randomly, i.e., \{M_1, M_2, \cdots, M_j\} (1 \leq i \leq n, k \leq j \leq n).

(4) Select $c \in \{1, 2, \cdots, j\}$ randomly and execute the following formula:

$m'_i(s, t) = m'_1(s, t)Q(s, t) = m'_1(s, t) \oplus m'_2(s, t) \oplus \cdots \oplus m'_j(s, t)$. $m'_i(s, t)$, otherwise.

(5) Generate $j$ secret sharing matrices \{M_1, M_2, \cdots, M_j\}.

(6) Repeat steps 2–5 ($s \cdot t$) times to generate $n$ secret sharing matrices \{M_1, M_2, \cdots, M_n\}.

Algorithm 1: $(k, m, n)$—RGWVCS.

Figure 2: Shadow encrypting architecture of the designed RGWVCS. The left half of the encryption architecture describes the generation process of the subpixel and encrypted secret sharing matrices, while the right half is the decryption process of secret sharing matrices.

Table 1: Encryption structure for a single black-white pixel, and the sets $\mathbb{B}^0$ and $\mathbb{B}^1$ represent matrices (row: share, column: strategy, 0: white, 1: black).

| Pixel | Share 1 | Strategy 1 | Share 2 | Strategy 2 | Subpixel matrix |
|-------|---------|------------|---------|------------|----------------|
| [ ]   |         | [ ]        |         | [ ]        | $\mathbb{B}^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ |
| [ ]   |         | [ ]        |         | [ ]        | $\mathbb{B}^1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ |

3.4. Feasibility and Safety Analysis. After the detailed introduction and analysis of the relevant algorithms, we will carry out theoretical analysis on the security and visual recognition of the designed scheme from Conditions 1 and 2.

Lemma 1. In the proposed $(k, m, n)$-RGWVCS from Construction 1, [0, 1] are assigned to \{m_1(s, t), m_2(s, t), \cdots, m_m(s, t)\} randomly in the third step. If $S'(s, t) = m_1(s, t) \oplus \cdots \oplus m_{k-1}(s, t)$, we can deduce $P(S'\mid CS0) = 0 = P(S'\mid CS1) = 0 = (1/2)^{k-1}$. 


Proof. In the proposed \((k, m, n)\)-RGWVCS from Construction 1, \([0, 1]\) are assigned to \(\{m_1'(s, t), m_2'(s, t), \ldots, m_n'(s, t)\}\) randomly using the Monte Carlo method in the third step. That means that the probability of \(m\) being equal to 0 and 1 is equivalent, i.e., \(P(m'(s, t) = 0) = P(m'(s, t) = 1) = 1/2\). The white areas of the secret image \(S\) are denoted as \(CS_0 = \{(s, t) | S(s, t) = 0, 1 \leq s \leq H, 1 \leq t \leq W\}\). Therefore, \(S'[CS_0] = S'(s, t) = m_1'(s, t) \otimes \cdots \otimes m_k'(s, t)\). Given that \(P(m'(s, t) = 0) = P(m'(s, t) = 1) = 1/2\), so \(P(S'[CS_0] = 0) = (1/2)^{k-1}\). By the same token, \(P(S[CS1] = 0) = (1/2)^{k-1}\).

Lemma 2. In the proposed \((k, m, n)\)-RGWVCS from Construction 1, if \(S(s, t) = 0\), \(P(m_1'(s, t) \otimes m_2'(s, t) \otimes \cdots \otimes m_k'(s, t) = 0) = P(m_1'(s, t) \otimes m_2'(s, t) \otimes \cdots \otimes m_k'(s, t) = 0) = (1/2)^{k-1}\). On the contrary, if \(S(s, t) = 1\), \(P(m_1'(s, t) \otimes m_2'(s, t) \otimes \cdots \otimes m_k'(s, t) = 0) = 0\).

Proof

(1) Firstly, when \(S(s, t) = 0\), we will prove the following:

\[
P\left(m_1'(s, t) \otimes \cdots \otimes m_k'(s, t) = 0\right) = P\left(m_1'(s, t) \otimes \cdots \otimes m_k'(s, t) = 0\right) = (1/2)^{k-1}.
\]

(4)

If \(m_k'(s, t) = 0\), then \(P(m_1'(s, t) \otimes \cdots \otimes m_k'(s, t) = 0) = P(m_1'(s, t) \otimes \cdots \otimes m_k'(s, t) = 0) = 0\) is set up because \(m_k'(s, t)\) is transparent and \(m_1'(s, t) \otimes \cdots \otimes m_k'(s, t) = 0\). Thus, \(m_1'(s, t) \otimes \cdots \otimes m_k'(s, t) = 0\). According to the third step, we have

\[
S(s, t) = m_1'(s, t) \otimes m_2'(s, t) \otimes \cdots \otimes m_k'(s, t).
\]

If \(m_k'(s, t) = 1\), \(m_k'(s, t)\) is equal to one of \(m_1'(s, t), m_2'(s, t), \ldots, m_k'(s, t)\). If not, \(m_k'(s, t)\) is complementary to each bit of \(m_1'(s, t), m_2'(s, t), \ldots, m_k'(s, t)\), thus \(m_1'(s, t) = m_2'(s, t) = \cdots = m_k'(s, t) = 0\). According to the third step, we have

\[
S(s, t) = m_1'(s, t) \otimes m_2'(s, t) \otimes \cdots \otimes m_k'(s, t)
\]

so that \(S(s, t) = 0 \otimes 0 \otimes \cdots \otimes 0 = 1\) with contradiction to \(S(s, t) = 0\). Therefore, \(m_k'(s, t)\) is equal to one of \(m_1'(s, t), m_2'(s, t), \ldots, m_k'(s, t)\), \(m_1'(s, t) \otimes \cdots \otimes m_k'(s, t) = m_1'(s, t) \otimes \cdots \otimes m_k'(s, t)\); therefore, it can be proved that \(P(m_1'(s, t) \otimes \cdots \otimes m_k'(s, t) = 0) = P(m_1'(s, t) \otimes \cdots \otimes m_k'(s, t) = 0) = (1/2)^{k-1}\).

(2) Secondly, when \(S(s, t) = 1\), we will prove the following:

\[
P\left(m_1'(s, t) \otimes m_2'(s, t) \otimes \cdots \otimes m_k'(s, t) = 0\right) = 0.
\]

(5)

If \(m_k'(s, t) = 0\), then \(m_k'(s, t)\) is complementary to one of \(m_1'(s, t), m_2'(s, t), \ldots, m_k'(s, t)\). Otherwise, \(m_k'(s, t)\) is equal to each bit of \(m_1'(s, t), m_2'(s, t), \ldots, m_k'(s, t)\), thus \(m_1'(s, t) = m_2'(s, t) = \cdots = m_k'(s, t) = 0\). According to the third step, we have \(S(s, t) = m_1'(s, t) \otimes m_2'(s, t) \otimes \cdots \otimes m_k'(s, t) = 0\). Therefore, \(m_k'(s, t)\) is complementary to one of \(m_1'(s, t), m_2'(s, t), \ldots, m_k'(s, t)\), \(m_1'(s, t) \otimes m_2'(s, t) \otimes \cdots \otimes m_k'(s, t) = 1\); therefore, it can be proved that \(P(m_1'(s, t) \otimes m_2'(s, t) \otimes \cdots \otimes m_k'(s, t) = 0) = 0\).

If \(m_k'(s, t) = 1\), \(P(m_1'(s, t) \otimes m_2'(s, t) \otimes \cdots \otimes m_k'(s, t) = 0) = 0\) is satisfied because \(m_k'(s, t)\) is opaque and \(m_1'(s, t) \otimes m_2'(s, t) \otimes \cdots \otimes m_k'(s, t) = 1\).

In conclusion, if we superpose \(m_1'(s, t), m_2'(s, t), \ldots, m_k'(s, t)\), contrast will be visible to the naked eye, i.e., the secret image will be recovered, which is the core to secret recovery in \((k, m, n)\)-RGWVCS. Otherwise, if we superpose any \(k - 1\) shares \(m_1'(s, t), m_2'(s, t), \ldots, m_k'(s, t)\), \(\alpha = 0\) due to Lemma 1.
Theorem 1. The designed scheme is an effective (k, m, n)-RGWVCS structure.

Proof. Firstly, based on Lemma 2, when \( j < k \), the generated \( j \) bits cannot cover \( m^1(s, t), m^2(s, t), \ldots, m^k(s, t) \). \( S'(s, t) = m^1(s, t) \otimes \cdots \otimes m^j(s, t) \), \( P(S'[CS0] = 0) = (1/2)^j \), and \( P(S'[CS1] = 0) = (1/2)^j \). Hence, \( P_0 = P_1 \) when \( j < k \) so that Condition 2 is satisfied. Secondly, when \( j \geq k \), the generated \( j \) bits can cover \( m^1(s, t), m^2(s, t), \ldots, m^k(s, t) \) with a certain probability. \( S'(s, t) = m^1(s, t) \otimes \cdots \otimes m^k(s, t) \) on account of \( P(S'[CS0] = 0) = (1/2)^{k-j} \), \( P(S'[CS1] = 0) = 0 \), and \( P_0 > P_1 \), the designed scheme satisfies Condition 1. Finally, based on the above justification of Conditions 1 and 2, the proposed scheme is an effective (k, m, n)-RGWVCS structure.

Proposition 1. The scheme is designed to take the possible existence of the privileged into account.

Proof. Through the analysis of the designed method, a larger weight leads to a larger probability of covering \( m^1(s, t), m^2(s, t), \ldots, m^k(s, t) \), because the \( k \) initial secret sharing matrices \( \{ M_1, M_2, \ldots, M_k \} \) are constructed corresponding to \( \omega_1, \omega_2, \ldots, \omega_w \) in the first step of Algorithm 1. This indicates that \( \alpha_{i_1j_1 \rightarrow i_2j_2} > \alpha_{i_1j_1 \rightarrow i_3j_3} \) when \( \sum_{i=1}^{j_1} \omega_i \sum_{i=1}^{j_2} \omega_i \) and \( \alpha_{i_1j_1 \rightarrow i_2j_2} > \alpha_{i_1j_1 \rightarrow i_3j_3} \) where \( j \geq k \).

3.5. Practical Application. There is a lot of class division in real life, and being high class also means having certain privileged rights. The traditional visual secret sharing scheme ignores the existence of real privileges and becomes unsuitable for all real situations. The weighted visual secret sharing scheme with privileges can solve this problem well. The following company is taken as an example.

In this case of the company above, there are two classes, including manager and clerk. Managers are superior to their clerks and thus have a greater capacity of secret recovery. It can be seen from Figure 4 that when \( m \leq n < k \), the combination of \( n \) clerks cannot recover \( S \), while the combination of a manager and \( n-1 \) clerks can recover \( S \), highlighting the effectiveness of the privilege. When \( n \geq k \), although the shares of \( n \) clerks can recover the secret image, the quality of \( S' \) is lower than that recovered by one manager and \( n-1 \) clerks. It also highlights the superiority of the privilege enjoyed by the privileged. Most of the existing weighted visual secret sharing schemes give high-weighted participants the privilege of recovering higher-quality secret images. However, the proposed visual secret sharing scheme considering the privileged not only gives the privileges that right but also gives the privileged the privilege to be capable of recovering \( S \) while the same number of ordinary participants cannot recover \( S \). This makes the privileged more prominent and more relevant to the actual situation.

4. Experimental Results and Discussion

In this section, we will show the performance of RGWVCS through experimental results, in which the validity of the scheme is verified from the quality and characteristics of the encrypted and decrypted images, and the superiority of the scheme is illustrated by comparing with other schemes.

4.1. Display of Image Recovery. In the designed RGWVCS for \( (3, 2, 4) \) threshold, secret image \( S \) is divided into four encrypted images \( M_1, M_2, M_3, \) and \( M_4 \). When the privileged people are considered in the secret recovery, at least two encrypted images are required for restoring the secret. Conversely, when no privileged people participate in the secret recovery, a minimum of three encrypted images are required.

It can be seen from Figure 5 that when \( S_q = 1 \), what is displayed is the encrypted images \( M_1, M_2, M_3, \) and \( M_4 \). When \( S_q = 2 \), the result of any two encrypted images superimposed is shown in the figure. The figure shows that half of the six possible combinations can complete the secret recovery. The commonality of the combinations that can complete the secret recovery is that they all contain the privileged \( M_4 \). This is in line with the designed scheme that only \( m(m = 2) \) participants are needed to complete the secret recovery when the privileged participates in the secret recovery. In terms of the recognition of recovered secrets, it can be concluded that the superimposed weight is proportional to the secret recognition. When \( S_q = 3 \), any combination of three encrypted images can accomplish the secret recovery. As with \( S_q = 2 \), the greater the total weight of participants, the higher the degree of secret identification. When \( S_q = 4 \), i.e., all participants \( M_1, M_2, M_3, \) and \( M_4 \) are superposed together, it can recover \( S \) losslessly. The recovered \( S' \) is identical to the binary secret image \( S(\alpha = 1) \).

So, according to the above analysis, we can draw the following conclusions:

1. The experimental results of \( S_q = 2 \) and \( S_q = 3 \) agree with the \( (3, 2, 4) \) threshold, and the design idea of considering the privileged is at least three participants are needed to complete the secret recovery when the privileged is not considered; otherwise, only two participants are needed.

2. The quality of secret recovery is proportional to the total weight of participants.

4.2. Contrast and Weight Analysis. In this section, we will first use the contrast as the main indicator to accurately describe the quality of the recovered secret images from different combinations. Then, we will analyse the relation between contrast and weight. Finally, we will compare the contrast between our scheme and relevant schemes.

From Table 2, we can see that the contrast obtained by the superposition of any two encrypted images in \( M_1, M_2, \) and \( M_3 \) is always 0. Once \( M_4 \) participates in the secret recovery, it only needs 2 encrypted images to restore \( S \) that can be recognized by the naked eye. With the increase in the total weight of the participants, the recognition degree of the secret image is also higher; that is, the clarity of the secret is directly proportional to the total weight of the participants. The analysis shows that the contrast is positively correlated
with the weight, and the image quality after recovery is better than relevant schemes. In Figure 6, we analyse the relation between the contrast and total weight of the decrypted image with the different combinations, where $Q_1$, $Q_2$, $Q_3$, and $Q_4$ are the four abnormal points. For $Q_1$, the total weight of the participants $\omega (\omega = 0.5)$ is the same in combination $M_3 \oplus M_4$ and $M_1 \oplus M_4$. However, $M_2 \oplus M_4$ cannot recover the secret while $M_1 \oplus M_4$ can make the secret identifiable. This phenomenon of the same weight but different decoding ability shows the superiority of the privileged in the designed scheme. For $Q_2$ and $Q_4$, as can be seen from the figure, the trend around $Q_2$ and $Q_4$ is basically the same. Both $Q_2$ and $Q_4$ are maximum points, which indicates that the contrast is positively correlated with the total weight. For $Q_3$, the total weight at this point is as high as 0.9 while the contrast is only 0.4189. This phenomenon of high weight and low contrast is in urgent need of solution. In terms of the rest of the features, the designed scheme has the following characteristics: (1) no pixel expansion; (2) no codebook design; and (3) no weight leakage.

For fear of the influence of randomness of the secret image in above part, we carried out much more identical tests with the designed scheme and other related schemes, in which we selected randomly 100 binary images with different sizes and patterns for encryption and decryption. Finally, we calculated the average contrast for different combinations in 100 tests to prove the superiority of the designed scheme. In the experiment, we set that $k = 2, n = 4$, $\omega_1 = 0.1$, $\omega_2 = 0.2$, $\omega_3 = 0.3$, and $\omega_4 = 0.4$.

Table 3 shows the contrast values of the secret restored images after superimposed with the proposed privileged scheme and the relevant representative WVCS schemes. The results show that the image restoration quality of the proposed scheme is superior to that of other schemes in general except for [3, 4]. Since in the proposed scheme, the $n - k$ bits in the tail must have the same value as a random bit in the front $k$ bits, and thus in the secret recovery phase, the proposed scheme improves the coverage of the front $k$ bits and enhances the clarity of the secret image recovered after superposition.

4.3. Feature Comparison. In this section, we will compare the quality of the recovered image and a series of characteristics of the proposed scheme with some typical WVCS schemes with admirable features, such as Yang et al. [30], Fan [31], and Tu et al. [32] schemes. While we are concerned about the quality of the recovery image, we are also concerned about other features of the designed scheme, such as pixel expansion, codebook design, and weight leakage.

In Table 4, our design scheme is compared with other related schemes in a series of main features where the threshold value represents the threshold parameter supported by the scheme; recovery measure refers to the recovery methods that may be used by the solution; no pixel expansion indicates that the share distributed to the participants has the same size as $S$; no codebook design means that there is no codebook design in the generation phase of shares; and the scheme will be more secure and practical without weight leakage after weighted treatment.

From Table 4, we can see that the proposed RGWVCS has the following superiorities: (1) there is no pixel expansion; (2) no codebook design; (3) $(k, m, n)$ threshold, the privileged are considered in the scheme; (4) the generated shares have no weight leakage; and (5) the image quality is better than that of the correlation weighted scheme, and the secret image can be recovered losslessly. To sum up, in a series of representative characteristic indicators, the scheme we designed is superior to other relevant schemes.

After comparing the characteristics of different schemes, we use the objective evaluation index recall to quantitatively compare our scheme with others. The formula of recall is as follows, where $TP$ is the number of samples with the restored pixel value of 1 and the judgment is correct, and $FN$ is the number of samples with the restored pixel value of 0 and the judgment is wrong. It can be seen from Figure 7 that the program proposed in this paper has an average recall of 87.6% due to the addition of the privilege mechanism, which is higher than all the schemes that participated in the comparison. The schemes proposed by Tan et al. and Liu et al. have relatively moderate results due to weight leakage. Yang et al. and Shamir et al. proposed the schemes earlier, and they have varying degrees of feature defects, so the recall is low.

From this, we can see the advanced nature of the scheme proposed in this article.
The superposed quantity (Sq) is calculated as follows:

\[ \text{Sq} = 1 \]

\[ \text{Sq} = 2 \]

\[ \text{Sq} = 3 \]

\[ \text{Sq} = 4 \]

**Figure 5:** The outcomes of the proposed RGWVCS for (3, 2, 4) threshold where Sq refers to the number of shares stacked when recovering the secret. The image S is the selected original heart-shaped binary secret image of size 454 × 454. When \( S_q = 1 \), \( M_1, M_2, M_3, \) and \( M_4 \) are four encrypted images of the same size as S. The weights of \( M_1, M_2, M_3, \) and \( M_4 \) are \( \omega_1 = 0.1, \omega_2 = 0.2, \omega_3 = 0.3, \) and \( \omega_4 = 0.4 \), respectively. \( M_4 \) has the maximum weight so that he is a privileged.

**Table 2:** The contrast and weight of the decrypted image formed by superimposing shares.

| Superimposed encrypted image | Contrast | Weight |
|------------------------------|----------|--------|
| \( M_1 \)                   | —        | 0.1    |
| \( M_2 \)                   | —        | 0.2    |
| \( M_3 \)                   | —        | 0.3    |
| \( M_4 \)                   | —        | 0.4    |
| \( M_1 \oplus M_2 \)        | —        | 0.3    |
| \( M_1 \oplus M_3 \)        | —        | 0.4    |
| \( M_1 \oplus M_4 \)        | —        | 0.5    |
| \( M_1 \oplus M_3 \)        | 0.1266   | 0.5    |
| \( M_2 \oplus M_3 \)        | 0.1732   | 0.6    |
| \( M_3 \oplus M_4 \)        | 0.2581   | 0.7    |
| \( M_4 \oplus M_1 \oplus M_2 \) | 0.2525 | 0.6    |
| \( M_4 \oplus M_1 \oplus M_3 \) | 0.2804 | 0.7    |
| \( M_4 \oplus M_1 \oplus M_4 \) | 0.3399 | 0.8    |
| \( M_4 \oplus M_2 \oplus M_3 \) | 0.4189 | 0.9    |
| \( M_4 \oplus M_2 \oplus M_4 \) | 1       | 1      |
Table 3: The contrast of the proposed scheme under the (3, 2, 4) threshold, compared with Tu et al. [32], Fan et al. [31], and Yang et al. [30].

| Collected shadows | Ours | Tu et al. [32] | Fan et al. [31] | Yang et al. [30] |
|-------------------|------|---------------|-----------------|-----------------|
| [1, 2]            | —    | 0.1035        | 0.1105          | 0.1096          |
| [1, 3]            | —    | 0.1226        | 0.1526          | 0.1531          |
| [1, 4]            | 0.2432| 0.1505        | 0.1993          | 0.1985          |
| [2, 3]            | —    | 0.1681        | 0.1981          | 0.1986          |
| [2, 4]            | 0.2759| 0.1872        | 0.2486          | 0.2491          |
| [3, 4]            | 0.2962| 0.2176        | 0.3021          | 0.3045          |
| [1, 2, 3]         | 0.2925| 0.2249        | 0.2488          | 0.2485          |
| [1, 2, 4]         | 0.3486| 0.2523        | 0.3038          | 0.3040          |
| [1, 3, 4]         | 0.3821| 0.2841        | 0.3623          | 0.3642          |
| [2, 3, 4]         | 0.4414| 0.3192        | 0.4263          | 0.4278          |
| [1, 2, 3, 4]      | 1     | 0.3873        | 0.4988          | 0.4996          |

Table 4: A comparison of series of representative features between the designed scheme and relevant VCSs.

| Proposer          | Threshold | Recovery efficiency (complexity) | No pixel expansion | No codebook design | No weight leakage | Weighted |
|-------------------|-----------|----------------------------------|--------------------|--------------------|-------------------|----------|
| Shamir et al. [1] | (k, n)    | OR(O(1))                         | ✓                  | ✓                  | ✓                 | ✓        |
| Yang et al. [30]  | (2, n)    | OR(O(1))                         | ✓                  | ✓                  | ✓                 | ✓        |
| Tan et al. [40]   | (k, n)    | Modular (O(k))                   | ✓                  | ✓                  | ✓                 | ✓        |
| Liu et al. [41]   | (k, n)    | OR/XOR (O(1)/O(k))               | ✓                  | ✓                  | ✓                 | ✓        |
| Fan et al. [31]   | (k, n)    | OR(O(1))                         | ✓                  | ✓                  | ✓                 | ✓        |
| Tu et al. [32]    | (k, n)    | OR(O(1))                         | ✓                  | ✓                  | ✓                 | ✓        |
| Ours              | (k, m, n) | OR(O(1))                         | ✓                  | ✓                  | ✓                 | ✓        |
\[ R = \frac{TP}{TP + FN} \]  

5. Conclusions

The traditional \((k, n)\)-threshold visual secret sharing scheme encrypts a secret image into \(n\) noise shares, and the hidden secret in the secret image can be recovered by superimposing \(k\) or more shares. Nevertheless, those methods did not consider differences in the importance of participants, so each participant in the scheme has the same level of privilege, that is, the same secret recovery capability. This paper designs a novel random grid-based weighted visual cryptography scheme for a \((k, m, n)\) \((m < k < n)\) threshold (RGWVCS). This scheme takes the differences between privileged participants and ordinary participants into account and gives the privileged people a better decryption ability than ordinary people. When privileged people participate in secret recovery, only \(m\) participants are needed, and when no privileged person participates, \(k\) participants are needed. Through the analysis of the experimental results and the comparison with the relevant schemes, the designed scheme has several features as follows: (1) there is no pixel expansion; (2) no codebook design; (3) \((k, m, n)\) threshold, the privileged are considered in the scheme, (4) the generated shares have no weight leakage, and (5) the contrast of the designed RGWVCS is, on average, increased by 32.85% compared with the relevant schemes which shows that the image quality of the revealed secret image is greatly enhanced. In the future, we will further modify the algorithm to improve the resolution of secret images and the security of encryption. Furthermore, the current visual secret sharing scheme can only be used for binary image encryption, and grayscale and color images cannot be well encrypted and restored. We will work to make the designed scheme also applicable to the encryption of grayscale and color images.

Data Availability

Some or all data, models, or code that support the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the National Key R&D Program of China under grant no. 2018YFB01003205; by the National Natural Science Foundation of China under grant nos. U1836208, U1536206, U1836110, 61972207, 61602253, and 61672294; by the Engineering Research Center of Digital Forensics, Ministry of Education; by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD) Fund; and by the Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET) Fund, China.

References

[1] M. Naor and A. Shamir, “Visual cryptography,” in Advances in Cryptology—EUROCRYPT’94, pp. 1–12, Springer-Verlag, Berlin, Germany, 1995.
[2] R. Blakley, “Safeguarding cryptographic keys,” in Proceedings of the National Computer Conference, pp. 313–317, Monval, NJ, USA, 1979.
[3] Shamir, “How to share a secret,” Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.
[4] M. Naor and B. Pinkas, “Visual authentication and identification,” Advances in Cryptolog—CRYPTO’97, Springer-Verlag, Berlin, Germany, pp. 322–336, 1997.
[5] M. Naor and A. Shamir, “Visual cryptography ii: improving the contrast via the cover base,” in Security Protocols, pp. 197–202, Springer, Berlin, Germany, 1996.
[6] S. J. Shyu and M. C. Chen, “Optimum pixel expansions for threshold visual secret sharing schemes,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 960–969, Sep. 2011.
[7] S. J. Shyu and M. C. Chen, “Minimizing pixel expansion in visual cryptographic scheme for general access structures,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 25, no. 9, pp. 1557–1561, 2015.
[8] C.-C. Chang and J.-C. Chuang, “An image intellectual property protection scheme for gray-level images using visual secret sharing strategy,” Pattern Recognition Letters, vol. 23, no. 8, pp. 931–941, 2002.
[9] R. Lukac and K. N. Plataniotis, “Bit-level based secret sharing for image encryption,” Pattern Recognition, vol. 38, no. 5, pp. 767–772, 2005.
[10] G. Atieniese, C. Blundo, A. D. Santis, and D. R. Stinson, “Extended capabilities for visual cryptography,” Theoretical Computer Science, vol. 250, no. 1-2, pp. 143–161, 2001.
[11] C. Blundo, A. De Santis, and D. R. Stinson, “On the contrast in visual cryptography schemes,” Journal of Cryptology, vol. 12, no. 4, pp. 261–289, 1999.
[12] X. Yan, S. Wang, X. Niu, and C.-N. Yang, “Halftone visual cryptography with minimum auxiliary black pixels and uniform image quality,” Digital Signal Processing, vol. 38, pp. 53–65, 2015.
[13] C.-C. Lin and W.-H. Tsai, “Visual cryptography for gray-level images by dithering techniques,” Pattern Recognition Letters, vol. 24, no. 1-3, pp. 349–358, 2003.
[14] C.-N. Yang, L.-Z. Sun, and S.-R. Cai, “Extended color visual cryptography for black and white secret image,” Theoretical Computer Science, vol. 609, pp. 143–161, 2016.
[15] S. Cimato, R. De Prisco, and A. De Santis, “Probabilistic visual cryptography schemes,” The Computer Journal, vol. 49, no. 1, pp. 97–107, 2006.
[16] I. Kang, G. R. Arce, and H. K Lee, “Color extended visual cryptography using error diffusion,” IEEE Transactions on Image Processing: A Publication of the IEEE Signal Processing Society, vol. 20, no. 1, pp. 132–145, 2011.
[17] J. Chen, T.-S. Chen, H.-C. Hsu, and Y.-H. Lin, “Using multi-ring shadow image of visual cryptography to hide more secret messages,” The Imaging Science Journal, vol. 57, no. 2, pp. 101–108, 2009.
[18] S. Drost, “New results on visual cryptography,” in Advances in Cryptology—CRYPTO, pp. 401–415, Springer, Berlin, Germany, 1996.
[19] S. J. Shyu and H. W. Jiang, “General constructions for threshold multiple-secret visual cryptographic schemes,” IEEE Transactions on Information Forensics and Security, vol. 8, no. 5, pp. 733–743, 2013.
[20] C.-N. Yang, H.-W. Shih, C.-C. Wu, and L. Harn, "$k$ out of $n$ region incrementing scheme in visual cryptography," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 22, no. 5, pp. 799–810, 2012.

[21] Y. C. Chen, G. Horng, and D. S. Tsai, "Comment on "Cheating prevention in visual cryptography"" *IEEE Transactions on Image Processing*, vol. 21, no. 7, pp. 3319–3323, 2012.

[22] M. Hu and W. G. Tzeng, "Cheating prevention in visual cryptography," *IEEE Transactions on Image Processing*, vol. 16, no. 6, pp. 36–45, 2007.

[23] X. Liu, S. Wang, X. Yan, and W. Zhang, "Random grid-based threshold visual secret sharing with improved visual quality and lossless recovery ability," *Multimedia Tools and Applications*, vol. 77, no. 16, pp. 20673–20696, 2018.

[24] S. P. Kannoja and J. Kumar, "XOR-based visual secret sharing scheme using pixel vectorization," *Multimedia Tools and Applications*, vol. 80, no. 10, pp. 14609–14635, 2021.

[25] S. Shivani and S. Agarwal, "Novel basis matrix creation and preprocessing algorithms for friendly progressive visual secret sharing with space-efficient shares," *Multimedia Tools and Applications*, vol. 76, no. 6, pp. 8711–8744, 2017.

[26] S. Shivani and S. Agarwal, "Progressive visual cryptography with unexpanded meaningful shares," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 12, no. 4, pp. 1–24, 2016.

[27] S. Shivani and S. Agarwal, "VPVC: verifiable progressive visual cryptography," *Pattern Analysis & Applications*, vol. 21, no. 1, pp. 139–166, 2016.

[28] S. Shivani, "Multi secret sharing with unexpanded meaningful shares," *Multimedia Tools & Applications*, vol. 77, no. 5, pp. 6287–6310, 2017.

[29] Y.-C. Hou, Z.-Y. Quan, and C.-F. Tsai, *A Privilege-Based Visual Secret Sharing Model*, Academic Press, Cambridge, MA, USA, 2015.

[30] C.-N. Yang, J.-K. Liao, and D.-S. Wang, "New privilege-based visual cryptography with arbitrary privilege levels," *Journal of Visual Communication and Image Representation*, vol. 42, pp. 121–131, 2017.

[31] H. C. Chao, "Random-grid based progressive visual secret sharing scheme with adaptive priority," *Digital Signal Processing*, vol. 68, pp. 69–80, 2017.

[32] T. Y. Tu, T. H. Chen, J. Yang, and C. H. Wang, "A weighted threshold visual cryptography," *Communications in Computer and Information Science*, vol. 1013, 2019.

[33] X. Yan, S. Wang, A. A. A. El-Latif, and X. Niu, "Random grids-based visual secret sharing with improved visual quality via error diffusion," *Multimedia Tools and Applications*, vol. 74, no. 21, pp. 9279–9296, 2015.

[34] X. Yan, X. Liu, and C.-N. Yang, "An enhanced threshold visual secret sharing based on random grids," *Journal of Real-Time Image Processing*, vol. 14, no. 1, pp. 61–73, 2018.

[35] G. Gao, X. Wu, S. Yao, Z. Cui, C. Zhou, and X. Sun, "Reversible data hiding with contrast enhancement and tamper localization for medical images," *Information Sciences*, vol. 385-386, pp. 250–265, 2017.

[36] M. Alloghi, M. M. Alani, D. Al-Jumailly et al., "A systematic review on the status and progress of homomorphic encryption technologies," *Journal of Information Security and Applications*, vol. 48, Article ID 102362, 2019.

[37] X. Jia, D. Wang, D. Nie, X. Luo, and J. Z. Sun, "A new threshold changeable secret sharing scheme based on the Chinese remainder theorem," *Information Sciences*, vol. 473, no. 13–30, 2019.

[38] G. Gao, Z. Cui, and C. Zhou, "Blind reversible authentication based on PEE and CS reconstruction," *IEEE Signal Processing Letters*, vol. 25, no. 7, pp. 1099–1103, 2018.

[39] X. Yan, Y. Lu, H. Huang, L. Liu, and S. Wan, "Clarity corresponding to contrast in visual cryptography," in *Proceedings of the Social Computing: Second International Conference of Young Computer Scientists, Engineers and Educators, ICYC-SEE 2016*, pp. 249–257, Harbin, China, August 2016.

[40] L. Tan, Y. Lu, X. Yan, L. Liu, and L. Li, "Weighted secret image sharing for a $(k, n)$ threshold based on the Chinese remainder theorem," *IEEE Access*, vol. 7, pp. 59278–59286, 2019.

[41] F. Liu, X. Yan, L. Liu, Y. Lu, and L. Tan, "Weighted visual secret sharing with multiple decryptions and lossless recovery," *Mathematical Biosciences and Engineering*, vol. 16, no. 5, pp. 5750–5764, 2019.