electronics

MDPI

Article

A *n*-out-of-*n* Sharing Digital Image Scheme by Using Color Palette

Ching-Nung Yang [1], Qin-Dong Sun [2], Yan-Xiao Liu [2,*] and Ci-Ming Wu [1]

[1] Department of CSIE, National Dong Hwa University, Hualien 97401, Taiwan
[2] Department of Computer Science and Engineering, Xi'an University of Technology, Xi'an 710021, China
* Correspondence: liuyanxiao@xaut.edu.cn; Tel.: +86-029-8231-2231

Received: 15 April 2019; Accepted: 13 July 2019; Published: 17 July 2019

Abstract: A secret image sharing (SIS) scheme inserts a secret message into shadow images in a way that if shadow images are combined in a specific way, the secret image can be recovered. A 2-out-of-2 sharing digital image scheme (SDIS) adopts a color palette to share a digital color secret image into two shadow images, and the secret image can be recovered from two shadow images, while any one shadow image has no information about the secret image. This 2-out-of-2 SDIS may keep the shadow size small because by using a color palette, and thus has advantage of reducing storage. However, the previous works on SDIS are just 2-out-of-2 scheme and have limited functions. In this paper, we take the lead to study a general n-out-of-n SDIS which can be applied on more than two shadow. The proposed SDIS is implemented on the basis of 2-out-of-2 SDIS. Our main contribution has the higher contrast of binary meaningful shadow and the larger region in color shadows revealing cover image when compared with previous 2-out-of-2 SDISs. Meanwhile, our SDIS is resistant to colluder attack.

Keywords: secret image sharing; digital image; n-out-of-n scheme; color palette; colluder attack

1. Introduction

A secret image sharing (SIS) scheme inserts a secret message into shadow images in a way that if shadow images are combined in a specific way, the secret image can be recovered. A SIS scheme is usually referred to by a threshold (k, n) SIS, where $k \leq n$, and can insert a secret image into n shadow images (referred to as shadows). In a (k, n)-SIS, we may recover the secret image by using any k shadows, but cannot recover the secret image from $(k-1)$ or fewer shadows. There are various types of SIS. Here, we give a brief survey for three major types of SIS schemes: the visual cryptography scheme (VC), the polynomial-based SIS (PSIS), and the bit-wise Boolean-operation based SIS.

The so-called VC [1–6] has a novel stacking-to-see property such that the involved participants can easily stack shadows to visually decode the secret through the human eye. This property makes VC applicable in many scenarios. Although VC has the ease of decoding, it has poor visual quality of reconstructed image. Another SIS adopts $(k-1)$-degree polynomial like Shamir's secret sharing [7] to design (k, n)-PSIS [8–15]. There are two major differences between VC and PSIS: the quality of recovered image and the decoding method. Unlike VC provided with the poor visual quality, the recovered secret image of PSIS is distortion-less. However, the decoding of VC only needs stacking operation but PSIS uses the computation of Lagrange interpolation to recover secret image. Some SIS schemes are based on Boolean operations [16–20]. Note: the stacking operation of VC, strictly speaking, is also a Boolean OR operation. However, this OR operation of VC is pixel-wise operation, which applied on black-and-white dots. However, Boolean operation in [16–20] is bit-wise operations, and can obtain a high-quality secret image (a distortion-less image like PSIS scheme). Besides, using -wise Boolean has much lower complexity when compared with Lagrange interpolation.

Recently, Wei et al. use the bit-wise XOR operation to design a $(2,2)$ sharing digital image scheme (SDIS) [17] to share a 256-color (or true color) digital image. Wei et al.'s $(2,2)$-SDIS is also a type of (k,n)-SIS where $k = n = 2$. Wei et al.'s $(2,2)$-SDIS is the first SIS scheme using a 256-color palette. This color palette has 256 colors, where each color is composed of red (R), green (G), and blue (B) color planes. Each color and is chosen from a palette of 16,777,216(=2^{24}) colors (24 bits: each color plane has 8 bits). In VGA cards, 256 on-screen colors are chosen from a color palette, and these colors are most visible to the human eye and meanwhile conserve a bandwidth. When using a color palette, each pixel is represented by a color index in a 256-color color palette. Consider an example, a 256×256-pixel image. The file size is $256 \times 256 \times 1$ bytes (color indices) $+256 \times 3$ bytes (color palette) = 66,304 bytes, but is $256 \times 256 \times 3$ = 196,608 bytes for using 24-bit true color format. Thus, the file size of a color image can be kept small when represented by a color palette. Because Wei et al.'s $(2,2)$-SDIS is based on color palette, and thus it has the advantage of reducing storage.

However, there are three weaknesses in Wei et al.'s SDIS: the incorrect assignment of color palette data for the color index 255, the erroneous recovery in secret image, and the partial region in shadow revealing the cover image. In [19], Yang et al. address these weaknesses and propose a new $(2,2)$-SDIS. Both Wei et al.'s $(2,2)$-SDIS and Yang et al.'s $(2,2)$-SDIS are simple 2-out-of-2 scheme and have limited applications. In this paper, we take the lead to study a general (n,n)-SDIS, which can be applied on any $n \geq 3$. The main weakness of Wei et al.'s $(2,2)$-SDIS is the incorrect assignment of color palette data for some color indices, and this is tackled by using a complicated approach, partitioned sets, in Yang et al.'s $(2,2)$-SDIS. In the proposed (n,n)-SDIS, because of the number of shadows more than two, i.e., $n \geq 3$, a simple approach reducing Hamming weigh of a temporary block is adopted to easily solve this weakness. In addition, performance of our (n,n)-SDIS are enhanced when compared with the previous $(2,2)$-SDIS. The rest of this paper is organized as follows. Section 2 reviews Wei et al.'s $(2,2)$-SDIS and Yang et al.'s $(2,2)$-SDIS. The proposed (n,n)-SDIS is presented in Section 3. Also, an approach of enhancing visual quality of color meaningful shadow is introduced. A very extreme attack, the $(n-1)$-colluder attack, on the proposed (n,n)-SDIS is discussed in Section 4. The experiment, discussion and comparison are in Section 5. Finally, Section 6 concludes the paper.

2. Preliminaries

Notations in this paper and their descriptions are listed in Table 1. These notations are used throughout the whole paper to describe all the schemes, Wei et al.'s $(2,2)$-SDIS [17], Yang et al.'s $(2,2)$-SDIS [19], and the proposed (n,n)-SDIS.

In [17], Wei et al. first proposed a simple $(2,2)$-SDIS to insert a 256-color digital image SI into two binary noise-like shadows (NS_1 and NS_2). In Wei et al.'s $(2,2)$-SDIS, every 9-bit block B, i.e., $b_1 - b_9$, is obtained from the 256-color secret image SI and the color palette CP. Afterwards, the block B is subdivided into two blocks $B^{(1)}$ and $B^{(2)}$ on shadow 1 NS_1 and shadow 2 NS_2, respectively, by using XOR operation. As shown in Figure 1, $B = B^{(1)} \oplus B^{(2)}$, where each bit $b_i = b_i^{(1)} \oplus b_i^{(2)}$, $1 \leq i \leq 9$. Both shadow blocks of $B^{(1)}$ and $B^{(2)}$ are $\boxed{Y}$ blocks. Accomplish all blocks until all pixels in SI and the data in CP are processed. Because every pixel in SI is represented as a block, shadow sizes are nine times expanded. The first 8 bits $b_1 - b_8$ in B represents a color index, and the ninth bit b_9 in every block of NS_1 (i.e., the bit $b_9^{(1)}$) is collected to covey the CP information. Therefore, from the XOR-ed results $NS_1 \oplus NS_2$ we may obtain color indices and the CP to recover SI. There are other two types of shadows for Wei et al.'s $(2,2)$-SDIS. Noise-like shadows (NS_1, NS_2) can be extended to two binary meaningful shadows (BS_1, BS_2) and two color meaningful shadows (CS_1, CS_2), on which binary cover image BCI and color cover image CCI can be, respectively, visually viewed. In addition, Wei et al.'s $(2,2)$-SDIS can also be extended to directly insert a true color SI without using CP.

Table 1. Notations and Descriptions.

Notation	Description
CP	a 256-color color palette
SI	a secret image with the size with the size $(M \times N)$ pixels
CCI, BCI	binary (black-and-white) over image and color cover image with the size $(M \times N)$ pixels
NS_i	n noise-like shadows with the size $(3M \times 3N)$ (respectively, $(5M \times 5N)$) subpixels for 256-color (respectively, true color) secret image, where $i = 1, 2, ..., n$
BS_i	binary meaningful shadows with the size $(3M \times 3N)$ (respectively, $(5M \times 5N)$) subpixels for 256-color (respectively, true color) secret image
CS_i	color meaningful shadows with the size $(3M \times 3N)$ (respectively, $(5M \times 5N)$) subpixels for 256-color (respectively, true color) secret image
B	a 3×3-subpixel block B including 8-bit color index $b_1 - b_8$ and one bit b_9 (Note: the bit b_9 in B is collected to covey the CP information for the proposed (n, n)-SDIS)
B_r	a 3×3-subpixel block B_r including the first three 8-tuples, $(r_1 - r_8)$, $(g_1 - g_8)$, and $(bl_1 - bl_8)$, are used to represent R, G and B color planes, and the other one bit in B_r is p_9.
$B^{(i)}$	a 3×3-pixel block on shadow i, where $i = 1, 2, ..., n$, including 8-bit $b_1^i - b_8^i$ and one bit b_9^i. (Note: the ninth bit in every block $B^{(1)}$ (i.e., $b_9^{(1)}$) of NS_1 is collected to covey the CP information for Wei et al.'s $(2, 2)$-SDIS and Yang et al.'s $(2, 2)$-SDIS)
$xByW$	x black subpixels and y white subpixels in a block
$\boxed{X}$, $\boxed{Y}$	$\boxed{X}$ and $\boxed{Y}$ blocks have $6B3W$ and $5B4W$ subpixels, respectively
$H(\bullet)$	Hamming weight function, the number of $''1''$ in a binary vector
$W(\bullet)$	Operation of Wei et al.'s $(2, 2)$-SDIS, i.e., $W(B) = B^{(1)} \oplus B^{(2)}$ where both are $\boxed{Y}$ blocks
$Y(\bullet)$	Operation of Yang et al.'s $(2, 2)$-SDIS, i.e., $Y(B) = B^{(1)} \oplus B^{(2)}$ where one is $\boxed{X}$ block and the other is $\boxed{Y}$ block

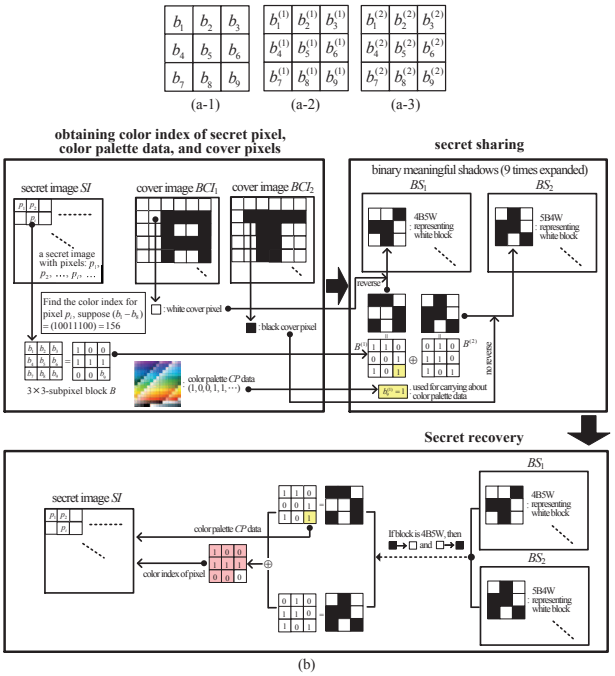


Figure 1. Blocks of $(2, 2)$-SDIS: (**a**) secret block B, shadow blocks $B^{(1)}$ and $B^{(2)}$ (**b**) diagrammatical representation of Wei et al.'s $(2, 2)$-SDIS with binary meaningful shadows.

For more clearly describing Wei et al.'s $(2,2)$-SDIS, Figure 1b illustrates diagrammatical representation of Wei et al.'s $(2,2)$-SDIS with binary meaningful shadows, which includes three processes: (i) obtaining color indices of secret pixels, color palette data, and cover pixels, (ii) secret sharing, and (iii) secret recovery. Consider a secret pixel pi with a color index $(b_1, b_2, ..., b_8) = (10011100) = 156$, and we may have $(b_1^{(1)}, b_2^{(1)}, ..., b_8^{(1)}) = (110001100)$ with $b_9^{(1)} = 1$ for carrying about CP data (suppose we embed "1" for this time), and $(b_1^{(2)}, b_2^{(2)}, ..., b_8^{(2)}) = (010110101)$ with $b_9^{(2)} = 1$. Then, we have $(b_1^{(1)}, b_2^{(1)}, ..., b_8^{(1)}) \oplus (b_1^{(2)}, b_2^{(2)}, ..., b_8^{(2)}) = (b_1, b_2, ..., b_8)$. Meantime, both blocks $B^{(1)} = (b_1^{(1)}, b_2^{(1)}, ..., b_9^{(1)})$ and $B^{(2)} = (b_1^{(2)}, b_2^{(2)}, ..., b_9^{(2)})$ are $5B4W$ blocks. For the corresponding position of this secret pixel pi, the cover pixels of BCI_1 and BCI_2 are white and black, respectively. We reverse the shadow $B^{(1)} = (b_1^{(1)}, b_2^{(1)}, ..., b_9^{(1)}) = (110001101)$ block to (001110010) $(4W5B)$ to represent the white color pixel in BCI_1, and we do not change $B^{(2)} = (b_1^{(2)}, b_2^{(2)}, ..., b_9^{(2)}) = (010110101)$ $(5B4W)$ to represent the black color pixel in BCI_2. In secret recovery, the color index can be easily derived from the exclusive OR result from $(b_1^{(1)}, b_2^{(1)}, ..., b_8^{(1)}) \oplus (b_1^{(2)}, b_2^{(2)}, ..., b_8^{(2)})$. In addition, the CP data can be obtained from every $b_9^{(1)}$ in BS_1.

However, Wei et al's $(2,2)$-SDIS has some weaknesses. For the color index 255, it has a problem with embedding the data of color palette. In addition, Wei et al.'s $(2,2)$-SDIS with color meaningful shadows cannot correctly extract the block data for white cover pixels, and this will cause erroneous recovery in the secret image. Moreover, Wei et al.'s SDIS uses $\boxed{Y}$ blocks on both shadows. Five black dots in a block B may not sufficiently demonstrate the visual quality of meaningful shadows.

It is obvious that more black subpixels in every block may enhance the visual quality of meaningful shadows BS_1 and BS_2, and CS_1 and CS_2. Accordingly, in [19], Yang et al. adopted $\boxed{X}$ block and $\boxed{Y}$ block half and half on blocks $B^{(1)}$ and $B^{(2)}$, such that the average number of black subpixels in $B^{(1)}$ and $B^{(2)}$ is enhanced from 5 to 5.5. This enhancement improved the visual quality of meaningful shadows. Meanwhile, Yang et al.'s $(2,2)$-SDIS also solved the other two weaknesses of Wei et al.'s $(2,2)$-SDIS.

3. Motivation and Design Concept

As described in Section 2, there are three weaknesses in Wei et al.'s SDIS: (1) the incorrect assignment of the color palette data for the color index 255, (2) the partial regions in meaningful shadows showing the content of the cover image, and (3) the erroneous recovery in secret image if the cover pixel is white in color meaningful shadows. Yang et al.'s $(2,2)$-SDIS already tackled these weaknesses.

By delving into these three weaknesses, we can see that the third weakness is a minor weakness caused from an intrinsic nature of color. A trivial approach in [19], using a near white color pixel instead of white pixels in cover image, is very efficient in addressing this weakness. Therefore, the approach can be still adopted in the proposed (n,n)-SDIS for solving this minor weakness. Our contribution is not just the extension from 2-out-of-2 scheme to n-out-of-n scheme. The proposed (n,n)-SDIS, where $n \geq 3$, has better solutions for other two major weaknesses. Because the number of shadows is more than two, we can easily solve the first weaknesses (note: the detail will be described in Section 3). However, Yang et al.'s $(2,2)$-SDIS uses a very complicated approach by partitioned sets to solve this weakness. For the second weakness, our (n,n)-SDIS uses $\boxed{X}$ blocks in most shadows This approach has large average black subpixels in shadow blocks to enhance visual qualities of meaningful shadows. In addition, the proposed (n,n)-SDIS embeds the CP information in b_9 but both $(2,2)$-SDISs [17,19] use $b_9^{(1)}$ in shadow block $B^{(1)}$. The bit b_9 obtained from the XOR-ed result B is more securely protected than the bit $b_9^{(1)}$ in one shadow block $B^{(1)}$.

A secret block $B = (b_1...b_9)$ has 8 bits $(b_1...b_8)$ to represent a color index, and one bit b_9 for representing the data of color palette CP. Together with CP, this color index can represent a pixel in secret image SI. All 9-bit blocks are obtained from the secret image SI and the color palate CP. Suppose that T is a 9-bit temporary block. Equations (1) and (2) are main statements in this paper, on which we can design the proposed (n,n)-SDIS. As shown in Equation (1), we may randomly generate

$(n-2)$ $\boxed{X}$ blocks $B^{(i_j)}, 1 \leq j \leq n-2$, and then determine a temporary block T via these $(n-2)$ blocks and the block B (see upper equation in Equation (1)). The content of T is provisional. Afterwards, T is divided into two blocks $\{B^{(j_1)}, B^{(j_2)}\}$ where $\{j_1, j_2\} = \{1, 2, ..., n\} - \{i_1, ..., i_{n-2}\}$. Using lower equation in Equation (1), we may insert T into two blocks based on Wei et al.'s $(2,2)$-SDIS or Yang et al.'s $(2,2)$-SDIS, which is dependent on the Hamming weigh of block T. In next subsection, we prove that lower equation in Equation (1) can be successfully accomplished. Via Equation (1), we can derive $B = B^{(1)} \oplus B^{(2)} \oplus ... \oplus B^{(n)}$ in Equation (2).

$$\begin{cases} & \overbrace{\quad\quad}^{(n-2)\text{ random }\boxed{X}\text{ blocks}} \\ T = B \oplus & B^{(i_1)} \oplus ... \oplus B^{(i_{n-2})} \\ & \overbrace{\quad\quad}^{\text{other two blocks}} \\ T = \oplus & B^{(j_1)} \oplus B^{(j_2)} \end{cases} \tag{1}$$

$$\begin{cases} T = B \oplus B^{(i_1)} \oplus ... \oplus B^{(i_{n-2})} \\ \Rightarrow B = T \oplus B^{(i_1)} \oplus ... \oplus B^{(i_{n-2})} \\ \Rightarrow B = B^{(j_1)} \oplus B^{(j_2)} \oplus B^{(i_1)} \oplus ... \oplus B^{(i_{n-2})} \\ \Rightarrow B = B^{(1)} \oplus ... \oplus B^{(n)}, (\{j_1, j_2\} \bigcup \{i_1, ..., i_{n-2}\} = \{1, ..., n\}) \end{cases} \tag{2}$$

Equation (2) implies that the block B can be subdivide into n shadow blocks $B^{(1)}, B^{(2)}, ..., B^{(n)}$, and meanwhile can be recovered from $B = B^{(1)} \oplus ... \oplus B^{(n)}$. All the n shadows in the proposed (n,n)-SDIS are illustrated in Figure 2. The operation of lower equation in Equation (1) using Wei et al.' $(2,2)$-SDIS is shown in Figure 2a, and using Yang et al.'s $(2,2)$-SDIS is shown in Figure 2b.

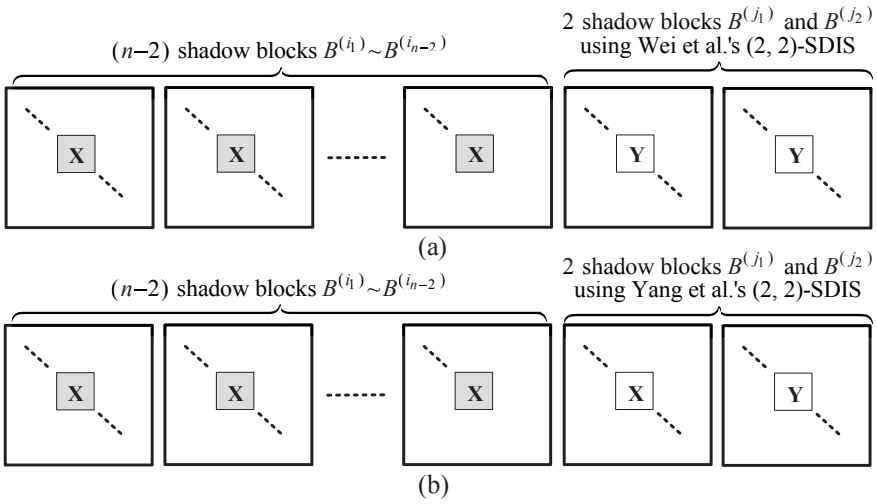


Figure 2. Shadows of the proposed (n,n)-SDIS: (**a**) using Wei et al.'s $(2,2)$-SDIS for $B^{(j_1)}$ and $B^{(j_2)}$ (**b**) using Yang et al.'s $(2,2)$-SDIS for $B^{(j_1)}$ and $B^{(j_2)}$.

Moreover, in [17], the authors claimed that the $(2,2)$-SDIS has a novel application to cover the transmission of confidential images. For example, as a supplementary aid to existing symmetric cryptography standards like DES which requires a pre-shared key, the $(2,2)$-SDIS remains a safe and less risky means for key distribution. Because the prosed scheme is extended from 2-out-of-2 to n-out-of-n, it implies that our (n,n)-SDIS can be applied on a group key distribution, which includes n members in this group. Besides the application in key distribution, the proposed scheme can be also applied to protection of secret image among multiple users. For instance, the colorful image of traffic or medical information are confidential, and our scheme provides a secure and high efficiency approach to safely keeping such image among n users, only all n users are able to recover the image with high quality.

Finally, in a shadow $NS_i, 1 \leq i \leq n$ there are $\boxed{X}$ blocks with percentage of $\frac{n-1.5}{n} (= \frac{1}{2} \times \frac{n-1}{n} + \frac{1}{2} \times \frac{n-2}{n})$, and $\boxed{Y}$ blocks with percentage of $\frac{1.5}{n} (= \frac{1}{2} \times \frac{1}{n} + \frac{1}{2} \times \frac{2}{n})$, respectively. The more $\boxed{X}$ blocks have the large number of black subpixels and may enhance visual qualities of meaningful shadows, and these percentages have more effective performance for large n.

4. The Proposed (n, n)-SDIS

4.1. Sharing and Recovering Algorithms

A block diagram of the proposed (n, n)-SDIS is illustrated in Figure 3. Shadows $NS_1 - NS_n$ are noise-like, which is the same as Boolean-operation based SIS [18]. For the proposed (n, n)-SDIS, we can complement the blocks for the corresponding white cover pixels to generate binary meaningful shadows $(BS_1 - BS_n)$ from noise-like shadows $(NS_1 - NS_n)$, i.e., $6B3W$ (or $5B4W$) for black color and $3B6W$ (or $4B5W$) for white color. However, the scheme in [18] does dot has this property. On the other hand, to implement color meaningful shadows (CS_1, CS_n), the 1s in blocks are replaced with the color of the corresponding cover pixel, and leave 0s blank. Therefore, we only describe how to generate noise-like shadows, and how to recover the secret image and color palette from n noise-like shadows.

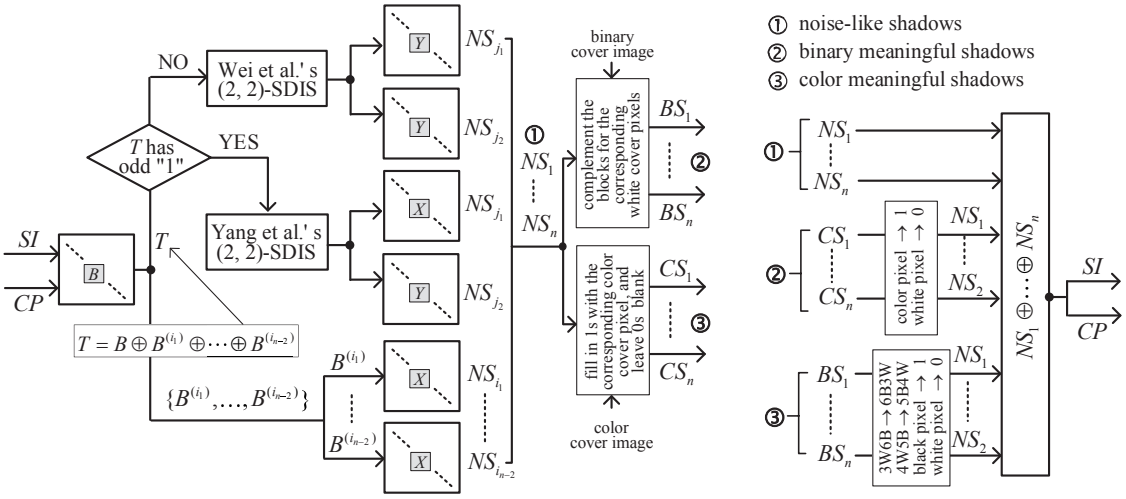


Figure 3. Block diagram of the proposed (n, n)-SDIS

For noise-like shadows (NS_1, NS_n), detailed procedures of sharing and recovering procedures are briefly described step by step as follows.

Sharing Procedure

(S-1) Obtain the block $B = (b_1, b_2, ...b_9)$ from the secret image SI and the color palate CP.
(S-2) Randomly generate $(n-2)$ $\boxed{X}$ blocks $B^{(i_1)}, B^{(i_2)}, ..., B^{(i_{n-2})}$.
(S-3) By $(n-2)$ random blocks and the block B, calculate the temporary block T via $T = B \oplus B^{(i_1)} \oplus ... \oplus B^{(i_{n-2})}$.
(S-4) If $H(T)$ is 9, we reduce its Hamming weight to $H(T) = 7$ via modifying any one shadow block of $\{B^{(i_1)}, ..., B^{(i_{n-2})}\}$.

/* (1) In Lemma 1, we prove that the reduction of Hamming weight can always be accomplished (2) After step (S-4), the Hamming weight distribution is $0 \leq H(T) \leq 8$ */.

(S-5) If $H(T)$ is odd $(H(T) = 1, 3, 5, 7)$ then construct two other shadows $B^{(j_1)}, B^{(j_2)}$ by $Y(T) = \{B^{(j_1)}, B^{(j_2)}\}$; else by $W(T) = \{B^{(j_1)}, B^{(j_2)}\}$, where $\{j_1, j_2\} \bigcup \{i_1, ...i_{n-2}\} = \{1, 2, ..., n\}$.

/* In Lemma 2, we prove that $\{B^{(j_1)}, B^{(j_2)}\}$ can be obtained from $Y(T)$ for odd $H(T)$, and from $W(T)$ for even $H(T)$. */

(S-6) Process all the blocks, and output shadow blocks $B^{(1)}...B^{(n)}$ on n noise-like shadows $NS_1 - NS_n$, respectively.

Recovering procedure:

(S-1) Obtain B by XOR-ing $(B^{(1)} \oplus ... \oplus B^{(n)})$ via from n noise-like shadows $NS_1 - NS_n$.
/* Theorem 1, demonstrates that we can obtain the original block from $B = (B^{(1)} \oplus ... \oplus B^{(n)})$ */
(S-2) Recover the color index $(b_1 - b_8)$ and the data of color palette b_9, respectively, from B.
(S-3) Repeat the above until all blocks in $NS_1 \oplus ... \oplus NS_n$ are processed, and finally SI and CP can be recovered.

4.2. Extension of (n, n)-SDIS to Share True Color Secret Image

Same as $(2, 2)$-SDIS and VC in [5], the proposed (n, n)-SDIS can be used to share a true color image. To share a true color secret image, we use a 25-subpixel block B_r, which the first three 8-tuples, $r_1, ..., r_8$, $g_1, ..., g_8$, and $bl_1, ..., bl_8$, are used to represent R, G and B color planes. The other one bit in B_r is p_9. This 25-subpixel block B_r is shown in Figure 4a. Because we share R, G and B colors directly, we do not need to use the bit p_9 to covey any information. Thus, this bit p_9 could be abandoned, or used as authentication bits to provide authentication capability like VC in [6] and PSIS in [10]. Collect $(x_1...x_8)$, where $x \in \{r, g, bl\}$, and append the bit p_9 to form red, green, and blue shadow blocks B_x where $x \in \{r, g, bl\}$ as shown in Figure 4b.

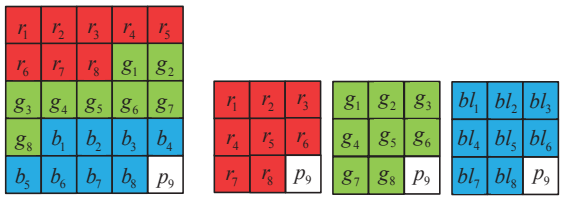


Figure 4. Blocks for sharing true clor image: (**a**) 25-bit B_T (**b**) 9-bit B_r, B_g, B_{bl}.

Detailed procedures of the proposed (n, n)-SDIS for sharing and recovering true color image are briefly described step by step as follows.

Sharing procedure:

(S′-1) Obtain 24-bit true color $r_1, ..., r_8$, $g_1, ..., g_8$, and $bl_1, ..., bl_8$ from the secret image SI, and random generate a bit p_9 to form a 25-bit block B_r, as shown in Figure 4a.
/* Parity bit p_9 is not used to covey any information, and thus it can be randomly generated */
(S′-2) Subdivide the true color block B_T to red, green, and blue shadow blocks B_r, B_g, B_{bl}.
(S′-3) Using B_r, B_g, B_{bl} as 9-bit block B in (S-1), respectively, to generate n shadow blocks $B_r^{(i)}, B_g^{(i)}, B_{bl}^{(i)}$, where $1 \leq i \leq n$, through (S-1) (S-6).
(S′-4) Collect every first 8 bits in $B_r^{(i)}, B_g^{(i)}, B_{bl}^{(i)}$, and append a black subpixel in the 25-th subpixel to generate a 25-bit shadow block $B^{(i)}$, where $1 \leq i \leq n$.
/* Because we do not use the 25-th bit p_9 in the XOR-ed result B_T to convey any information, we can use black subpixel in 25-th subpixel for all shadow blocks to enhance the number of black subpixels. */
(S′-5) Process all the blocks, and output blocks $B^{(1)} - B^{(n)}$ on n noise-like shadows $NS_1 - NS_n$, respectively.

Recovering procedure:

(R′-1) Obtain every 25-bit block B_T by XOR-ing $(B^{(1)} \oplus B^{(2)} \oplus ... \oplus B^{(n)})$ via XOR-ing n noise-like shadows $NS_1 - NS_n$.

(R′-2) Recover a true color from the first 24 bits in B_T, i.e., $r_1, ..., r_8$, $g_1, ..., g_8$, and $bl_1, ..., bl_8$.
(R′-3) Repeat the above until all blocks in $(NS_1 \oplus NS_2 ... \oplus NS_n)$ are processed, and finally a true color SI is obtained.

4.3. Enhancing Visual Quality of Color Meaningful Shadow

Consider sharing 256-color (respectively, true color) SI, noise-like shadows $NS_i, 1 \leq i \leq n$, are $3M \times 3N$ (respectively, $5M \times 5N$) times expanded. Based on noise-like shadow NS_i, we can fill in 1s in shadow blocks with the color of the corresponding cover pixel in CCI, and leave 0s blank to generate color meaningful shadow CS_i. Consider the case sharing 256-color SI. As shown in Figure 5a, there is a pixel with a blue color $\boxed{C}$ in CCI. Suppose that the block $B^{(i)}$ at corresponding position for this pixel in NS_i is $(b_1^{(i)} ... b_9^{(i)}) = (110101101)$ (see Figure 5b), and this block $B^{(i)}$ is a $\boxed{X}$ block with $6B3W$ sub-pixels (see see Figure 5c). By putting the blue cover pixel $\boxed{C}$ into all black sub-pixels in Figure 5c, we have color meaningful shadow $CS_{(i)}$ in Figure 5d. Noise-like shadow and color meaningful shadow have the same size $3M \times 3N$ subpixels and 9 times expanded when compared with CCI.

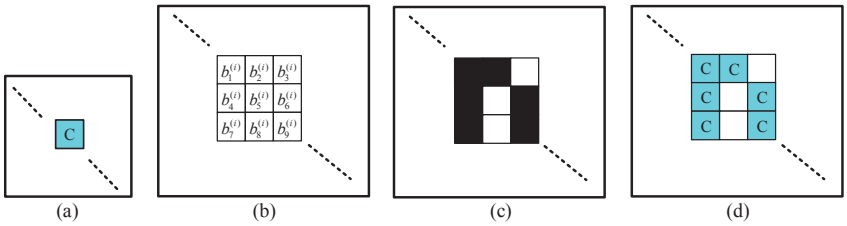


Figure 5. Block patterns: (**a**) a pixel with a color in CCI (**b**) the corresponding block $B^{(i)}$ in NS_i (**c**) the corresponding $6B3W$ block in NS_i (**d**) the corresponding block in CS_i

As shown in Figure 5d, the color at 1s in a block are the same. This is because SI and CCI have the same size with $M \times N$ pixels. To enhance visual quality of CS_i, we use a large color cover image CCI' with $3M \times 3N$ pixels (note: the original CCI has only $M \times N$ pixels). Obviously, this larger CCI' has the high resolution than CCI. As shown in Figure 6, our new approach uses a large CCI' (see Figure 6a). By putting the color pixels in to into all 1s of $B^{(1)}$ in Figure 6b, we have the CS_i' in Figure 6c. Because the color meaningful shadow CS_i' has more colors, and will have the high resolution. By the same argument, this approach can also be applied to sharing true color SI.

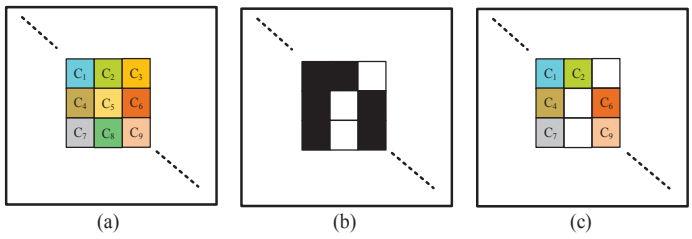


Figure 6. Block patterns: (**a**) 9 color pixels with color $C_1 - C_9$ in CCI' (**b**) the corresponding block $B^{(i)}$ in NS_i (**c**) the corresponding color block in CS_i'.

5. Theorem and Security Analysis

5.1. Main Theorems and Examples

Lemma 1. *Suppose that the block T in Equation (1) is all-1 block, i.e., $H(T) = 9$. We may change any two positions (one is $1 \rightarrow 0$ and the other is $0 \rightarrow 1$) in any one block $B^{(i_j)}, 1 \leq j \leq n-2$, such that the equation $B = T \oplus B^{(i_1)} \oplus ... \oplus B^{(i_{n-2})}$ holds, and $H(T)$ is reduced from 9 to 7. Meanwhile, all $(n-2)$ blocks $B^{(i_j)}, 1 \leq j \leq n-2$, are still $\boxed{X}$ blocks.*

Proof. As shown in Equation (1), all these $(n-2)$ blocks $B^{(i_1)} - B^{(i_{n-2})}$ are $\boxed{X}$ blocks. We choose one block $B^{(i_j)}$, and modify any two positions of $1 \to 0$ and $0 \to 1$. This modification will change the 1 in the block T to 0 at these two chosen modified positions. After that, $H(T)$ is reduced to $9-2=7$. Meanwhile, because we change two positions by $1 \to 0$ and $0 \to 1$, respectively, the Hamming weight $H(B^{(i_j)})$ is unchanged, and this shadow block $B^{(i_j)}$ is still a $\boxed{X}$ block. □

Lemma 2. *Blocks $B^{(j_1)}, B^{(j_2)}$ in step (S-5) can be obtained from $Y(T)$ for odd $H(T)$, and from $W(T)$ for even $H(T)$.*

Proof. Let X_1 be $\boxed{X}$ block, and both Y_1 and Y_2 be $\boxed{Y}$ blocks. We first prove that the possible Hamming weights of (Y_1, Y_2) are $0, 2, 4, 6, 8$, and the possible Hamming weights of (X_1, Y_2) are $1, 3, 5, 7$. Because both blocks Y_1 and Y_2 have the same Hamming weight 5, the number of positions of $1 \to 0$ and $0 \to 1$ crossing from vectors Y_1 to Y_2 should be the same. Suppose that this number is y. Therefore, the (Y_1, Y_2) has the following form (see Equation (3)), where $0 \le y \le 4$. Obviously, the Hamming weight of $(Y_1 Y_2)$ in Equation (3) is $2y$, and thus $H(Y_1 Y_2)$ may be $0, 2, 4, 6, 8$. □

$$\begin{cases} Y_1 = \overbrace{1...1}^{y} \ \overbrace{0...0}^{y} \ \overbrace{1...1}^{5-y} \ \overbrace{0...0}^{5-y} \\ Y_2 = \ \ 0...0 \ \ 1...1 \ \ 1...1 \ \ 0...0 \\ Y_1 \oplus Y_2 = 1...1 \ \ 1...1 \ \ 0...0 \ \ 0...0 \end{cases} \quad \begin{matrix} \\ \downarrow \ \uparrow \ \updownarrow \ \updownarrow \\ \\ \end{matrix} \tag{3}$$

Consider the XOR-ed block $(X_1 \oplus Y_2)$. Because blocks X_1 and Y_2 have Hamming weights 6 and 5, respectively. The number of positions of $1 \to 0$ and $0 \to 1$ crossing from vectors X_1 to Y_2 should differ with one. Suppose that the number crossing from vectors X_1 to Y_2 of $1 \to 0$ is $x+1$, and the number of $0 \to 1$ is x. Therefore, the $(X_1 \oplus Y_2)$ has the following form (see Equation (4)), where $0 \le x \le 3$. The Hamming weight of $(X_1 Y_2)$ in Equation (4) is $(2x+1)$, and thus $H(X_1 \oplus Y_2)$ may be $1, 3, 5, 7$.

$$\begin{cases} X_1 = \overbrace{1...1}^{x+1} \ \overbrace{0...0}^{x} \ \overbrace{1...1}^{5-x} \ \overbrace{0...0}^{3-x} \\ Y_2 = \ \ 0...0 \ \ 1...1 \ \ 1...1 \ \ 0...0 \\ X_1 \oplus Y_2 = 1...1 \ \ 1...1 \ \ 0...0 \ \ 0...0 \end{cases} \quad \begin{matrix} \\ \downarrow \ \uparrow \ \updownarrow \ \updownarrow \\ \\ \end{matrix} \tag{4}$$

Because Wei et al.'s $(2,2)$-SDIS uses two $\boxed{Y}$ blocks (say Y_1 and Y_2), therefore using Wei et al.'s $(2,2)$-SDIS has $H(Y_1 \oplus Y_2)$ with even values $0, 2, 4, 6, 8$. On the other hand, there are one $\boxed{X}$ block and one $\boxed{Y}$ block (say X_1 and Y_2) when using Yang et al.'s $(2,2)$-SDIS. Thus, using Yang et al.'s $(2,2)$-SDIS has $H(X_1 \oplus Y_2)$ with odd values $1, 3, 5, 7$. Finally, the above implies that $\{B^{(j_1)}, B^{(j_2)}\}$ can be obtained from $Y(T)$ for odd $H(T) = 1, 3, 5, 7$, and can be obtained from $W(T)$ for even $H(T) = 0, 2, 4, 6, 8$.

The following theorem shows that the proposed (n,n)-SDIS is a n-out-of-n sharing scheme that we can recover SI and CP from n noise-like shadows $(NS_1 - NS_n)$, and cannot obtain SI and CP from $(n-1)$ or fewer shadows.

Theorem 1. *The proposed (n,n)-SDIS is n-out-of-n sharing scheme that the XOR-ed result of n shadow blocks can represent* 0 255 *color indices and the data of color palette.*

Proof. We first prove that sharing procedure can successfully generate n shadow blocks $B^{(i)}, 1 \le i \le n$. Suppose that a block $B = (\overbrace{b_1...b_8}^{colorindex}, \overbrace{b_9}^{colorpalette})$ is composed of 8-bit color index (0 255) and 1-bit data of color palette, which are obtained from SI and CP. By Equation (1), we first randomly generate $(n-2)$ $\boxed{X}$ blocks $B^{(i_j)}, 1 \le j \le n-2$, and then calculate the temporary block T via $T = B \oplus B^{(i_1)} \oplus ... \oplus B^{(i_{n-2})}$. After step (S-4), the Hamming weight distribution of $H(T)$ is 0 8 (see Lemma 1). By Lemma 2, we

can obtain $\{B^{j_1}, B^{(j_2)}\}$ from $Y(T)$ (respectively, $W(T)$) for odd $(1,3,5,7)$ (respectively, even $(0,2,4,6,8)$ $H(T)$. Finally, we have n shadow blocks $\{B^1, ..., B^n\}$. Process all the blocks, and we can generate n noise-like shadows.

Next, we consider the recovery. As shown in Equation (2), we can recover the original block $B = (b_1...b_9)$ from $B = B^{(1)} \oplus ... \oplus B^{(n)}$. Therefore, we can determine the color index $(b_1...b_8)$ and the data of color palette b_9. After obtaining all blocks, we can recover SI and CP. Because of $B = B^{(1)} \oplus ... \oplus B^{(n)}$, it is obvious that we cannot recover the original block B via $(n-1)$ or fewer shadow blocks. □

Let the ratio of average number of black subpixels in a block (i.e., the regions in shadows showing the content of cover image) for Wei et al.'s $(2,2)$-SDIS, Yang et al.'s $(2,2)$-SDIS, and the proposed (n,n)-SDIS be R_W, R_Y, R_P. In addition, let the contrasts of binary meaningful shadows for Wei et al.'s $(2,2)$-SDIS, Yang et al.'s $(2,2)$-SDIS, and the proposed (n,n)-SDIS be C_W, C_Y, C_P. The following theorem demonstrates $R_W \leq R_Y \leq R_P$ and $C_W \leq C_Y \leq C_P$.

Theorem 2. *The ratio of average numbers of black subpixels in a 9-bit block for Wei et al.'s $(2,2)$-SDIS, Yang et al.'s $(2,2)$-SDIS, and the proposed (n,n)-SDIS are $R_W = \frac{5}{9}, R_Y = \frac{5.5}{9}, R_P = \frac{6-1.5/n}{9}$ where $R_W < R_Y < R_P$. The contrasts of binary meaningful shadows for Wei et al.'s $(2,2)$-SDIS, Yang et al.'s $(2,2)$-SDIS, and the proposed (n,n)-SDIS are $C_W = \frac{1}{9}, C_Y = \frac{2}{9}, C_P = \frac{3-3/n}{9}$, where $C_W < C_Y < C_P$.*

Proof. Wei et al.'s $(2,2)$-SDIS has all $\boxed{Y}$ blocks on both shadows, and thus $R_W = \frac{5}{9}$. On the other hand, both shadows of Yang et al.'s $(2,2)$-SDIS are composed of $\boxed{X}$ and $\boxed{Y}$ blocks half and half. Therefore, we have $R_Y = \frac{(6+5)/2}{9} = \frac{5.5}{9}$. For the proposed (n,n)-SDIS, Step (S-5) implies that Yang et al.'s $(2,2)$-SDIS and Wei et al.'s $(2,2)$-SDIS are evenly used in the proposed (n,n)-SDIS. This is because the Hamming weights $H(T)$ are odd and even half and half. Therefore, the value of R_P is derived as follows.

$$\begin{cases} R_P = \frac{1}{2} \times \overbrace{\frac{((n-2)\times 6 + 2\times 5)/n}{9}}^{using Weiet.al(2,2)-SDIS} + \\ \frac{1}{2} \times \underbrace{\frac{((n-1)\times 6 + 1\times 5)/n}{9}}_{using Weiet.al(2,2)-SDIS} \\ = \frac{3-1/n}{9} + \frac{3-0.5/n}{9} = \frac{6-1.5/n}{9} \end{cases} \tag{5}$$

It is obvious that $R_P \geq \frac{5.5}{9}$ with equality for $n = 3$. From these values $R_W = \frac{5}{9}, R_Y = \frac{5.5}{9}, R_P = \frac{6-1.5/n}{9}$, we have $R_W < R_Y < R_P$

The contrast is the difference of blackness for black block and white block. In binary meaningful shadows $BS_1 - BS_n$, we complement the blocks for the corresponding white cover pixels to generate white shadow blocks. Thus, if the number of black subpixels in a black shadow block is n_B, then the he number black subpixels in a white shadow block is $9 - n_B$. Thus, we have $C_W = \frac{5-(9-5)}{9} = \frac{1}{9}, C_Y = \frac{5.5-(9-5.5)}{9} = \frac{2}{9}, C_P = \frac{6-1.5/n-(9-6+1.5/n)}{9} = \frac{3-3/n}{9}$. It is obvious that $C_P \geq \frac{2}{9}$ with equality for $n = 3$. From these values $C_W = \frac{1}{9}, C_Y = \frac{2}{9}, C_P = \frac{3-3/n}{9}$ we have $C_W < C_Y \leq C_P$. □

An illustrative example gives a quick understanding for the proposed (n,n)-SDIS.

Example 1. *Share and recover the following information $(c,d) = (176,0)$ and $(49,1)$, where c is the color index and d is the data of color palette, by the proposed $(4,4)$-SDIS.*

Given $(c,d) = (176,0)$, we have the block $B = (\overbrace{b_1...b_8}^{c}, \overbrace{b_9}^{d}) = (\overbrace{10110000}^{176}, \overbrace{0}^{0})_2$. By step (S-2), we randomly generate two $\boxed{X}$ blocks (say $B^{(1)}, B^{(2)}$). Suppose that these two random blocks are

$B^{(1)} = (101110110)$ and $B^{(2)} = (111101001)$ with $H(B^{(1)}) = H(B^{(2)}) = 6$, and then we obtain the temporary block T via the following equation.

$$\begin{cases} T = B \oplus B^{(1)} \oplus B^{(2)} \\ = (101100000) \oplus (101110110) \oplus (111101001) \\ = (111111111) \end{cases} \tag{6}$$

Because of $H(T) = 9$, we should modify any two positions (one is $1 \to 0$ and the other is $0 \to 1$) in one block (say $B^{(2)}$), to reduce $H(T)$ from 9 to 7. For example, we may modify $B^{(2)}$ as (111101100). Finally, we have $T = (111111010)$ with $H(T) = 7$, and meanwhile the new block $B^{(2)} = (111101100)$ is still a $\boxed{X}$ block. Since $H(T) = 7$ is odd, we apply Yang et al.'s $(2,2)$-SDIS to obtain $Y(111111010) = 7$, which can be determined from Equation (7). Finally, all four shadow blocks are $B^{(1)} = (101110110), B^{(2)} = (111101100), B^{(3)} = (110110101), B^{(4)} = (001001111)$, where $B^{(1)}, B^{(2)}, B^{(3)}$ are $\boxed{X}$ blocks, and $B^{(4)}$ is $\boxed{Y}$ block.

$$\begin{cases} B^{(3)} = (110110101) : \boxed{X} \\ \overset{\oplus}{B^{(4)}} = (001001111) : \boxed{Y} \\ T = (111111010) \end{cases} \tag{7}$$

Consider another case $(c,d) = (49,1)$. We have the block $B = (\overbrace{001100011}^{49}, \overbrace{1}^{1})_2$. From step (S-2), we randomly select two $\boxed{X}$ blocks (say $B^{(1)}, B^{(2)}$). Suppose that these two random blocks are $B^{(1)} = (011111001)$ and $B^{(2)} = (110011011)$, and then we obtain the temporary block T via Equation (8).

$$\begin{cases} T = B \oplus B^{(1)} \oplus B^{(2)} \\ = (001100011) \oplus (011111001) \oplus (110011011) \\ = (100000001) \end{cases} \tag{8}$$

Since $H(T) = 2$ is even, we apply Wei et al.'s $(2,2)$-SDIS to obtain $Y(100000001) = (B^{(3)}, B^{(4)})$, which can be determined from Equation (9). Finally, all four blocks are $B^{(1)} = (011111001), B^{(2)} = (110011011), B^{(3)} = (110101010), B^{(4)} = (010101011)$, where $B^{(1)}, B^{(2)}$ are $\boxed{X}$ blocks, and $B^{(3)}, B^{(4)}$ are $\boxed{Y}$ blocks.

$$\begin{cases} B^{(3)} = (110101010) : \boxed{Y} \\ \overset{\oplus}{B^{(4)}} = (010101011) : \boxed{Y} \\ T = (100000001) \end{cases} \tag{9}$$

For recovery, consider the case: $B^{(1)} = (101110110), B^{(2)} = (111101100), B^{(3)} = (110110101), B^{(4)} = (001001111)$. The XOR-ed result is $B = B^{(1)} \oplus B^{(2)} \oplus B^{(3)} \oplus B^{(4)} = (101100000)$, and thus $(c,d) = (176,0)$. For the other case: $B^{(1)} = (011111001), B^{(2)} = (110011001), B^{(3)} = (110101010), B^{(4)} = (010101011)$, the XOR-ed result is $B = B^{(1)} \oplus B^{(2)} \oplus B^{(3)} \oplus B^{(4)} = (101100000)$. Therefore, we have $(c,d) = (49,1)$.

Let $R_P^{'}$ be the ratio of average numbers of black subpixels in a 25-bit shadow block for the proposed (n,n)-SDIS sharing true color image. The following theorem demonstrates $R_P^{'} > R_P$, i.e., the meaningful shadows of sharing true color secret image have the better visual quality than those of sharing 256-color secret image.

Theorem 3. *The ratio of average numbers of black subpixels in a* 25*-bit block for the proposed* (n,n)*-SDIS sharing true color image is* $R_P^{'} = \frac{17}{25} - \frac{0.16}{n}$*, where* $R_P^{'} > R_P$*.*

Proof. If the blocks $B_r^{(i)}, B_g^{(i)}, B_{bl}^{(i)}$ are $\boxed{X}$ (respectively, $\boxed{Y}$) blocks, then the first 8 bits in $B_r^{(i)}, B_g^{(i)}, B_{bl}^{(i)}$ has 6 black subpixels with $\frac{C_8^6}{C_9^6}$ percentage and 5 black subpixels with $\frac{C_8^5}{C_9^6}$ percentage (respectively, 5 black subpixels with $\frac{C_8^5}{C_9^5}$ percentage and 4 black subpixels with $\frac{C_8^4}{C_9^5}$ percentage). The average number of black pixels for the first 8 bits in $B_r^{(i)}, B_g^{(i)}, B_{bl}^{(i)}$ is $6 \times \frac{C_8^6}{C_9^6} + 5 \times \frac{C_8^5}{C_9^6} = \frac{16}{3}$ for $\boxed{X}$ blocks, and is $5 \times \frac{C_8^5}{C_9^5} + 4 \times \frac{C_8^4}{C_9^5} = \frac{40}{3}$ for $\boxed{X}$ blocks. Therefore, the average number of black subpixels in every 8 bits in the first 24 bits of $B^{(i)}$ is $\frac{16n-4}{3n}$, as derived below.

$$\begin{cases} \overbrace{\frac{1}{2} \times ((n-2) \times 16/3 + 2 \times 40/9)/n}^{using Weiet.al(2,2)-SDIS} + \\ \overbrace{\frac{1}{2} \times ((n-1) \times 16/3 + 1 \times 40/9)/n}^{using Yanget.al(2,2)-SDIS} \\ = \frac{24n-8}{9n} + \frac{24n-4}{9n} = \frac{16n-4}{3n} \end{cases} \tag{10}$$

Because the 25-th bit in shadow block is always 1, and thus the value of R_P' is determined as $R_P' = \frac{3 \times (16n-4)/3n+1}{25} = \frac{17}{25} - \frac{0.16}{n}$. The following equation implies $R_P' > R_P$.

$$\begin{cases} R_P' = \frac{17}{25} - \frac{0.16}{n} > \frac{6}{9} - \frac{0.16}{n} > \frac{6}{9} - \frac{1.5/9}{n} \\ \frac{6-1.5/n}{9} = R_P \end{cases} \tag{11}$$

□

5.2. Security Analysis: The $(n-1)$-Colluder Attack

Here, we consider an attack way that $(n-1)$ participants collude together and want to figure out SI and CP. The $(n-1)$-colluder attack is a very extreme attack for the proposed (n,n)-SDIS, because it needs $(n-1)$ participants jointly providing their shadows for guessing SI and CP. We first discuss the $(n-1)$-colluder attack on Wei et al.'s $(2,2)$-SDIS and Yang et al.'s $(2,2)$-SDIS. Suppose that Participant 1 wants to predict SI and CP from his own shadow NS_1. Because the color palette CP information is conveyed by the ninth bit $b_9^{(1)}$ of every block on NS_1. Therefore, the CP can be completely obtained from NS_1. Even though Participant 1 has the color palette CP, but he cannot obtain the information about color index. An attacker has $\frac{1}{256} \approx 0.004$ probability to figure out the correct color index $(b_1 ... b_8)$ of block B without any shadow. This value of $\frac{1}{256}$ is a brute-force probability, which tries all possible 256 colors in the color palette. However, for the $(n-1)$-colluder attack, Participant 1 has $B^{(1)}$. By cryptanalytic attacks relying on knowing one shadow (the first eight bit of $B^{(1)}$), Participant 1 may guess the color index. Let the successful probability to recover the block B for Wei et al.'s $(2,2)$-SDIS and Yang et al.'s $(2,2)$-SDIS be P_W and P_Y, respectively, when collecting one shadow. Because both shadow blocks of Wei et al.'s $(2,2)$-SDIS are all $\boxed{Y}$ blocks $(5B4W)$, obviously P_W is $\frac{1}{C_9^5} = \frac{1}{126} \approx 0.008$. On the other hand, shadow blocks of Yang et al.'s $(2,2)$-SDIS are evenly composed of $\boxed{X}$ blocks and $\boxed{Y}$ blocks. Thus, $P_Y = \frac{1/C_9^6 + 1/C_9^5}{2} = \frac{1/84 + 1/126}{2} \approx 0.01$. Both probabilities 0.08 and 0.01 are higher than the brute-force probability 0.004. However, these probabilities 0.08 and 0.01 are still practically secure for guessing 256 colors.

Let the successful probability to recover the block B for $(n-1)$-colluder attack, for the proposed (n,n)-SDIS, be P_P. In the following theorem, we theoretically prove $P_P = \frac{1}{C_9^6} - \frac{3}{2n} \times (\frac{1}{C_9^6} - \frac{1}{C_9^5})$.

Theorem 4. *The successful probability to recover the block B in the proposed (n,n)-SDIS for $(n-1)$-colluder attack is $P_P = \frac{1}{C_9^6} - \frac{3}{2n} \times (\frac{1}{C_9^6} - \frac{1}{C_9^5})$, where $P_W \leq P_Y \leq P_P$.*

Proof. Suppose that there are $(n-1)$ shadows (say $B^{(1)} - B^{(n-1)}$) for reconstruction, on which we may guess the type of shadow block in the corresponding position of $B^{(n)}$. The block $B^{(n)}$ has $\boxed{X}$ block and $\boxed{Y}$ block with $\frac{2n-3}{2n}$ probability and $\frac{3}{2n}$ probability, respectively, which are derived below.

$$\begin{cases} \frac{1}{2} \times \frac{\overbrace{C_2^2 \cdot C_{n-2}^1}^{Weietal's(2,2)SDIS}}{C_n^{n-1}} + \frac{1}{2} \times \frac{\overbrace{C_1^1 \cdot C_{n-1}^1}^{Yanget.al's(2,2)-SDIS}}{C_n^{n-1}} = \frac{2n-3}{2n} \\ (B^{(n)} : \boxed{X}) \\ \frac{1}{2} \times \frac{\overbrace{C_2^1 \cdot C_{n-2}^{n-2}}^{Weietal's(2,2)SDIS}}{C_n^{n-1}} + \frac{1}{2} \times \frac{\overbrace{C_1^1 \cdot C_{n-1}^{n-1}}^{Yanget.al's(2,2)-SDIS}}{C_n^{n-1}} = \frac{3}{2n} \\ (B^{(n)} : \boxed{Y}) \end{cases} \tag{12}$$

If $B^{(n)}$ is $\boxed{X}$ block (respectively, $\boxed{Y}$ block), there is $\frac{1}{C_9^6}$ (respectively, $\frac{1}{C_9^5}$) probability to guess the correct color index $(b_1...b_8)$, which is better than brute-force probability $\frac{1}{256}$. Thus, P_P is calculated as follows.

$$P_P = \overbrace{\frac{2n-3}{2n} \times \frac{1}{C_9^6}}^{\boxed{X}block} + \overbrace{\frac{3}{2n} \times \frac{1}{C_9^5}}^{\boxed{Y}block} = \frac{1}{C_9^6} - \frac{3}{2n} \times (\frac{1}{C_9^6} - \frac{1}{C_9^5}) \tag{13}$$

□

Since $P_W = \frac{1}{C_9^5}$ and $P_Y = \frac{1/C_9^5 + 1/C_9^6}{2}$, we have $P_W < P_Y$. About P_Y and P_P, the relation is derived as follows.

$$\begin{cases} P_P = \frac{1}{C_9^6} - \frac{3}{2n} \times (\frac{1}{C_9^6} - \frac{5}{9}) = \frac{2n-3}{2n} \times \frac{1}{C_9^6} + \frac{3}{2n} \times \frac{1}{C_9^5} \\ = \frac{n}{2n} \times \frac{1}{C_9^6} + (\frac{n-3}{2n} \times \frac{1}{C_9^6} + \frac{3}{2n} \times \frac{1}{C_9^5}) \\ \geq \frac{n}{2n} \times \frac{1}{C_9^6} + (\frac{n-3}{2n} \times \frac{1}{C_9^5} + \frac{3}{2n} \times \frac{1}{C_9^5}) \\ = \frac{1/C_9^5 + 1/C_9^6}{2} = P_Y \end{cases} \tag{14}$$

For $n = 3$, the value of P_P is $P_P = \frac{1/C_9^5 + 1/C_9^6}{2} = P_Y$, and P_P approaches to $\frac{1}{C_9^6}$ for large n. In fact, the value of $\frac{1}{C_9^6} = \frac{1}{84} \approx 0.012$ is almost the same as $P_y \approx 0.01$. For this extreme case, the $(n-1)$-colluder attack, the security of the proposed (n,n)-SDIS is close to that of Yang et al.'s $(2,2)$-SDIS. By the same argument, for other cases collecting $(n-2)$ or shadows, the possible combination of collected shadows is more difficult to analyze compared with collecting $(n-1)$ shadows, and even less than the brute-force probability.

In the proposed (n,n)-SDIS, the color palette information is conveyed by b_9 (the ninth bit in B), but not the ninth bit $b_9^{(1)}$ of the block $B^{(1)}$ in NS_1. Therefore, the color palette CP may be obtained from only one shadow for Wei et al.'s $(2,2)$-SDIS and Yang et al.'s $(2,2)$-SDIS. Even though an attacker has the CP information, he still cannot obtain the secret image SI. For the proposed (n,n)-SDIS, the color palette information in B is securely protected and only can be determined from XOR-ing n blocks $B^{(1)} \oplus ... \oplus B^{(n)}$. This makes the cryptanalysis is more difficult for the proposed (n,n)-SDIS. The following theorem demonstrates the successful probability P_C to recover a correct color in CP for the proposed (n,n)-SDIS when collecting $(n-1)$ shadows.

Theorem 5. *The successful probability to recover a correct color in CP for the proposed (n,n)-SDIS when collecting $(n-1)$ shadows is $P_C = (\frac{2}{3} - \frac{1/6}{n})^{24}$.*

Proof. Each color information in CP is encapsulated in 24 blocks, which every block should be derived from $B = B^{(1)} \oplus ... \oplus B^{(n)}$. If colluders have $(n-1)$ shadows (say $NS_1 - NS_{n-1}$), for a block B, they have the XOR-ed result $B^{'} = B^{(1)} \oplus ... \oplus B^{(n-1)}$, and can guess that the shadow block $B^{(n)}$ is $\boxed{X}$ block and $\boxed{Y}$ block with $\frac{2n-3}{2n}$ probability and $\frac{3}{2n}$ probability, respectively. For $\boxed{X}$ block, it implies that we have $\frac{6}{9}$ probability that the bit b_9 is the complementary bit $b_9^{'}$ in $B^{'}$. On the other hand, we have $\frac{5}{9}$ probability that the bit b_9 is the complementary bit $b_9^{'}$ in $B^{'}$ for $\boxed{Y}$ block. Therefore, the average probability of guessing b_9 is derived as $\overbrace{\frac{2n-3}{2n} \times \frac{6}{9}}^{\boxed{X}\,block} + \overbrace{\frac{3}{2n} \times \frac{5}{9}}^{\boxed{Y}\,block} = \frac{2}{3} - \frac{1/6}{n}$ Note: every block has one-bit color palette information, and a true color is represented by 24-bit R, G, and B color planes. Because colluders can guess the bit b_9 with $\frac{2}{3} - \frac{1/6}{n}$ probability, P_C is $(\frac{2}{3} - \frac{1/6}{n})^{24}$. □

Therefore, the value $P_C = (\frac{2}{3} - \frac{1/6}{n})^{24}$ is less than $(\frac{2}{3})^{24} \approx 5.94 \times 10^{-5}$, and this implies that the color palette cannot be recovered under $(n-1)$-colluder attack.

6. Evaluation and Comparisons

6.1. Experimental Results

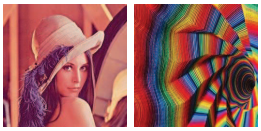
Seven experiments (Experiments $A - H$) are conducted to evaluate the proposed (n,n)-SDIS from various aspects: (A) noise-like shadows NS_1, NS_2, NS_3 sharing 256-color image for $(3,3)$-SDIS (B) binary meaningful shadows BS_1, BS_2, BS_3 sharing 256-color image for $(3,3)$-SDIS (C) color meaningful shadows CS_1, CS_2, CS_3 sharing 256-color image for $(3,3)$-SDIS (D) color meaningful shadows CS_1, CS_2, CS_3 sharing true color image for $(3,3)$-SDIS (E) binary meaningful shadows $(NS_1 - NS_4)$ and color meaningful shadows $(CS_1 - CS_4)$ for $(4,4)$-SDIS (F) binary meaningful shadows $(NS_1 - NS_5)$ and color meaningful shadows $(CS_1 - CS_5)$ for $(5,5)$-SDIS (G) color meaningful shadows $CS_1^{'}, CS_2^{'}, CS_3^{'}$ sharing 256-color image for $(3,3)$-SDIS by the approach of enhancing visual quality.

Experiments $A - D$ are the $(3,3)$-SDIS. Experiment A has noise-like shadows, and other four experiments are meaningful shadows. Experiments D demonstrates sharing true color secret image. Experiments E and F demonstrate binary and color meaningful shadows for $(4,4)$-SDIS and $(5,5)$-SDIS, respectively. In Experiment G, we redo Experiment C to enhance the visual quality of color meaningful shadows by using the approach in Figure 6.

In all experiments, five binary cover images $BCI_1 - BCI_5$ with black-and-white printed texts $\boxed{A}$, $\boxed{B}$, $\boxed{C}$, $\boxed{D}$, $\boxed{E}$, and five color cover images $CCI_1 - CCI_5$ with photos of birds are used. In addition, two secret images SI_1 (Lena: 256-color image), SI_2 (Kaleidoscope: true color image) are used. All these images $BCI_1 - BCI_5$ (see Figure 7), $CCI_1 - CCI_5$ (see Figure 8), and SI_1, SI_2 (see Figure 9) are 256×256 pixels.

Figure 7. Five color cover images with photos of birds: (**a**) BCI_1 (**b**) BCI_2 (**c**) BCI_3 (**d**) BCI_4 (**e**) BCI_5.

Figure 8. Five color cover images with photos of birds: (**a**) CCI_1 (**b**) CCI_2 (**c**) CCI_3 (**d**) CCI_4 (**e**) CCI_5.



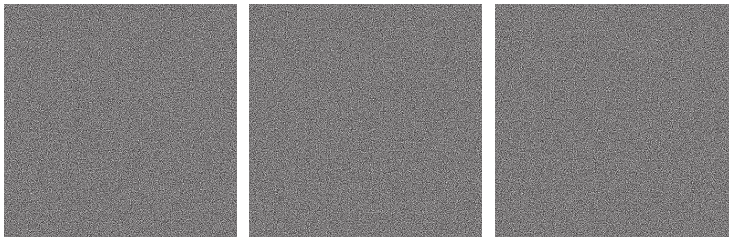
(a) (b)

Figure 9. Two secret images: (**a**) SI_1: 256-color Lena (**b**) SI_2: true color Kaleidoscope.

Because shadows may be 9 or 25 times expanded in experiments, for demonstrating all the images in a single page, the shadow images in experiments are not correctly proportional.

Experiment A. Three noise-like shadows $NS_1 - NS_3$ of the proposed $(3,3)$-SDIS sharing a 256-color secret image are demonstrated.

The secret image SI_1: 256-color Lena in Figure 9a is used to test the proposed $(3,3)$-SDIS. Each noise-like shadow has $\frac{2n-3}{2n} = \frac{6-3}{6} = 50\%$ $\boxed{X}$ blocks and $\frac{3}{2n} = \frac{3}{6} = 50\%$ $\boxed{Y}$ blocks, which are the same as Yang et al.'s $(2,2)$-SDIS. As shown in Figure 10, three noise-like shadows are expanded to 768×768 pixels. Via recovering procedure, we can recover the original 256-color secret image Lena.

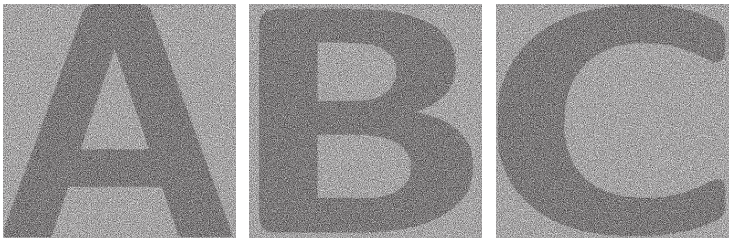


(a) (b) (c)

Figure 10. Noise-like shadows of the proposed $(3,3)$-SDIS: (**a**) NS_1 (**b**) NS_2 (**c**) NS_3.

Experiment B. Three binary meaningful shadows $BS_1 - BS_3$ of the proposed $(3,3)$-SDIS sharing a 256-color secret image are demonstrated.

By revering (respectively, unchanging) the color of subpixels in a block of $B^{(1)}$, $B^{(2)}$, and $B^{(3)}$ on NS_1, NS_2 and NS_3 in **Experiment A** to represent the white (respectively, black) color in $BCI_1 - BCI_3$ (A, B, and C in Figure 7a–c). The proposed $(3,3)$-SDIS has the contrast $C_P = \frac{3-(3/n)}{9} = \frac{3-(3/3)}{9} = \frac{2}{9}$ (see Theorem 2). It is observed that the printed-texts A, B, and C are revealed indeed on $BCI_1 - BCI_3$, with the size of 768×768 pixels (see Figure 11a–c). Consider recovery. We first transfer the $3B6W$ block and $4B5W$ block to $6B3W$ block and $5B4W$ block, respectively. Afterwards, via the recovering procedure, we may recover the 256-color secret image Lena.



(a) (b) (c)

Figure 11. Binary meaningful shadows of the proposed $(3,3)$-SDIS: (**a**) BS_1 (**b**) BS_2 (**c**) BS_3.

Experiment C. Three color meaningful shadows $CS_1 - CS_3$ of the proposed $(3,3)$-SDIS sharing a 256-color secret image are demonstrated.

By adopting the color pixels in $CCI_1 - CCI_3$ into black subpixels in blocks $B^{(1)}, B^{(2)}$, and $B^{(3)}$ on NS_1, NS_2 and NS_3, respectively, we generate three color meaningful shadows $CS_1 - CS_3$ with the size of 768×768 pixels. Each color meaningful shadow has $R_P = \frac{6-(1.5/n)}{9} = \frac{6-(1.5/3)}{9} = \frac{5.5}{9}$. As shown in Figure 12a–c, it is observed that the images of three photos of birds in Figure 8a–c are revealed on $CS_1 - CS_3$. Consider recovery. We first transfer the color subpixel in every block to $''1''$s and white subpixel to $''0''$. Afterwards, via the recovering procedure, we may recover the 256-color secret image Lena.

(a) (b) (c)

Figure 12. Color meaningful shadows of the proposed $(3,3)$-SDIS: (**a**) CS_1 (**b**) CS_2 (**c**) CS_3.

Experiment D. Three color meaningful shadows $CS_1 - CS_3$ of the proposed $(3,3)$-SDIS sharing a true color secret image are demonstrated.

The secret image SI_2: true color Kaleidoscope is used to test the proposed $(3,3)$-SDIS sharing a true color secret image. For a secret pixel, we use the information of R, G, and B color planes to form a 25-bit block. By adopting the color pixels in $CCI_1 - CCI_3$ into three 25-subixle shadow blocks, we can generate three color meaningful shadows $CS_1 - CS_3$ with the size of 1280×1280 pixels (25 times expanded). Each color meaningful shadow has $R_P^{'} = \frac{17}{25} - \frac{0.16}{n} = 0.627$ (see Theorem 3) larger than $R_P = \frac{5.5}{9} = 0.611$ in Experiment C, to show the content of cover image. As shown in Figure 13a–c, it is observed that the images $CCI_1 - CCI_3$ are revealed on $CS_1 - CS_3$. Via the recovering procedure, we may recover the true color secret image Kaleidoscope.

Experiment E. Four binary meaningful shadows $BS_1 - BS_4$ and four color meaningful shadows $CS_1 - CS_4$ of the proposed $(4,4)$-SDIS sharing a 256-color secret image are demonstrated.

Four binary cover images printed-texts in Figure 7a–d, and four color cover images $CCI_1 - CCI_4$ in Figure 8a–d are used. Finally, four binary meaningful shadows $BS_1 - BS_4$, and four color meaningful shadows $CS_1 - CS_4$ are illustrated in Figure 14a,b, respectively. All these shadows have the sizes of 768×768 pixels. Binary meaningful shadows of $(4,4)$-SDIS have $C_P = \frac{3-(3/n)}{9} = \frac{3-(3/4)}{9} = \frac{2.25}{9}$, and color meaningful shadows of $(4,4)$-SDIS have $R_P = \frac{6-(1.5/n)}{9} = \frac{6-(1.5/4)}{9} = \frac{5.625}{9}$. Both values are greater than $\frac{2}{9}$ (Experiment B) and $\frac{5.5}{9}$ (Experiment C), respectively.

Experiment F. Five binary meaningful shadows $BS_1 - BS_5$ and five color meaningful shadows $CS_1 - CS_5$ of the proposed $(5,5)$-SDIS sharing a 256-color secret image are demonstrated.

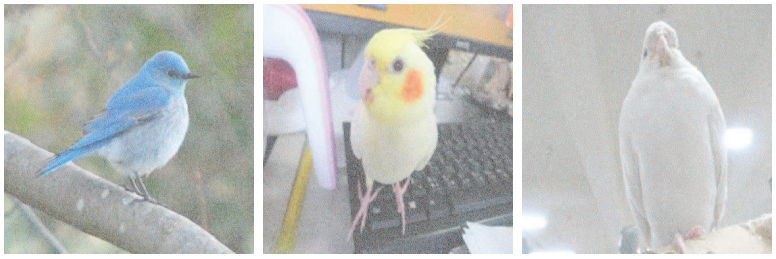
Five color cover images printed-texts in Figure 7a–e, and five color cover images $CCI_1 - CCI_5$ in Figure 8a–e are used. Finally, fiver binary meaningful shadows $BS_1 - BS_5$, and five color meaningful shadows $CS_1 - CS_5$ are illustrated in Figure 15a,b, respectively. All these shadows have the sizes of 768×768 pixels. Binary meaningful shadows of $(5,5)$-SDIS have $C_P = \frac{3-(3/n)}{9} = \frac{3-3/5}{9} = \frac{2.4}{9}$, and color meaningful shadows of $(5,5)$-SDIS have $R_P = \frac{6-(1.5/n)}{9} = \frac{6-1.5/5}{9} = \frac{5.7}{9}$. Both values are better than those of $(3,3)$-SDIS.

Experiment G. Redo Experiment C, but use the approach of enhancing visual quality of color meaningful shadows. Three $CS_1^{'} - CS_3^{'}$ are demonstrated.

In Experiment C, three 256×256-pixel color cover images $CCI_1 - CCI_3$ in Figure 8a–c are used. To enhance the visual quality of $CS_1 - CS_3$, we use another three 768×768-pixel $CCI_1^{'} - CCI_3^{'}$, which

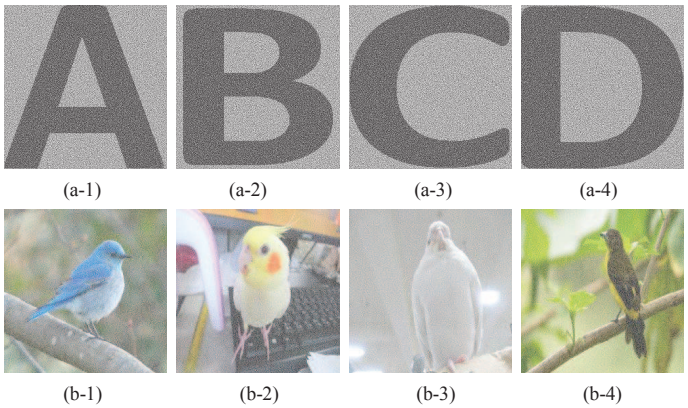
has high resolution. These three images $CCI_1^{'} - CCI_3^{'}$ are omitted here for brevity. By using the approach in Figure 6, we use color pixels in $CCI_1^{'} - CCI_3^{'}$ into black subpixels in blocks $B^{(1)}$, $B^{(2)}$, and $B^{(3)}$ on NS_1, NS_2 and NS_3, respectively to generate three color meaningful shadows $CS_1^{'} - CS_3^{'}$ with the size of 768×768 pixels. As shown in Figure 16a–c, it is observed that Figure 16 has better visual quality than Figure 12. However, the photos $CCI_1 - CCI_3$ used in this experiment may not clearly demonstrate the enhancement. Here, we use a cover image, a colorful centered fractal, for testing. Figure 17(a-1,b-1) shows two color meaningful shadows using the original one and new enhancement, respectively. For clear observation, cropped image areas of Figure 17(a-1,b-1) are shown in Figure 17(a-2,b-2). Visual inspection of cropped image areas in Figure 17(a-2,b-2) reveals that the original method spoils some edges and fine details in shadow images. Our enhancement has clear color sharpness, especially the clearness of edges.

For fairer comparison, we adopt visual quality assessment, the structural similarity (SSIM) index, and the feature similarity (FSIM) index to compare Figure 17(a-1) and Figure 17 (b-1). Let the original image be a colorful centered fractal with the size $768 * 768$ pixels. According to the image quality assessment from Laboratory for Computational Vision in New York University (please refer to https://www.cns.nyu.edu/~lcv/ssim/#usage), to calculate SSIM and FSIM for color images, it would be better to convert the color image to gray image with the formula $0.2989R + 0.5870G + 0.1140B$, and then calculate its SSIM and FSIM. Finally, SSIM and FSIM of Figure 17(a-1) are 0.2532 and 0.8400, and SSIM and FSIM of Figure 17(b-1) are 0.3300 and 0.8498, respectively. These values of SSIM and FSIM demonstrate a consistency with the performance in Figure 17(a-2,b-2).



(a) (b) (c)

Figure 13. Color meaningful shadows of the proposed $(3,3)$-SDIS sharing a true color secret image: (**a**) CS_1 (**b**) CS_2 (**c**) CS_3.



(a-1) (a-2) (a-3) (a-4)

(b-1) (b-2) (b-3) (b-4)

Figure 14. Binary snd color meaningful shadows of the proposed: (**a**) $BS_1 - BS_4$ (**b**) $CS_1 - CS_4$.

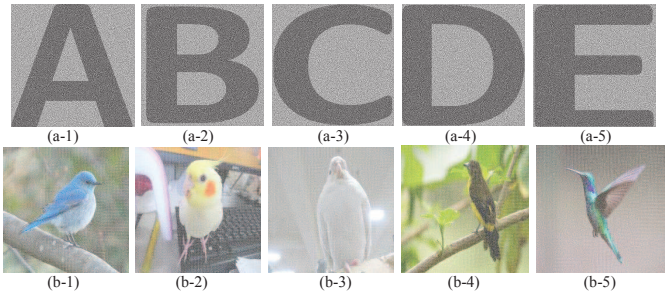


Figure 15. Binary snd color meaningful shadows of the proposed: (**a**) $BS_1 - BS_5$ (**b**) $CS_1 - CS_5$.

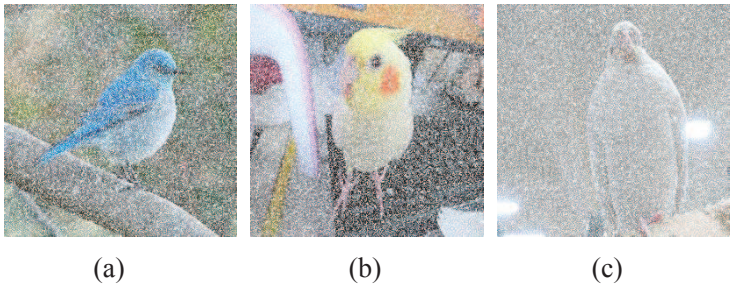


Figure 16. Color meaningful shadows of $(3,3)$-SDIS by the approach of enhancing visual quality: (**a**) $CS_1^{'}$ (**b**) $CS_2^{'}$ (**c**) $CS_3^{'}$.

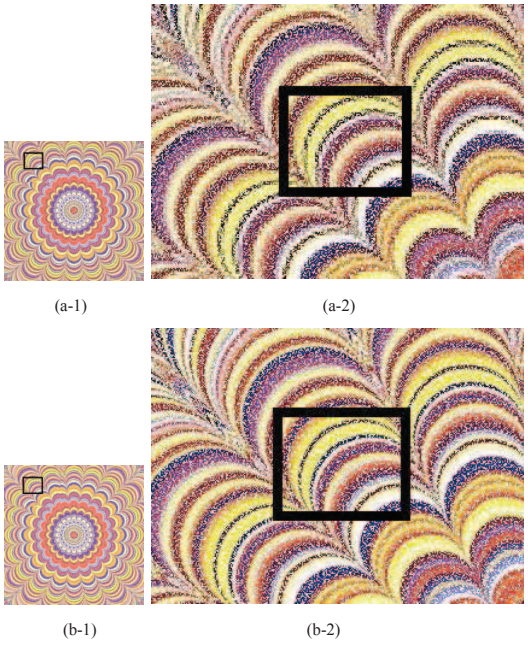


Figure 17. Color meaningful shadows and enlarged parts of cropped image area for $(3,3)$-SDIS: (**a**) using the original method (**b**) using the approach of enhancing visual quality.

6.2. Discussion and Comparison

6.2.1. Enhancing R_P

In step (S-2), we first randomly generate $(n-2)\boxed{X}$ blocks $B^{(i_1)}, B^{(i_2)}, ..., B^{(i_{n-2})}$. Afterwards, in step (S-5), we evenly use Wei et al.'s $(2,2)$-SDIS and Yang et al.'s $(2,2)$-SDIS to generate two other shadows $B^{(j_1)}, B^{(j_2)}$, where $\{j_1, j_2\} = \{1...n\} - \{i_1...i_{n-2}\}$. Finally, R_P is $\frac{6-(1.5/n)}{9}$ (see Equation (5)). In fact, we may further enhance R_P by using $\boxed{W}$ block instead of $\boxed{X}$ block to generate $(n-2)$

$B^{(i_1)}, B^{(i_2)}, ..., B^{(i_{n-2})}$, where $\boxed{W}$ block may be $7B2W$ or $8B1W$. When using $\boxed{W} = 6B3W$, the approach changes back to the original (n, n)-SDIS. By this approach, the R_P is enhanced to $\frac{7-3.5/n}{9}$ and $\frac{8-5.5/n}{9}$ for $\boxed{W} = 7B2W$ and $\boxed{W} = 8B1W$, as derived in Equations (15) and (16), respectively.

$$\begin{cases} R_P = \frac{1}{2} \times \overbrace{\frac{((n-2)\times 7 + 2\times 5)/n}{9}}^{Weietal's(2,2)SDIS} + \\ \frac{1}{2} \times \overbrace{\frac{((n-2)\times 7 + 1\times 5 + 1\times 6)/n}{9}}^{Yanget.al's(2,2)-SDIS} \\ = \frac{3.5-(2/n)}{9} + \frac{3.5-(1.5/n)}{9} = \frac{7-(3.5/n)}{9} \end{cases} \tag{15}$$

$$\begin{cases} R_P = \frac{1}{2} \times \overbrace{\frac{((n-2)\times 8 + 2\times 5)/n}{9}}^{Weietal's(2,2)SDIS} \\ + \frac{1}{2} \times \overbrace{\frac{((n-2)\times 8 + 1\times 5 + 1\times 6)/n}{9}}^{Yanget.al's(2,2)-SDIS} \\ = \frac{4-(3/n)}{9} + \frac{4-(2.5/n)}{9} = \frac{8-(5.5/n)}{9} \end{cases} \tag{16}$$

Consider $(n-1)$-colluder attack for the case using $\boxed{W}$ block with Hamming weight w. The following theorem demonstrates the successful probability to recover the block B under $(n-1)$-colluder attack.

Theorem 6. *When using $\boxed{W}$ block in the proposed (n, n)-SDIS, the successful probability to recover the block B for $(n-1)$-colluder attack is $R_P = \frac{2n-4}{2n} \times \frac{1}{C_9^w} + \frac{1}{2n} \times \frac{1}{C_9^6} + \frac{3}{2n} \times \frac{1}{C_9^5}$.*

Proof. Suppose that using $\boxed{W}$ block with Hamming weight w in step (S-2). Consider the case that colluders already have $(n-1)$ shadows (say $B^{(1)} - B^{(n-1)}$) for reconstruction. Based on these $(n-1)$ shadows, colluders may guess the type of shadow block $B^{(n)}$ in the other shadow, The block $B^{(n)}$ has $\boxed{W}$ block, $\boxed{X}$ block and $\boxed{Y}$ block with $\frac{2n-4}{2n}$ probability, $\frac{1}{2n}$ probability and $\frac{3}{2n}$ probability, respectively, which are derived below. Note: if $\boxed{W}$ is $6B3W$ Equation (17) is reduced to Equation (12).

$$\begin{cases} \overbrace{\frac{1}{2} \times \frac{C_2^2 \times C_{n-1}^1}{C_n^{n-1}}}^{Weietal's(2,2)SDIS} + \overbrace{\frac{1}{2} \times \frac{C_1^1 \times C_1^1 \times C_{n-2}^1}{C_n^{n-1}}}^{Yanget.al's(2,2)-SDIS} \\ = \frac{2n-4}{2n}(B^{(n)} is \boxed{W} block) \\ \overbrace{\frac{1}{2} \times {}^{0}+\frac{1}{2} \times \frac{C_1^1 \times C_1^1 \times C_{n-2}^{n-2}}{C_n^{n-1}}}^{Yanget.al's(2,2)-SDIS} = \frac{1}{2n}(B^{(n)} is \boxed{X} block) \\ \overbrace{\frac{1}{2} \times \frac{C_2^1 \times C_{n-2}^{n-2}}{C_n^{n-1}}}^{Weietal's(2,2)SDIS} + \overbrace{\frac{1}{2} \times \frac{C_1^1 \times C_1^1 \times C_{n-2}^{n-2}}{C_n^{n-1}}}^{Yanget.al's(2,2)-SDIS} = \\ \frac{3}{2n}(B^{(n)} is \boxed{Y} block) \end{cases} \tag{17}$$

There is probability $\frac{1}{C_9^w}, \frac{1}{C_9^5}, \frac{1}{C_9^6}$ to guess the correct block B when $B^{(n)}$ is $\boxed{W}$ block, $\boxed{X}$ block, and $\boxed{Y}$ block, respectively. Therefore, the P_P is calculated as follows.

$$P_P = \overbrace{\frac{2n-4}{2n} \times \frac{1}{C_9^w}}^{\boxed{W}} + \overbrace{\frac{1}{2n} \times \frac{1}{C_9^5}}^{\boxed{X}} + \overbrace{\frac{3}{2n} \times \frac{1}{C_9^5}}^{\boxed{Y}} \tag{18}$$

□

The value of P_P is $\frac{1}{C_9^7} - \frac{0.038}{n}$ and $\frac{1}{C_9^8} - \frac{0.204}{n}$ for $w = 7$ and 8. The values are about $\frac{1}{C_9^7} = \frac{1}{36}$ and $\frac{1}{C_9^8} = \frac{1}{9}$, respectively, for large n. Even though these values are larger than $P_P = \frac{1}{C_9^6} - \frac{3}{2n}(\frac{1}{C_9^6} - \frac{1}{C_9^5})$ for using $\boxed{W}$ block in step (S-2), it is still practically secure for applications. This is because our CP information is protected in the XOR-ed result, but not conveyed on $b_9^{(1)}$ in $B^{(1)}$ like (22)-SDIS [17,19]. For example, when using $8B1W$ as $\boxed{W}$ block. If colluders have $(n-1)$ shadows (say $NS_1 - NS_{n-1}$), for a block B, they have the XOR-ed result $B^{'} = B^{(1)} \oplus ... \oplus B^{(n-1)}$, and can guess the shadow block $B^{(n)}$ is $\boxed{W}$ block with a very high probability for large n (note: $\frac{2n-4}{2n} \to 1$ for large n). It implies that there is about $\frac{8}{9}$ probability that the bit b_9 in B is the complementary bit $b_9^{'}$ of $B^{'}$. By using the same argument in proof of Theorem 5, for this case, the successful probability to recover a correct color in CP is $P_C = (\frac{8}{9})^{24} \simeq 0.059$. Therefore, we cannot get the correct CP back. Although colluders may recover the first 8 bits $(b_1 - b_8)$ in B, i.e., a color index by complementing the first 8 bits $(b_1^{'} - b_8^{'})$ in $B^{'}$ with $\frac{1}{9}$ probability. This probability of guessing a color index is larger than the brute-force probability $\frac{1}{256}$. However, colluders do not have the correct CP, and thus they cannot recover the original SI. Obviously, it is more difficult to apply $(n-1)$-colluder attack on using $7B2W$ as $\boxed{W}$ block, because P_C is $(\frac{7}{9})^{24} \simeq 0.0024$. This is why we claim that using $\boxed{W}$ block is still practically secure for applications.

To demonstrate the above phenomenon, we use $8B1W$ as $\boxed{W}$ block in the proposed $(5,5)$-SDIS. Five color meaning shadows using color cover images $CCI_1 - CCI_5$ in Figure 8a–e are illustrated in Figure 18a, where the approach of enhancing visual quality in Section 4.3 is also adopted. Figure 18b are the 256-color SI (Lena), and its corresponding CP. The recovered 256-color secret image $SI^{'}$ and the color palette $CP^{'}$ are shown in Figure 18c. It is observed that these five color meaning shadows in Figure 18a have high resolutions with $R_P = \frac{8-5.5/n}{9} = 0.767$ for $n = 5$, which have better visual qualities than those in Figure 15b. From, Figure 18c, there is not any secret information of CP and SI leaked for $(n-1)$-colluder attack.

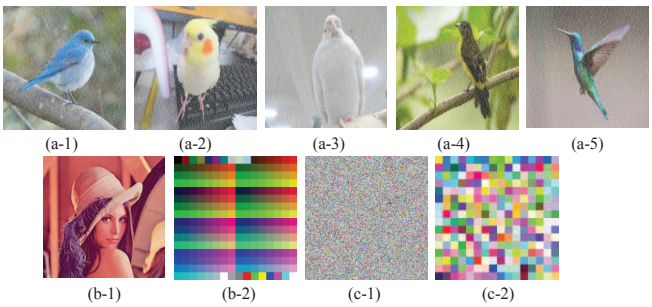


Figure 18. The proposed $(5,5)$-SDIS using $8B1W$ block (**a**) five color meaningful shadows (**b**) 256-color SI and its corresponding CP (**c**) the recovered 256-color SI^1 and color palette $CP^{'}$ under $(n-1)$-colluder attack.

6.2.2. Comparison

We extend $(2,2)$-SDIS to the proposed (n,n)-SDIS. Because the percentage of $\boxed{X}$ block is greater than 50%, the resolution of binary and color meaningful shadows are enhanced. Note: Yang et al.'s $(2,2)$-SDIS uses $\boxed{X}$ block and $\boxed{Y}$ block half and half, while Wei et al.'s $(2,2)$-SDIS only uses $\boxed{Y}$ blocks. On the other hands, Wei et al.'s $(2,2)$-SDIS has the incorrect assignment of color palette data for the color index 255. This problem comes from from all-1 9-bit vector. In [19], Yang et al. adopted a complicated approach using partitioned sets to address this problem. In the proposed (n,n)-SDIS, the number of shadows of (n,n)-SDIS is more than two, i.e., $n \geq 3$. Thus, we can easily adopt a simple approach by reducing $H(T)$ to $H(T) = 7$ in step (S-4) via modifying any one shadow block to solve this problem. Meantime, as described in Section 5.1, we may enhance R_P and simultaneously retain the practical security by using $\boxed{W}$ block.

As shown in Table 2, a complete comparison is given among Wei et al.'s $(2,2)$-SDIS, Yang et al.'s $(2,2)$-SDIS, and the proposed (n,n)-SDIS. The comparison includes the structure of block, percentages

of blocks, the region in color meaningful shadows revealing cover image, the contrast of binary meaningful shadows, enhancing R_P, the embedding of color palette data, where to embed color palette data, enhancing visual quality of color meaningful shadows, encoding/decoding complexity, and the security. About the security, although the successful probability to recover B under $(n-1)$-colluder attack $P_P = \frac{1}{C_9^6} - \frac{3}{2n}(\frac{1}{C_9^6} - \frac{1}{C_9^5}) \simeq \frac{1}{C_9^6} = 0.012$ for large n is larger than $P_W = \frac{1}{C_9^5} = 0.008$ and $P_Y = \frac{1/C_9^6 + 1/C_9^5}{2} = 0.01$. This value is still practical secure for practical application. Besides, the CP of the proposed (n,n)-SDIS cannot be obtained under $(n-1)$-colluder attack, but the CP of $(2,2)$-SDIS can be obtained from only one shadow. Based on this observation, the proposed (n,n)-SDIS is much securer than $(2,2)$-SDIS.

Table 2. Comparison of Three SDIS Schemes.

		Wei et al.'s $(2,2)$-SDIS	**Yang et al.'s $(2,2)$-SDIS**	**The Proposed (n,n)-SDIS**
number of shadows		2	2	$n \geq 3$
structure of block		$\boxed{Y}$ block	$\boxed{X}$ and $\boxed{Y}$ blocks	$\boxed{X}$ and $\boxed{Y}$ blocks
percentage of block		$\boxed{Y}$:100%	$\boxed{X}$:50%, $\boxed{Y}$:50%	$\boxed{X}$:$\frac{2n-3}{2n}$, $\boxed{Y}$:$\frac{3}{2n}$
region in color shadows revealing cover image		$R_W = \frac{5}{9}$	$R_Y = \frac{5.5}{9}$	$R_P = \frac{6-1.5/n}{9}$
		$R_W < R_Y \leq R_P$		
contrast of binary meaningful shadows		$C_W = \frac{1}{9}$	$C_Y = \frac{2}{9}$	$C_P = \frac{3-3/n}{9}$
		$C_W < C_Y \leq C_P$		
enhancement of R_P		No	No	Yes
embedding the data of color palette data		having a problem for the color index 255	using partitioned sets for some color indices	using a simple approach by reducing Hamming weight
where to embed color palette data		the bit $b_9^{(1)}$ in $B^{(1)}$	the bit $b_9^{(1)}$ in $B^{(1)}$	the bit b_9 in the XOR-ed B
enhancing visual quality of color meaningful shadows		No	No	Yes
encoding/decoding complexity		XOR operation	XOR operation; lookup table	XOR operation
security	probability to recover B under $(n-1)$-colluder	$P_W = \frac{1}{C_9^5}$	$P_Y = \frac{1/C_9^5 + 1/C_9^6}{2}$	$P_P = \frac{1}{C_9^6} - \frac{3}{2n}(\frac{1}{C_9^6} - \frac{1}{C_9^5})$
		$P_W < P_Y \leq P_P$		
	probability to obtain CP under $(n-1)$-colluder	CP can be obtained from only one shadow	CP can be obtained from only one shadow	$P_C = (\frac{2}{3} - \frac{1/6}{n})^{24}$

7. Conclusions

In this paper, we discussed the general (n,n)-SDIS, which can be applied to any $n \geq 3$. The proposed (n,n)-SDIS is skilfully implemented on basis of previous $(2,2)$-SDIS. Our main contribution is theoretically to prove the proposed (n,n)-SDIS being able to resist $(n-1)$ colluder attack. Meanwhile, the contrast of binary meaningful shadow and the region in color shadows revealing cover image are both enhanced. The main weakness of Wei et al.'s $(2,2)$-SDIS is the incorrect assignment of color palette data for some color indices, and this is tackled by using partitioned sets in Yang et al.'s $(2,2)$-SDIS. In the proposed (n,n)-SDIS, because of the number of shadows more than two, i.e., $n \geq 3$, a simple approach reducing Hamming weigh of a temporary block can be adopted to easily solve this weakness. Since the proposed (n,n)-SDIS is based on color palette and resistant to $(n-1)$-colluder attack, and also enhances the visual quality of meaningful shadows, it is suitable for modern visual communication applications where features such as secure transmission, storage sensitive, and high-quality image reconstruction are required.

Author Contributions: Designing scheme, writing—original draft preparation, C.-N.Y.; security analysis, Q.-D.S.; editing and responding to reviewer, Y.-X.L.; experiment, C.-M.W.

Funding: Ministry of Science and Technology, under Grant MOST 107-2221-E-259-007, 108-2221-E-259-009-MY2; Natural Science Foundation of China under Grant No. 61502384,61571360,61872289.

Conflicts of Interest: The authors declare there is no conflicts of interest regarding the publication of this paper

References

1. Naor, M.; Shamir, A. Visual cryptography. In *Advances in Cryptology-EUROCRYPT'94*; LNCS 950; Springer: Berlin/Heidelberg, Germany, 1995; pp. 1–12.
2. Shyu, S.J.; Jiang, H.W. General constructions for threshold multiple-secret visual cryptography Schemes. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 733–743. [CrossRef]
3. Yang, C.N.; Wu, C.C.; Lin, Y.C. *k* out of *n* region-based progressive visual cryptography. *IEEE Trans. Circuits Syst. Video Technol.* **2017**. [CrossRef]
4. Karolin, M.; Meyyappan, T.; Thamarai, S.M. Encryption and decryption of color images using visual cryptography. *Int. J. Pure Appl. Math.* **2018**, *118*, 277–281.
5. Kansal, I.; Kasana, S.S. Sharing two true colour images using $(3,3)$-extended visual cryptography technique. *J. Mod. Opt.* **2018**, *65*, 1949–1959.
6. Yang, C.N.; Wu, F.H.; Peng, S.L. Enhancing multi-factor cheating prevention in visual cryptography based minimum (k,n)-connected graph. *J. Vis. Commun. Image Represent.* **2018**, *55*, 660–676. [CrossRef]
7. Shamir, A. How to share a secret. *Commun. Assoc. Comput. Mach.* **1979**, *22*, 612–613. [CrossRef]
8. Thien, C.C.; Lin, J.C. Secret image sharing. *Comput. Graph.* **2002**, *26*, 765–770. [CrossRef]
9. Liu, Y.X.; Yang, C.N.; Wu, C.M.; Sun, Q.D.; Bi, W. Threshold changeable secret image sharing scheme based on interpolation polynomial. *Multimed. Tools Appl.* **2019**, *78*, 18653–18667. [CrossRef]
10. Yang, C.N.; Chen, T.S.; Yu, K.H.; Wang, C.C. Improvements of image sharing with steganography and authentication. *J. Syst. Softw.* **2007**, *80*, 1070–1076. [CrossRef]
11. Pakniat, N.; Noroozi, M.; Eslami, Z. Secret image sharing scheme with hierarchical threshold access structure. *J. Vis. Commun. Image Represent.* **2014**, *25*, 1093–1101. [CrossRef]
12. Liu, Y.X.; Zhang, Y.Z.; Yang, C.N. Reducing file size and time complexity in secret sharing based document protection. *Math. Biosci. Eng.* **2019**, *16*, 4802–4817. [CrossRef]
13. Kanso, A.; Ghebleh, M. An efficient lossless secret sharing scheme for medical images. *J. Vis. Commun. Image Represent.* **2018**, *56*, 245–255. [CrossRef]
14. Li, P.; Liu, Z.; Yang, C.N. A construction method of (t,k,n)-essential secret image sharing scheme. *Signal Process. Image Commun.* **2018**, *65*, 210–220. [CrossRef]
15. Wu, X.; Yang, C.N.; Zhuang, Y.T.; Hsu, S.C. Improving recovered image quality in secret Image sharing by simple modular arithmetic. *Signal Process. Image Commun.* **2018**, *66*, 42–49. [CrossRef]
16. Lukac, R.; Plataniotis, K.N. Bit-level based secret sharing for image encryption. *Pattern Recognit.* **2005**, *38*, 767–772. [CrossRef]
17. Wei, S.C.; Hou, Y.C.; Lu, Y.C. A technique for sharing a digital image. *Comput. Stand. Interfaces* **2015**, *40*, 53–61. [CrossRef]
18. Yang, C.N.; Chen, C.H.; Cai, S.R. Enhanced Boolean-based multi secret image sharing scheme. *J. Syst. Softw.* **2016**, *116*, 22–34. [CrossRef]
19. Yang, C.N.; Wu, C.H.; Yeh, Z.X.; Wang, D.; Kim, C. A new sharing digital image scheme with clearer shadow images. *Comput. Stand. Interfaces* **2017**, *51*, 118–131. [CrossRef]
20. Liu, Y.X.; Yang, C.N.; Wu, S.Y.; Chou, Y.S. Progressive (k,n) secret image sharing schemes based on Boolean operations and covering codes. *Signal Process. Image Commun.* **2018**, *66*, 77–86. [CrossRef]