J. Vis. Commun. Image R. 33 (2015) 31–41

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

journal homepage: www.elsevier.com/locate/jvci

Friendly progressive random-grid-based visual secret sharing with adaptive contrast ☆,☆☆

Chih-Hung Lin [a], Yao-Sheng Lee [b], Tzung-Her Chen [b,*]

[a] Graduate Institute of Mathematics and Science Education, National Chiayi University, Chiayi 621, Taiwan, ROC
[b] Department of Computer Science and Information Engineering, National Chiayi University, Chiayi 600, Taiwan, ROC

ARTICLE INFO

Article history:
Received 19 August 2014
Accepted 31 August 2015
Available online 8 September 2015

Keywords:
Visual secret sharing
Random grid
Pixel expansion
Friendly
Progressive
Chaos
Adaptive contrast
Visual cryptography

ABSTRACT

Visual secret sharing (VSS) schemes providing secret communication services are classified into two categories depending on the method of encoding the secret: visual cryptography (VC)-based and random grid (RG)-based schemes. A friendly progressive version of the VC-based VSS scheme was presented in 2008; however, it is marred by pixel expansion, which is the innate deficiency of conventional VC-based VSS schemes. This paper proposes a suitable user-friendly RG-based VSS scheme with progressive secret reconstruction and without pixel expansion. The experimental results of the developed scheme validated its feasibility, and a theoretical analysis demonstrated its visual quality and security.

1. Introduction

Visual secret sharing (VSS) has attracted considerable attention in academia, and an increasing number of VSS applications, such as image encryption [1], visual authentication [2], image hiding [3], and digital watermarking [4], have been developed. Naor and Shamir [4] first proposed visual cryptography (VC) in 1994. VC can encode a secret image into numerous meaningless shared images, where each shared image alone does not reveal any information about the secret. Specifically, Naor and Shamir presented a *k-out-of-n* (k,n)-VSS concept that entails dividing a secret image into n shares, and reconstructing the original image requires stacking at least k shares. However, conventional VC-based VSSs have several drawbacks. Three of the major drawbacks are outlined as follows: (1) pixel expansion, (2) requirement of a sophisticated codebook designed for various applications, and (3) management of increasingly meaningless shares.

Managing an increasing number of meaningless shares is challenging because all shares for different secrets available are noise-like and are therefore difficult to manage or use and require careful labeling and storage. To manage a high number of meaningless shares, Ateniese et al. [6] proposed an extended VC scheme that involves encoding a secret into numerous meaningful shares. A meaningful share implies that a logo message used for identification appears on the share. Thus, managing the shares is easy. Zhou et al. [7] proposed a halftone VC to achieve meaningful shares. The sizes of the encoded shared images obtained using both extended VC [6] and halftone VC [7] were at least four times larger than those of secret images. To mitigate this problem, Tsai et al. [8] proposed a VC-based VSS scheme to generate meaningful shares; in this scheme, the pixel expansion was reduced to two, achieving higher meaningfulness and lower pixel expansion rate compared with schemes presented in previous studies [6,7].

Although the aforementioned VSS schemes can completely reveal the original secrets, they cannot achieve the goal of progressive image sharing, in which the more shared images are superimposed, the higher the quality of the recovered secret becomes. Jin et al. [9] proposed the first progressive VC scheme. However, this method requires extra computation, which violates the essential assumption of VSS. Fang and Lin [10] proposed another VC-based progressive method, which did not require extra computation; nevertheless, pixel expansion was four times higher compared with other methods. To avoid pixel expansion, Hou and Quan [18] presented a progressive VC scheme with unexpanded shares. When the goal of progressive secret reconstruction is achieved, the progressive schemes presented in previous studies [9,10,18] were not user-friendly in managing the meaningless shares.

☆ This paper has been recommended for acceptance by M.T. Sun.
☆☆ This work was presented in part at The 5th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP2009), Kyoto, Japan, 2009 [20].

* Corresponding author.
E-mail address: thchen@mail.ncyu.edu.tw (T.-H. Chen).

http://dx.doi.org/10.1016/j.jvcir.2015.08.018
1047-3203/

Fang [11] combined the progressive VC-based VSS [10] and friendly VC-based VSS methods to form a new scheme. However, Fang's scheme is marred by a pixel expansion of up to four times.

More recently, researchers have begun to focus on a random grid (RG)-based VSS scheme first proposed by Kafri and Keren [12] in 1987. Inspired by Kafri and Keren's scheme, Shyu [13] proposed two RG-based VSS schemes for managing both gray-level and color images. To remove the limitation of (2,2) RG-based VSS [12,13], Shyu [15] and Chen and Tsao proposed their own $(2,n)$ and (n,n) [14] and (k,n) schemes [17]. The friendly RG-based VSS scheme [19] lacks the design of a progressive secret construction. To meet this requirement, in 2009, Chen and Lee [20] and Chen [21] have presented friendly progressive RG-based VSS schemes. Previous studies have failed to theoretically demonstrate the security and accuracy of VSS schemes in terms of friendliness and progression. Recent studies have not addressed the trade-off in visual quality, called contrast-flexibility trade-off, between reconstructed secrets and logo images obtained through generated RGs.

This paper proposes a friendly and progressive VSS (FPVSS) scheme involving RGs. In this scheme, a contrast-flexibility trade-off between reconstructed secrets and logo images was obtained through generated RGs. Moreover, the FPVSS scheme is superior to existing VSS schemes in terms of user-friendliness and progressive secret reconstruction. The proposed scheme exhibits the following advantages: (1) eliminating pixel expansion, (2) eliminating the necessity of designing a sophisticated codebook, (3) managing shares in an easy and friendly manner, (4) progressively reconstructing the secret, and (5) providing adaptive contrast. Its accuracy was validated through a theoretical analysis, and several experiments were conducted to demonstrate its feasibility.

The remainder of this paper is organized as follows. Section 2 describes the proposed scheme. Sections 3 and 4 demonstrate the performance and experimental results, respectively. Sections 5 and 6 present further discussions and conclusions.

2. Proposed method

In the proposed scheme, a secret image S is encoded into n meaningful RGs G_k with distinct logo images L_k. A secret image $S = \{S[i,j] | S[i,j] = 0 \text{ or } 1,\ 0 \leqslant i \leqslant (w-1),\ 0 \leqslant j \leqslant (h-1)\}$, and n logo images $L_k = \{L_k[i,j] | L_k[i,j] = 0 \text{ or } 1,\ 0 \leqslant i \leqslant (w-1),\ 0 \leqslant j \leqslant (h-1)\}$ $(k = 1, 2, \ldots, n)$, serving as references for the generated shared images, are used as inputs. The value 0 or 1 is adopted to represent a transparent or an opaque pixel. The proposed scheme outputs n meaningful RGs $G_k = \{G_k[i,j] | G_k[i,j] = 0 \text{ or } 1,\ 0 \leqslant i \leqslant (w-1),\ 0 \leqslant j \leqslant (h-1)\}$ $(k = 1, 2, \ldots, n)$ of the same size.

In the decoding phase, the staking of any two of the RGs reveals the secret, and the two logo images disappear by becoming noise-like. In addition, the higher the number of stacked RGs is, the higher the quality of the secret becomes.

2.1. Design guideline

In the proposed scheme, to meet the contrast-flexibility requirement, the parameter t $(1 \leqslant t \leqslant w \times h)$ is designed to control the quality of the logo images and reconstructed secret image. The higher the value of t is, the higher the quality of the reconstructed image becomes. By contrast, the lower the value of t is, the higher the quality of the logo images becomes.

The design concept involves encoding a secret or logo pixel (Fig. 1). To demonstrate this, we must determine the current encoding process used to manage the secret or logo images with the probability determined using the parameter t. If a secret pixel $S[i,j]$ is selected, all n RG pixels $G_k[i,j]$ are generated using the $(2,n)$-based RGVSS [14]. Otherwise, the value of $G_k[i,j]$ equals that of the logo pixel $L_k[i,j]$, and the color of the other $n-1$ grid-pixel values $G_r[i,j]$ $(r = 1, 2, \ldots, n \text{ but } r \neq k)$ is black.

2.2. Encoding

Before describing the details of the encoding process, we define the required functions as follows.

Definition 1 (*Random pixel value generation function*). ***Chaos*(.):** $r \leftarrow Chaos(n)$, r is the output of function *Chaos*(.) with input n, where *Chaos*(.) is the function used to generate a random value r by using a logistic map [16]. The logistic map is defined as follows: $x_{k+1} = 4x_k(1-x_k)$ $x_k \in (0,1)$. In this case, an initial value x_0 is selected as an input, where each value of the random number sequence r is obtained using the equation $r = x_k \times 10^{13} \bmod n$, where $r \in \{0, 1, \ldots, n-1\}$. □

The encoding processes comprise the following steps.

Step 1: Quality: Determine the quality parameter t that makes the grid pixels generated by the secret pixel $S[i,j]$ with probability $\frac{t}{n+t}$ and one of the n logo pixels $L_k[i,j]$ with probability

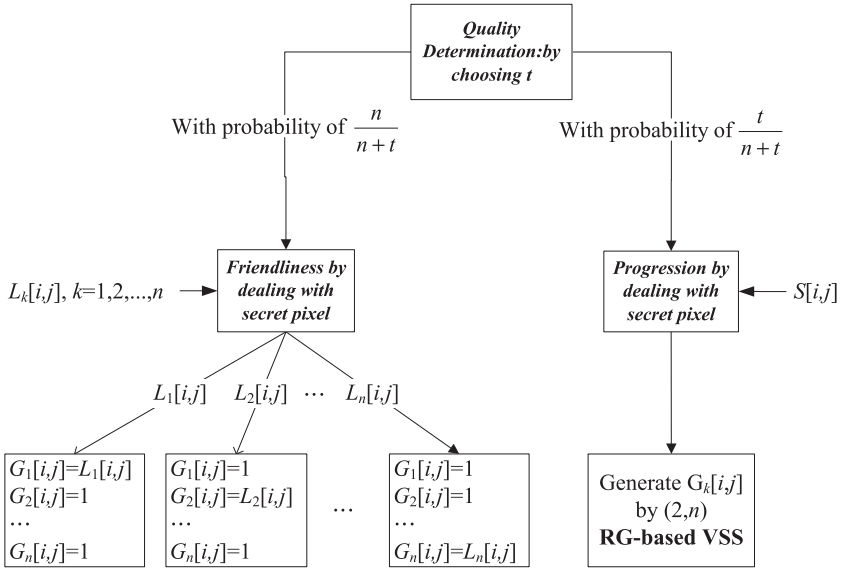

Fig. 1. The main concept of the proposed scheme for encoding a secret or logo pixel.

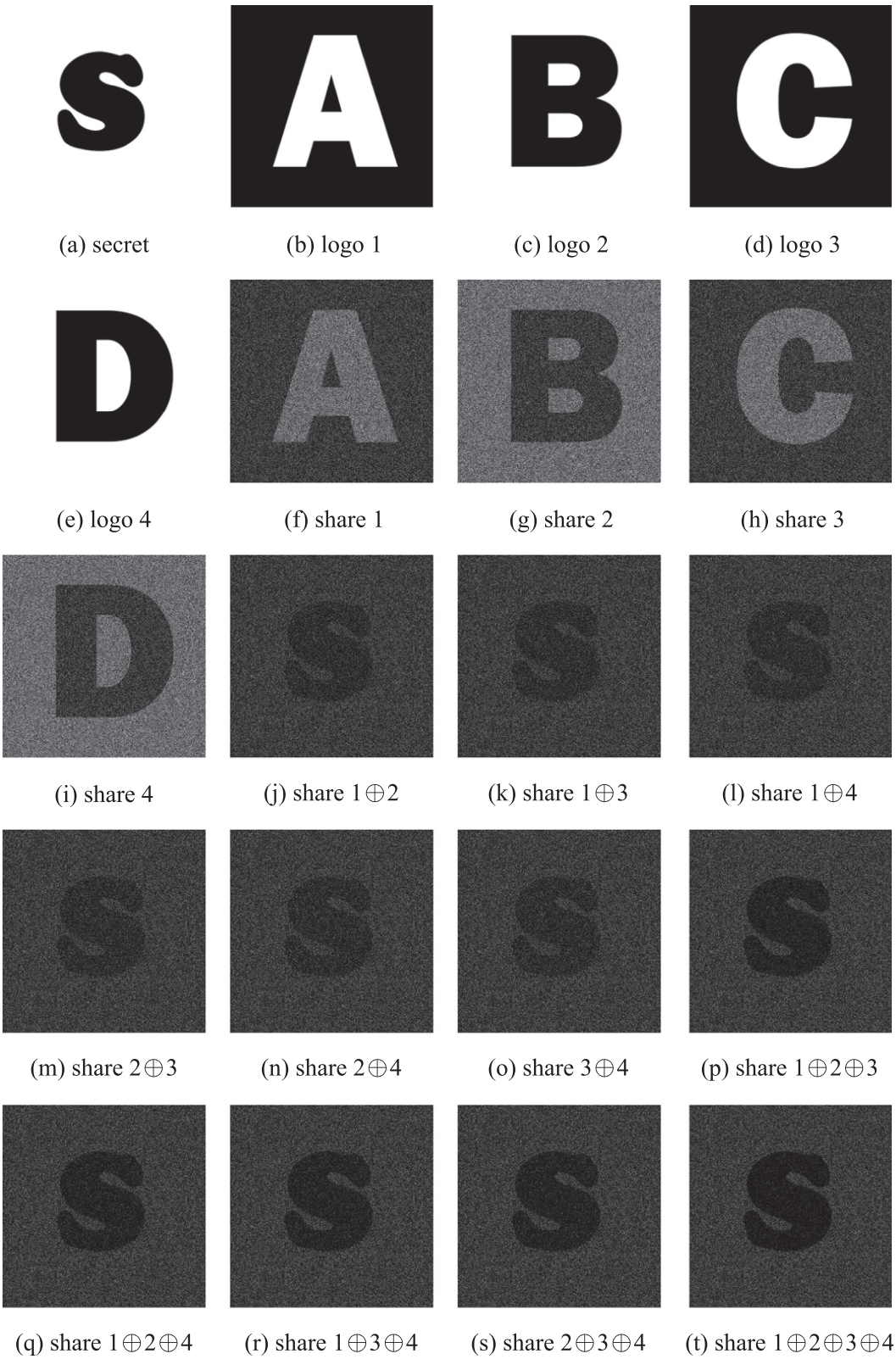

Fig. 2. The experimental results of **Simulation 1** with $t = 1$: (a) a binary secret image, (b–e) binary logos, (f–i) four meaningful random-grids, (j–o) two shared images stacked, (p–s) three shared images stacked, and (t) all shared images stacked.

$\frac{1}{n+t}$. Therefore, we must randomly select a value $x = Chaos(n + t) + 1$, where the x value is between 1 and $n + t$. If x is greater than n, the progression operations in **Step 2** are performed; otherwise, the friendliness operation in **Step 3** is performed. In the proposed scheme, the probability of encoding a secret pixel is $\frac{t}{n+t}$ and that of encoding an individual logo pixel is $\frac{1}{n+t}$.

Step 2: Progression: The purpose of progression is to generate grid pixels aimed at dealing with the secret by using the capability of

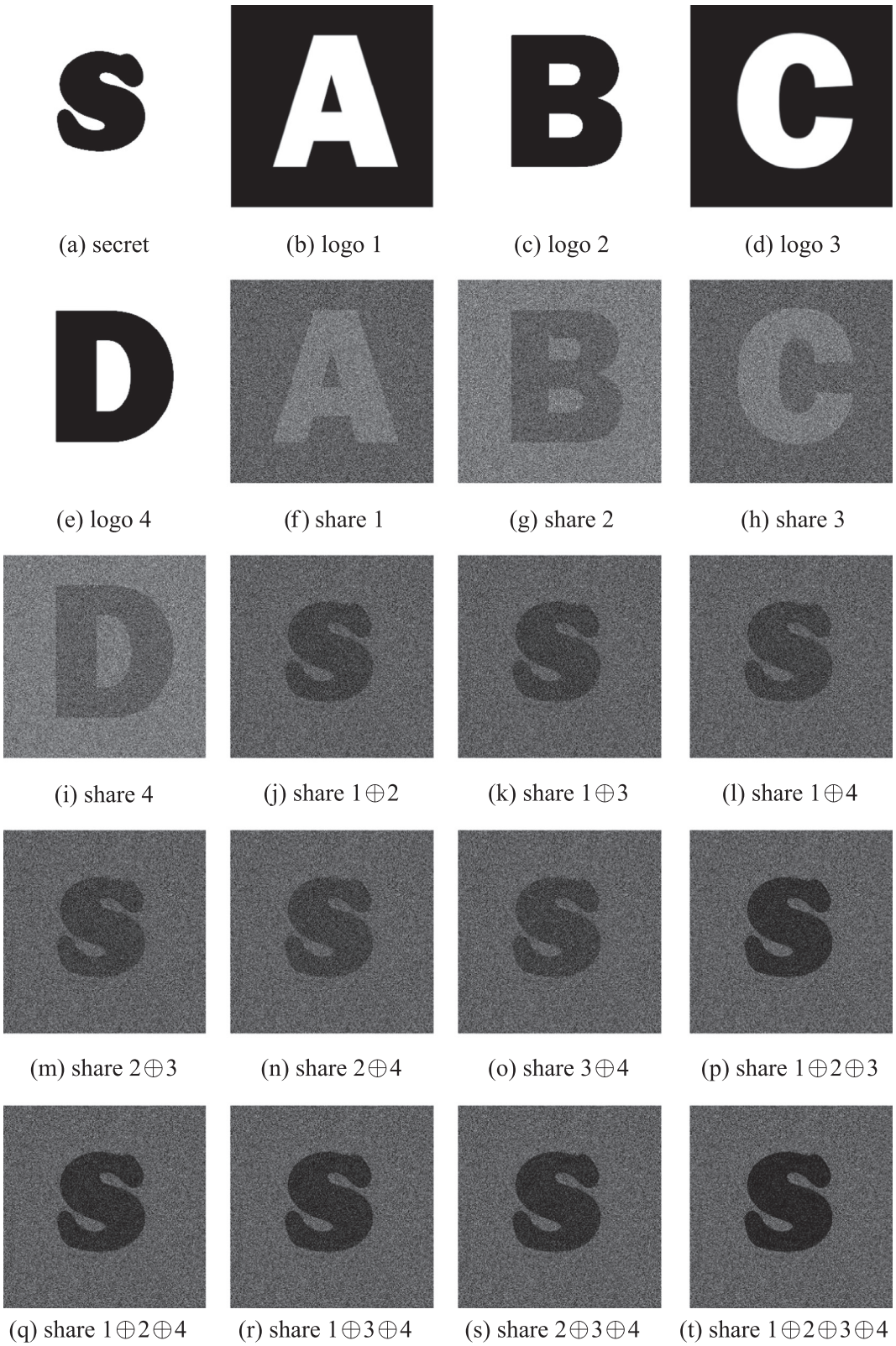

Fig. 3. The experimental results of **Simulation 1** with $t = 4$: (a) a binary secret image, (b–e) binary logos, (f–i) four meaningful random-grids, (j–o) two shared images stacked, (p–s) three shared images stacked, and (t) all shared images stacked.

progression. To perform this task, we randomly generate a bit value $r = Chaos(2)$, where $r \in \{0, 1\}$, and assign r to $G_1[i,j]$, where $r = 0$ for the color white with probability $\frac{1}{2}$ and $r = 1$ for the color black with probability $\frac{1}{2}$. If the corresponding secret pixel $S[i,j]$ is white, the value of $G_p[i,j]$ is equivalent to that of $G_1[i,j]$ for $p = 2,3,\ldots,n$. Otherwise, the values of $G_p[i,j]$ are randomly generated using $Chaos(2)$. Finally, $G_1[i,j]$, $G_2[i,j]$,..., and $G_n[i,j]$ are generated, after which **Step 4** is performed.

Step 3: Friendliness: Generate the grid pixels to be used to display the logo message on RGs. The value $x \in [1,\ldots,n]$ is determined in **Step 1**. This implies that the logo pixel on the xth logo (e.g., $L_x[i,j]$) is selected to conduct the encoding process. The value of the grid pixel $G_x[i,j]$ is equivalent to that of $L_x[i,j]$, and the color of the other $n-1$ grid pixels $G_r[i,j]$ ($r = 1, 2,\ldots,k-1,k+1,\ldots,n$) is set to black. Specifically, $G_k[i,j] = \begin{cases} L_x[i,j], & \text{if } k = x \\ 1, & \text{otherwise} \end{cases}$, where $k = 1, 2,\ldots,n$.

Step 4: Repetition: Repeat **Steps 1–3**, until all of the pixels of the RGs are generated.

The algorithm of the proposed encoding process is briefly illustrated in the following pseudocode.

Input: Parameter t; a binary secret image $S = \{S[i,j] | S[i,j] = 0 \text{ or } 1,\ 0 \leqslant i \leqslant (w-1),\ 0 \leqslant j \leqslant (h-1)\}$; and n logo images $L_k = \{L_k[i,j] | L_k[i,j] = 0 \text{ or } 1,\ 0 \leqslant i \leqslant (w-1),\ 0 \leqslant j \leqslant (h-1)\}$, where $k = 1,2,\ldots,n$.

Output: n meaningful RGs $G_k = \{G_k[i,j] | G_k[i,j] = 0 \text{ or } 1,\ 0 \leqslant i \leqslant (w-1),\ 0 \leqslant j \leqslant (h-1)\}$, and $k = 1, 2,\ldots,n$.

//**Step 1**

$x \leftarrow \text{chaos}(n+t) + 1$

If $x > n$ go to **Step 2; otherwise** go to **Step 3**

//**Step 2**

$G_1[i,j] \leftarrow Chaos(2)$

For ($p = 2; p \leqslant n; p$++)

$G_p[i,j] = \begin{cases} G_{p-1}[i,j], & \text{if } S[i,j] = 0 \\ Chaos(2), & \text{otherwise} \end{cases}$

Go to **Step 4**

//**Step 3**

For ($l = 1; l \leqslant n; l$++)

$G_k[i,j] = \begin{cases} L_l[i,j], & \text{if } k = l \\ 1, & \text{otherwise} \end{cases}$

//**Step 4**

Repeat **Steps 1–3**, until all i, j ($0 \leqslant i \leqslant w$ and $0 \leqslant j \leqslant h$) are done.

2.3. Decoding

The decoding process entails directly stacking two or more RGs to disclose the original secret information detectable by the human visual system. In addition, the higher the number of RGs stacked, the clearer the revealed original secret becomes. Notably, in the moment of disclosing the secret it needs precise alignment since of the difficulty of stacking printed shares by hands. The quality of disclosed secret is affected by physical factors, such as printing quality, light and viewing angle deviations.

3. Performance analyses

This section presents the security and visual quality performance analysis.

Assumption 1. All RGs G_k ($k = 1,2,\ldots,n$) generated using the proposed scheme were divided into two sub-RGs: G_k^F was generated using **Step 3** and G_k^P was generated using **Step 2**; $G_k = G_k^F \| G_k^P$, where || is a concatenation operation. The expected number of pixels in G_k^F and G_k^P are $\frac{n}{n+t}(w \times h)$ and $\frac{t}{n+t}(w \times h)$, respectively. The pixels in the sub-RG G_k^F are used to illustrate the logo message on the RGS, whereas those in the sub-RG G_k^P are aimed at achieving the goal of progressive visual quality. □

Definition 2 (*Average light transmission*). For a certain pixel c in a binary image C, $l[c]$ represents the light transmission of c. The light transmission of an opaque pixel $c \in C$ is defined as $l[c] = 0$ ($l[c] = 1$ for a transparent pixel). The average light transmission of C with a size of $w \times h$ is defined as $L[C] = \frac{1}{w \times h}\sum_{i=1}^{w}\sum_{j=1}^{h} l[C[i,j]]$. □

Definition 3 (*Corresponding area representation*). Assume that $S(c)$ is the corresponding area of all the pixels for color c in the secret image S that satisfies $\begin{cases} S_{(0)} \cup S_{(1)} = S \\ S_{(0)} \cap S_{(1)} = \varnothing \end{cases}$. Furthermore, regarding the reconstructed image B, the corresponding area with respect to the all-white or all-black area in secret image S is denoted by $B[S_{(0)}]$ or $B[S_{(1)}]$, respectively. □

Definition 4 (*Contrast*). To estimate the visual quality of the reconstructed image B for a secret image S, the contrast σ is defined as $\sigma = \frac{L[B[S_{(0)}]] - L[B[S_{(1)}]]}{1 + L[B[S_{(1)}]]}$, where $L[B[S_{(0)}]]$ and $L[B[S_{(1)}]]$ denote the average light transmissions of the partial area in B, which correspond to the transparent and opaque pixels in S, respectively. The higher the value of σ is, the higher is the quality required to recognize the secret S. □

Definition 5 (*Visually recognizable*). The reconstructed binary image B is recognized as the secret image S when the contrast $\sigma > 0$. In principle, if $L[B[S_{(0)}]] > L[B[S_{(1)}]]$, B can be recognized as S visually. By contrast, if $L[B[S_{(0)}]] = L[B[S_{(1)}]]$, B is meaningless. □

Lemma 1. Upon stacking R ($n \geqslant R \geqslant 2$) independent grids $G_1, G_2, \ldots, G_R$, generated using a chaos function to form a stacked image G^R, the expected average light transmission of $L[G^R]$ is $\left(\frac{1}{2}\right)^R$.

Proof. By induction on R,

(1) For $R = 2$, let b_1 be a certain pixel of RG G_1 and b_2 be the corresponding pixel at the same position in G_2. If each grid pixel in G_1 and G_2 is generated using a chaos function, the respective probability for generating a black or white pixel is $\frac{1}{2}$. When superimposing two pixels b_1 and b_2 denoted as $b_{1\oplus 2}$, we have probabilities $\frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$ and $\frac{3}{4}$ to obtain white and black pixels, respectively, so that the expected $L[G^2] = \frac{1}{w \times h}\left(\sum_{i=1}^{\left(\frac{1}{2}\right)^2 w \times h} 1 + \sum_{i=1}^{\left(1-\left(\frac{1}{2}\right)^2\right) w \times h} 0\right) = \frac{1}{4}$ according to **Definition 2**.

(2) Assume that the claim holds for $R-1$; that is, $L[G^{R-1}] = \left(\frac{1}{2}\right)^{R-1}$.

This implies that if $R-1$ independent RGs are stacked, $\left(\frac{1}{2}\right)^{R-1} w \times h$ pixels are transparent and $\left(1 - \left(\frac{1}{2}\right)^{R-1}\right) w \times h$ are black in G^{R-1}. Furthermore, we must prove that the claim holds for R.

(3) When G^{R-1} and G_R are superimposed, $\frac{1}{2}\left(\frac{1}{2}\right)^{R-1} w \times h$ pixels are transparent and $\left(1 - \frac{1}{2}\left(\frac{1}{2}\right)^{R-1}\right) w \times h$ are black in G^R.

The expected average light transmission of the superimposed result is $L[G^R] = L[G^{R-1} \oplus G_R] = \frac{1}{w \times h}\left(\sum_{i=1}^{\frac{1}{2}\left(\frac{1}{2}\right)^{R-1} w \times h} 1 + \sum_{i=1}^{\left(1-\frac{1}{2}\left(\frac{1}{2}\right)^{R}\right) w \times h} 0\right) = \left(\frac{1}{2}\right)^R$. □

Theorem 1 (*Security*). RGs are meaningless for secrets. In other words, an RG alone does not disclose the information of the secret image.

Proof. According to **Assumption 1**, each RG G_k comprises G_k^F with a size of $\frac{n}{n+t}w \times h$ and G_k^P with a size of $\frac{t}{n+t}w \times h$. Two properties must now be satisfied: (1) G_k^F is meaningless for the secret image and (2) G_k^P is meaningless for the secret image.

Case 1: G_k^F is meaningless for the secret image

According to **Step 3**, the encoding process has no information about the secret image. Hence, G_k^F is independent of the secret image.

Case 2: G_k^P is meaningless for the secret image

According to **Step 2**, each grid pixel in G_1^P is generated using a chaos function, with a $\frac{1}{2}$ probability of the pixel being black or $\frac{1}{2}$ probability of it being white. The average light transmission of G_1^P is $L\left[G_1^P[S_{(0)}]\right] = L[G_1^P[S_{(1)}]] = \frac{1}{\frac{t}{n+t}w \times h}\sum_{i=1}^{\frac{t}{n+t}w \times h}\frac{1}{2} = \frac{1}{2}$. According to the proposed scheme, the grid pixel in $G_d^P[S_{(0)}]$ ($d = 2, 3, \ldots, n$) is equal to that in $G_1^P[S_{(0)}]$ and the grid pixel in $G_d^P[S_{(1)}]$ is generated using a chaos function, with a $\frac{1}{2}$ probability of the pixel being black or $\frac{1}{2}$ probability of it being white. The average light transmission of G_d^P is $L[G_d^P[S_{(0)}]] = L\left[G_d^P[S_{(1)}]\right] = \frac{1}{\frac{t}{n+t}w \times h}\sum_{i=1}^{\frac{t}{n+t}w \times h}\frac{1}{2} = \frac{1}{2}$.

Fig. 4. The experimental results of **Simulation 2** with $t = 1$: (a) a gray level secret image *Lena*, (b–e) four meaningful random-grids, (f–k) two shared images stacked, (l–o) three shared images stacked, and (p) all shared images stacked.

We can then obtain the contrast $\sigma = \frac{L\left[G_k^F[S_{(0)}]\right] - L\left[G_k^F[S_{(1)}]\right]}{1 + L\left[G_k^F[S_{(1)}]\right]} = \frac{\frac{1}{2} - \frac{1}{2}}{1 + \frac{1}{2}} = 0$. Hence, the secret is not disclosed on a single RG according to **Definition 5**.

Therefore, RG G_k alone does not disclose the information of the secret image. □

Theorem 2 (*Friendliness*). RGs are meaningful for logo images; that is, a logo message can be visually recognized in an RG.

Proof. According to **Step 3**, $\frac{1}{n+t}(w \times h)$ grid pixels in G_k^F are designed to manage the logo image L_k and $\frac{n-1}{n+t}(w \times h)$ black grid pixels in G_k^F are designed to mask the logo image L_m $(m \neq k)$. According to **Definition 2**, the average light transmissions of the corresponding areas in G_k^F, with respect to the white and black areas in the logo image L_k $(1 \leqslant k \leqslant n)$, are $L\left[G_k^F[L_{k(0)}]\right] = \frac{1}{\frac{n}{n+t}w \times h}\left(\sum_{i=1}^{\frac{1}{n+t}w \times h} 1 + \sum_{i=1}^{\frac{n-1}{n+t}w \times h} 0\right) = \frac{1}{n}$ and $L\left[G_k^F[L_{k(1)}]\right] = \frac{1}{\frac{n}{n+t}w \times h}\left(\sum_{i=1}^{\frac{1}{n+t}w \times h} 0 + \sum_{i=1}^{\frac{n-1}{n+t}w \times h} 0\right) = 0$, respectively.

Fig. 5. The experimental results of **Simulation 2** with $t = 4$: (a) a gray level secret image *Lena*, (b–e) four meaningful random-grids, (f–k) two shared images stacked, (l–o) three shared images stacked, and (p) all shared images stacked.

We then obtain the contrast $\sigma = \frac{L[G_k^F[L_{k(0)}]] - L[G_k^F[L_{k(1)}]]}{1+L[G_k^F[L_{k(1)}]]} = \frac{\frac{1}{n}-0}{1+0} = \frac{1}{n} > 0$. Finally, the proposition that each RG G_k is meaningful with respect to the logo image is true. □

Theorem 3 (*Visual quality of the secret*). Because of the superimposition of R RGs to form a stacked result G^R ($n \geqslant R \geqslant 2$), the contrast of the reconstructed result in the proposed scheme is greater than zero.

Proof. Assume $G^R = G^{FR} \,||\, G^{PR}$, where || is a concatenation operation, and G^{FR} and G^{PR} denote the stacked results of superimposing R sub-RGs G^F and G^P, respectively. To examine the visual quality of G^R, we must first compute the expected average light transmissions of G^{FR} and G^{PR}.

Case 1: The expected average light transmission of G^{FR} is zero.

According to **Step 3**, $n-1$ black grid pixels and a logo pixel are determined. Therefore, stacking any two or more RGs yields at least one black pixel in the same position such that the logo information disappears. The expected average light transmissions of G^{FR} are $L\left[G^{FR}[S_{(0)}]\right] = \frac{1}{\frac{n}{n+t}w\times h}\sum_{i=1}^{\frac{n}{n+t}w\times h} 0 = 0$ and $L[G^{FR}[S_{(1)}]] = \frac{1}{\frac{n}{n+t}w\times h}\sum_{i=1}^{\frac{n}{n+t}w\times h} 0 = 0$.

Case 2: The expected average light transmission of G^{PR} is greater than zero.

In **Step 2**, G_1 is generated using a chaos function, and the expected average light transmission of G_1 is $L[G_1[S_{(0)}]] = L[G_1[S_{(1)}]] = \frac{1}{2}$. Because the grid pixel in G_d ($2 \leqslant d \leqslant n$) is equal to that in G_1 when the corresponding secret pixel is white, $L[G^{PR}[S_{(0)}]] = L[G_1[S_{(0)}]] = \frac{1}{2}$. Moreover, because the grid pixels in G_d are generated using a chaos function when the corresponding secret pixels are black, the sub-RGs are independent. Therefore, we obtain the expected average light transmission of the stacked result G^{PR} $L[G^{PR}[S_{(1)}]] = \left(\frac{1}{2}\right)^R$ according to **Lemma 1**.

Finally, we obtain the expected average light transmissions $L[G^R[S_{(0)}]] = L[G^{PR} \| G^{FR}[S_{(0)}]] = \frac{1}{w\times h}\left(\sum_{i=1}^{\frac{t}{n+t}w\times h}\frac{1}{2} + \sum_{i=1}^{\frac{n}{n+t}w\times h} 0\right) = \frac{1}{2}\times\frac{t}{n+t}$ and $L[G^R[S_{(1)}]] = L[G^{PR} \| G^{FR}[S_{(1)}]] = \frac{1}{w\times h}\left(\sum_{i=1}^{\frac{t}{n+t}w\times h}\left(\frac{1}{2}\right)^R + \sum_{i=1}^{\frac{n}{n+t}w\times h} 0\right) = \left(\frac{1}{2}\right)^R \times \frac{t}{n+t}$.

The contrast is $\sigma = \frac{L[G^R[S_{(0)}]] - L[G^R[S_{(1)}]]}{1+L[G^R[S_{(1)}]]} = \frac{\frac{1}{2}\times\frac{t}{n+t} - \left(\frac{1}{2}\right)^R\times\frac{t}{n+t}}{1+\left(\frac{1}{2}\right)^R\times\frac{t}{n+t}} = \frac{t(2^{R-1}-1)}{2^R(n+t)+t} > 0$.

Therefore, the proof is complete. □

Theorem 4 (*Progressive visual quality*). The contrast in the reconstructed result obtained by stacking two or more RGs (e.g., R ($n \geqslant R \geqslant 2$)) in the proposed scheme increases progressively.

Proof. To demonstrate the property of progressive secret reconstruction, equation σ was differentiated as follows:

$$\sigma' = \frac{\left[\frac{d}{dR}t(2^{R-1}-1)\right]\times[2^R(n+t)+t] - [t(2^{R-1}-1)]\times\left[\frac{d}{dR}(2^R(n+t)+t)\right]}{(2^R(n+t)+t)^2}$$
$$= \frac{t(2n+3t)(\ln\ 2)2^{R-1}}{(2^R(n+t)+t)^2} > 0$$

Because the variables R, n, and t are always positive, the value σ' is positive. Hence, σ is an increasing progressive equation dependent on the parameter R. Finally, the proof is complete. □

4. Experimental results

Several experiments were conducted to demonstrate the feasibility of the proposed method in terms of user-friendliness and progressive secret reconstruction.

4.1. Simulation 1: With different quality parameters

In this simulation, a binary image, character s (Fig. 2(a)), with a size of 1024×1024, was considered a secret image, and four images, characters A, B, C, and D (two dark and two light; Fig. 2 (b–e)), were considered logo images. The four logos were of the same size. After the completion of the encoding operations by using the quality parameter $t = 1$, four meaningful RGs with the same size were generated (Fig. 2(f–i)). Both the darker and lighter logos can be visually recognized in Fig. 2(f–i). Fig. 2(j–t) illustrates the stacked images. The higher the number of RGs stacked was, the clearer is the original secret that was reconstructed. Fig. 3 illustrates another experimental result with $t = 4$.

4.2. Simulation 2: With complex secret images

Second, a binary image, classic test image *Lena* (Fig. 4(a)), with a size of 4096×4096 was considered the secret image. To present the detail of complex secret images, the size of both the secret and four logos was 4096×4096. After the encoding operations involving the quality parameter $t = 1$, four meaningful RGs with the same size were generated (Fig. 4(b–e)). Fig. 4(f–p) depicts the stacked images.

Fig. 5 illustrates another experimental result with $t = 4$. Notably, the larger the size of the image was, the clearer the reconstructed original secret became.

4.3. Simulation 3: Accuracy of Theorem 1 and Theorem 4

To verify the accuracy of the theoretical contrast presented by **Theorem 3** and the property of the progressive visual quality presented by **Theorem 4**, the experimental contrast was computed.

Table 1
Number of white and black pixels in the specific area of the reconstructed image in **Simulation 1**, as in Fig. 2.

R	2	3	4
# of $G^R[S_{(1)}] = 1$	160,662	164,811	166,948
# of $G^R[S_{(1)}] = 0$	8411	4262	2125
# of $G^R[S_{(0)}] = 1$	791,752	791,752	791,752
# of $G^R[S_{(0)}] = 0$	87,751	87,751	87,751
$L[G^R[S_{(1)}]]$	0.049748	0.025208	0.012569
$L[G^R[S_{(0)}]]$	0.099773	0.099773	0.099773
Experimental σ	0.047655	0.072732	0.086122
Theoretic σ	$\frac{1}{21} = 0.047619$	$\frac{3}{41} = 0.073170$	$\frac{7}{81} = 0.086419$

Table 2
Number of white and black pixels in the specific area of the reconstructed image in **Simulation 2**, as in Fig. 5.

R	2	3	4
# of $G^R[S_{(1)}] = 1$	7,746,374	8,300,386	8,576,118
# of $G^R[S_{(1)}] = 0$	1,107,140	553,128	277,396
# of $G^R[S_{(0)}] = 1$	5,942,416	5,942,416	5,942,416
# of $G^R[S_{(0)}] = 0$	1,981,286	1,981,286	1,981,286
$L[G^R[S_{(1)}]]$	0.1250509	0.062476	0.031332
$L[G^R[S_{(0)}]]$	0.2500455	0.250045	0.250045
Experimental σ	0.1111013	0.176541	0.212069
Theoretic σ	$\frac{1}{9} = 0.111111$	$\frac{3}{17} = 0.176470$	$\frac{7}{33} = 0.212121$

Tables 1 and 2 list the values of the experimental and theoretical contrasts, where R represents the number of RGs stacked to reconstruct the secret, G^R is the result, and # denotes the number of pixels in a specific area. The experiment results in the final two rows are nearly identical. A higher visual quality was observed when more RGs were stacked.

Fig. 6 shows the theoretical and experimental contrasts, indicating the variability of the theoretical contrast σ for stacking k RGs in the proposed method. As such, higher k and t imply a higher visual quality of the reconstructed secret.

5. Discussion

To highlight the advantages of the proposed FPVSS scheme, several aspects of the scheme are explained.

(1) Pixel expansion

The kernel technique of the proposed scheme is based on the RG-based VSS. Here, the proposed scheme benefits more from saving the bandwidth and storage compared with VC-based schemes, because of the elimination of pixel expansion.

(2) Codebook design

The codebook design is sometimes essential and may aggravate the problem of pixel expansion. The proposed FPVSS schemes can eliminate the redesign overhead.

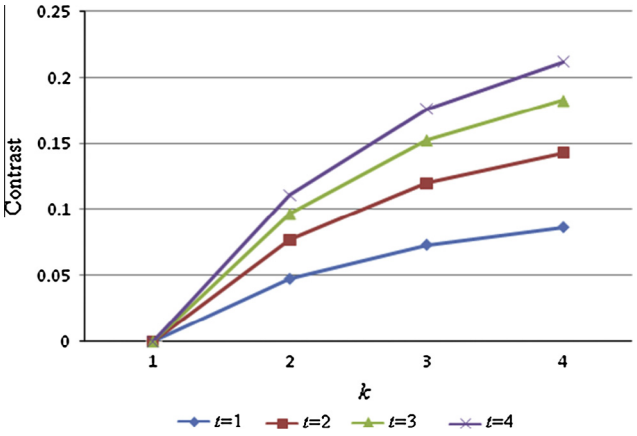

Fig. 6. The relationship between the contrast and the corresponding numbers k and n of the stacked random-grids when n is four.

(3) Easy to manage

The conventional VSS scheme entails encoding a secret image into several meaningless shared images; therefore, managing an increasing number of shared images for users is difficult. By contrast, the proposed scheme generates meaningful shares.

(4) Progressive visual quality

The experimental results revealed that the proposed scheme progressively increased the visual quality when more RGs are stacked.

(5) Contrast flexibility

Participants can select the parameter t ($1 \leqslant t \leqslant w \times h$) to control the quality of the logo images and reconstructed secret image. The higher the value of t is, the higher the quality of the reconstructed image becomes. The lower the value of t is, the higher the quality of logo images becomes. Therefore, the proposed scheme is more practical than those presented by previous studies.

Table 3 lists the main advantages of the proposed scheme compared with previous schemes. The advantage of the proposed scheme is that users can manage the RGs in a friendly manner. The other advantage is that the size of the generated RGs has no pixel expansion. Finally, the progressive method enables revealing the secret by using different levels.

The proposed scheme can be extended to manage the gray-level and color secret images such as those in previous studies [14,15,17,19]. Readers may refer to [14,15,17,19] for further details. The empirical results encoding gray-level X-ray/IR and color images are demonstrated in Appendices A and B, respectively.

6. Conclusions

We propose an effective RG-based VSS scheme that combines the advantage of friendly management and progressive secret disclosure and overcomes the disadvantages of VC-based VSS. The proposed scheme is superior to schemes presented in previous studies. It achieves the goal of friendly and progressive secret sharing without suffering from pixel expansion when providing adaptive contrast. Furthermore, the theoretical analysis and experimental results demonstrate its accuracy and feasibility.

Table 3
Comparison between related works and the proposed scheme.

Schemes	Kernel technique	Pixel expansion rate	Without computation in decryption	Visually progressive	Friendly	Contrast-flexibility
Naor and Shamir [5]	VC	4	Yes	No	No	N/A
Ateniese et al. [6]	VC	4	Yes	No	Yes	N/A
Zhou et al. [7]	VC	4	Yes	No	Yes	N/A
Tsai et al. [8]	VC	2	Yes	No	Yes	N/A
Jin et al. [9]	VC	4	No	Yes	No	N/A
Fang and Lin [10]	VC	4	Yes	Yes	No	N/A
Fang [11]	VC	4	Yes	Yes	Yes	Not addressed
Hou and Quan [18]	VC	1	Yes	Yes	No	N/A
Kafri and Keren [12]	RG	1	Yes	No	No	N/A
Shyu [13]	RG	1	Yes	No	No	N/A
Chen and Tsao[14]	RG	1	Yes	No	No	N/A
Chen and Tsao [17]	RG	1	Yes	No	No	N/A
Chen and Tsao [19]	RG	1	Yes	No	Yes	N/A
Chen [21]	RG	1	Yes	Yes	Yes	Not addressed
The proposed scheme	RG	1	Yes	Yes	Yes	Addressed

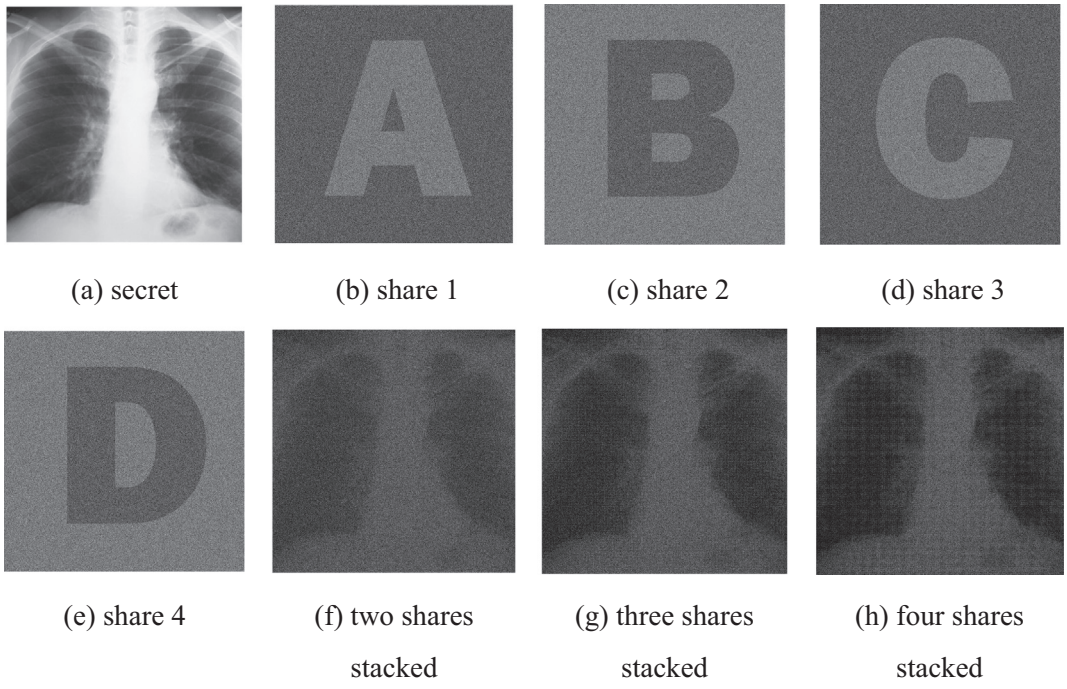

Fig. 7. The experimental results of an **X-ray image** with $t = 4$: (a) a secret image, (b–e) four meaningful random-grids, (f) two shared images stacked, (g) three shared images stacked, and (h) all shared images stacked.

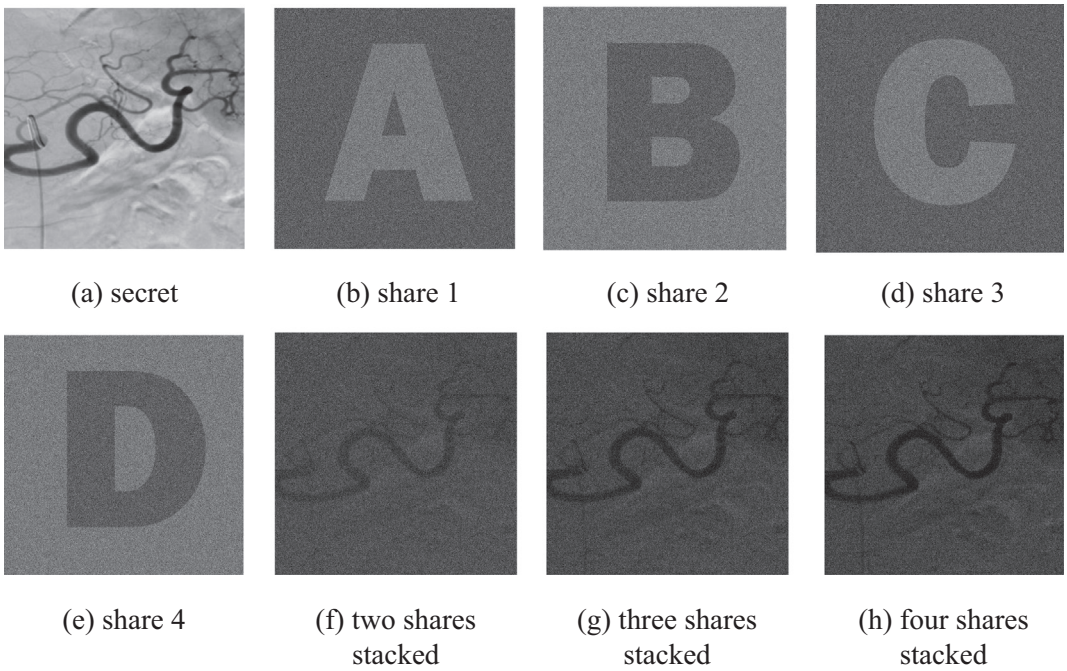

Fig. 8. The experimental results of an **IR image** with $t = 4$: (a) a secret image, (b–e) four meaningful random-grids, (f) two shared images stacked, (g) three shared images stacked, and (h) all shared images stacked.

Acknowledgments

This research was partially supported by Ministry of Science and Technology, R.O.C., under contract no. MOST 103-2221-E-415-017 and MOST 104-2221-E-415-013. The authors would like to thank the anonymous referees and the associate editor for your valuable suggestions that have resulted in the improvement of the correctness and completeness of the paper. They also thank I-Chun Weng for her assistance with the revision for conducting the further experiments.

Appendix A

See Fig. 7.

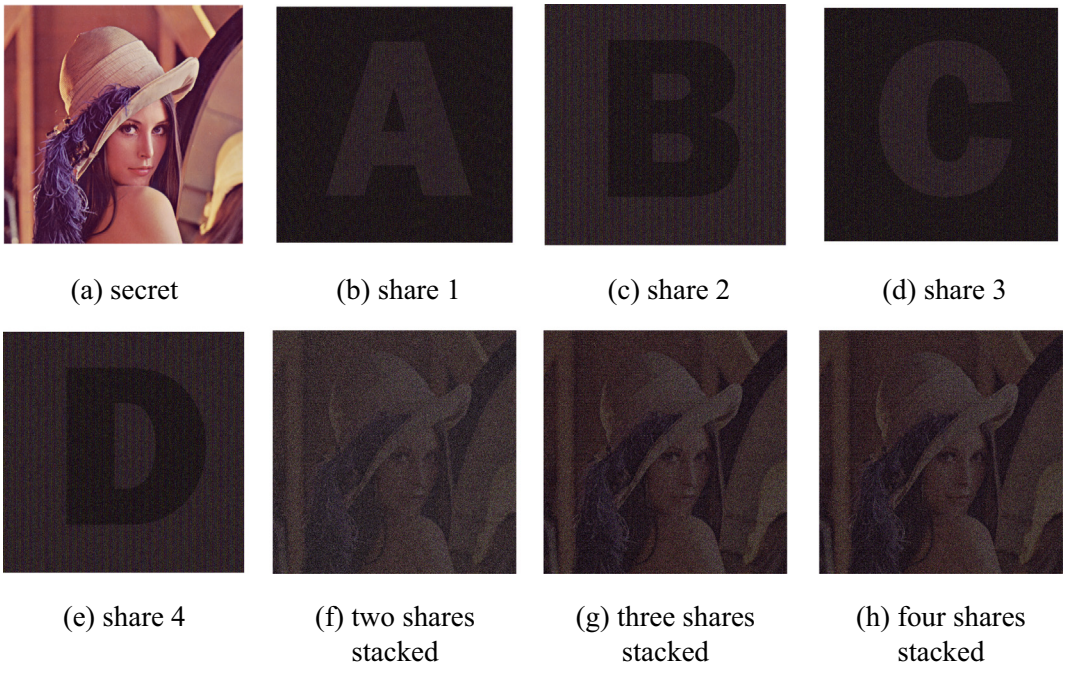

Fig. 9. The experimental results of a **color image** with $t = 4$: (a) a secret image, (b–e) four meaningful random-grids, (f) two shared images stacked, (g) three shared images stacked, and (h) all shared images stacked. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Appendix A.1

See Fig. 8.

Appendix B

See Fig. 9.

References

[1] R. Lukac, K.N. Plataniotis, Bit-level based secret sharing for image encryption, Pattern Recogn. 38 (5) (2005) 767–772.
[2] M. Naor, B. Pinkas, Visual authentication and identification, in: Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, Lecture Notes in Computer Science, Santa Barbara, California, USA, vol. 1294, 1997, pp. 322–336.
[3] W.P. Fang, J.C. Lin, Visual cryptography with extra ability of hiding confidential data, J. Electron. Imag. 15 (2) (2006) 023020-1–023020-7.
[4] T.H. Chen, D.S. Tsai, Owner-customer right protection mechanism using a watermarking scheme and a watermarking protocol, Pattern Recogn. 39 (8) (2006) 1530–1541.
[5] M. Naor, A. Shamir, Visual cryptography, in: Proceedings of Advances in Cryptology: Eurocrypt94, Lecture Notes in Computer Science, vol. 950, 1995, pp. 1–12.
[6] G. Ateniese, C. Blundo, A.D. Santis, D.R. Stinson, Extended capabilities for visual cryptography, Theoret. Comput. Sci. 250 (2001) 143–161.
[7] Z. Zhou, G.R. Arce, G.D. Crescenzo, Halftone visual cryptography, IEEE Trans. Image Process. 15 (8) (2006) 2441–2453.
[8] D.S. Tsai, T.H. Chen, G. Horng, On generating meaningful shares in visual secret sharing scheme, Imag. Sci. J. 56 (2008) 49–55.
[9] D. Jin, W.Q. Yan, M.S. Kankanhalli, Progressive color visual cryptography, J. Electron. Imag. 14 (2005) 033019.
[10] W.P. Fang, J.C. Lin, Progressive viewing and sharing of sensitive images, Pattern Recogn. Image Anal. 16 (4) (2006) 632–636.
[11] W.P. Fang, Friendly progressive visual secret sharing, Pattern Recogn. 41 (2008) 1410–1414.
[12] O. Kafri, E. Keren, Encryption of pictures and shapes by random grids, Opt. Lett. 12 (6) (1987) 377–379.
[13] S.J. Shyu, Image encryption by random grids, Pattern Recogn. 40 (3) (2007) 1014–1031.
[14] T.H. Chen, K.H. Tsao, Visual secret sharing by random grids revisited, Pattern Recogn. 42 (2009) 2203–2217.
[15] S.J. Shyu, Image encryption by multiple random grids, Pattern Recogn. 42 (2009) 1582–1596.
[16] A. Kanso, N. Smaoui, Logistic chaotic maps for binary numbers generations, Chaos, Soliton. Fract. 40 (5) (2009) 2557–2568.
[17] T.H. Chen, K.H. Tsao, Threshold visual secret sharing by random grids, J. Syst. Softw. 84 (2011) 1197–1208.
[18] Y.C. Hou, Z.Y. Quan, Progressive visual cryptography with unexpanded shares, IEEE Trans. Circ. Syst. Video Technol. 21 (2011) 1760–1764.
[19] T.H. Chen, K.H. Tsao, User-friendly random grid-based visual secret sharing, IEEE Trans. Circ. Syst. Video Technol. 21 (2011) 1693–1703.
[20] T.H. Chen, Y.S. Lee, Yet another friendly progressive visual secret sharing scheme, in: Proceedings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP-2009), 2009, pp. 353–356.
[21] S.K. Chen, Friendly progressive visual secret sharing using generalized random grids, Opt. Eng. 48 (2009) 117001.