A Threshold-based Image Recovery Scheme for Image Publishing

Zhen Wu[1], Yining Liu[1, 2], Kim-Kwang Raymond Choo[3]
[1] School of Information and Communication, Guilin University of Electronic Technology, China
[2] Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, China
[3] Information Systems and Cyber Security, University of Texas at San Antonio, USA
wuzhen35@163.com, ynliu@guet.edu.cn, raymond.choo@fulbrightmail.org

Abstract

As businesses capitalize on access to a wider global audience via their online presence, the demand for better quality marketing materials has skyrocketed, for example partly evidenced by the demand for images. There are two key entities in the image publishing ecosystem, namely: image publisher and the customer. In such a business model, either the customer needs to pay first or the image publisher delivers the service first. However, there are trade-offs between either approach. Therefore, in this paper, an image recovery scheme for image publishing is proposed. Specifically, the image publisher provides customers with a browsing service, where customers can browse through the lower quality images before deciding which image(s) to purchase. Besides, the image publisher can set different price ranges or tiers, for example, based on the quality of the images or on the quality of the images and the quantity of the entire transaction (e.g., bulk/group discount). Findings from our simulations demonstrate the utility of the proposed scheme.

Keywords: Threshold-based image protection, Image publishing, Image progressive recovery

1 Introduction

Image publishing ecosystem is the supply of images that are often licensed for specific uses, and examples include traditional macrostock photography, midstock photography and microstock photography [1]. There are two key entities in an image publishing ecosystem, namely: image publisher and customer. The relevance of image publishing in today's society is, perhaps, evidenced by the various commercial offerings. The price of a single image varies, say between $1 and $15 [2-4]. Images are used in a variety of settings, including in marketing and other visually demanding applications [5-6]. However, striking a balance between the interests of the image publisher and the needs of the customers can be challenging. For example, should a customer pay for the image or should the image publishing ecosystem delivers the image first? In the former payment model, the image publisher may lose prospective customers who are unwilling to pay for images without first browsing through the images. However, allowing the customers to first browse through images without paying, there are risks of copyright violation (e.g., taking a screen-capture of the browsed image or copying the image, without paying for it).

One of the building blocks in achieving a win-win payment model is image progressive recovery. The latter differs from conventional image encryption. For example, image encryption schemes such as chaos-based image encryption schemes [7-9] and compressive sensing based image encryption schemes [10-12], AES or DES based image encryption schemes [13-15], data encryption and decryption operations are carried out between two authorized entities. Besides, the data obtained by the decrypting entity is the same as the original complete data. In other words, it does not allow the decrypting entity to decrypt part of the data. Image progressive recovery, however, allows an image to be shared among multiple authorized entities and can be gradually recovered by different decrypting entities.

Another building block is threshold-based image protection scheme, which has been widely utilized for image protection among multiple parties [16]. Specifically, an image can be decomposed into multiple shares that are distributed to shareholders securely. The image is recovered only when the number of collaborating shareholders reaches the threshold [17-18]. Using such a scheme, images and other multimedia data can be losslessly recovered because the human eye is close to the low-pass or loss-tolerant filter [19-20]. Therefore, progressive is a characteristic that distinguishes multimedia from data. There are a number of schemes that achieve progressive recovery, such as progressive threshold-based image protection schemes [21-23] and progressive visual cryptography schemes [24-26]. All

*Corresponding Author: Yining Liu; E-mail: ynliu@guet.edu.cn
DOI: 10.3966/160792642021032202013

these progressive schemes have a common characteristic in the sense that the image can be progressively recovered, and the quality depends on the number of parties involved (i.e., quality of the recovered image increases with the number of participating parties). In the context of our proposed scheme, when there are more paying customers, higher quality images can be obtained.

Therefore, in this paper, we propose a win-win payment model, by allowing prospective customers to browse through low-quality images so that it can inform their buying process. The higher-quality images can be accessed by paying customers. In addition, the image publisher can also customize its offerings, for example by having tiered pricing. We coin this model as the win-win image recovery scheme for image publishing ecosystem.

The rest of this paper is organized as follows. The relevant background materials are presented in Section 2. We will introduce the proposed scheme in Section 3, prior to describing and presenting the simulation findings in Section 4. We then conclude this paper in Section 5.

2 Preliminaries

Threshold-based image protection scheme is one of two key building blocks in our proposed approach, and we will now revisit the scheme presented in [16].

For positive integers k and n, where $k \le n$, the image protection scheme based on a (k,n) threshold is a method of sharing an image to n parties and at least k parties cannot obtain any useful information of the image. Supposing the set of parties are denoted as $\mathcal{P}$, $\mathcal{M}$ be a finite set of pixel values in the image, and each share takes value in a finite set $\mathcal{S}$. All the pixel values space $\mathcal{M}$ and the share space $\mathcal{S}$ are identified with a finite field $\mathbb{F}_p$ of size p. For the pixel values in a gray image are in the range of [0, 255], the prime number p is usually set as $p = 251$.

Sharing phase

Step 1. The image I is first employed a reversible permutation operation to acquire a permutated image $\hat{I}$ Meanwhile, all pixel values larger than 250 in $\hat{I}$ should be truncated to 250.

Step 2. Divide $\hat{I}$ into several units. Each unit contains k non-lapped pixels a_0, a_1, ..., a_{k-1} that could be used to construct a $k-1$ degree polynomial $f(x)$.

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1} \bmod p \qquad (1)$$

Step 3. Suppose each party is associated with a finite field element α, the results $f(\alpha_1)$, $f(\alpha_2)$, ..., $f(\alpha_n)$ are pixel values in the corresponding shares.

Step 4. Repeat step 2 and step 3 until all units have been processed, the n shares SC_1, SC_2, ..., SC_n have been constructed and then send them to n parties in $\mathcal{P}$.

Revealing phase

Step 1. Let $\mathcal{A}$ denote the set of parties who involved in reconstructing the image, where the size of $|\mathcal{A}| \ge k$, and let $SC_{\mathcal{A}}$ denote the set of shares held by involved parties in $\mathcal{A}$. It means that no less than k distinct elements α and the corresponding value $f(\alpha)$ are known. Therefore, the $k-1$ degree polynomial $f(x)$ can be reconstructed.

Step 2. The coefficients in $f(x)$ are pixel values a_0, a_1, ..., a_{k-1} in each unit.

$$f(x) = \sum_{i=1}^{k} y_i \prod_{j=1, i \ne j}^{k} \frac{x - x_j}{x_i - x_j} \bmod p \qquad (2)$$

Step 3. Repeat step 2 - 3 until all pixels have been processed in shares, the permutated image $\hat{I}$ can be recovered.

Step 4. The image I can be revealed when the corresponding reversible permutation operation has been employed on $\hat{I}$.

3 Proposed Scheme

Image publishing ecosystem is the supply of images consists of two entities, namely image publisher and customer, respectively. Image publishers own various images. The image publisher makes profits by selling these images to customers and customers purchase images of different quality according to their own needs. Several qualities of an image can be set for paid customers and customers can access images of different quality levels according to their payment. Figure 1 shows an example of proposed scheme.

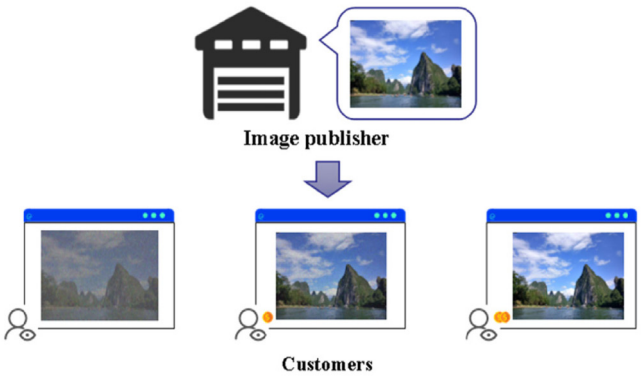


Figure 1. An example of the proposed scheme

In the proposed scheme, there is a $((t_1,t_2),s,k,n)$ threshold, where $1 \le t_1 < t_2 \le k$, $s \le n$, $t_2 \le s$ and $k \le n$. All images in the image publishing platform are from the big data environment. When a customer sends a request to the image publisher for a pre-browsing service, the image publisher firstly decomposes the

image into n shares including s essential shares and $n-s$ non-essential shares. These shares are random-looking. Then, the image publisher will send k shares including t_1 essential shares the customer. Because some pixels in the image can be recovered when there are t_1 essential shares in k shares, the customer can recover a lower-quality image. When the customer is interested, the customer can access images of different quality levels according to the degree of payment. More and more pixels can be recovered as the number of essential shares increased, the image can be reconstructed completely until the number of essential shares grows to t_2 and the image can be recovered at a high resolution. Thus, the customer will receive other essential shares from the image publisher and higher-quality images can be obtained according to their payment.

The proposed scheme consists of two phases, namely image decomposition phase, and image phase. The details of the scheme can be described as follows.

3.1 Image Decomposition

In the image decomposition phase, given an image from the image publisher, the image can be decomposed into n shares. These n shares consist of s essential shares with higher priorities and $n-s$ non-essential shares. The image decomposition algorithm is presented in Algorithm 1.

Algorithm 1. Image decomposition

Input: an image I of size $W \times H$ with (i,j)th pixel $I_{i,j}$, where $(i,j) \in \{(i,j) | 1 \le i \le W, 1 \le j \le H\}$, and five integers t_1, t_2, s, k, n ($1 \le t_1 < t_2 \le k$, $s \le n$, $t_2 \le s$ and $k \le n$).

Output: s essential shares SC_1, SC_2, ..., SC_s and $(n-s)$ non-essential shares SC_{s+1}, SC_{s+2}, ..., SC_n.

```
For ( i = 1; i < H; i++ ) do
    For ( j = 1; j < W; j++ ) do
        Generate (k − 1) random elements;
        Construct a polynomial as Eqn. (3);
        Generate a random element t ∈ [t1, t2];
        Construct g(x) = f^(t)(x);
        For ( r = 1; r ≤ n; r++ ) do
            If ( r ≤ s ) then
                SC_r[i, j] ← f(α_r)
            else
                SC_r[i, j] ← f^(t)(α_r)
            end
        end
    end
end
```

Step 1. Suppose there is an image I will be published. Let $S_{i,j}$ denoted as the pixel value at the position of (i,j) in I, where $(i,j) \in \{(i,j)\}$, $1 \le i \le W$, and $1 \le j \le H$. Repeat steps 2-4 until all the pixels in the image have been processed.

Step 2. Construct a $(k-1)$ degree polynomial as Eqn. (3), where p is a prime number, r_1, r_2, ..., r_{k-1} are arbitrary random numbers over finite field $\mathbb{F}_p$.

$$f(x) = S_{i,j} + r_1 x + r_2 x^2 + \cdots + r_{k-1} x^{k-1} \bmod p \qquad (3)$$

Step 3. Suppose each share is associated with a finite field element α, s essential shares can be generated as $SC_1 = f(\alpha_1)$, $SC_2 = f(\alpha_2)$, ..., $SC_s = f(\alpha_s)$.

Step 4. Select a random number $t \in [t_1, t_2]$ for each $S_{i,j}$, then the $(k-t-1)$ degree polynomials $g(x)$ can be constructed as Eqn. (4),

$$\begin{aligned} g(x) &= f^{(t)}(x) \\ &= c_1 x + c_2 x^2 + \cdots + c_{k-t-1} x^{k-t-1} \bmod p \end{aligned} \qquad (4)$$

where the coefficients are as follows.

$$\begin{aligned} c_1 &= r_t \times \frac{r_t!}{(r_t - t)!}, \\ c_2 &= r_{t+1} \times \frac{r_{t+1}!}{(r_{t+1} - t)!}, \\ &\cdots \\ c_{k-t-1} &= r_{k-1} \times \frac{r_{k-1}!}{(r_{k-1} - t)!}. \end{aligned} \qquad (5)$$

Step 5. The other $(n-s)$ non-essential shares can be generated by calculating $SC_{s+1} = f^{(t)}(\alpha_{s+1})$, $SC_{s+2} = f^{(t)}(\alpha_{s+2})$, ..., $SC_n = f^{(t)}(\alpha_n)$.

3.2 Image Progressively Recovery Phase

In the image progressively recovery phase, the decomposed image can be progressively recovery by different shares. Therefore, the image publisher can provide different services for paid customers and others customers. When a customer asks for an image, the image publisher will send some shares (including fewer essential shares) to the customer. This customer can use these shares to recover a lower quality image for free. When there are paid customers or multiple customers co-promote, the image publisher will send some other shares (including more essential shares) to these customers and recover a higher quality image.

In the image progressively recovery phase, assuming that the collected shares participating in recovering consist of l_1 essential shares and l_2 non-essential shares. To recover the image, there is a requirement that the collected shares must meet both the threshold condition and the essential condition in the proposed

scheme. The threshold condition and essential condition can be described as follows.

$$\begin{cases} \text{Threshold condition:} & l_1 + l_2 \geq k \\ \text{Essential condition:} & l_1 > t \end{cases}$$

When the collected shares meet both the threshold condition and essential condition, the image can be recovered. The more the essential shares participating in, the higher the quality of the recovered image. Thus, the image can be progressively recovered.

Step 1. Extracting an unprocessed pixel from each essential shares and non-essential shares in the same position, respectively. These pixels can be denoted as $(\alpha_1, f(\alpha_1))$, $(\alpha_2, f(\alpha_2))$, …, $(\alpha_{l_1}, f(\alpha_{l_1}))$ and $(\alpha_{s+1}, f(\alpha_{s+1}))$, $(\alpha_{s+2}, f(\alpha_{s+2}))$, …, $(\alpha_{s+l_2}, f(\alpha_{s+l_2}))$.

Step 2. Using l_1 pixel values in essentia shares and l_2 pixel values in non-essential shares, l_1+l_2 linear equations can be constructed and the coefficient matrix A_X of the corresponding l_1+l_2 linear equations can be described as Eqn. (6).

Since the rank of A_X is $l_1+l_2 \geq k$, the l_1+l_2 linear equations has a unique solution.

$$A_X = \begin{bmatrix} {\alpha_1}^0 & {\alpha_1}^1 & \cdots & {\alpha_1}^t & {\alpha_1}^{t+1} & {\alpha_1}^{t+2} & \cdots & {\alpha_1}^{k-1} \\ {\alpha_2}^0 & {\alpha_2}^1 & \cdots & {\alpha_2}^t & {\alpha_2}^{t+1} & {\alpha_2}^{t+2} & \cdots & {\alpha_2}^{k-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ {\alpha_{l_1}}^0 & {\alpha_{l_1}}^1 & \cdots & {\alpha_{l_1}}^t & {\alpha_{l_1}}^{t+1} & {\alpha_{l_1}}^{t+2} & \cdots & {\alpha_{l_1}}^{k-1} \\ 0 & 0 & \cdots & {\alpha_{s+1}}^1 & {\alpha_{s+1}}^2 & {\alpha_{s+1}}^3 & \cdots & {\alpha_{s+1}}^{k-t-1} \\ 0 & 0 & \cdots & {\alpha_{s+2}}^1 & {\alpha_{s+2}}^2 & {\alpha_{s+2}}^3 & \cdots & {\alpha_{s+2}}^{k-t-1} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & {\alpha_{s+l_2}}^1 & {\alpha_{s+l_2}}^2 & {\alpha_{s+l_2}}^3 & \cdots & {\alpha_{s+l_2}}^{k-t-1} \end{bmatrix} \quad \textbf{(6)}$$

Step 3. Repeat Step 1-2 until all pixels in shares have been processed, the image can be recovered.

4 Experimental Results and Analysis

4.1 Experiment Results

Figure 2 displays the results of proposed scheme based on ((1, 4), 4, 4, 8) threshold for a grayscale image. The test image can be provided for customers with four levels of qualities. Figure 2(a) shows an image 'Clock' published on the image publishing ecosystem, which size is 256×256. When a customer sends a request to the image publisher for a pre-browsing service, image publisher firstly decompose the 'Clock' into four essential shares (SC_1 - SC_4) and four non-essential shares (SC_5 - SC_8), which are presented in Figure 2(b) and Figure 2(c), respectively. Then, the image publisher will send four shares including one essential share the customer. And Figure 2(d-1) shows the recovered image which can be freely obtained by customers. Higher quality images are available when a customer pays some fees. The higher the fee paid, the higher the quality of the image available. Other higher qualities of the recovered images are presented from Figure 2(d-2) to Figure 2(d-4), respectively.

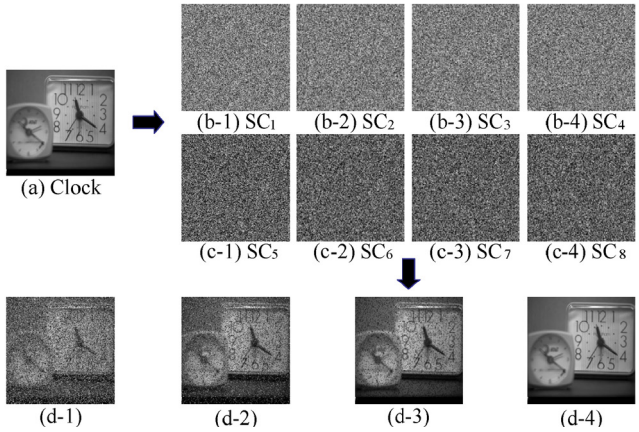


Figure 2. Simulation results of the proposed scheme based on ((1, 4), 4, 4, 8) threshold for a grayscale image, (a) an image from an image publisher (b) four essential shares, (c) four non-essential shares, (d) four different-quality images can be offered to consumers

Figure 3 displays the results of the proposed scheme based on ((1, 5), 5, 5, 10) threshold for a grayscale image. The test image can be provided for customers with five levels of qualities. Figure 3(a) shows the test image called 'Peppers' published by an image publisher, which size is 256×256. When a consumer requests a service to the image publisher, five essential shares (SC_1 - SC_5) and five non-essential shares (SC_6 - SC_{10}) can be generated and presented in Figure 3(b) and Figure 3(c), respectively. Figure 3(d) shows five different-quality images can be offered to the consumer. Figure 3(d-1) shows the recovered image based on four shares including an essential share, which can be freely obtained by customers. Higher quality images are available when a customer pays some fees. The higher the fee paid, the higher the quality of the image available. Other qualities of the recovered images are presented from Figure 3(d-2) to Figure 3(d-5), respectively.

Figure 4 displays the results of the proposed scheme based on ((1, 4), 4, 4, 8) threshold for a color image. Figure 4(a) shows the test image called 'Lena' from a publisher, which size is 256×256. All simulation results above prove that all the shares produced by the proposed scheme for both grayscale and color image are random-looking. And the image publishers can offer several levels of services for customers.

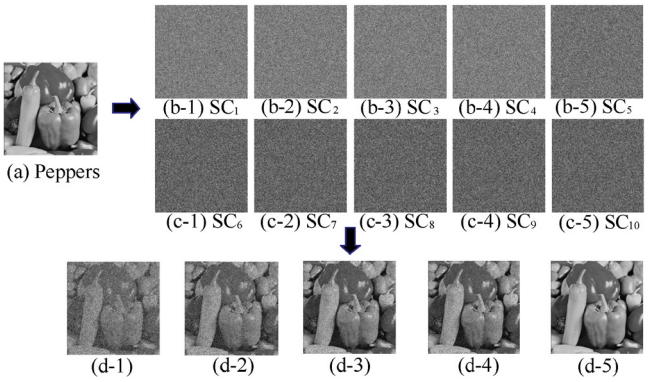


Figure 3. Simulation results of the proposed scheme based on ((1, 5), 5, 5, 10) threshold for a grayscale image, (a) test image 'Peppers' from an image publisher, (b) five essential shares (SC_1 - SC_5), (c) five non-essential shares (SC_6 - SC_{10}), (d) five different-quality images can be offered to consumers

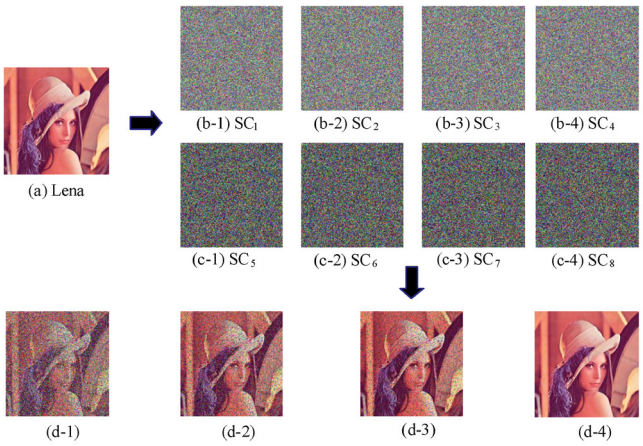


Figure 4. Simulation results of the proposed scheme based on ((1, 4), 4, 4, 8) threshold for a color image, (a) test image 'Lena' from the image publisher, (b) four essential shares threshold (SC_1 - SC_4), (c) four non-essential shares (SC_5 - SC_8), (d) four different-quality images can be offered to consumers

Excepting global progressively recovery, there are some simulation results demonstrate that the proposed scheme also can be implemented to a regional progressive recovery. Figure 5 shows simulation results of regional progressive recovery on a gray image 'Couple' with a ((1, 4), 4, 4, 8) threshold. Figure 6 shows simulation results of regional progressive recovery on a color image'Car' with a ((1, 3), 3, 3, 6) threshold. All simulation results discussed above confirm that the proposed scheme can achieve both global progressively recovery and regional progressive recovery.

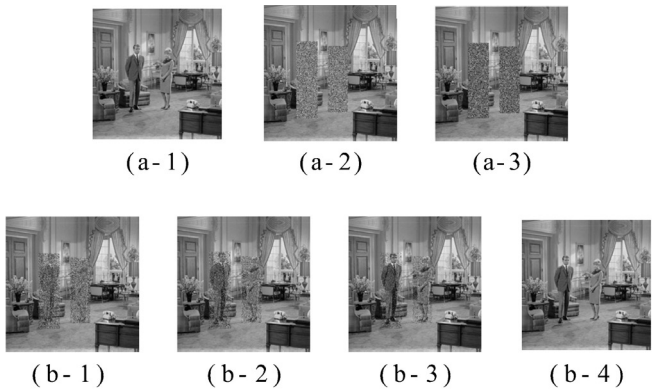


Figure 5. Simulation results of regional progressively recovery on a gray image with ((1, 4), 4, 4, 8) threshold

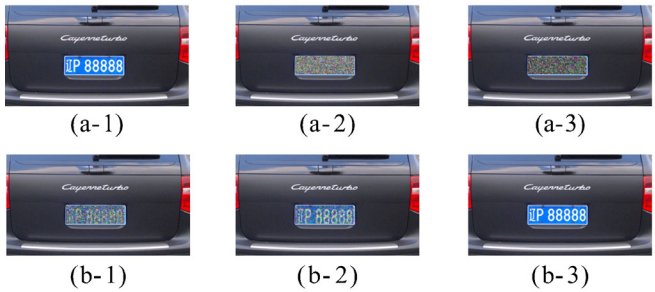


Figure 6. Simulation results of regional progressively recovery on a color image 'Car' with ((1, 3), 3, 3, 6) threshold

4.2 Computation Overhead

4.2.1 Histogram Analysis

Histogram of a digital image can assess the tonal distribution of pixels by the form of graphical. The *x*-axis and *y*-axis of the histogram represent the intensity levels and the number of pixels in the image with the corresponding intensity level, respectively. Figure 7 displays the histograms for the image 'Clock' and all the shares in Figure 2. Figure 7(a) displays the histogram of the image 'Clock' and the histogram of each essential shares and each non-essential shares are shown in Figure 7(b) and Figure 7(c), respectively. It can be seen from each histogram of shares that the pixels in each share nearly reach to the uniform distribution and the randomness between shares. Figure 7(d) displays the histograms for reconstructed images, which can prove that the image publishers can offer several levels of services for customers. Higher quality images are available when a customer pays some fees. The higher the fee paid, the higher the quality of the image available.

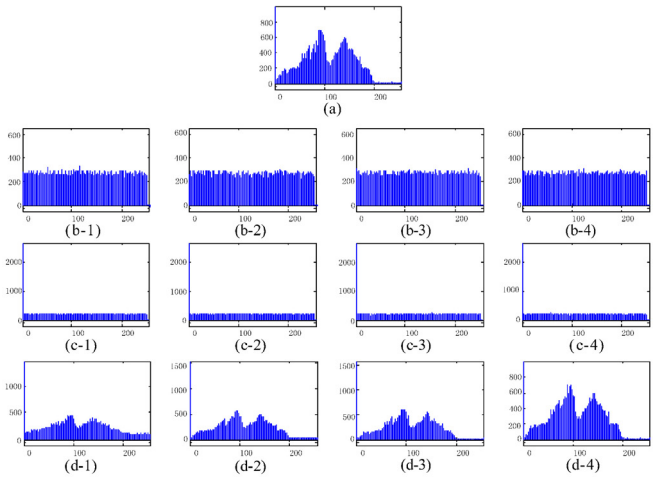


Figure 7. Histograms for all the images in Figure 2, (a) histogram for the image 'Clock', (b) histograms for essential shares, (c) Histograms for non-essential shares, (d) histograms for different quality of recovered images

4.2.2 Correlation

Correlation between a pair of the variable is a statistical measure that is used to assess how strongly the pair of the variable is related to each other. If there are two images I_1, I_2 with the same size $W \times H$, the correlation coefficient can be exhibited as Eqn. (7). When $Corr(I_1, I_2) = 0$, there is no relation between I_1 and I_2. When $0 < Corr(I_1, I_2) < 1$, I_1 and I_2 are related. The greater the absolute value of the correlation coefficient, the stronger the correlation, the closer the correlation coefficient is to -1 or 1.

$$Corr(I_1, I_2) = \frac{\sum_W \sum_H (I_1 - \bar{I}_1)(I_2 - \bar{I}_2)}{\sqrt{\sum_W \sum_H (I_1 - \bar{I}_1)^2 \sum_W \sum_H (I_2 - \bar{I}_2)^2}} \quad \textbf{(7)}$$

In the proposed scheme, the correlation can be utilized to measure the relation among pixels in the shares. The average vertical correlation coefficient, average horizontal correlation coefficient and average diagonal correlation coefficient of the generated shares in the proposed scheme based on ((1, 4) 4, 4, 8) threshold in Figure 2 are listed in Table 1.

Table 1. The average correlation coefficients of shares

Type of shares	Horizontal	Vertical	Diagonal
Essential shares	-0.0036	-0.0038	0.0032
Non-essential shares	-0.0041	-0.0031	0.0016

4.2.3 MSE and RMSE

Mean square error (MSE) defines the square of the differences of the corresponding pixels between two images I_1 and I_2. It is another similarity measure that is generally used to assess the quality difference between the shares and the original image. MSE can be described as Eqn. (8).

$$MSE = \frac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} (I_1(i,j) - I_2(i,j))^2 \quad \textbf{(8)}$$

Root mean square error (RMSE) defines the square root of MSE, which can be described as Eqn. (9).

$$RMSE = \sqrt{MSE} \quad \textbf{(9)}$$

Generally, both MSE and RMSE values would be closer to zero when the reconstructed image is closer to the corresponding image. Besides, both MSE and RMSE values would be greater among generated shares. Table 2 gives some MSE and RMSE values between the image 'Clock' and the generated shares in the proposed scheme based on ((1, 4) 4, 4, 8) threshold.

Table 2. MSE and RMSE values between original image and each share

Images	MSE	RMSE
I, SC_1	0.00863	0.0929
I, SC_2	0.00849	0.0921
I, SC_3	0.00847	0.0921
I, SC_4	0.00837	0.0915
I, SC_5	0.00944	0.0972
I, SC_6	0.00942	0.0971
I, SC_7	0.00944	0.0972
I, SC_8	0.00943	0.0971

4.2.4 PSNR and SSIM

Peak signal to noise ratio (PSNR) is employed to measure the quality of the reconstructed image relative to the corresponding original image. PSNR can be exhibited as Eqn. (10). The larger of PSNR value, the more similarities between the reconstructed image and the corresponding original image and $PSNR = +\infty$ indicates the reconstructed image is the original image.

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} \text{ dB} \quad \textbf{(10)}$$

A structural similarity index measure (SSIM) is employed to analyze the visual impact of an image. There are three characteristics luminance, contrast and structure in an image and the value of SSIM are equal to the multiplicative combination of these three characteristics. The value of SSIM ranges in -1 to 1 and can be calculated as Eqn. (11), where μ_{I_1}, μ_{I_2}, σ_{I_1}, σ_{I_2} and $\sigma_{I_1 I_2}$ stand for the local means, standard deviations and cross-covariance for two images I_1 and

I_2. Usually, the coefficients can be set as $C_3 = \frac{C_1}{2}$, $\alpha = \beta = \gamma = 1$.

$$SSIM(I_1, I_2) = [l(I_1, I_2)]^{\alpha} \times [c(I_1, I_2)]^{\beta} \times [s(I_1, I_2)]^{\gamma}, \quad (11)$$

where $l(I_1, I_2) = \frac{2\mu_{I_1}\mu_{I_2} + C_1}{\mu_{I_1}^2 + \mu_{I_2}^2 + C_1}$,

$$c(I_1, I_2) = \frac{2\sigma_{I_1}\sigma_{I_2} + C_2}{\sigma_{I_1}^2 + \sigma_{I_2}^2 + C_2},$$

$$s(I_1, I_2) = \frac{2\sigma_{I_1 I_2} + C_3}{\sigma_{I_1 I_2} + C_3}.$$

The larger of SSIM value, the more similar between the reconstructed image and the corresponding original image and SSIM = 1 indicates the reconstructed image is the original image.

We use two different thresholds as examples to measure the quality of the reconstructed images in the proposed scheme. The test images are from Figure 2(d) and Figure 3(d), respectively. Each examples are supposed that there are enough shares collected which including l essential shares. Table 3 gives some PSNR and SSIM values of different reconstructed images.

Table 3. PSNR and SSIM values of different quality of recovered images

Threshold	Level of service	PSNR	SSIM
((1,4)4,4,8)	$l = 1$	11.2607	0.0595
	$l = 2$	13.8081	0.1241
	$l = 3$	16.0679	0.2814
	$l = 4$	$+\infty$	1
((1,5)5,5,10)	$l = 1$	10.4050	0.1465
	$l = 2$	11.8728	0.2284
	$l = 3$	14.0437	0.3499
	$l = 4$	15.7622	0.4853
	$l = 5$	$+\infty$	1

4.2.5 NPCR and UACI

The number of pixels change rate (NPCR) represents the ratio of different gray values of different encrypted images at the same location. The unified average changing intensity (UACI) represents the average variation density between different encrypted images, which is usually used for image encryption performance analysis. Both NPCR and UACI can assess the randomness between any two shares and they also are useful for determining the efficiency of the proposed scheme against differential attacks. NPCR and UACI can be exhibited as Eqn. (12) and Eqn. (13), respectively.

$$NPCR(I_1, I_2) = \frac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} D(i, j), \quad (12)$$

where $D(i, j) = \begin{cases} 0, & if\ I_1(i, j) = I_2(i, j) \\ 1, & if\ I_1(i, j) \neq I_2(i, j) \end{cases}$.

$$UACI(I_1, I_2) = \frac{1}{W \times H} \sum_{i=1}^{W} \sum_{j=1}^{H} \frac{|I_1(i, j) - I_2(i, j)|}{255} \quad (13)$$

To evaluate the randomness of the shares in the proposed scheme with threshold ((1, 4), 4, 4, 8) in Figure 2. Simply, let a share SC_1 as an example to compare with other shares and the results of NPCR and UACI values are listed in Table 4. As we can see from Table 4, all NPCR values over 99% and all UACI values over 32% , which indicates the proposed scheme can withstand the differential attacks.

Table 4. MSE and RMSE values between original image and each share

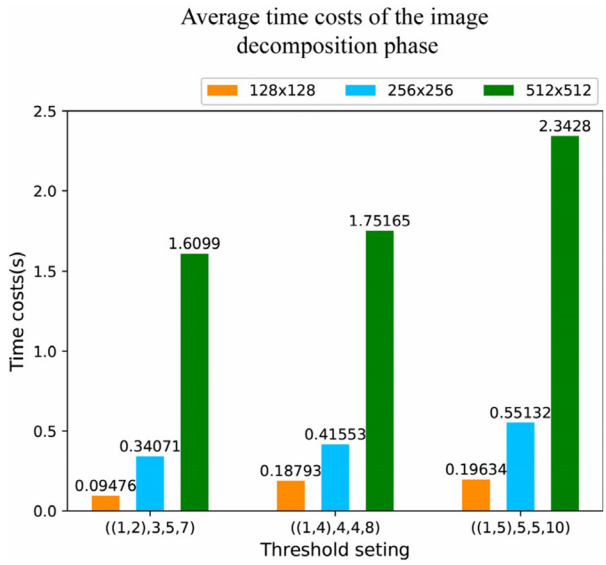
Images	NPCR	UACI
SC_1, SC_2	**0.99626**	**0.3293**
SC_1, SC_3	**0.99609**	**0.3270**
SC_1, SC_4	0.99615	0.3273
SC_1, SC_5	0.99604	0.3680
SC_1, SC_6	0.99597	0.3639
SC_1, SC_7	0.99582	0.3629
SC_1, SC_8	0.99580	0.3699

4.3 Time Costs

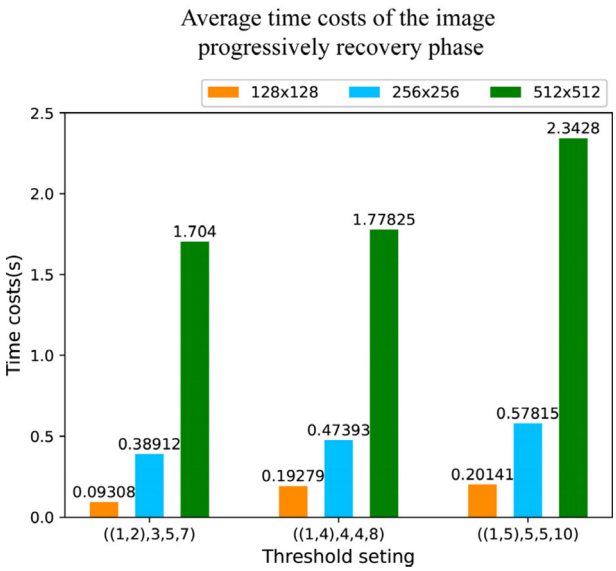
For different thresholds and sizes of images, the computational times in image decomposition phase and image progressively recovery phase are listed in Table 5. In addition, Figure 8 also presents the average time costs of the proposed scheme. Since the computation complexity of Lagrange interpolation is about $O(N^2)$, where N is the number of pixels in an image. As we can see from Table 5 and Figure 8, the proposed scheme is efficient for it has a lower computational complexity and fewer time costs. Therefore, the proposed scheme can be applied to the image publishing ecosystem in reality.

5 Conclusion

Given the increasing digitalization of our society and the widespread availability of image acquiring devices (e.g., mobile devices with high-quality lens), more images will be acquired and traded. This necessitates the design of a progressive image recovery scheme for the image producers, agency (which hosts the image publishing ecosystem that can be used to publish the images), and the customers. Findings from



(a) average time costs of the image decomposition phase



(b) average time costs of the image progressively recovery phase

Figure 8. Average time costs of the proposed scheme

Table 5. Computational times in sharing phase and recovering phase of the proposed scheme

Threshold	Image size	Average computational time (s)	
		Decomposi-tion phase	Recovery phase
((1,2)3,5,7)	128×128	0.09476	0.09308
	256×256	0.34071	0.38912
	512×512	1.60990	1.7040
((1,4)4,4,8)	128×128	0.18793	0.19279
	256×256	0.41553	0.47393
	512×512	1.75165	1.77825
((1,5)5,5,10)	128×128	0.19684	0.20141
	256×256	0.55132	0.57815
	512×512	2.34280	2.45347

our experimental results demonstrated that the computational complexity and time costs incurred by both the image publisher and the customer are low (i.e., lightweight) and hence, practical. Future research directions include incorporating other features such as support for e-payment and reviews for the traded images.

Acknowledgements

This work was partly supported by Natural Science Foundation of China under grant No. 61662016 and No. 62072133, Key projects of Guangxi Natural Science Foundation under grant No. 2018GXNSFDA281040.

References

[1] P. Frosh, Inside the image factory: stock photography and cultural production, *Media, Culture and Society*, Vol. 23, No. 5, pp. 625-646, September, 2001.

[2] W. Feighery, Tourism, stock photography and surveillance: a foucauldian interpretation, *Journal of Tourism and Cultural Change*, Vol. 7, No. 3, pp. 161-178, October, 2009.

[3] L. Shifman, The cultural logic of photo-based meme genres, *Journal of Visual Culture*, Vol. 13, No. 3, pp. 340-358, December, 2014.

[4] J. Gluckler, R. Panitz, Unpacking social divisions of labor in markets: Generalized blockmodeling and the network boom in stock photography, *Social Networks*, Vol. 47, pp. 156-166, October, 2016.

[5] K. K. Tseng, R. Zhang, C. M. Chen, M. M. Hassan, DNetUnet: a semi-supervised CNN of medical image segmentation for super-computing AI service, *The Journal of Supercomputing*, pp. 1-22, August, 2020.

[6] E. K. Wang, C. M. Chen, M. M. Hassan, A. Almogren, A deep learning based medical image segmentation technique in Internet-of-Medical-Things domain, *Future Generation Computer Systems*, Vol. 108, pp. 135-144, July, 2020.

[7] Z. Zhu, W. Zhang, K. Wong, H. Yu, A chaos-based symmetric image encryption scheme using a bit-level permutation, *Information Sciences*, Vol. 181, No. 6, pp. 1171-1186, March, 2011.

[8] E. Y. Xie, C. Li, S. Yu, J. Lü, On the cryptanalysis of Fridrich's chaotic image encryption scheme, *Signal Processing*, Vol. 132, pp. 150-154, March, 2017.

[9] Q. Zhang, J. Han, Y. Ye, Image encryption algorithm based on image hashing, improved chaotic mapping and DNA coding, *IET Image Processing*, Vol. 13, No. 14, pp. 2905-2915, December, 2019.

[10] M. Zhang, X. Tong, J. Liu, Z. Wang, J. Liu, B. Liu, J. Ma, Image compression and encryption scheme based on compressive sensing and Fourier transform, *IEEE Access*, Vol. 8, pp. 40838-40849, February, 2020.

[11] A. S. Unde, P. P. Deepthi, Design and analysis of compressive sensing-based lightweight encryption scheme for multimedia IoT, *IEEE Transactions on Circuits and Systems*,

Part II: Express Briefs, Vol. 67, No. 1, pp. 167-171, January, 2020.

[12] D. Xiao, F. Li, M. Wang, H. Zheng, A novel high-capacity data hiding in encrypted images based on compressive sensing progressive recovery, *IEEE Signal Processing Letters*, Vol. 27, pp. 296-300, January, 2020.

[13] N. Islam, Z. Shahid, W. Puech, Denoising and error correction in noisy AES-encrypted images using statistical measures, *Signal Processing-Image Communication*, Vol. 41, pp. 15-27, February, 2016.

[14] G. Qian, Q. Jiang, S. Qiu, A new image encryption scheme based on DES algorithm and chua's circuit, *IEEE International Workshop on Imaging Systems and Techniques*, Shenzhen, China, 2009, pp. 168-172.

[15] R. Yang, Z. Zheng, S. Tao, S. Ding, Image steganography combined with DES encryption pre-processing, *6th International Conference on Measuring Technology and Mechatronics Automation*, Zhangjiajie, China, 2014, pp. 323-326.

[16] C. Thien, J. Lin, Secret image sharing, *Computers and Graphics*, Vol. 26, No. 5, pp. 765-770, October, 2002.

[17] X. Yan, Y. Lu, L. Liu, A general progressive secret image sharing construction method, *Signal Processing: image Communication*, Vol. 71, pp. 66-75, February, 2019.

[18] H. Prasetyo, C. Hsia, Lossless progressive secret sharing for grayscale and color images, *Multimedia Tools and Applications*, Vol. 78, No. 17, pp. 24837-**24862**, September, 2019.

[19] Y. Hou, Z. Quan, Progressive visual cryptography with unexpanded shares, *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 21, No. 11, pp. 1760-1764, November, 2011.

[20] Y. Hou, Z. Quan, C. Tsai, Progressive Visual Cryptography with Friendly and Size Invariant Shares, *The International Arab Journal of Information Technology*, Vol. 15, No. 2, pp. 321-330, March, 2018.

[21] Y. Guo, Z. Ma, M. Zhao, Polynomial based progressive secret image sharing scheme with smaller shadow size, *IEEE Access*, Vol. 7, pp. 73782-73789, May, 2019.

[22] T. Bhattacharjee, S. P. Maity, Progressive and hierarchical share-in-share scheme over cloud, *Journal of Information Security and Applications*, Vol. 46, pp. 108-120, June, 2019.

[23] Y. Hu, Y. Liu, A progressively essential secret image sharing scheme using hierarchy shadow, *Journal of Information Security and Applications*, Vol. 47, pp. 371-376, August, 2019.

[24] N. C. Mhala, A. R. Pais, Contrast enhancement of Progressive Visual Secret Sharing (PVSS) scheme for gray-scale and color images using super-resolution, *Signal Processing*, Vol. 162, pp. 253-267, September, 2019.

[25] P. Chiu, K. Lee, Efficient constructions for progressive visual cryptography with meaningful shares, *Signal Processing*, Vol. 165, pp. 233-249, December, 2019.

[26] C. Yang, C. Wu, Y. Lin, k out of n region-based progressive visual cryptography, *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 29, No. 1, pp. 252-262, January, 2019.

Biographies

Zhen Wu received the B. E. degree in Computer Science and Technology from Zhengzhou University, Henan, China, in 2016. She is a Ph.D candidate in School of Information and Communication, Guilin University of Electronic Technology, Guilin, China. Her research interest focuses on security and privacy in image sharing.

Yining Liu received the B.S. degree in applied mathematics from Information Engineering University, Zhengzhou, China, in 1995, the M.S. degree in computer software and theory from the Huazhong University of Science and Technology, Wuhan, China, in 2003, and the Ph.D. degree in mathematics from Hubei University, Wuhan, in 2007. He is currently a professor with school of Computer and Information Security, Guilin University of Electronic Technology, Guilin, China. His research interests include the information security protocol and data privacy.

Kim-Kwang Raymond Choo received the Ph.D. in Information Security in 2006 from Queensland University of Technology, Australia. He currently holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio (UTSA). He was included in Web of Science's Highly Cited Researcher in the field of Cross-Field.