Sharing a Large Secret Image Using Meaningful Shadows Based on VQ and Inpainting

Zhi-Hui Wang[1], Kuo-Nan Chen[2], Chin-Chen Chang[3, 4] and Chuan Qin[4]
[1] School of Software, Dalian University of Technology
Dalian, Liaoning, China
[e-mail: wangzhihui1017@gmail.com]
[2] Department of Computer Science and Information Engineering, National Chung Cheng University
Ming-Hsiung, Chiayi 621, Taiwan
[e-mail: ckn95p@cs.ccu.edu.tw]
[3] Department of Computer Science and Information Engineering, Asia University
Taichung 41354, Taiwan
[e-mail: alan3c@gmail.com]
[4] Department of Information Engineering and Computer Science, Feng Chia University
Taichung City 40724, Taiwan
[e-mail: qin@usst.edu.cn]
*Corresponding author: Chin-Chen Chang

Received July 21, 2015; revised September 8, 2015; accepted September 23, 2015; published December 31, 2015

Abstract

This paper proposes a novel progressive secret image-hiding scheme based on the inpainting technique, the vector quantization technique (VQ) and the exploiting modification direction (EMD) technique. The proposed scheme first divides the secret image into non-overlapping blocks and categorizes the blocks into two groups: complex and smooth. The blocks in the complex group are compressed by VQ with PCA sorted codebook to obtain the VQ index table. Instead of embedding the original secret image, the proposed method progressively embeds the VQ index table into the cover images by using the EMD technique. After the receiver recovers the complex parts of the secret image by decoding the VQ index table from the shadow images, the smooth parts can be reconstructed by using the inpainting technique based on the content of the complex parts. The experimental results demonstrate that the proposed scheme not only has the advantage of progressive data hiding, which involves more shadow images joining to recover the secret image so as to produce a higher quality steganography image, but also can achieve high hiding capacity with acceptable recovered image quality.

Keywords: Vector Quantization, EMD, secret sharing, image inpainting

1. Introduction

In contrast to traditional information transmission, such as mail by the post office and delivery services of a delivery company, the Internet provides fast and convenient data transfer for thousands of users via worldwide networks. However, the Internet environment is public, so how to provide secure data transfer via the Internet becomes an important research subject. To date, two techniques, cryptography [1-3] and steganography [4-6], have been widely employed. The main idea behind cryptography is to encrypt data with a secret key. The procedure of encryption is essentially the re-encoding of data into meaningless ciphertext. Attackers cannot decode the ciphertext into the original data without the secret key. However, the meaningless appearance of the ciphertext readily attracts the attention of the malicious attacker. Steganography focuses on how to embed data into cover objects, such as video, audio, and digital images. The intent is to embed data by making the smallest possible distortion to the cover object; thus, steganography may draw less attention from attackers than cryptography [23-27]. The most representative method of image-based steganography is least significant bit (LSB) substitution [7-9], which embeds the secret data by directly substituting the LSB of the cover pixels in the image with the secret bits. Since the change of the LSB of the pixel has the smallest influence on the value of the pixel, this method can achieve the goal of embedding secret data while keeping low distortion of the cover image.

In contrast to the cryptography and steganography one-sender-to-one-receiver data transfer structure, the secret data sharing technique [10] embeds data in multi-images and sends the shadows to multi-receivers. Thus, the secret data can be retrieved by some receivers instead of all of them. As a result, even though some receivers lose their shadows, the secret data still can be reconstructed through cooperation among the residue receivers. Due to the development of the digitalization of our society, there are more and more sensitive digital image files need to be protected. Therefore, a lot of researchers are working on how to protect image type of secrets in secret sharing. The proposed methods of the previous works could be classified into two categories [11]. The first category is the polynomial-based secret image sharing, which hides the information of the image into the coefficients of the polynomial so that the secret image could be reconstructed lossless if and only if the polynomial is rebuilt during the secret image recover procedure. The other category is visual secret sharing (also called visual cryptography). The first (t, n) visual secret sharing scheme was proposed by Naor and Shamir [12]. Noar and Shamir's scheme generates n shadows for a secret image and prints them on n transparencies. Any t or more than t transparencies stacked together could decrypt the secret image visually and approximately. Different from the polynomial-based secret image sharing, visual secret image sharing does not need complex computation and cryptographic knowledge to decrypt the secret image. However, there is a common limitation for aforementioned two categories, which is the superposing result of the shadow is either decrypted secret image correctly or exposed nothing of the secret image. In order to break this limitation, some researchers have been studied to solve how to sharing secret image progressively in visual secret sharing, which means that the more the participants work together, the higher quality of secret image they can retrieve. Fang and Lin proposed a progressively secret image sharing scheme for binary images [13]. In this scheme, the participants are weighted, which means, the important participant could have more than one shadows while other ordinary participant could have only one shadow each. In order to extend the application of progressively secret image sharing, Jin *et al.* [14] proposed a new scheme that could support both grayscale and

color images with the use of halftoning and a novel microblock encoding scheme. There is a short come of Fang and Lin's scheme and Jin et al.'s scheme, which is the generated shadows are noise-like shadows. It will be very hard for users to identify and manage them. Accordingly, some schemes were designed to generate user friendly shadows, which are shrunken versions of the secret image [15-16]. Surly these schemes provide easier way for shadows identification and management. However, this kind of shadow reveals some information of the secret image, so it is not applicable in secret image protecting applications. In order to provide the user friendly shadows generated mechanism and secret image sharing function in a progressive way simultaneously, Fang proposed a novel user friendly progressively secret image sharing scheme[17]. Fang's scheme expands a pixel in the halftone secret image to a 2×2 pixels block and generates new blocks for meaningful shadows from it according to another meaningful image. To fix the pixel expansion problem in Fang's scheme, Chang et al. proposed a new 2×2 sized block-wise operation based user friendly progressive visual secret sharing scheme [11]. In Chang et al's scheme, the size of the secret image equals the size of the shadow image and the recovered secret image, in other words, the hiding capacity of Chang et al's scheme is better than Fang's scheme. To further improve the hiding capacity in the user friendly progressive secret image sharing mechanism, this paper proposes a novel progressive grayscale secret image sharing scheme based on VQ, EMD and image inpainting techniques. On the one hand, totally different from previous works' block mapping mechanism, our proposed scheme skillfully design a procedure of progressively embedding the VQ indices of the complex part of the secret image into the cover images, and then, get the high quality shadow images. On the other hand, since the smooth part can be reconstructed vary well by using the inpainting technique with valid surrounding information, the proposed scheme reduces the information of the secret image to the information of the complex part of the secret image. As a result, the constructed shadow image is much smaller than the shadow image constructed in the previous works.

The following is a brief description of the proposed scheme. First, the proposed scheme extracts the complex blocks of the secret image and compresses them by using the vector quantization (VQ) technique [18, 19]. Second, the compression result of the last step is embedded into multiple cover images via the exploiting modification direction (EMD) technique [20] and LSB. The inpainting technique [21, 22] is adopted at the last step to recover the secret image. The advantages of the proposed scheme include achieving progressive secret image recovery and sharing secret images by using relatively smaller cover images with a high-quality stego image.

The rest of this paper is organized as follows. The VQ technique, EMD technique and PDE based image inpainting technique are introduced as related works in Section 2. Section 3 illustrates the detailed procedures of the proposed method. The experimental results are provided in Section 4. Finally, the conclusion is presented in Section 5.

2. Related Work

The proposed scheme uses the VQ technique to compress the complex blocks of the secret image, adopts the EMD technique to embed the compression result in the cover images and utilizes the PDE based image inpainting technique to reconstruct the smooth part of the secret image; thus, VQ, EMD and PDE based image inpainting technique are introduced in this section.

2.1 VQ technique

Gray proposed the VQ compression technique in 1984 [18]. The procedures of VQ can be separated into three phases: codebook generation, image encoding, and image decoding. The Linde-Buzo-Gray (LBG) algorithm is the classic method for generating the codebook, which contains N k-dimensional codewords $\{cw_i\}_{i=0}^{N-1}$. The first step of image encoding is dividing the image into $h \times w$ non-overlapping blocks. Every block b contains $k = h \times w$ pixels, which can be treated as a k-dimensional vector bv. Then, the encoding method finds the most similar codeword cw_j for bv in $\{cw_i\}_{i=0}^{N-1}$ by computing the Euclidean distance, where $0 \le j \le N-1$. The index j of cw_j in the codebook is kept as the compression result of bv. After all blocks of the image find their corresponding cowords, the image can be compressed into a VQ index table. **Fig. 1** shows the flow chart of the VQ encoding phase.

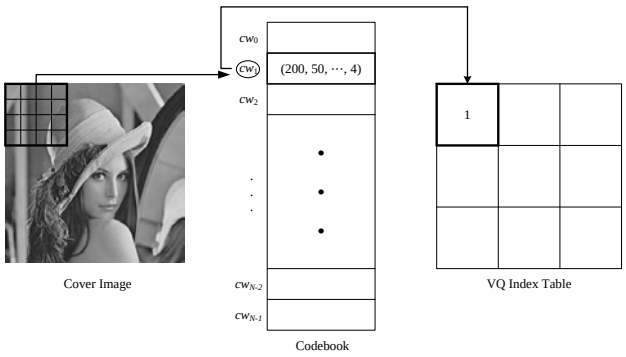


Fig. 1. VQ encoding phase

The VQ decoding phase of the receiver involves finding the corresponding codeword according to the index in the VQ index table. The image can be reconstructed by finding all corresponding codewords of the VQ index table. The flow chart of the VQ decoding phase is shown in **Fig. 2**.

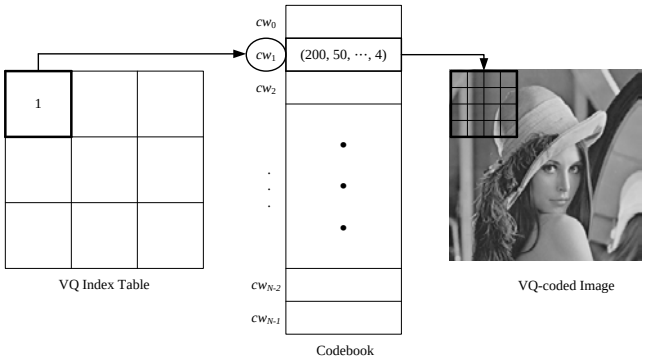


Fig. 2. VQ decoding phase

2.2 EMD Technique

Zhang and Wang proposed the EMD information hiding technique in 2006 [21]. The main concept is that the secret data are expressed in a (2*n*+1)-based counting system first, and then are embedded in *n* pixels in the cover image. The detailed procedure of data embedding is as follows. First, the pixels of the cover image are separated into several clusters, which contain *n* pixels $\{p_i\}_{i=1}^{n}$ and will be used to embed a (2*n*+1)-based secret digit *d*. Second, a function *f*() is designed to calculate a (2*n*+1)-based number *f* by using all pixels of a cluster:

$$f = f(p_1, p_2, \ldots, p_n) = \left[\sum_{i=1}^{n}(p_i \times i)\right] \bmod (2n+1). \tag{1}$$

Third, the EMD method compares the to-be-embedded secret digit *d* with the computed number *f*. If the result is $d = f$, *d* is embedded in the current pixel cluster automatically without changing any pixel's value in the cluster. Otherwise, the EMD method calculates a new value $s = (d - f) \bmod (2n+1)$. If $s \le n$, then $p_s = p_s + 1$; otherwise, $p_{2n+1-s} = p_{2n+1-s} - 1$.

2.3 PDE Based Image Inpainting Technique

This subsection presents Qin *et al.*'s PDE based image inpainting method using anisotropic heat transfer model [22], which can propagate both the structure and texture information from surrounding region into damaged region simultaneously. Qin *et al.* analogize image inpainting with a heat transfer process, let *u* be a damaged image, *Ω* be the region to be inpainted in *u*, and *∂Ω* be the boundary of *Ω*. The procedure of fixing an image is treated as propagating the information of valid pixels from the exterior to the interior of *Ω*. The authors use a heat transfer model for homogenous medium, and consider the image as a temperature field by regarding the pixel value *u(x, y)* as the temperature.

To avoid edge blurring effects, in Qin *et al.*'s model, they decompose the gray-level propagation into two orthogonal directions. As a result, a spatially variable and content-dependent coordinate system *O*-*ξη* is introduced to replace the fixed Cartesian system *O*-*xy*. Let the unit coordinate vectors in the *O*-*xy* system be *i* and *j*, then, any point in the space could be expressed by a vector *r*=*xi*+*yj*, which becomes *r*=*ξp*+*ηq* in the *O*-*ξη* system, where *ξ* and *η* are the two components in the isophote and gradient directions respectively, and *p* and *q* are the two orthogonal unit vectors:

$$p = \frac{1}{|\nabla u|}\left(\frac{\partial u}{\partial y} i - \frac{\partial u}{\partial x} j\right), q = \frac{1}{|\nabla u|}\left(\frac{\partial u}{\partial x} i - \frac{\partial u}{\partial y} j\right) \quad . \tag{2}$$

Here is the anisotropic heat transfer model in the PDE form:

$$\frac{\partial u(x,y;t)}{\partial t} = \frac{\partial^2 u(x,y;t)}{\partial \xi^2} + c^2 \frac{\partial^2 u(x,y;t)}{\partial \eta^2}, (x,y) \in \Omega \tag{3}$$

where c^2 is the propagation strength alone *q* varies spatially, and *c* is defined as following:

$$c = \sqrt{e^{-\frac{1}{k}|\nabla u(x,y;t)|}} \tag{4}$$

where *k* is a predetermined threshold to differentiate smooth and fluctuating regions. Eq.(3) can only be used for structure inpainting, the texture term *Δu(x,y;α,d,t)* can be expressed as:

$$\Delta_t u(x,y;a,d,t) = \frac{\partial^2 \Delta u(x,y;d,t)}{\partial \xi_a^{\ 2}} + c^2 \frac{\partial^2 u(x,y;t)}{\partial \eta_a^{\ 2}}, (x,y) \in \Omega \tag{5}$$

where $a \in [0,\pi]$ is the angle between the texture direction and the horizontal line, and d the scale of texture periodicity. And ξ_a and η_a correspond to the texture direction and its perpendicular direction respectively.

Let *A* and *B* are weights for structure and texture respectively, $A+B \equiv 1$ and $A, B \in [0,1]$, we get the equation for simultaneous structure and texture inpainting:

$$\frac{\partial u(x,y;t)}{\partial t} = A\Delta_s u(x,y;t) + B\Delta_t u(x,y;a,d,t), (x,y) \in \Omega, \tag{6}$$

where the structure term $\Delta_s u(x,y;t)$ denotes the right part of equal sign in Eq. (3).

3. The Proposed Scheme

This paper proposes an EMD technique and inpainting technique based progressive image-hiding scheme. The proposed method extracts the complex blocks of the secret image and compresses them using the VQ technique, where the codeword in the VQ codebook are sorted by PCA first. The compressed result is embedded in all cover images and delivered to all participants to achieve the goal of progressive recovery of the complex blocks of the secret image, while the residue of the secret image is recovered by the inpainting technique based on the reconstructed information. The more participants join the reconstruction phase, the higher the quality of the secret image they will obtain.

The detailed secret image-embedding procedure is as follows:

Step 1. Divide the secret image *I* into $\sqrt{k} \times \sqrt{k}$ sized non-overlapping blocks, where *k* is the number of dimensions of the codeword, i.e., $\{cw_i\}_{i=1}^{N}$, in VQ codebook *C*.

Step 2. Extract the complex blocks $\{B_j\}_{j=1}^{r}$ according to the variance value *d* of each block. If the variance value *d* of the current block is greater than the predefined threshold *t*, then the current block is determined to be a complex block. While finding all complex blocks, a location map $L = \{l\}_{u=1}^{\frac{H}{\sqrt{k}} \times \frac{W}{\sqrt{k}}}$ is used to indicate whether a block is complex or not, where $l \in \{0,1\}$, $l=1$ and $l=0$ indicate a complex block and a smooth block, respectively.

Step 3. Compress the *r* complex blocks into $\sqrt{r} \times \sqrt{r}$ sized VQ index table $IT = \{I_q\}_{q=1}^{r}$ by using the VQ technique, where *I* is the index value and the code words in the VQ codebook are sorted by PCA technique before the compression process.

Step 4. Choose x cover images $\{CI_v\}_{v=1}^{x}$, whose size is $\frac{H}{\sqrt{k}}\times\frac{W}{\sqrt{k}}$, to embed the VQ index table IT and the location map L. The location map L is embedded in the first two cover images, $CI_1=\{CI_1P_u\}_{u=1}^{\frac{H}{\sqrt{k}}\times\frac{W}{\sqrt{k}}}$ and $CI_2=\{CI_2P_u\}_{u=1}^{\frac{H}{\sqrt{k}}\times\frac{W}{\sqrt{k}}}$, where CI_1P_u and CI_2P_u are the pixels in cover images CI_1 and CI_2, respectively, and each pixel is expressed by 8 bits as $CIP=\{b_1b_2...b_8\}$. The embedding space of L is the last bit plane of CI_1 and CI_2. The L is embedded by modifying the last bit plane of CI_1 and CI_2 to satisfy $L=\{l\}_{u=1}^{\frac{H}{\sqrt{k}}\times\frac{W}{\sqrt{k}}}=\{CI_1P_u(b_8)\}_{u=1}^{\frac{H}{\sqrt{k}}\times\frac{W}{\sqrt{k}}}\oplus\{CI_2P_u(b_8)\}_{u=1}^{\frac{H}{\sqrt{k}}\times\frac{W}{\sqrt{k}}}$. IT is progressively embedded in every two overlapping cover images by the EMD technique. For the first two cover images, CI_1 and CI_2, first divide the codebook size N into $2n+1$ parts, which is expressed as $\{g1_x\}_{x=0}^{2n}$. Second, find the corresponding part x for index I_q, and embed it in the first 7 bits of every pixel of CI_1 and CI_2 using the EMD technique, introduced in Section 2. For example, assume $N=256$, $n=2$, $I_1=160$, and the corresponding cover pixels after embedding the location map are $CI_1P_1=32$ and $CI_2P_1=147$, then the divided five parts of the codebook are $g1_0=[0,50]$, $g1_1=[51,101]$, $g1_2=[102,152]$, $g1_3=[153,203]$, and $g1_4=[204,255]$, and $I_1=160$ belongs to $g1_3=[153,203]$, which means $x=3$. Since the decimal values of CI_1P_1 and CI_2P_1 's first seven bits are 16 and 73, according to the EMD technique and **Fig. 3**, the stego decimal values of CI_1P_1 and CI_2P_1 's first seven bits are 17 and 73 after embedding $x=3$ in them. Finally, the stego pixel pair ($CI'_1P_1=34$, $CI'_2P_1=147$) is calculated by connecting the last bit of CI_1P_1 and CI_2P_1 to the new first seven bits.

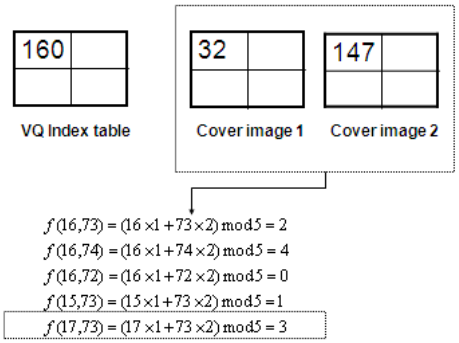


Fig. 3. The embedding example of cover images CI_1 and CI_2

For the second two cover images, $CI'_2=\{CI'_2P_u\}_{u=1}^{\frac{H}{\sqrt{k}}\times\frac{W}{\sqrt{k}}}$ and $CI_3=\{CI_3P_u\}_{u=1}^{\frac{H}{\sqrt{k}}\times\frac{W}{\sqrt{k}}}$, further divide the previous parts in $g1$ into $2n+1$ additional parts $\{g2_y\}_{y=0}^{2n}$ for each of them and

find the new corresponding part *y* for I_q. *y* is embedded in CI_2' and CI_3 also using the EMD technique. In contrast to the embedding procedure of embedding *x* in the first two cover images, *y* is embedded by only modifying the pixel value in CI_3 while keeping the pixel value in CI_2' unchanged. As to the previous example, since $I_1 = 160$ belongs to $g1_3 = [153,203]$, further divide $g1_3 = [153,203]$ into five parts, $g2_0 = [153,162]$, $g2_1 = [163,172]$, $g2_2 = [173,182]$, $g2_3 = [183,192]$, and $g2_4 = [193,203]$, and determine that $I_q = 160$ belongs to $g2_0$, which means $y = 0$. Assume that the corresponding pixel values are 147 and 230 in cover images CI_2' and CI_3, respectively; the stego pixel values are 147 and 229 after embedding $y = 0$ while keeping 147 unchanged, as shown in **Fig. 4**. The embedding procedure for the rest of the cover images is the same as the embedding procedure for CI_2' and CI_3.

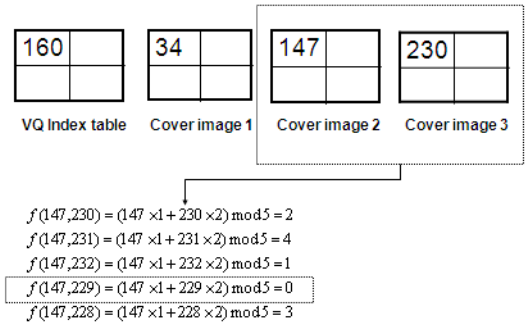


Fig. 4. The embedding example of cover images CI_2' and CI_3

At the receiver end, the participants provide their stego images, VQ codebook, *n*, and the size of the secret image $H \times W$. The decoding procedure follows the order of the stego image and the more participants cooperate, the higher the quality of the secret image they can reconstruct. The details of the secret image reconstruction process are described below.

Step 1. Extract the location map *L* of the blocks by calculating $L = \{l\}_{u=1}^{\frac{H}{\sqrt{k}} \times \frac{W}{\sqrt{k}}} = \{CI_1' P_u(b_8)\}_{u=1}^{\frac{H}{\sqrt{k}} \times \frac{W}{\sqrt{k}}} \oplus \{CI_2' P_u(b_8)\}_{u=1}^{\frac{H}{\sqrt{k}} \times \frac{W}{\sqrt{k}}}$ with stego images CI_1' and CI_2'. After this, the number of complex blocks *r* can be observed by *L*.

Step 2. Extract the first *r* pixels from CI_1' and CI_2' in order from up to down and left to right. Calculate the secret pixel value belonging to the specified part of *g*1 by using the EMD technique with the decimal values of the first seven bits from the corresponding pixels in CI_1' and CI_2'. The current reconstructed index value equals the average integer value of the part to which it belongs. Since all code words in the codebook were sorted by PCA in the secret-embedding procedure, the more closely the index values are, the more similar the blocks reconstructed from them are.

Step 3. For the rest, for every two overlapping stego images, calculate the secret index value belonging to the specified part by directly using the EMD technique with the decimal values of the corresponding pixels in them. This allows the secret pixel value to be reconstructed by the average value of the new corresponding part. For example, calculate the secret index value

belonging to the specified part of $g2$ by using the EMD technique with the decimal values of the corresponding pixels in CI'_2 and CI'_3. The new more accurate secret index value equals to the average value of the part from $g2$ to which it belongs.

As for the example of the secret image-embedding phase, the first seven bits' decimal values 17 and 73 can be calculated by the corresponding pixel values $CI'_1P_1 = 32$ and $CI'_2P_1 = 147$ from the first stego image CI'_1 and the second stego image CI'_2, respectively. The serial number 3 of the part is found by using the EMD technique with 17 and 73, which means the current secret index value belongs to $g1_3 = [153,203]$. As a result, the secret index value is recovered as 178, which equals the average integer value of $g1_3 = [153,203]$, by using CI'_1 and CI'_2. If three participants cooperate to recover the secret image, assume the corresponding pixels in CI'_2 and CI'_3 are $CI'_2P_2 = 147$ and $CI'_3P_1 = 229$, respectively. The new serial number of the part in $g2$ is calculated as $f(147,229) = (147 \times 1 + 229 \times 2) \bmod 5 = 0$, which means the current secret index value belongs to $g2_0 = [153,162]$. In addition, the more accurate value of the current secret index is recovered as 158 by computing the average integer value of $g2$, as shown in **Fig. 5**.

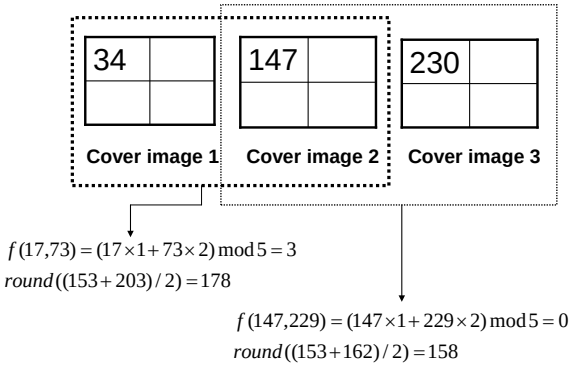


Fig. 5. The example of the secret pixel value recovered by using three stego images

After reconstructing all complex blocks' VQ index table, the complex part of the secret image can be rebuilt by decompressing the VQ index table according to the location map L. Then, the smooth blocks are recovered by using Qin et al.'s image inpainting technique [22] based on the information of the reconstructed complex blocks. Finally, the secret image can be progressively extracted with high quality.

4. Experimental Results and Analysis

In this section, the experimental results are provided to evaluate the performance of the proposed scheme. The programs for the experiments were run on a personal computer with the Windows 7 operating system. The CPU was AMD Phenom(tm) II X4 945 3.0GHz, 2G RAM. We wrote the programs in Matlab 7.6.0.324.

In 2012, He *et al.* proposed a simple yet effective blind image quality assessment [28], which outperforms conventional image quality assessment algorithms. However, in order to compare the image quality with other progressive data hiding techniques, the peak signal-to-noise ratio (*PSNR*) was adopted here to evaluate the image quality in our experimental results, which are defined as:

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} \tag{7}$$

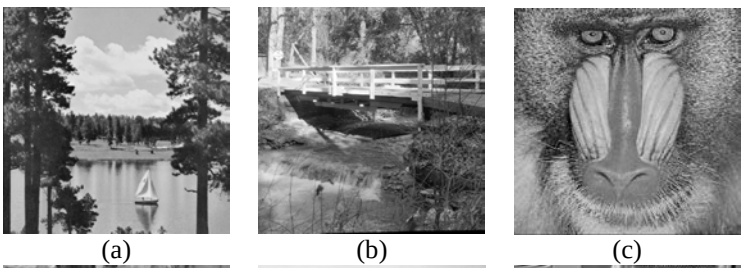
where $MSE = (1/G \times F) \sum_{i=1}^{G \times F} (X_i - X_i^{'})^2$, in which G and F are the height and width of the image, and X_i and $X_i^{'}$ are the cover image's pixel value and stego image's pixel value, respectively. The ratio r of the secret image size $H \times W$ to the shadow image size $H' \times W'$ is used to evaluate the hiding capacity of the proposed scheme, which is defined as Eq. (8).

$$r = \frac{H \times W}{H' \times W'} \tag{8}$$

The first part of our experiments was designed to highlight the differences based on the two different test secret image types, the complex image and the smooth image, when threshold t of the variance in every block to separate the complex blocks from the smooth blocks is a fixed value. In the experimental tests, the three cover images were 256 gray levels of 256×256 size, as shown in **Fig. 6**. The six secret images were 256 gray levels of 512×512 size, as shown in **Fig. 7**. The size of the VQ codebook was 1024 with 16 dimensions. The threshold t was set as $t = 3$.

(a) (b) (c)

Fig. 6. Cover images: (a) Couple, (b) Lena, and (c) F16



(a) (b) (c)

(d) (e) (f)

Fig. 7. Secret images: (a) Lake, (b) Bridge, (c) Baboon, (d) Man, (e) Goldhill, and (f) Barbara

The numbers of complex blocks and smooth blocks in the test secret images are shown in **Table 1**, which also presents the percentage of the smooth blocks among the total blocks. **Table 1** clearly indicates that Lake, Bridge, and Baboon are more complex than Man, Goldhill, and Barbara.

Table 2 records the experimental results of test images. In **Table 2**, most of the smooth secret images can achieve a bit better stego images than the complex images, since the quantity of the data embedded in the stego images related to the number of VQ indices calculated from the complex blocks.

Table 1. The numbers of complex blocks and smooth blocks in test secret images

	Total Blocks (4×4)	**Complex Blocks**	**Smooth Blocks**
Lake	16384	15139	1245 (8%)
Bridge	16384	15959	425 (3%)
Baboon	16384	14994	1390 (8%)
Man	16384	13468	2916 (18%)
Goldhill	16384	12316	4068 (25%)
Barbara	16384	12869	3515 (21%)

Table 2. The experimental results of all test images

Secret image	***PSNR* of stego image (dB)**			***PSNR* of recovered secret image by using stego image 1 and 2 (dB)**	***PSNR* of recovered secret image by using stego image 1, 2 and 3 (dB)**	**Hiding capacity (ratio *r*)**
	Stego image 1	**Stego image 2**	**Stego image 3**			
Lake	50.65	51.12	51.74	15.78	19.70	4
Bridge	50.43	50.91	51.54	15.54	19.34	4
Baboon	50.67	51.16	51.80	15.77	18.05	4
Man	51.54	51.13	52.23	15.93	19.46	4
Goldhill	51.47	52.54	51.81	15.43	20.13	4
Barbara	51.67	51.35	52.30	16.25	19.19	4

The more complex blocks in the secret image, the more data should be embedded in the stego images. All stego images' *PSNR*s are higher than 50 in **Table 2**, which guarantees high security performance of the proposed scheme because it is extremely difficult to distinguish the difference between the stego image and the cover image if the *PSNR* of the stego image is higher than 50. It can be observed that the hiding capacity (ration *r*) of the proposed scheme is 4, which means the shadow size is only 1/4 of the secret image size.

Fig. 8 and **Fig. 9** show the experimental results of hiding two representative test secret images from two groups into three cover images. Each figure presents the secret image used in the experiment, the separation result of complex blocks and smooth blocks, which are indicated by black blocks in the figure, the image quality of the three stego images and their visual effect, and the recovered secret image quality by using two stego images and three stego images, respectively.

(a) Secret Image

(b) Selected Blocks

(c) Stego Image 1 (50.43 dB)

(d) Stego Image 2 (50.91 dB)

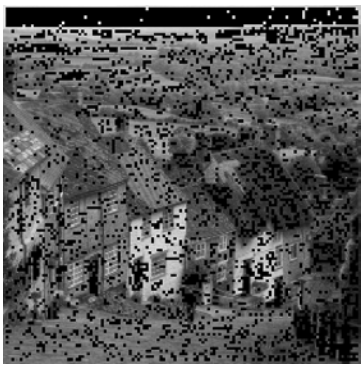
(e) Stego Image 3 (51.54 dB)

(f) Recovered Image by Stego Image 1 and 2 (15.54 dB)

(g) Recovered Image by Stego Image 1, 2, and 3 (19.34 dB)

Fig. 8. The experimental results obtained by using Bridge as secret image and using Couple, Lena, and F16 as cover images

(a) Secret Image



(b) Selected Blocks

(c) Stego Image 1 (51.47 dB)

(d) Stego Image 2 (52.54 dB)

(e) Stego Image 3 (51.81 dB)

(f) Recovered Image by Stego Image 1 and 2 (15.43 dB)

(g) Recovered Image by Stego Image 1, 2, and 3 (20.13 dB)

Fig. 9. The experimental results obtained by using Goldhill as secret image and using Couple, Lena, and F16 as cover images

Based on either **Fig. 8** and **Fig. 9** or **Table 2**, the improved image quality of the recovered secret image obtained by using three stego images demonstrates that the proposed scheme can successfully achieve progressively reconstructed secret images.

The second part of our experiments was designed to show the influence of threshold t on the performance of the proposed scheme and to compare the effectiveness of our proposed scheme with Chang *et al.*'s scheme [11]. In the experimental tests, the three cover images were 256 gray levels of 512×512 size Tiffany. The secret image was 256 gray levels of 512×512 size Barbara. The size of the VQ codebook was 1024 with 16 dimensions.

Table 3 shows the variation of *PSNR* values of stego images and recovered images when threshold t varies. It can be observed that as t increase the visual quality of stego

images also increase while PSNR of recovered images decrease. It is due to that when *t* increase, more blocks can be judged ad smooth blocks leading to fewer complex blocks for VQ to encode.

Table 3. The *PSNR* values of stego images and recovered images (dB)

Threshold	Percentage of inpainting blocks	Stego image 1	Stego image 1	Stego image 1	Recoverd secret image by using stego image 1 and 2	Recoverd secret image by using stego image 1, 2 and 3
$t = 2$	5%	58.41	56.85	57.20	16.69	20.15
$t = 2.25$	10%	58.60	56.89	57.45	16.78	20.08
$t = 2.5$	13%	58.71	57.02	57.51	16.80	20.05
$t = 2.75$	17%	58.84	57.09	57.68	16.78	19.60
$t = 3$	21%	59.05	57.23	57.91	16.21	19.03
$t = 3.25$	24%	59.12	57.28	58.03	15.94	18.09
$t = 3.5$	27%	59.24	57.38	58.21	15.12	16.91

Table 4 shows the influence of threshold *t* on the execution time of the proposed scheme. It can be observed that as the threshold *t* increase, the execution time of recovering smooth blocks by inpainting technique increases. It happens because the number of the smooth blocks increases along with *t* increases. As a result, the inpainting time was spent on recovering the smooth blocks increases as well.

Table 4. Execution time of the proposed scheme (unit: second)

Threshold	Embedding on the sender side			Recovery on the receiver side	
	VQ compression	Block judgment	Embedding	Recover complex blocks by VQ index	Recover smooth blocks by inpainting
$t = 2$	54.858813	0.699179	0.299679	0.219352	38.733764
$t = 2.25$	54.318997	0.706826	0.285548	0.212267	43.803771
$t = 2.5$	57.606361	0.698661	0.283543	0.203756	45.911831
$t = 2.75$	56.067346	0.745639	0.269640	0.198793	50.773733
$t = 3$	54.890731	0.750866	0.265199	0.188394	54.233431
$t = 3.25$	55.135923	0.750272	0.276708	0.180206	56.472835
$t = 3.5$	55.199559	0.751426	0.271201	0.171320	59.672190

Fig. 10 show the experimental results of hiding secret image Barbara into three same cover images Tiffany. It presents the secret image used in the experiment, the separation result of complex blocks and smooth blocks, which are indicated by black blocks in the figure, the image quality of the three stego images and their visual effect, and the recovered secret image quality by using two stego images and three stego images with impaiting procedure, respectively. Here, the threshold $t = 2$.

(a) Secret Image

(b) Selected Blocks

(c) Stego Image 1 (58.41 dB)

(d) Stego Image 2 (56.85 dB)

(e) Stego Image 3 (57.20 dB)

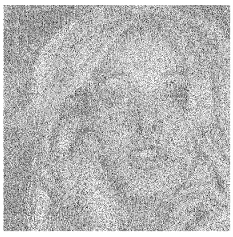
(f) Recovered Image by Stego Image 1 and 2 (16.69 dB)

(g) Recovered Image by Stego Image 1, 2, and 3 (20.15 dB)

Fig. 10. The experimental results obtained by using Barbara as secret image and using Tiffany as all cover images

In order to demenstrate the effectiveness of the proposed scheme, we compared our proposed scheme with Chang et al's scheme [11] in visual quality of the stego image, visual quality of the recovered secret image, hiding capacity and computational complexity. **Fig. 11** and **Fig. 12** show the comparison results in visual quality of the stego images and visual quality of the recovered secret images. Here the threshold $t = 2$ in out proposed scheme and the quality factor Q_f used in Chang et al.'s scheme is 1/3 [11].

(a) The proposed scheme



(b) Chang et al.'s scheme

Fig. 11. Comparison for the generated one shadow between the proposed scheme and Chang et al.'s scheme

(a) Computation result with 3 shadows by the proposed scheme

(b) Stacking result with 12 shadows by Chang et al's scheme

Fig. 12. Comparison for the restored secret images between the proposed scheme and Chang et al.'s scheme

According to the two figures, **Fig. 11** and **Fig. 12**, it is found that the proposed scheme degrades the image qualities of the shadows and the recovered secret image more slightly than Chang et al.'s scheme. The hiding capacity of the proposed scheme in the second part of the experiments is assigned as same as the hiding capacity in Chang et al's scheme to observe differece of the out put images' visual quality. However, it can be seen from Table 2, which is obtained from the first part of our experiments, since the shadow size equals the secret image size in Chang et al.'s scheme [11], the hiding capacity of our proposed scheme could achieve 4 times larger than that of Chang et al.'s scheme. This advantage makes the proposed scheme more suitable for the applications with the low bandwidth requirement. Chang et al's scheme is capable of restoring secret images with different resolutions only by stacking different quantities of shadows together, while the proposed scheme has to recover the complex blocks of the secret image by decompressing the VQ indices and recover the smooth blocks by doing inpainting procedure to restore the secret image. In other words, the computation complexity of the proposed scheme is higher than Chang et al's scheme. **Table 4** shows that the execution time of the proposed scheme is about 1 minute on both sender and receiver side, respectively.

5. Conclusion

This paper proposes a new progressive secret image recovery scheme. The proposed scheme achieves not only high hiding capacity, which is proved by the secret image being four times larger than the cover image, but also by high stego image quality, which is higher than 50 dB, as shown in the experimental results. Observation of the visual effect provided in the experimental results—that the recovered secret image achieves higher quality by using three stego images than by using two stego images—demonstrates that the proposed scheme has the function of progressively recovering the secret image. In the future work, we will focus on

improving the computation complexity of the proposed scheme.

References

[1] National Institute of Standards & Technology, "Data encryption standard (DES)," *Federal Information Processing Standards Publication*, vol. 46, January, 1977.

[2] National Institute of Standards & Technology, "Announcing the advanced encryption standard (AES)," *Federal Information Processing Standards Publication*, vol. 197, no. l, 2001.

[3] R. L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, February, 1978. Article (CrossRef Link)

[4] H. Luo, F. X. Yu, H. Chen, Z. L. Huang, H. Li and P. H. Wang, "Reversible data hiding based on block median preservation," *Information Sciences*, vol. 181, no. 2, pp. 308-328, January, 2011. Article (CrossRef Link)

[5] F. Peng, X. Li and B. Yang, "Adaptive reversible data hiding scheme based on integer transform," *Signal Processing*, vol. 92, no. 1, pp. 54-62, January, 2012. Article (CrossRef Link)

[6] C. C. Chang, K. N. Chen, C. F. Lee and L. J. Liu, "A secure fragile watermarking scheme based on chaos-and-hamming code," *Journal of Systems and Software*, vol. 84, no. 9, pp. 1462-1470, September, 2011. Article (CrossRef Link)

[7] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognition*, vol. 37, no. 3, pp. 469-474, March, 2004. Article (CrossRef Link)

[8] C. C. Chen and C. C. Chang, "LSB-based steganography using reflected gray code," *IEICE Transactions on Information and Systems*, vol. E91-D, no. 4, pp. 1110-1116, April, 2008. Article (CrossRef Link)

[9] C. H. Yang, "Inverted pattern approach to improve image quality of information hiding by LSB substitution," *Pattern Recognition*, vol. 41, no. 8, pp. 2674-2683, August, 2008. Article (CrossRef Link)

[10] A. Shamir, "How to share a secret," *Communications of the Association for Computing Machinery*, vol. 22, no. 11, pp. 612-613, November, 1979. Article(CrossRefLink)

[11] C. C. Chang, Y. P. Hsieh, and C. C. Liao, "A visual secret sharing scheme for progressively restoring secrets," *Journal of Electronic Science and Technology*, vol. 9, no. 4, pp. 325-331, December, 2011.

[12] N. Noar and A. Shamir, "Visual cryptography," *Advances in Cryptology: Eurocrypt'94*, Spring-Verlag, Berlin, Germany, pp. 1-12, 1995.

[13] W. P. Fang, J. C. Lin, "Progressive viewing and sharing of sensitive images," *Pattern Recognition and Image Analysis*, vol. 16, no. 4, pp. 632-636, 2006. Article(CrossRefLink)

[14] D. Jin, W. Q. Yan, and M. S. Kankanhalli "Progressive color visual cryptography," *Journal of Electronic Imaging*, vol. 14, no. 3, pp. 033019.1-033019.13, 2005.

[15] C. C. Thien and J. C. Lin, "An image-sharing method with user-friendly shadow images," *IEEE Transactions on Circuits and Systems*, vol. 13, no. 12, pp. 1161-1169, 2003.

[16] C. N. Yang, K. H. Yu, and R. Lukac., "User-friendly image sharing using polynomials with different primes," *International Journal of Imaging Systems and Technology*, vol. 17, no. 1, pp. 40-47, June, 2007. Article(CrossRefLink)

[17] W. P. Fang, "Friendly progressive visual secret sharing," *Pattern Recognition*, vol. 41, no. 4, pp. 1410-1414, April, 2008. Article(CrossRefLink)

[18] R. M. Gray, "Vector quantization," *IEEE Transactions on Acoustics, Speech and Signal Processing*, vol. 1, no. 2, pp. 4-29, 1984.

[19] Y. Linde, A. Buzo and R. M. Gray, "An algorithm for vector quantizer design," *IEEE Transactions on Communications*, vol. 28, no. 1, pp. 84-95, January,1980. Article(CrossRefLink)

[20] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," *IEEE Communications Letters*, vol. 10, no. 11, pp. 781-783, November, 2006. Article(CrossRefLink)

[21] C. Qin, F. Cao and X. P. Zhang, "Efficient image inpainting using adaptive edge-preserving propagation," *The Imaging Science Journal*, vol. 59, no. 4, pp. 211-218, August, 2011. Article(CrossRefLink)
[22] C. Qin, S. Z. Wang and X. P. Zhang, "Simultaneous inpainting for image structure and texture using anisotropic heat transfer model," *Multimedia Tools and Applications*, vol. 56, no. 3, pp. 469-483, 2012. Article(CrossRefLink)
[23] X. B. Gao, L. L. An, Y. Yuan, D. C. Tao and X. L. Li, "Lossless data embedding using generalized statistical quantity histogram," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 21, no. 8, pp. 1061-1069, August, 2011. Article(CrossRefLink)
[24] L. L. An, X. B. Gao, X. L. Li, D. C. Tao , C. Deng and J. Li "Robust reversible watermarking via clustering and enhanced pixel-wise masking," *IEEE Transactions on Image Processing*, vol. 21, no. 8, pp. 3598-3611, August, 2012. Article(CrossRefLink)
[25] C. C. Wu, S. J. Kao, and M. S. Hwang, "A high quality image sharing with steganography and adaptive authentication scheme," *The Journal of Systems and Software*, vol. 84, no. 12, pp. 2196-2207, December, 2011. Article(CrossRefLink)
[26] C. C. Wu, M. S. Hwang, and S. J. Kao, "A new approach to the secret image sharing with steganography and authentication," *The Imaging Science Journal*, vol. 57, no. 3, pp. 140-151, June, 2009. Article(CrossRefLink)
[27] S. F. Chiou, I. E. Liao, and M. S. Hwang, "A capacity-enhanced reversible data hiding scheme based on SMVQ," *The Imaging Science Journal*, vol. 59, no. 1, pp. 17-24, February, 2011. Article(CrossRefLink)
[28] L. H. He, D. C. Tao, X. L. Li and X. B. Gao, "Sparse representation for blind image quality assessment," in *Proc. of 2012 IEEE Conference on Computer Vision and Pattern Recognition*, Providence, Rhode Island, USA, pp. 1146-1153, June 16-21, 2012.

Zhi-Hui Wang received the BS degree in software engineering in 2004 from the North Eastern University, Shenyang, China. She received her MS degree in software engineering in 2007 and the PhD degree in software and theory of computer in 2010, both from the Dalian University of Technology, Dalian, China. Since November 2011, she has been a visiting scholar of University of Washington. Her current research interests include information hiding and image compression.

Kuo-Nan Chen received his Ph.D in Computer Science and Information Engineering from National Chung Cheng University. He is currently an engineer at ASUSTeK Computer Inc., Taiwan. His research interests include image data hiding and image processing technologies.

Chin-Chen Chang was born in Taichung, Taiwan, in 1954. He received his B.S. degree in applied mathematics in 1977 and the M.S. degree in computer and decision sciences in 1979, both from the National Tsing Hua University, Hsinchu, Taiwan. He received his Ph.D in computer engineering in 1982 from the National Chiao Tung University, Hsinchu, Taiwan. During the academic years of 1980-1983, he was on the faculty of the Department of Computer Engineering at the National Chiao Tung University. From 1983-1989, he was on the faculty of the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. From August 1989 to July 1992, he was the head of, and a professor in, the Institute of Computer Science and Information Engineering at the National Chung Cheng University, Chiayi, Taiwan. From August 1992 to July 1995, he was the dean of the college of Engineering at the same university. From August 1995 to October 1997, he was the provost at the National Chung Cheng University. From September 1996 to October 1997, Dr. Chang was the Acting President at the National Chung Cheng University. From July 1998 to June 2000, he was the director of Advisory Office of the Ministry of Education of the R.O.C. From 2002 to 2005, he was a Chair Professor of National Chung Cheng University. Since February 2005, he has been a Chair Professor of Feng Chia University. In addition, he has served as a consultant to several research institutes and government departments. His current research interests include database design, computer cryptography, image compression and data structures. He is a fellow of the IEEE.

Chuan Qin received the B.S. and M.S. degrees in electronic engineering from Hefei University of Technology, Anhui, China, in 2002 and 2005, respectively, and the Ph.D. degree in signal and information processing from Shanghai University, Shanghai, China, in 2008. Since 2008, he has been with the faculty of the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, where he is currently a Lecturer. He also has been with Feng Chia University at Taiwan as a Postdoctoral Researcher from July 2010 to June 2012. His research interests include image processing and multimedia security.