Inter-Secured Joint Image Compression with Encryption Purpose Based on Fractal Mating Coding

Hsuan T. Chang, **Member, SPIE,** and Chung C. Lin

Photonics and Information Laboratory
Department of Electrical Engineering
National Yunlin University of Science and Technology
Douliu Yunlin, 64045 Taiwan ROC

Abstract

In this study, a pioneer secure coding concept for pairwise images is revealed and implemented by the use of the proposed fractal mating coding scheme, in which the domain pools consist of the domain blocks selected from the pairwise images to explore both the intra- and inter-image similarities. In addition to the pairwise relation, the mating ratios denoting the percentages of the domain blocks selected from both images are utilized. Further encryption can be achieved by the use of block mean permutation and mating of the fractal codes. The security level is high because that the jointly coded images cannot be correctly reconstructed without all the required information. The computer experiments show that the coding performance can be greatly improved from conventional fractal coding schemes and the inter-secured purpose for pairwise images is successfully achieved.

Keywords: fractal, mating ratio, secure coding, joint image compression, image encryption.

1 Introduction

Recently the methods of data security/protection for electronic commerce or the distribution over Internet have been drastically developed. The techniques for image and video content protection are usually achieved by watermarking,[1−4] secure image coding/encryption,[5,6] and/or image secret sharing schemes.[7] By using watermarking schemes one can claim the data authority via the insertion of visible or invisible marks. Image encryption schemes[8−12] shuffle the original content into noise-like data, which cannot be correctly reconstructed without the key used in the encryption stage. On the other hand, modern image secret sharing schemes[13−19] are based on visual cryptography[20,21] and human visual system characteristics.[22] Since a secret image can be recovered without any computation, the disadvantage of complex computation required in traditional cryptography can be released.

In general, the encryption and watermarking techniques are solely utilized to secure images or video clips. However, most image and video data are compressed to save the bandwidth and amount for transmission and storage purposes, respectively. Therefore, many approaches,[23–27] which combine both the compression and encryption techniques, were proposed such that the compressed data can be transmitted or stored with more efficient and highly-secured ways. For example, the modifications of discrete-cosine-transform (DCT) and wavelet coefficients in the JPEG[28] and JPEG-2000[29] codecs, respectively, constitute a popular choice in various secure coding schemes. Without properly decryption of the transform coefficients, the compressed images cannot be correctly reconstructed. On the other hand, selective or partial encryption solutions[30,31] for the compressed data were also proposed. These solutions reduce the key size in the encryption system and the massive computational complexity required in overall encryption. The integrated compression and encryption systems for video, audio, and multimedia also have been investigated for content protection purposes.[1,24,25] Obviously, the research on joint compression and encryption/watermarking has been received a great attention and has become a significant issue in current multimedia applications.

Images are considered as independent and separate data sources in conventional still-image coding framework. For example, an image is transformed to the frequency domain and then the spectral coefficients are quantized and recorded as the compressed data in current coding standards such as JPEG and JPEG-2000. Then the encryption/security schemes are applied on the image/video data. In addition to applying the encryption/security schemes on the independent image data, here a novel technique, which implements inter-secured joint image compression together with image encryption using an adapted fractal coding technique, is proposed. The major difference between the proposed and above-mentioned work is that both the encoding and decoding processes of selected pairwise images are no longer independent. Instead of using conventional encryption/security schemes to protect images, two jointly coded images can protect each other without using considerable extra information. For a currently encoded image, this can be achieved by accessing the content in the other image during the encoding process.

In this study, the *fractal mating coding* (FMC) scheme is proposed to increase the diversity of the domain pool and to benefit the security property. In addition to extracting the self-similarity in a single image in conventional fractal coding techniques, the inter-similarity between the selected pairwise images is also explored. The key idea is to construct the domain pools using the domain blocks selected from both the pairwise images. Consequently, the best matching domain block of the range block in the current image may be found in the other image. In decoding, two images must be iteratively reconstructed with an interlacing order. Otherwise, the self-decoded images will be seriously distorted. For the images with strong inter-similarities in block-based perspective, the proposed FMC scheme can improve the rate-distortion performance. Even two dissimilar images are jointly coded, the rate-distortion performance can be preserved as well because the mating ratio can be selected as small as possible.

The proposed FMC scheme also provides secured transmission/storage for the jointly coded images. Without the pairwise relation, images cannot be totally retrieved because the range blocks coded by the domain blocks located in the other image cannot be correctly reconstructed. Furthermore, two encryption schemes are used to protect the coded result. First, a secret key is used to scramble the block means in the encoding stage. The block mean permutation can be obtained by performing exclusive OR (XOR) operations on a secret key and the pixel addresses. Second, the fractal codes of range blocks in both images can be exchanged by the use of a mating table. Only a noise-like image is reconstructed without the correct key and the mating table.

The rest of this paper is organized as follows: Section 2 briefly reviews the fractal coding techniques. The proposed FMC scheme and related security aspects are presented in Section 3. The simulation results are given in Section 4. Section 5 deals with the discussions on potential future work. Conclusions are finally drawn in Section 6.

2 Fractal Coding Techniques

Fractal image coding techniques have received a great attention more than ten years.[31] The idea is that the natural images are usually with self-similarity, which is a kind of redundancy and can be used in the image coding framework. In 1992, Jacquin proposed the fractal block coding (FBC) technique that can automatically encode an image by the use of the partitioned iterated function system.[32] In this conventional scheme, an image is partitioned into nonoverlapping range blocks. The larger domain blocks are selected from the same image and can overlap. A grayscale image is encoded by mapping the domain block D to the range block R using the contractive affine transformation (CAT) defined as[32]

$$\hat{R} = \iota\{\alpha \cdot (S \circ D) + \triangle g\}, \tag{1}$$

where $S\circ$ represents the contraction operation that downsizes the domain block to the size of range block. Then the parameters (called the fractal code) describing the CAT that has the minimum matching error between the original range block R and transformed range block $\hat{R}$ are transmitted or stored. The fractal code consists of the contrast scaling α, luminance shift $\triangle g$ or the block mean (the average pixel value of the range block) μ_R,[33] isometry ι, and the position P_D of the best-match domain block in the domain pool. Note that the uniform range blocks are directly coded by their mean values. For the range block that is not coded by the mean value, all of the N domain blocks $D_N^{(\text{Intra})}$ are sought to find the best affine-transformed domain block $\hat{R}$ that is the most closest to it. That is,

$$\underset{\forall\ \iota,\alpha,\triangle g, D\in D_N^{(\text{Intra})}}{\text{minimize}} ||R - \hat{R}||, \tag{2}$$

where the symbol $D_N^{(\text{Intra})}$ denotes that the domain blocks are selected the image itself and $||\cdot||$ denotes the L_2 norm. In decoding, the CATs denoted by fractal codes are applied to an arbitrary initial image and then the decoded image is repeatedly reconstructed by the use of CAT on the fractal codes until the iterated image converges.

Conventional FBC techniques search the similarity between the range and domain blocks in an image, which is then coded independently. However, the high similarity between the domain and range blocks in an image does not always exist. That is, certain best-matching domain blocks may still have large distortion with the range blocks. Although increasing the number of the domain blocks can reduce the distortion, the bit rate increases accordingly. On the other hand, the domain blocks selected from the same image may have some redundancy among them. Thus it is not easy to construct an efficient domain pool. As shown in previous literatures for fractal coding techniques,[33,35–39] some design methods are summarized as follows:
(1) Full search – select all the possible domain blocks in the whole image;

(2) Neighboring search – select the domain blocks locating at the neighboring region of the current range block;
(3) Subsampling search – the domain blocks that are uniformly subsampled from the whole image;
(4) Others – hierarchical (pyramid or quadratic) searching, block averaging, block-mean image, combinations of two or more methods.
For the methods above, the domain blocks are all selected from the coding image itself and thus only the intra-image similarity is explored.

In conventional FBC techniques, the coding performance of an image reflects the corresponding intra-image similarity. For images with high intra-image similarity, the coding performance must be better than that of the complex images with low intra-image similarity. In addition to the similarity that can be found in the image itself, there might exist other similarity between two different images. That is, the similar contents in two images can be regarded as the redundancy if two images are jointly considered for compression. Therefore, it is desirable to introduce the inter-image similarity for the images with low intra-image similarity while searching the similarity between the domain and range blocks in FBC techniques such that the coding performance can be improved. Based on the above idea, we here propose the FMC scheme in which the inter-image similarity can be explored by selecting the domain blocks from the other jointly coded image.

3 Fractal Mating Coding (FMC) Scheme

3.1 Inter-image Similarity

Conventional still-image coding techniques usually provide only the function for single-image compression. To the best of our knowledge, there is no method proposed to jointly compress two or more images in current image-coding standards. In conventional FBC schemes, only the self-similarity in an image is explored to reduce the redundancy in the image. Let N_A domain blocks D selected only from the currently coding image A be denoted as $D_{N_A}^{(\mathrm{intra})}$. That is, $D \in D_{N_A}^{(\mathrm{intra})}$ in Eq. (1). However, the self-similarity in some images, especially for certain complicated images, is not obvious.[40] The contraction operation that averages four neighboring pixels in a domain block to obtain one pixel in the coded range blocks is equivalent to low-pass filtering, which can blur the image. That is, the coding performance of a complicated/texture image is much lower than that of a simple image. Therefore, the introduction of higher inter-image similarity from another image would be helpful in improving the coding performance of a complicated image. To utilize the inter-image similarity in the image coding framework, however, at least two images must be jointly considered and coded together. This introduces the requirement of transmitting multiple images in the proposed FMC scheme. Compared with conventional FBC techniques, larger storage/memory requirement and higher computation complexity are the limitations since here two images are jointly considered rather than only one.

3.2 Domain Pool Construction and Mating Ratio

Consider to encode the image A in the proposed FMC scheme. The inter-image similarity is explored via selecting N_B domain blocks $D_{N_B}^{(\text{inter})}$ from the other jointly coded image B. The domain blocks selected from the two different images usually can provide larger diversity than that only from a single image. That is, the domain pool $\mathcal{D}$ is composed of the domain blocks from two images, i.e., $\mathcal{D} = \{D_{N_A}^{(\text{intra})}, D_{N_B}^{(\text{inter})}\}$. Therefore, the FMC scheme can explore both the intra- and inter-image similarities such that better coding performance can be expected.

Figures 1(a) and 1(b) show the methods to select the domain blocks in the proposed FMC scheme. To construct the domain pool for the image A, the domain blocks are selected from both the jointly coded images A and B. That is, the construction of the domain pool for the image A can be divided into two parts: First, N_A domain blocks $D_{N_A}^{(\text{intra})}$ are selected from the image A itself. Here the N_A neighboring blocks are covered in the nearest neighboring region ($L_x \times L_y$) of the current range block, and can be determined by[39]

$$L_x = L_y = \lceil \sqrt{N_A} \rceil, \tag{3}$$

where the symbol '$\lceil \cdot \rceil$' denotes the ceiling operation for the real number in it. Next, the other N_B domain blocks $D_{N_B}^{(\text{inter})}$ are selected by uniformly subsampling (with the sampling periods T_x and T_y pixels in horizontal and vertical directions, respectively) the other image B. Here the sampling periods T_x and T_y can be determined by[37]

$$T_x = T_y = \lfloor \frac{M}{\sqrt{N_B}} \rfloor, \tag{4}$$

where the symbol '$\lfloor \cdot \rfloor$' denotes the floor operation for the real number in it. For a given size N of the domain pool,

$$N = N_A + N_B. \tag{5}$$

The mating ratio r_{AB} of the image A with respect to the image B is defined as

$$r_{AB} = \frac{N_B}{N_A + N_B}, \tag{6}$$

which is within the range $[0, 1]$. The proposed FMC scheme is equivalent to the conventional FBC schemes if $N_B = 0$. On the other hand, the domain blocks can be totally selected from the other image B for the case $N_A = 0$. A similar idea of building the domain pool from another image was proposed by Leposy et. al.,[41] in which the codebook used in vector quantization (VQ)[42] of images can be seen as the domain pool in conventional FBC schemes. However, the images are still independently coded.

3.3 Encoding

Figure 2(a) shows the block diagram of the encoder in the proposed FMC scheme. In the input of the encoding stage, two different images A and B are jointly considered. Basically, only the construction of the domain pool is different from that in conventional FBC schemes. To obtain better coding performance of two jointly coded images, several mating ratios (that is, different values of r_{AB} and r_{BA}) are tested. Although testing several possible mating ratios slows down the encoding process, the decoding speed remains the same. Note that the mating ratio will also be transmitted to the decoder. However, only three bits are required to denote the mating ratio and thus the overhead is negligible.

Once the domain pool has been determined, the subsequent procedures are similar to that in conventional FBC schemes. The only difference is that the position P_D of the best-matching transformed domain block now is determined by

$$\underset{\forall\ \iota,\alpha,\triangle g,D\in\mathcal{D}}{\text{minimize}} ||R-\hat{R}||. \tag{7}$$

Note that the mean and variance of each range block should be calculated at first. If the variance of the range block is less than a threshold value E_{th}, the range block is coded by its mean value. Otherwise, the range block is coded by the CAT and denoted as the fractal code. A header is attached for each range block to specify the coding status of the range block. After encoding the image A, the similar procedures are applied to the other image B. The block mean permutation by use of a secret key and the mating of fractal codes of pairwise images will be described in Subsection 3.5.

An image does not always have strong self-similarity. Therefore, the best match domain block for the range block in the image A might be sought from the other image B. Consequently, the image A or B cannot be decoded only by the use of its own fractal codes.

3.4 Decoding

Figure 2(b) shows the block diagram of the decoding process, in which the reconstruction of the pairwise images should be proceed together. First of all, the decoder should acquire the pairwise relation that which two images are jointly encoded. The mating ratios r_{AB} and r_{BA} are used to determine the numbers of the domain blocks selected in the pairwise images. Initially, let $k=0$ and the iterated images be denoted as A_k and B_k. Then two initial images A_0 and B_0 are constructed by their block means. In decoding the image A_1, the process is similar to that in the conventional FBC schemes except that the domain blocks are selected from the images A_0 and B_0. Next, the other image B_1 can be determined from the images A_1 and B_0. In the k^{th} iteration, the domain pool of the iterated image A_k is constructed by the domain blocks selected from the $(k-1)^{\text{th}}$ iterated images A_{k-1} and B_{k-1}. Thus two images A_k and B_k are iteratively reconstructed in an interlacing order. If only the image A is decoded, the domain blocks located in the image B cannot be employed to decode the range blocks. This provides a secured decoding process, in which only the jointly encoded images can be correctly decoded.

3.5 Compressed Domain Encryption

In conventional FBC schemes, the range blocks in an image are classified as two types: (1) the uniform blocks that are coded by their block means; (2) the other blocks that are coded by the fractal code representing the CATs between the domain and range blocks. Generally the number of blocks belonging to the first type is larger than that of the second type, especially when the block size is small (for example, 4 × 4). In the proposed FMC scheme, the range blocks of the second type will be seriously distorted if only one image is decoded independently. However, it is easy to recognize the decoded image because the uniform range blocks are correctly reconstructed by the corresponding mean values. To make the self-decoded image be furthermore encrypted, here two encryption schemes are utilized.

The block mean permutation and mating the fractal code are integrated in the proposed FMC scheme. Figures 3(a) and 3(b) show the block diagrams of the proopsed encryption and decryption processes in the encoder and decoder, respectively. First, an XOR-based encryption method is applied to perform the permutation of block means in the proposed FMC scheme. Let $\mu_R(m, n)$ denote the mean value of the $(m, n)^{\text{th}}$ range block. Given the original fractal codes τ_A and τ_B, the mean values of all range blocks are exchanged by applying XOR operations on the secret keys s_A, s_B, respectively, and their addresses, m and n. That is,

$$\mu_R(m', n') = \mu_R(m \oplus s, n \oplus s), \tag{8}$$

where the symbol '$\oplus$' denotes the XOR operation. Therefore, the mean value $\mu_R(m, n)$ of the range block $R(m, n)$ becomes to $\mu_R(m', n')$ of another range block $R(m', n')$. Without the secret key, the decoded result can hardly be recognized because the mean values have been scrambled. To correctly reconstruct the range block $R(m, n)$ in the decoding stage, the correct addresses of the original mean value $\mu_R(m, n)$ must be retrieved by performing the XOR operation using the same secret key. That is,

$$\mu_R(m' \oplus s, n' \oplus s) = \mu_R(m, n). \tag{9}$$

Note that the images A and B can use different secret keys s_A and s_B during the block mean permutation. In addition to the pairwised information and mating ratios (r_{AB} and r_{BA}), both the secret keys (s_A and s_B) can also contribute to the security in the proposed FMC scheme.

Since the lengths of secret keys may be not enough to resist brute-force attacks, here the second encryption scheme, which applies the similar idea of the domain pool design in the compression domain, is proposed. The fractal codes τ_A and τ_B of the range blocks in two jointly coded images A and B are exchanged according to a mating table M_{AB}, which is an array of binary digits and whose size is the same as the number of range blocks. In the mating table, the binary digit '1' denotes that the fractal codes of two range blocks are exchanged, while the digit '0' means not. After applying the mating table on two original fractal codes τ_A and τ_B, the encrypted fractal codes $\hat{\tau}_A$ and $\hat{\tau}_B$ are obtained as the final compressed data for images A and B. The mathematical expressions for fractal code encryption and decryption using the mating table can be expressed as

$$[\tau_A, \tau_B] \oslash [M_{AB}] = [\hat{\tau}_A, \hat{\tau}_B] \tag{10}$$

and

$$[\hat{\tau}_A, \hat{\tau}_B] \oslash [M_{AB}] = [\tau_A, \tau_B], \tag{11}$$

respectively, where the symbol '$\oslash$' denotes the operation of exchanging the fractal codes of two corresponding blocks if the entry value in the matrix M_{AB} is unity. The binary digits in the mating table can be randomly generated and its size is large enough to prevent the brute-force attack. For example, the size of the mating table is 64×64 when a 512×512 image is partitioned into the range blocks of size 8×8. In the decoder shown in Fig. 3(b), the encrypted fractal codes $\hat{\tau}_A$ and $\hat{\tau}_B$ must be correctly decrypted with the same secret keys and mating table.

3.6 Security Level

In the proposed FMC scheme, only seriously distorted images are obtained if the two jointly encoded images are independently decoded. Therefore, the proposed FMC scheme can be considered as a joint coding scheme with the encryption purpose for multiple images. The security level is high because it is hard to guess that which pairwise images are jointly coded. Consider the applications for image databases. All the information below are required for correctly decoding the pairwise images: (1) the specific decoder based on the proposed FMC scheme; (2) the pairwise relation (key_1); Here the possible combinations depend on the number of images in the database. (3) the mating ratio (key_2), the key used for mean permutation (key_3), and the mating table (key_4) of both images. The data amount in the items (2) and (3) is small and thus can be delivered through a secured channel or further encrypted for the Internet transmission. Assume that an unauthorized user owns the specific decoder and the encrypted fractal codes of images. Let the number of images in the database be 1024, the levels of mating ratio be 5, the key used for mean permutation be 8-bit long, and the size of mating table be 64×64. To successfully decrypt the jointly coded pairwise images, the number of possible combinations for the keys ($key_1 \sim key_4$) will be $1024 \times 5 \times 2^8 \times 2^{64\times 64} > 2^{4116}$, which should be large enough from the unauthorized user's brute-force attack.

4 Experimental Results

In the computer simulation, two 512×512 images (Lena and Peppers) with the eight-bit grayscale resolution are used to test the proposed FMC scheme. The coding performance of the decoded image is evaluated by the peak signal-to-noise ratio (PSNR) and bit rate. An image is partitioned into range blocks of a single size, either 8×8 or 4×4; or an image is partitioned into two-level block sizes: 8×8 and 4×4. The PSNR of the decoded image is defined as

$$\text{PSNR} = 10 \log_{10} \frac{255^2 \cdot 512^2}{64 \sum_{i=1}^{N_8} \text{MSE}(R_{8_i}, \hat{R}_{8_i}) + 16 \sum_{i=1}^{N_4} \text{MSE}(R_{4_i}, \hat{R}_{4_i})} \quad \text{dB}, \tag{12}$$

where N_8 and N_4 are the total numbers of the 8×8 range block R_8 and the 4×4 range block R_4, respectively. The distortion between the original and coded range blocks is represented by the mean-squared error (MSE) measurement defined as

$$\text{MSE}(R, \hat{R}) = \frac{1}{m^2} \sum_{0<i,j\leq m} (R_{i,j} - \hat{R}_{i,j})^2, \tag{13}$$

where $m \times m$ is the block size and $R_{i,j}$ and $\hat{R}_{i,j}$ denote the grayscale values of the $(i,j)^{\text{th}}$ pixels in the original range block R and the coded range block $\hat{R}$, respectively. The variance threshold values $E_{\text{th}} = 25$ is used for both the 8×8 and 4×4 range blocks. The number N of domain blocks in the domain pool is 256. The bit rate calculation for different partitions can be found in our previous work.[38]

For an image partitioned into 8×8 or 4×4 range blocks, the block mean and variance are calculated. If the block variance is less than the threshold value, the range block is coded by its mean value. Otherwise, the range block is coded by the use of CAT. Tables 1 and 2 show the rate-PSNR comparisons of the proposed FMC method for the Lena and Peppers images under different mating ratios. Five mating ratios $\{r = 0, 0.25, 0.5, 0.75, 1.0\}$ are considered here. That is, the combinations (N_A, N_B) of the domain blocks selected from two images are $\{(256, 0), (192, 64), (128, 128), (64, 192), (0, 256)\}$. Table 1 shows that the case of 8×8 range blocks, the PSNR can be improved by 1.11 dB in the case $r = 0.75$ for the Lena image. On the other hand, the PSNR has been improved by 0.60 dB in the case $r = 0.75$ for the Peppers image. Table 2 shows that for the case of 4×4 range blocks, the PSNR can be improved by 0.74 dB in the case $r = 0.5$ for the Lena image. However, the PSNR has been improved only by 0.11 dB in the case $r = 0.25$ for the Peppers image. The PSNR decreases as the mating ratio r is greater than 0.5.

Consider the cases of two-level range block sizes. The number N of domain blocks in both the parent and child levels is also 256. The conditions that the parent range block is partitioned into four child range blocks can refer to our previous work.[37,43] Table 3 shows the rate-PSNR performance of two test images. In the cases of the mating ratios $r = 0.5$ for the Lena image and $r = 0.75$ for the Peppers image, the maximum PSNRs and minimum bit rates are obtained.

Tables 4 and 5 show the best coding results of applying the proposed FMC scheme on each pair of six images using the single and two-level block sizes, respectively. The PSNR values shown in the bold face in the diagonal are obtained from the conventional FBC schemes. The other PSNR values shown in the bold face are the highest values among all possible combinations of pairwise images and mating ratios. As shown in both tables, all the PSNR values are greatly improved for both the cases of the single and two-level block sizes. The inter-image similarities in the test images are different in both cases. For example, the best coding performance of the F-16 image occurs at the inter-image mating coding ($r = 1$) with the Peppers image under the case of single block size. For the case of two-level block sizes, however, the best coding performance occurs at the inter-image mating coding ($r = 0.75$) with the Building image. As shown in Tables 1–3, the performance depends on not only the range block size but also the definition of domain pools in both images. The size of the domain pool and the methods for domain block selection under different mating ratios in the other image are different. Tables 4 and 5 also show that, for a given image, the best mating ratios under different block sizes are also different. All the results shown in the tables are based on the domain pool of size 256. The best mating ratio could also change when different sizes (for example, 128 or 512) of the domain pools are used. The best mating ratios will be different when a different size 128 is used for the domain pools. Moreover, there are also many combinations for the parent and child domain pools in the case of two-level block sizes. Therefore, it is difficult to develop the theory for the issue of how to choose the optimal mating ratio in the proposed FMC scheme. For some special cases, however, when the two jointly coded images are quite different, the mating ratio should be much smaller than one.

In the proposed FMC scheme, both the jointly-encoded images must be decoded together. Consider the jointly coded Lena and Peppers images whose range blocks are of size 8×8. Figures 4(a)–4(f) show that the two iterated images are jointly reconstructed at the first, second, and thirteenth iterations. Both images are successfully reconstructed. However, consider the case of independently decoded image without the pairwise information. Figures 5(a) and 5(b) show the reconstructed images that are self-decoded by the use of their own fractal codes only. For the range blocks whose domain blocks are selected from the other image, they cannot be correctly reconstructed. These blocks are seriously distorted and the reconstructed images cannot be displayed with good quality. However, these distorted images are still recognizable. To further make the decoded images shown in Figs. 5(a) and 5(b) unrecognizable, the block mean permutation described in Section 2.3 is employed. Figures 6(a) and 6(b) show that the corresponding decoded images are noise-like when a secret key $s = 21$ is employed in the XOR operations. Obviously, the decoded images are very different from the original ones and thus cannot be recognized.

Consider only the effects of fractal codes encryption via the mating coding table in the encoder. Here three mating tables with different numbers of the randomly generated binary digit '1': 2565, 2050, and 1594, are used. That is, fractal codes of 62.6%, 50.0%, and 38.9% range blocks are exchanged. Figures 7(a)–7(c) show the corresponding decoding results when the mating tables are not used in the decoding stage. Consider the Lena image. More the fractal codes are exchanged, more the decoded results are similar to the Peppers image. Obviously, the decoded results are recognizable and not enough secured for image encryption purpose. To obtain a higher security level, both the block mean permutation and mating of fractal codes are utilized. Figures 8(a) and 8(b) show the incorrect decoding results when two encryption schemes are combined. Both decoded images are random enough and cannot be recognized. The decoded images can be correctly reconstructed only when all of the secret keys, mating ratios, pairwise information of both images, and mating table are correct. Since the number of possible combination of two keys is huge, the proposed FMC scheme can provide high security to protect the jointly coded images.

5 Discussions on Future Work

Recently, fractal-based watermarking methods have been proposed for image protection.[44,45] However, the embedding of a watermark usually degrades the image quality. The proposed FMC scheme provides an alternative to protect the image in the compression domain, which is more practical because images are stored or transmitted with the compressed form. Consider a set of images or an image database. Let an image be selected as the key image. All the other images can be jointly coded with the key image based on the proposed FMC scheme. Thus the compressed images are protected by the key image because they cannot be correctly decoded without the information of the secret image. The proposed FMC scheme shows a promising application for securing storage and distribution of the coded images.

As shown in the simulation results, the coding performance depends on the mating ratio and the selection of pairwise images. Given a set of images, all the possible mating ratios and selections of the pairwise images can be tested to find the optimal one. However, it requires massive computation and seems unrealistic in practical applications. In addition to the determination of the optimal mating ratio, it is also desirable to measure the inter-image similarity between every two images and then to select the pairwise images with the highest similarity as the input of the proposed FMC scheme.

Since the FBC technique is also called the self-VQ of images,[46] a possible approach to measure the intra and inter-image similarities based on VQ techniques of images could be a potential research topic. For example, the intra-image similarity can be measured by the coding performance determined by applying the original VQ on the image. The mean-removed blocks can be used as the training vectors in VQ and then the representative codewords (i.e., codebook) can be determined. For the image coded by the codebook generated from using the same image as the training image, higher coding performance corresponds to higher intra-image similarity. On the other hand, for the image coded by the codebook generated from using another image as the training image, higher coding performance corresponds to higher inter-image similarity. Therefore, the intra- and inter-image similarities can be estimated.

More than two images can be processed to extend the capability of the proposed FMC scheme. An intuitive and useful usage of the extended FMC scheme is the application on color image compression. Three spectral (R, G, B) components of a color image are expected to be with high inter-image similarities because strong local similarities usually exist among the three monochrome images. The selection of domain blocks from three images shall be different from the current FMC scheme. For each monochrome image, two mating ratios will be used to describe the domain blocks selection in three images. If the three monochrome images are jointly coded by the use of the proposed FMC scheme, the coding performance higher than that obtained by the use of independently coding each monochrome image based on conventional FBC scheme can be expected.

Finally, other image coding techniques can be considered to implement the aspect of the proposed inter-secured pairwise image compression with encryption. For example, the inter-image similarities can be sought by examining the DCT and wavelet coefficients between pairwise images in JPEG and JPEG-2000 standards, respectively. How to efficiently search for the inter-image similarity between the pairwise image will be a critical issue in applying the proposed method to other coding techniques.

6 Conclusion

In this study, the inter-secured pairwise image compression with encryption purpose is implemented by the proposed FMC scheme, which explores not only the intra- but also the inter-image similarities. The domain blocks selected from both the jointly coded images can construct the domain pool more efficiently. In decoding, the self-decoding image will be seriously distorted without the coding and encryption information of the jointly coded images. The proposed FMC scheme not only enhances the coding performance of conventional FBC techniques, but also provides the security that the pairwise relation, mating ratios, secret keys for block-mean permutation, and mating table of fractal codes can successfully protect the images from illegal users. Finally, the potential future work for the proposed FMC method is discussed.

Acknowledgment

The authors would like to thank the National Science Council of the Republic of China, Taiwan for financially supporting this research under Contract No. NSC 95-2221-E-224-070-MY2. On the other hand, the valuable comments from anonymous reviewers, which significantly improved this paper quality, are greatly appreciated.

References

[1] E.T. Lin, A.M. Eskicioglu, R.L. Lagendijk, and E.J. Delp, “Advances in digital video content protection,” *Proc. IEEE*, **93**(1), 171–183 (2005)

[2] C.I. Podilchuk and E.J. Delp, "Digital watermarking: algorithms and application," *IEEE Signal Processing Magazine*, **18**(4), 33–46 (2001)

[3] I.J. Cox, J. Kilian, F.T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. on Image Processing,* **6**(12), 1673–1687 (1997)

[4] C.-T. Hsu and J.-L. Wu, "Hidden digital watermarks in images," *IEEE Trans. on Image Processing*, **8**(1), 58–68 (1999)

[5] P.P. Dang and P.M.Chau, "Image encryption for secure Internet multimedia applications," *IEEE Trans. on Consumer Electronics*, **46**(3), 395–403 (2000)

[6] J.-C. Yeo and J.-I. Guo, "Efficient hierarchical chaotic image encryption algorithm and its VLSI realisation," *IEE Proc.- Vision, Image and Signal Processing*, **147**(2), 167–175 (2000)

[7] N. Naor and A. Shamir, "Visual Cryptography," *Advances in Cryptography: Eurocrypt'94, Lecture Notes in Computer Science*, **950**, pp. 1–12 (1995)

[8] A. Sinha and K. Singh, "Image encryption by using fractional Fourier transform and jigsaw transform in image bit planes," *Optical Engineering*, **44**(5), 057001 (2005)

[9] K. Martin, R. Lukac, and K.N. Plataniotis, "Efficient encryption of wavelet-based coded color images," *Pattern Recognition*, **38**(7), 1111–1115 (2005)

[10] R. Lukac and K.N. Plataniotis, "A cost-effective encryption scheme for color images," *Real-Time Imaging*, Special Issue on Multi-Dimensional Image Processing, **11**(5–6), 454–464 (2005)

[11] S. Imaizumi, G. Watanabe, M. Fujiyoshi, and H. Kiya, "Generalized hierarchical encryption of JPEG 2000 codestreams for access control," *Proc. IEEE International Conference on Image Processing*, **2**, pp. 1094–1097 (2005)

[12] S. Lian, J. Sun, D. Zhang, and Z. Wang, "A selective image encryption scheme based on JPEG2000 codec," *Lecture Notes in Computer Science*, **3332**, 65–72 (2004)

[13] R. Lukac and K.N. Plataniotis, "Bit-level based secret sharing for image encryption," *Pattern Recognition*, **38**(5), 767–772 (2005)

[14] H. Guo and N.D. Georganas, "A novel approach to digital image watermarking based on a generalized secret sharing schemes," *Multimedia Systems*, **9**, 249–260 (2003)

[15] R. Lukac and K.N. Plataniotis, "Digital image indexing using secret sharing schemes: A unified framework for single-sensor consumer electronics," *IEEE Trans. on Consumer Electronics*, **51**(3), 908–916 (2005)

[16] S. Sudharsan, "Shared key encryption of JPEG color images," *IEEE Trans. on Consumer Electronics*, **51**(4), 1204–1211 (2005)

[17] C.C. Lin and W.H. Tsai, "Secret image sharing with capability of share data reduction," *Optical Engineering*, **42**(8), 2340–2345 (2005)

[18] R. Lukac and K.N. Plataniotis, “Colour image secret sharing,” *IEE Electronics Letters*, **40**(9), 529–530 (2004)

[19] R. Lukac and K.N. Plataniotis, “Image representation based secret sharing,” *Communications of the CCISA*, Special Issue on Visual Secret Sharing, **11**(2), 103–114 (2005)

[20] D. Jin, W.Q. Yan, and M. S. Kankanhalli, “Progressive color visual cryptography,” *Journal of Electronic Imaging*, **14**(3), 033019 (2005)

[21] J.C. Hou, “Visual cryptography for color images,” *Pattern Recognition*, **36**(7), 1619–1629 (2003)

[22] C.S. Tsai and C.C. Chang, “A new repeating color watermarking scheme based on human visual model,” *Eurasip Journal on Applied Signal Processing*, **2004**(13), 1965–1972 (2004)

[23] P. Salama and B. King , “Efficient secure image transmission: compression integrated with encryption,” *Proc. SPIE*, **5681**, pp. 47–58 (2005)

[24] C.P. Wu and C.-C.J. Kuo, “Design of Integrated Multimedia Compression and Encryption Systems,” *IEEE Trans. on Multimedia*, **7**(5), 828–839 (2005)

[25] J. Wen, M. Severa, W.J. Zeng, M.H. Luttrell, and W. Jin, “A format-compliant configurable encryption framework for access control of video,” *IEEE Trans. on Circuits and Systems for Video Technology*, **12**(6), 545–557 (2002)

[26] H. Cheng and X. Li, “Partial encryption of compressed images and videos,” *IEEE Trans. on Signal Processing*, **48**(8), 2439–2451 (2000)

[27] W. Zeng and S. Lei, “Efficient frequency domain selective scrambling of digital video,” *IEEE Trans. on Multimedia*, **5**(3), 118–129 (2003)

[28] G. K. Wallace, “The JPEG still picture compression standard,” *Communications of the ACM*, **34**(4), 31–44 (1991)

[29] C. Christopoulos, A. Skodras, and T. Ebrahimi, “ The JPEG2000 still image coding system: an overview,” *IEEE Trans. on Consumer Electronics*, **46**(4), 1103–1127 (2000)

[30] T. Lookabaugh and D.C. Sicker, “Selective encryption for consumer applications,” *IEEE Communication Magazine*, **42**(5), 124–129 (2004)

[31] Y. Sadourny and V. Conan, “A proposal for supporting selective encryption in JPSEC,” *IEEE Trans. on Consumer Electronics*, **49**(4), 864–849 (2003)

[32] M. Barnsley, “A better way to compress images,” *Byte*, **13**(1), 215–223 (1988)

[33] A.E. Jacquin, “Fractal image coding: a review,” *Proc. IEEE*, **81**(10), 1451–1465 (1993)

[34] J.M. Beaumont, “Advances in block based fractal coding of still images,” *IEE Colloquium on ‘Application of Fractal Techniques in Image Processing*,’ 3/1–3/5 (1990)

[35] Y. Fisher, *Fractal Image Compression: Theory and Applications*, Y. Fisher, Ed. New York: Springer Verlag (1995)

[36] H.T. Chang and C.J. Kuo, “Adaptive schemes for improving fractal block coding of images,” *Journal of Information Science and Engineering*, **15**(1), 11–25 (1999)

[37] H.T. Chang and C.J. Kuo, “Iteration-free fractal image coding based on efficient domain pool design,” *IEEE Trans. on Image Processing*, **9**(3), 329–339 (2000)

[38] H.T. Chang and C.J. Kuo, “A novel non-iterative scheme for fractal image coding,” *Journal of Information Science and Engineering*, **17**(3), 429–443 (2001)

[39] H.T. Chang and C.J. Kuo, “An improved scheme for fractal image coding,” *IEEE 1995 International Symposium on Circuits and Systems*, **3**, pp. 1624–1627 (1995)

[40] G. Oien, R. Hamzaoui, and D. Saupe, “On the limitation of fractal image texture coding,” *Proc. 1996 IEEE Nordic Signal Processing Symposium* (1996)

[41] S. Lepsoy, P. Carlini, and G.E. Oien, “On fractal compression and vector quantization,” in *Fractal Image Encoding and Analysis: A NATO ASI Series Book*, Chapter 2, Y. Fisher (ed.), Springer Verlag (1998)

[42] A. Gersho and R.M. Grey, *Vector Quantization and Signal Compression*, Boston, MA: Kluwer (1992)

[43] H.T. Chang, “Gradient match and side match fractal vector quantizers for images,” *IEEE Trans. on Image Processing*, **11**(1), 1–9 (2002)

[44] P. Bas, J.-M. Chassery, and F. Davoine, “Using the fractal code to watermark images,” *1998 IEEE International Conference on Image Processing*, **1**, pp. 469–473 (1998)

[45] S. Roche and J.-L. Dugelay, “Image watermarking based on the fractal transform: a draft demonstration,” *1998 IEEE Second Workshop on Multimedia Signal Processing*, pp. 358–363 (1998)

[46] Y. Fisher, D. Rogovin, and T. P. Shen, “Fractal (self-VQ) encoding of video sequences,” *Proc. SPIE*, **2308**, pp. 1359–1370 (1994)

Hsuan T. Chang received his B.S. degree in electronic engineering from the National Taiwan Institute of Technology, in 1991, and M.S. and Ph.D. degrees in electrical engineering from National Chung Cheng University, Taiwan, in 1993 and 1997, respectively.

He was a visiting researcher at the Laboratory for Excellence in Optical Data Processing, Department of Electrical and Computer Engineering, Carnegie Mellon University, USA, from 1995 to 1996. He was an assistant professor in the Department of Electronic Engineering in Cheinkuo Institute of Technology, Changhua, Taiwan, from 1997 to 1999, an assistant professor in the Department of Information Management, Chaoyang University of Technology, Wufeng, Taiwan, from 1999 to 2001, and an assistant professor in the Department of Electrical Engineering of National Yunlin University of Science and Technology, Douliu, Taiwan, from 2001 to 2002, where he currently is an associate professor. His interests include image/video processing, optical information processing/computing, and bioinformatics. He has published more than 110 journal and conference papers. He served as the reviewer of several international journals and conferences and the session chair and program committee in domestic and international conferences.

Dr. Chang is a member of SPIE, Optical Society of America (OSA), International Who's Who (IWW), The Chinese Image Processing and Pattern Recognition Society, and a senior member of Institute of Electrical and Electronic Engineers (IEEE).

Chung C. Lin received his B.S. degree in electrical engineering from the National Formosa University of Science and Technology, Taiwan, in 2002, and M. S. in electrical engineering from the National Yunlin University of Science and Technology, Taiwan, in 2004, respectively. His research interests include image and video processing. He currently is an engineer in Asmobile Communication Inc., Taiwan.

Table 1: The PSNR (in dB) comparison for the case of single block size 8×8 under different mating ratios for two images.

Mating ratio r	0	0.25	0.5	0.75	1
Lena (0.223 bpp)	29.09	30.06	30.16	**30.20**	29.89
Peppers (0.252 bpp)	28.00	28.43	28.59	**28.60**	27.81

Table 2: The PSNR (in dB) comparison for the case of single block size 4×4 under different mating ratios for two images.

Mating ratio r	0	0.25	0.5	0.75	1
Lena (0.706 bpp)	33.30	33.51	**34.04**	33.86	33.10
Peppers (0.771 bpp)	31.20	**31.31**	31.23	31.04	30.69

Table 3: The rate-PSNR (in bpp and dB) comparison for the case of two-level block sizes 8×8 and 4×4 under different mating ratios for two images.

Mating ratio r	0	0.25	0.5	0.75	1
Lena	32.98	33.15	**33.61**	33.46	32.73
	0.481	0.487	0.477	0.477	0.491
Peppers	31.03	30.82	31.06	**31.12**	30.46
	0.598	0.587	0.587	0.591	0.602

Table 4: The best rate-PSNR (in bpp and dB) results of different pairs of images for the case of single block size 8×8.

							Max.
	Lena	Peppers	Building	F-16	Harbour	Baboon	ΔPSNR
Lena		r=0.75	r=0.75	r=0.75	r=0.75	r=0.5	
0.223 bpp	**29.09**	**30.20**	30.00	29.92	29.75	29.66	1.11
Peppers	r=0.75		r=0.5	r=0.5	r=0.75	r=0.5	
0.252 bpp	**28.60**	**28.00**	28.55	28.53	28.35	28.39	0.60
Building	r=0.75	r=0.75		r=0.75	r=0.75	r=0.5	
0.288 bpp	24.63	**24.74**	**22.99**	24.45	24.02	24.01	1.75
F-16	r=0.75	r=1	r=0.75		r=0.75	r=0.5	
0.214 bpp	27.70	**27.73**	27.38	**24.63**	27.13	27.27	3.10
Harbour	r=1	r=0.75	r=1	r=0.75		r=0.5	
0.264 bpp	23.61	**23.71**	23.56	23.57	**21.36**	23.38	2.35
Baboon	r=1	r=1	r=1	r=0.5	r=1		
0.317 bpp	22.70	**22.74**	22.64	22.66	22.54	**21.00**	1.74

Table 5: The best rate-PSNR (in bpp and dB) results of different pairs of images for the case of two-level block sizes 8 × 8 and 4 × 4.

	Lena	Peppers	Building	F-16	Harbour	Baboon	Max. ΔPSNR
Lena		r=0.5	r=0.5	r=0.5	r=0.75	r=0.25	0.63
	32.98	**33.61**	33.60	33.24	33.19	33.38	
	0.481	0.477	0.482	0.480	0.486	0.482	
Peppers	r=0.75		r=0.75	r=0.5	r=0.5	r=0.25	0.59
	31.12	**31.03**	**31.62**	31.13	31.49	31.17	
	0.591	0.598	0.603	0.594	0.599	0.600	
Building	r=1	r=0.5		r=0.75	r=0.5	r=0.25	0.85
	28.11	**28.56**	**27.71**	28.28	28.40	28.15	
	0.856	0.858	0.859	0.862	0.861	0.862	
F-16	r=0.75	r=0.5	r=0.75		r=0.5	r=0.25	1.50
	30.68	31.38	**31.77**	**30.27**	31.38	30.94	
	0.513	0.507	0.517	0.516	0.517	0.513	
Harbour	r=1	r=0.75	r=0.75	r=0.75		r=1	2.10
	25.93	26.11	**26.43**	26.30	**24.33**	26.00	
	0.788	0.784	0.787	0.784	0.786	0.797	
Baboon	r=1	r=1	r=1	r=1	r=1		2.99
	25.23	25.26	**25.67**	25.26	25.11	**22.68**	
	1.078	1.077	1.091	1.080	1.092	1.087	

Figure Captions:

Figure 1 The construction of the domain pools for the pairwise images: (a) N_A domain blocks are selected from the neighboring region $L_x \times L_y$ of current range block; (b) N_B domain blocks are uniformly subsampled with the sampling periods (T_x and T_y pixels in horizontal and vertical directions, respectively) from the other image.

Figure 2 The block diagrams of the encoder and decoder in the proposed FMC scheme.

Figure 3 The block diagrams of the (a) encryption and (b) decryption processes in the proposed FMC scheme.

Figure 4 The decoded results when both images are jointly reconstructed at the first, (a) and (b), second, (c) and (d), and thirteenth, (e) and (f), iterations. The range blocks are of size 8×8.

Figure 5 The decoded results when each image is independently decoded by its own fractal code: (a) Lena and (b) Peppers. The range blocks are of size 8×8.

Figure 6 Further encrypted results of Figs. 5(a) and 5(b), in which the block means have been scrambled using dyadic permutation.

Figure 7 The incorrect decoded results of the Lena and Peppers images when three different numbers of fractal codes of the range blocks are exchanged: (a) 2565, (b) 2050, (c) 1594.

Figure 8 Incorrect decoding results while mixing two encryption schemes for the (a) Lena and (b) Peppers images.

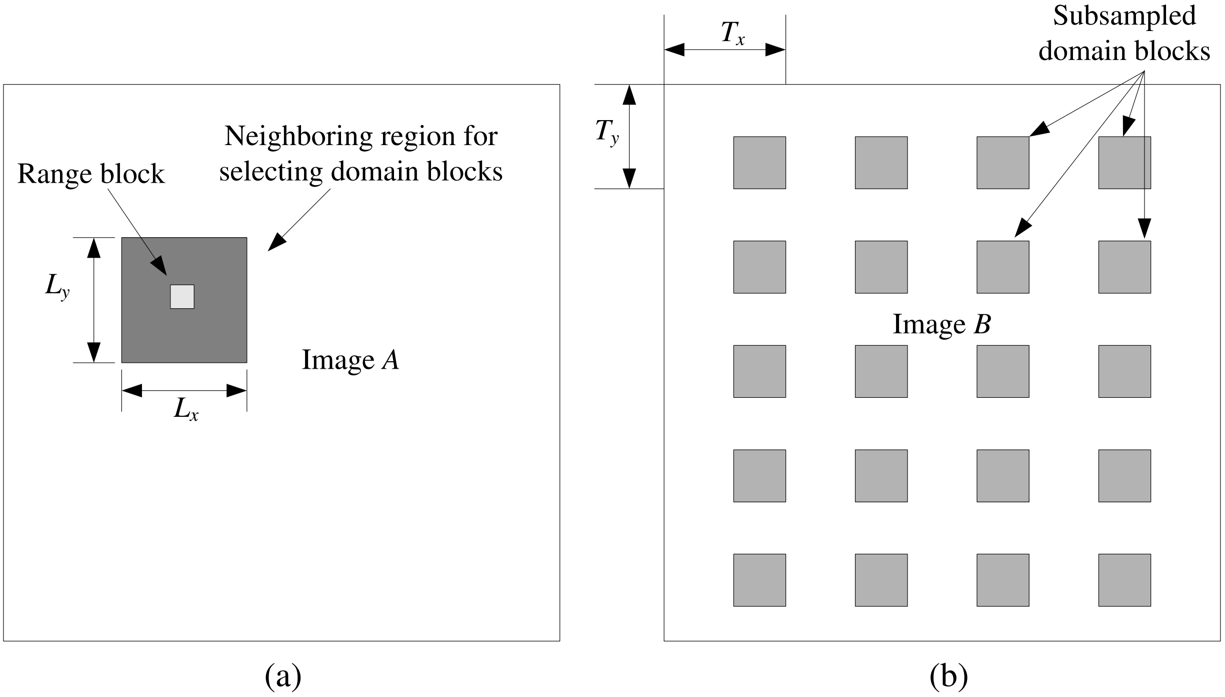


Figure 1: The construction of the domain pools for the pairwise images: (a) N_A domain blocks are selected from the neighboring region $L_x \times L_y$ of current range block; (b) N_B domain blocks are uniformly subsampled with the sampling periods (T_x and T_y pixels in horizontal and vertical directions, respectively) from the other image.

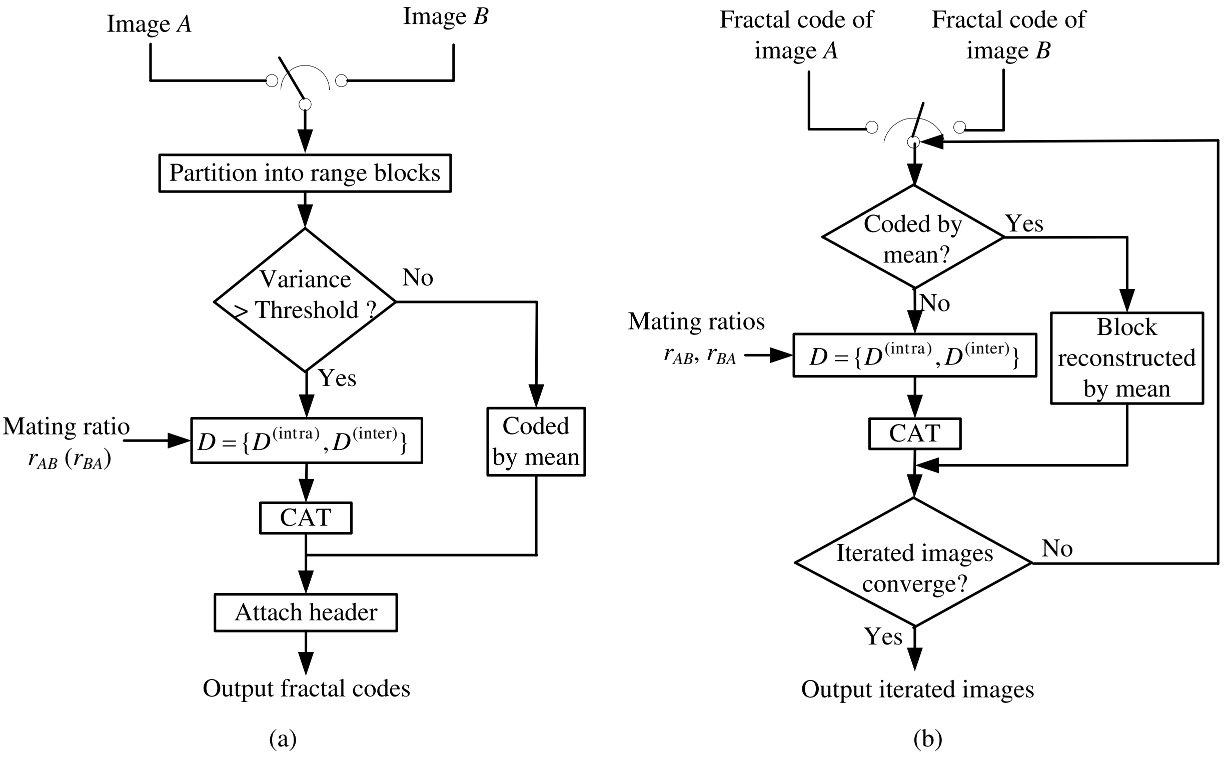


Image A
Image B
Partition into range blocks
Variance > Threshold ?
No
Yes
Mating ratio r_{AB} (r_{BA})
$D = \{D^{(\text{intra})}, D^{(\text{inter})}\}$
Coded by mean
CAT
Attach header
Output fractal codes
(a)
Fractal code of image A
Fractal code of image B
Coded by mean?
Yes
No
Mating ratios r_{AB}, r_{BA}
$D = \{D^{(\text{intra})}, D^{(\text{inter})}\}$
Block reconstructed by mean
CAT
Iterated images converge?
No
Yes
Output iterated images
(b)

Figure 2: The block diagrams of the (a) encoder and (b) deccoder in the proposed FMC scheme.

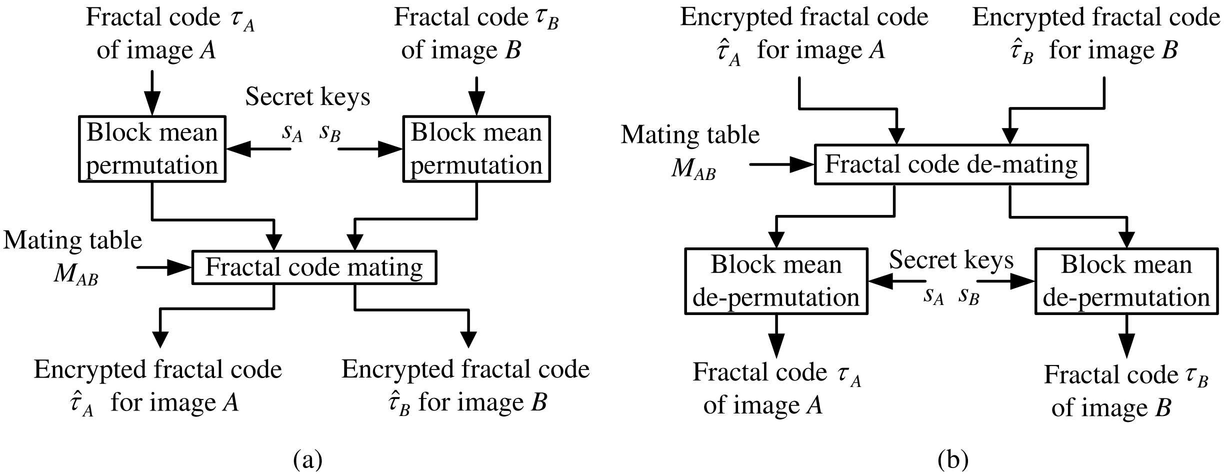
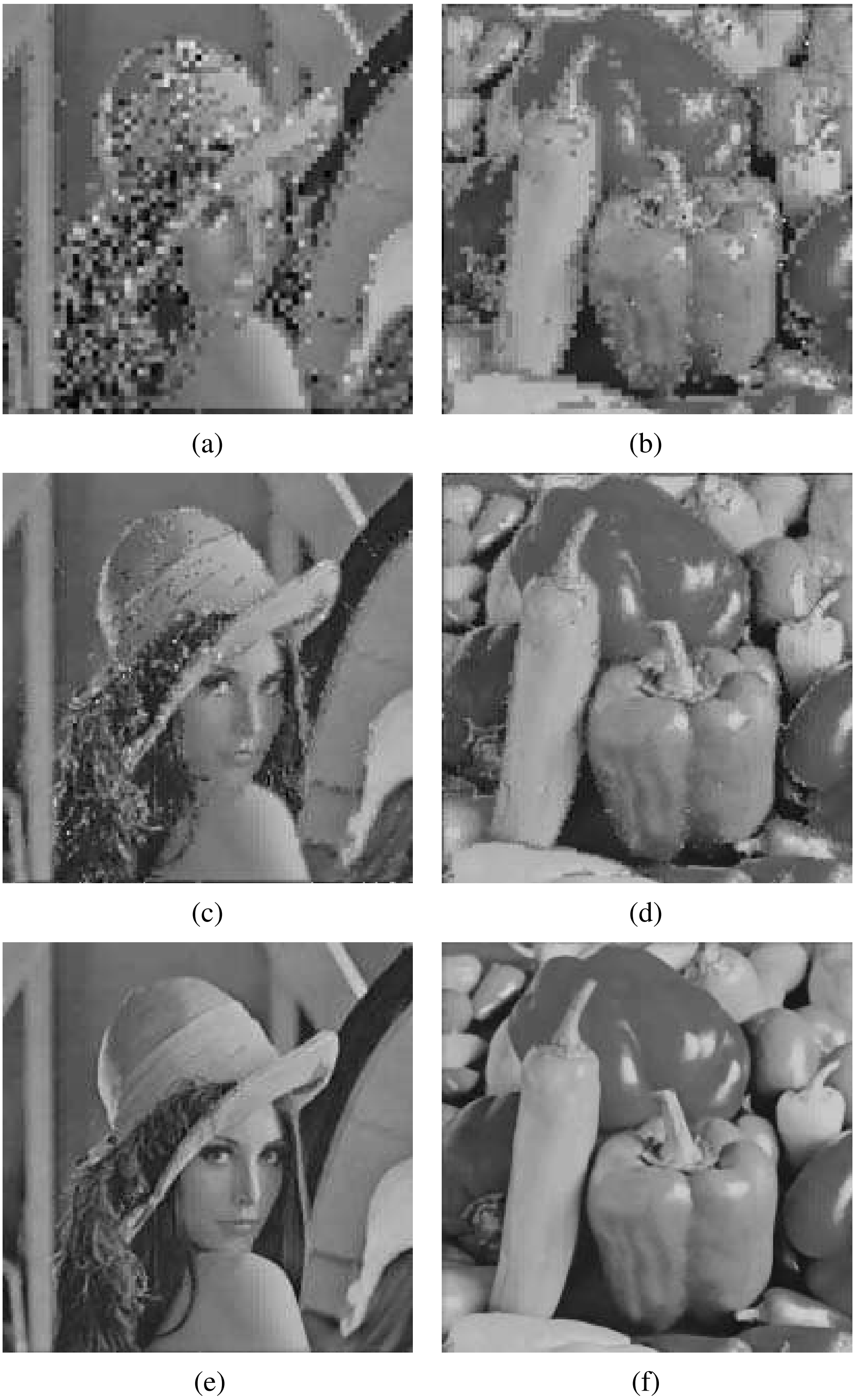

Fractal code τ_A of image A
Fractal code τ_B of image B
Secret keys
s_A s_B
Block mean permutation
Block mean permutation
Mating table M_{AB}
Fractal code mating
Encrypted fractal code $\hat{\tau}_A$ for image A
Encrypted fractal code $\hat{\tau}_B$ for image B
(a)
Encrypted fractal code $\hat{\tau}_A$ for image A
Encrypted fractal code $\hat{\tau}_B$ for image B
Mating table M_{AB}
Fractal code de-mating
Block mean de-permutation
Secret keys
s_A s_B
Block mean de-permutation
Fractal code τ_A of image A
Fractal code τ_B of image B
(b)

Figure 3: The block diagrams of the (a) encryption and (b) decryption processes in encoder and decoder, respectively, in the proposed FMC scheme.



(a)

(b)

(c)

(d)

(e)

(f)

Figure 4: The decoded results when both images are jointly reconstructed at the first, (a) and (b), second, (c) and (d), and thirteenth, (e) and (f), iterations. The range blocks are of size 8 × 8.

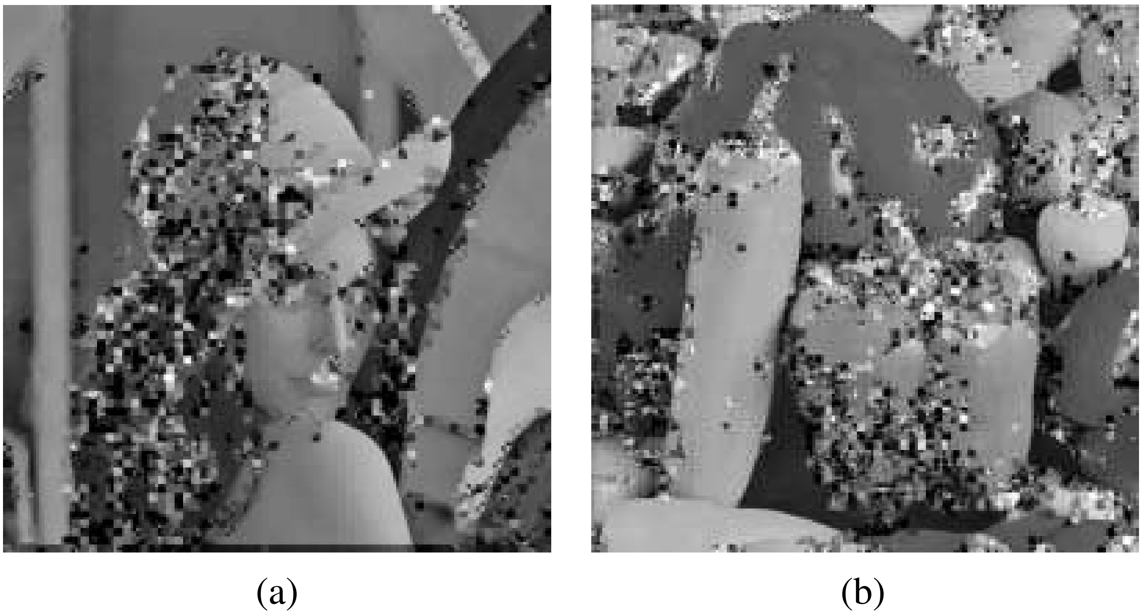


Figure 5: The decoded results when each image is independently decoded by its own fractal code: (a) Lena and (b) Peppers. The range blocks are of size 8 × 8.

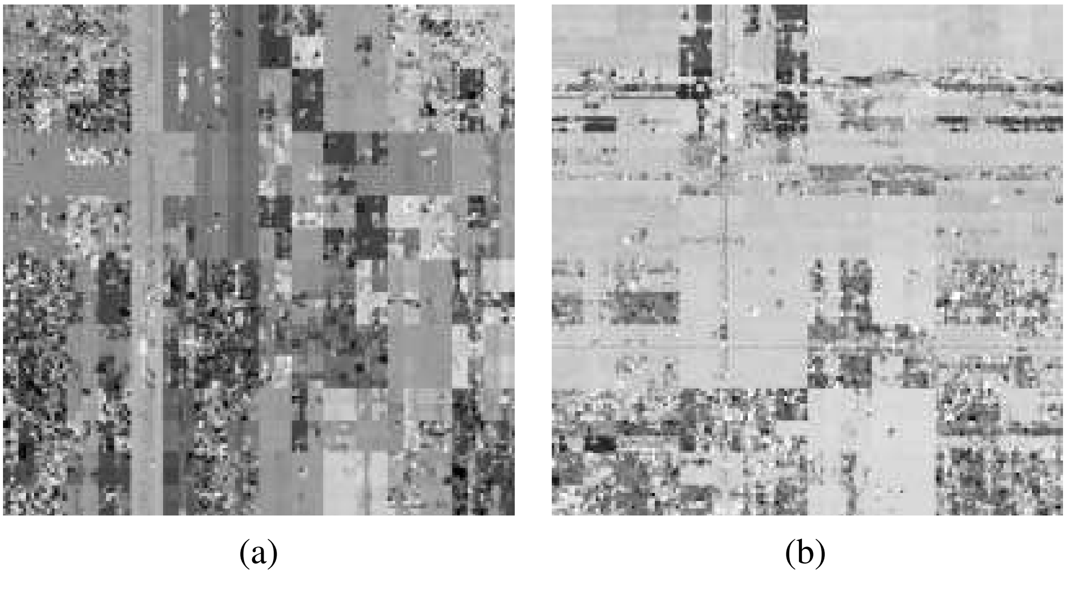
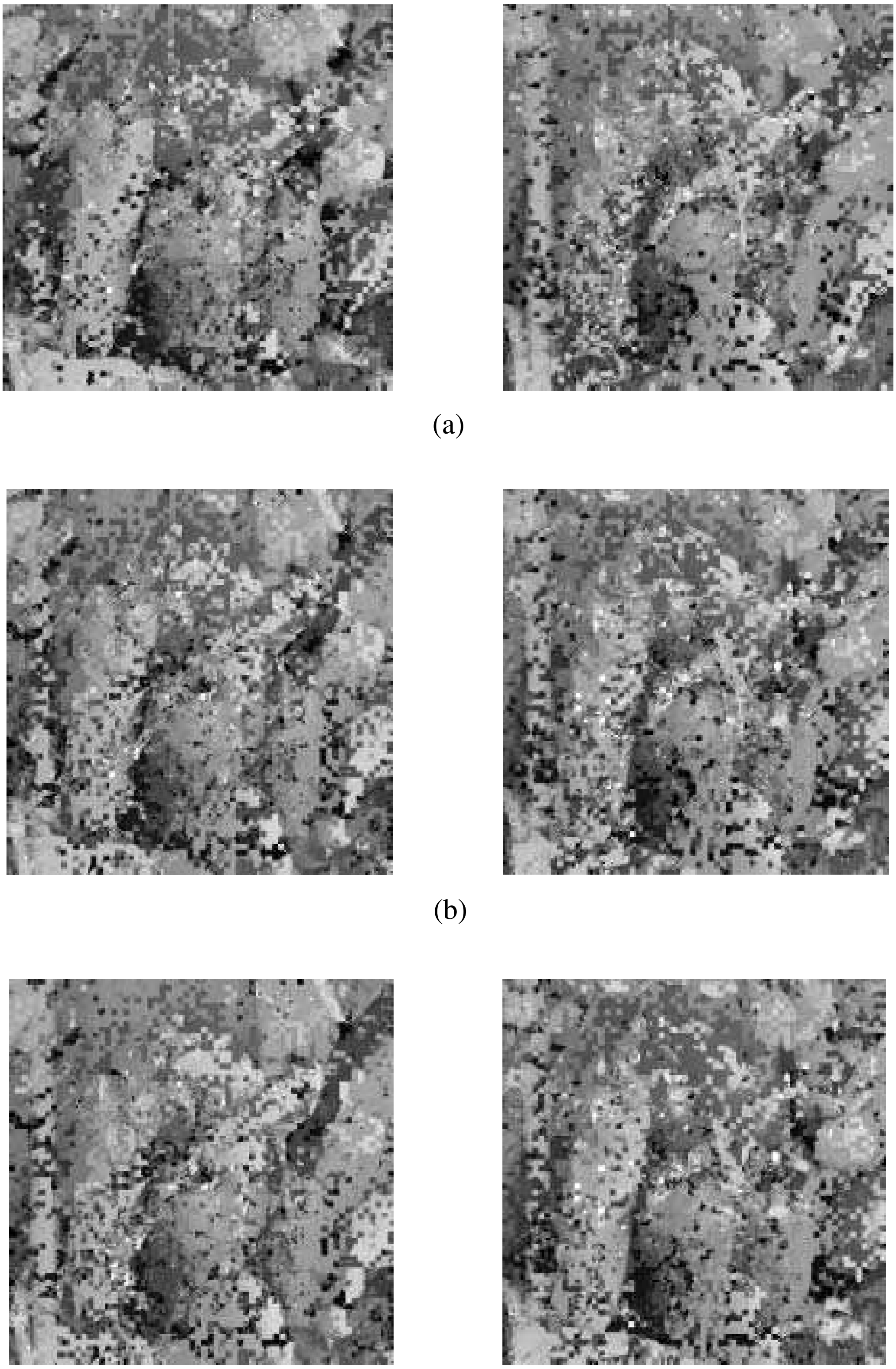


Figure 6: Further encrypted results of Figs. 5(a) and 5(b), in which the block means have been scrambled using dyadic permutation.

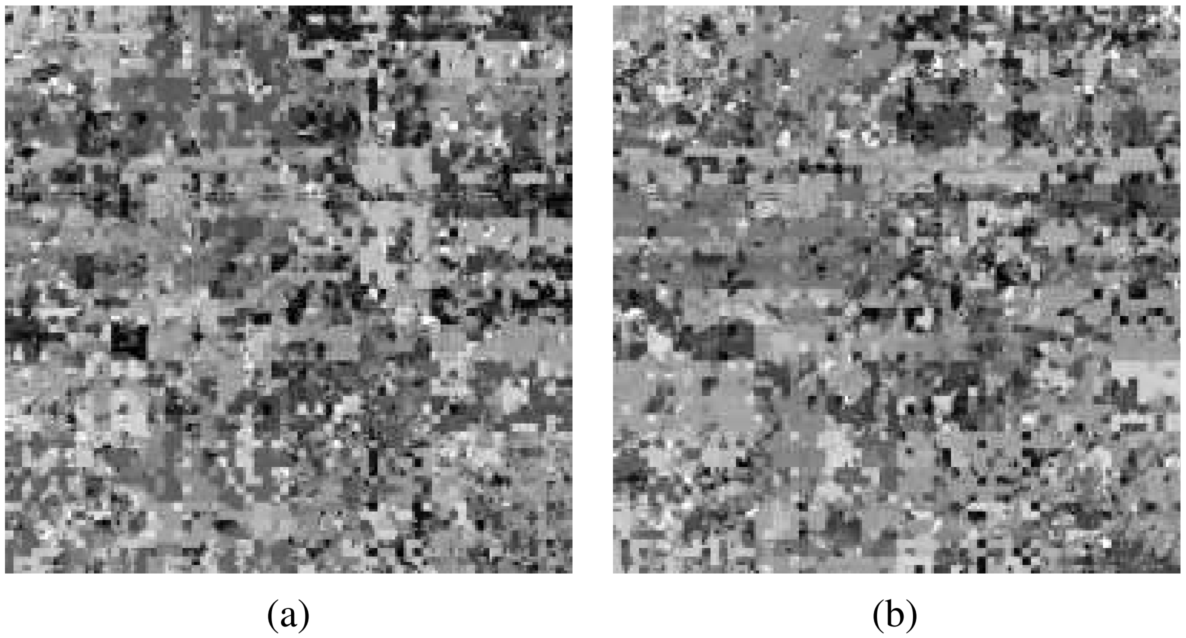


(a)

(b)

(c)

Figure 7: The incorrect decoded results of the Lena and Peppers images when three different numbers of fractal codes of the range blocks are exchanged: (a) 2565, (b) 2050, (c) 1594.



(a)

(b)

Figure 8: Incorrect decoding results while mixing two encryption schemes for the (a) Lena and (b) Peppers images.