Systems and Computers in Japan, Vol. 34, No. 9, 2003
Translated from Denshi Joho Tsushin Gakkai Ronbunshi, Vol. J85-D-II, No. 10, October 2002, pp. 1513–1521

Image Authentication Based on Fractal Image Coding without Contamination of Original Image

Miki Haseyama and Isao Kondo

School of Engineering, Hokkaido University, Sapporo, 060-8628 Japan

SUMMARY

Several digital watermarking methods proposed for the purpose of copyright protection embed signature data or images in the original images. Thus, they unavoidably produce degradation of the original images. Authors who create art works, however, desire to distribute their own originals unaltered. Therefore, this paper proposes a system for authentication of original images distributed without embedding any watermarks. The proposed method is based on fractal image coding, an image coding method. The IFS parameters obtained in fractal image coding are utilized as authentication parameters, and signature images for authentication are extracted using these parameters. © 2003 Wiley Periodicals, Inc. Syst Comp Jpn, 34(9): 1–9, 2003; Published online in Wiley InterScience (www.interscience.wiley.com). DOI 10.1002/scj.10468

Key words: authentication; IFS parameter; fractal image coding; watermark; copyright protection.

1. Introduction

Recently, the widespread use of the Internet, digital broadcasting, and DVD technology have made digital content easily obtainable. Further, a large number of image processing programs, which can modify or replicate digital content while keeping the original qualities have been distributed. Therefore, once the digital content is made available to the public, it may be copied by numerous people and placed on the Internet without the author's permission. In this context, digital watermarking methods have been proposed for copyright protection of digital content.

Watermarking methods can be classified into two groups according to the domain where the watermark is embedded: the spatial domain and the frequency domain [6]. Since most methods of the spacial domain type directly embed watermark data into the intensities of the original images, the procedures can be easily performed. However, the embedded data are easily deleted by several kinds of attacks, such as image compression, smoothing, and enlargement. Although the intensity of the watermark is sometimes set stronger to improve robustness to attack, this causes degradation of the quality of the watermarked images. On the other hand, the methods of the frequency domain type embed the watermark data into the frequency domain of the original images, and thus it becomes robust to attack [1]. However, methods based on orthogonal transformations such as FFT and DCT tend to produce block noise or mosquito noise in the watermarked images. In order to overcome this fault, some methods based on the wavelet transformation or spread spectrum techniques have been proposed, but they still cause contamination of the watermarked images, which depends on the strength of the watermark embedding [4]. Therefore, none of the methods noted above can avoid contamination of the digital image

Contract grant sponsor: Japan Society for the Promotion of Science [Grant-in-Aid for Scientific Research (C) 14550343].

created by the author (the original image) because they embed the watermark data into the original image. Actually, the creator of the artwork often desires to distribute his or her product within its original quality. However, the previous methods cannot satisfy this requirement because of the embedding scheme, which damages the original quality. The copyright of the artwork with the above requirement must still be protected, and a novel authentication method based on a scheme different from the previous methods is necessary in order to satisfy the requirement.

In this paper, a novel authentication method is proposed. It can authenticate the original image of the owner/creator without embedding any watermarks or signatures, because the embedding scheme damages the original quality. The proposed method consists of the following two systems: a signature generation system and a signature extraction system. The first system generates authentication keys, which compute the signature image desired to be extracted by the author from the original image. The authentication keys and the signature image computed from the keys are registered with an authorized authentication agency. The second system extracts a signature image, which is called an extracted signature, from a target image which the author desires to use to authenticate her/his own original image by using the authentication keys. The extracted signature image is compared with the registered signature at the authentication agency; and the target image is recognized as that created by the artist when the extracted signature is identified with the registered signature. According to the above explanation, since the proposed method does not require the embedding of any signatures into the original images in either system, it does not damage the original image at all.

These two systems are realized by fractal image coding [2, 3] and the authentication keys correspond to the IFS parameters of fractal image coding. Fractal image coding is an image compression technique which is derived by utilizing self-similarity, which is one of the structural features of images [5]. This method assumes that the images are composed of their own contractions, and the image model based on this assumption is defined by a contractive mapping which is determined by the IFS parameters. This image model is utilized in the proposed method to express the relationship between the two different images: the original image and the signature image; and thus a novel authentication method can be realized.

In this paper, Section 2 presents an outline of fractal image coding, which is utilized in the proposed method. In Sections 3.1 and 3.2, an authentication system which does not embed any signature image into the original image is proposed. Section 3.3 clarifies the difference between the procedures of the proposed method and fractal image coding and in particular describes the specialized procedures for image authentication in detail. Section 4 theoretically confirms that the proposed method actually works for authentication without problems. In Section 5, simulation results are presented to show the validity of the proposed method.

2. Fractal Image Coding

Fractal image coding, first proposed by Barnsley and Sloan [3], was completely automated by Jacquin in the form called fractal block coding[2]. Our method is realized by utilizing fractal block coding, whose procedures are as follows:

Procedure 1

A coding target image f, whose pixels have intensity $f(x, y)$ $(x = 1, \ldots, N; y = 1, \ldots, M)$, is given. The image f is partitioned into nonoverlapping *range blocks* of size $B \times B$ pixels R_i $(i = 1, 2, \ldots, n \mid n = N/B \times M/B)$.

Procedure 2

The image f is partitioned into overlapping *domain blocks* of size $2B \times 2B$ pixels with a one-pixel shift. They are denoted by D_j $[j = 1, 2, \ldots, m \mid m = (N - 2B + 1)(M - 2B + 1)]$, and the pixel intensities of the block are described by $f_{D_j}(x, y)$.

Procedure 3

The best matched block of the range block R_i, $\tilde{D}_i^{opt}$, is selected among all of these domain blocks, where the MSE (mean square error) between the blocks $\tilde{D}_i^{opt}$ and R_i is denoted by $d(R_i, \tilde{D}_i^{opt})$, and is defined as follows:

$$d(R_i, \tilde{D}_i^{opt}) \triangleq \min_{j,\theta,\lambda,s,o} d(R_i, \tilde{D}_j) \qquad (1)$$

In the above equation, $\tilde{D}_j$ is called the contracted domain block, and its pixel intensity $f_{\tilde{D}_j}(x, y)$ can be obtained by using $f_{D_j}(x, y)$ below:

$$f_{\tilde{D}_j}(\hat{x}, \hat{y}) = s f'_{D_j}(x', y') + o \qquad (2)$$

where

$$f'_{D_j}(x', y') = \frac{1}{4} \sum_{i=0}^{1} \sum_{l=0}^{1} f_{D_j}(2(x'-1)+i, 2(y'-1)+l)$$
$$(x' = 1, \ldots, B; \quad y' = 1, \ldots, B) \qquad (3)$$

$$\begin{pmatrix} \hat{x} \\ \hat{y} \end{pmatrix} = \begin{pmatrix} \cos\theta & -\lambda\sin\theta \\ \sin\theta & \lambda\cos\theta \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} + \begin{pmatrix} e \\ f \end{pmatrix}$$
$$(\hat{x} = 1, \ldots, B; \quad \hat{y} = 1, \ldots, B) \qquad (4)$$

In the above equation, $\theta \in \{0, \frac{1}{2}\pi, \pi, \frac{3}{2}\pi\}$ is the angle of rotation; e and f are coordinate offsets expressing the coordinate shift produced by rotation; and $\lambda \in \{1, -1\}$ is an operator for turning the block. The parameters s and o are called the scaling and offset coefficients, respectively.

Procedure 4

All of the range blocks $R_i(i = 1, \ldots, n)$ are processed by Procedure 3, and $\tilde{D}_i^{opt}(i = 1, \ldots, n)$ is obtained. The parameter which specifies the location of the domain block used for computing $\tilde{D}_i^{opt}$, which is called the location parameter, and θ, λ, s, and o, are the IFS parameters for range block R_i.

Fractal block coding has a decoding system as well as the encoding system described above. However, since our method utilizes only the encoding system, the decoding system is not explained in this paper.

3. The Proposed Authentication Method

The flow of procedures in the proposed method is shown in Fig. 1; the terms used in Fig. 1 correspond to those used in the following subsections.

3.1. Signature generation system

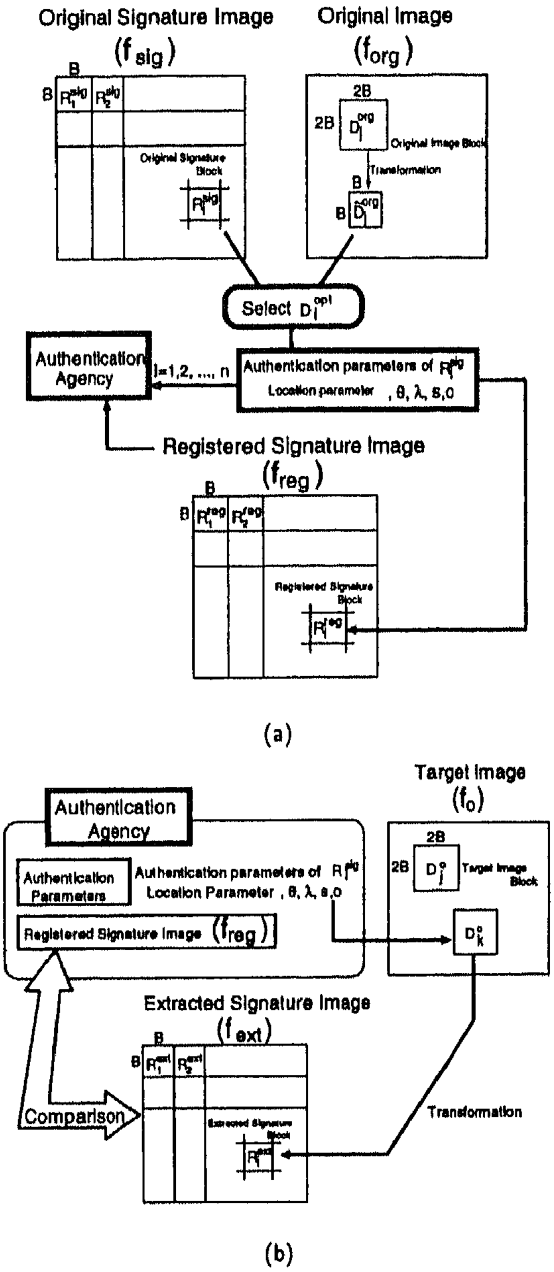
The signature image to be registered with the authentication agency (the registered signature image) is generated from the original image and the image that the author desires to be the signature image, which is called the original signature. The procedures in this signature generation system are detailed below. In the following description, since the system is based on fractal image coding, we show how our procedures correspond to the procedures of fractal image coding introduced in Section 2.

Procedure 1

The original signature f_{sig} is obtained, whose pixels have the intensities $f_{sig}(x, y)(x = 1, \ldots, N; y = 1, \ldots, M)$. The image f_{sig} is partitioned into nonoverlapping blocks of size $B \times B$ pixels $R_i^{sig}(i = 1, 2, \ldots, n \mid n = N/B \times M/B)$. These blocks are called the original signature blocks, which correspond to Procedure 1 of Section 2.

Procedure 2

An arbitrary area of the original image f_{org}, whose pixel intensities are denoted by $f_{org}(x, y)$ is specified by the author. The image f_{org} is partitioned into overlapping blocks of size $2B \times 2B$ pixels with a one-pixel shift. They are called the original image block and are denoted by $D_j^{org}(j = 1, 2, \ldots, m')$, where m' is the total number of D_j^{org}. The original image blocks correspond to the domain blocks in Procedure 2 of Section 2.



(a)

(b)

Fig. 1. (a) Signature generation system; (b) authentication system.

Procedure 3

The block $\tilde{D}_j^{org}$, whose intensities are computed by processing the pixel intensities of block D_j^{org} according to Eqs. (2) to (4), can be obtained. The parameters appearing in Eqs. (2) to (4)—θ, λ, s, and o—are computed by minimization of the MSE between blocks R_i^{sig} and $\tilde{D}_j^{org}$, where the obtained minimum MSE is denoted by $d(R_i^{sig}, \tilde{D}_j^{org})$. If $\tilde{D}_K^{org} \in \{\tilde{D}_1^{org}, \ldots, \tilde{D}_{m'}^{org}\}$, then all of the blocks $\tilde{D}_K^{org}$ which satisfy the following equation are selected:

$$d(R_i^{sig}, \tilde{D}_K^{org}) \leq \min_j d(R_i^{sig}, \tilde{D}_j^{org}) + T_{min} \quad (5)$$

Equation (5) is different from Eq. (1), because the parameter $T_{\min}$ appears only in Eq. (5). This parameter is used to specify a target area of the original image to be authenticated, and the reason for its introduction is explained in Section 3.3.

If only one block is selected from the $\tilde{D}_K^{org}$, let it be D_i^{opt}. If multiple blocks are selected from the $\tilde{D}_K^{org}$, the minimum overlapped block $\cup_{l=1}^{i-1} D_l^{opt}$ is selected from them, and denoted D_i^{opt}. The location parameters of the block used in computing D_i^{opt}—θ, λ, s, and o—are called the authentication parameters of the block R_i^{sig}, which correspond to the IFS parameters in Procedure 4 of Section 2.

Procedure 4

Let us substitute the authentication parameters of the block R_i^{sig}, which are obtained in Procedure 3, for the parameters of the following equation; then the pixel intensities of the registered signature block R_i^{reg} can be obtained, where R_i^{reg} is a block with a size of $B \times B$ pixels, and is a portion of the registered signature image f_{reg}, whose pixel intensities are $f_{reg}(x, y)$:

$$f_{R_i^{reg}}(\hat{x}, \hat{y}) = s f'_{D_k^{org}}(x', y') + o \tag{6}$$

where the relationship between $(\hat{x}, \hat{y})$ and (x', y') is the same as shown in Eq. (4), and $f'_{D_k^{org}}(x', y')$ is computed by using the pixel intensities of the block $f_{D_k^{org}}$ as follows:

$$\begin{aligned} & f'_{D_k^{org}}(x', y') \\ & = \frac{1}{4} \sum_{i=0}^{1} \sum_{j=0}^{1} f_{D_k^{org}}(2(x'-1)+i, 2(y'-1)+j) \\ & (x' = 1, \ldots, B; \quad y' = 1, \ldots, B) \end{aligned} \tag{7}$$

These procedures are repeated for each of the blocks R_i^{sig} $(i = 1, 2, \ldots, n)$; after processing, the resulting blocks R_i^{reg} $(i = 1, 2, \ldots, n)$ are placed in order of i without overlapping, giving the registered signature image f_{reg}.

In the above procedures, we can see that the authentication parameters are computed from the original image by referring to the original signature, and the registered signature image is generated by using the authentication parameters.

As shown in Procedures 1 and 2, in the procedures of the proposed system the range blocks and the domain blocks are obtained from different images, which is much different from the fractal block coding described in Section 2. The difference is necessary in order for the proposed method to realize a system which can generate the registered signature image from the original image. After this modification the IFS parameters can be utilized to express the relationship between the two images.

Further, although in Procedure 2 of Section 2 the domain blocks are selected from the whole image for encoding, in the proposed method they are selected from a restricted area of the target image, selected at the author's option. This modification is necessary for the proposed method to be used as an authentication system. The reason for its introduction is explained in Section 3.3 together with the reason for the introduction of $T_{\min}$.

3.2. Authentication system

If an image to be authenticated is obtained (target image), the target image and the authentication parameters are given to the authentication agency, and the signature image is extracted (extracted signature image). The extraction procedures are as follows.

Procedure 1

A target image f_o is obtained, whose pixel intensities are denoted by $f_o(x, y)$ $(x = 1, \ldots, N; y = 1, \ldots, M)$, and its authentication parameters registered with the authentication agency are prepared.

Procedure 2

The image f_o is partitioned into overlapping blocks of size $2B \times 2B$ pixels D_j^o $[j = 1, 2, \ldots, m \mid m = (N - 2B + 1)(M - 2B + 1)]$ with a one-pixel shift, which are called the target image blocks.

Procedure 3

According to the location parameter of R_i^{sig}, D_k^o is selected, with pixel intensities denoted by $f_{D_k^o}(x, y)$. The intensities $f_{D_k^o}(x, y)$ and the authentication parameters other than the location parameter are substituted for the parameters in the following equation, and $f_{R_i^{ext}}(x, y)$ is obtained. Here the block which consists of the pixels $f_{R_i^{ext}}(x, y)$ is denoted by R_i^{ext}, and is called the extracted signature block. The extracted signature block is a portion of the extracted signature image f_{ext}, whose pixel intensities are denoted by $f_{ext}(x, y)$:

$$f_{R_i^{ext}}(\hat{x}, \hat{y}) = s f'_{D_k^o}(x', y') + o \tag{8}$$

In the above equation, the correspondence between $(\hat{x}, \hat{y})$ and (x', y') is given by Eq. (4), and $f'_{D_k^o}(x', y')$ is computed as

$$\begin{aligned} & f'_{D_k^o}(x', y') \\ & = \frac{1}{4} \sum_{i=0}^{1} \sum_{j=0}^{1} f_{D_k^o}(2(x'-1)+i, 2(y'-1)+j) \end{aligned}$$

$$(x' = 1, \ldots, B; \quad y' = 1, \ldots, B) \tag{9}$$

Procedure 4

Procedure 3 is applied to all of the blocks R_i^{sig} ($i = 1, 2, \ldots, n$), and R_i^{ext} ($i = 1, 2, \ldots, n$) is obtained. These obtained blocks are placed in order of i without overlapping, and the extracted signature image f_{ext} is obtained.

Procedure 5

By comparison of the extracted signature image and the registered signature image, we judge whether the target image is the original image.

Using the above procedures, the signature image can be extracted from the target image without embedding the signature image into the original image. However, according to Eq. (9), the proposed method authenticates not only the original image f_{org} but also the images whose $\frac{1}{2}$ scale reductions are the same as the reduction of the original image. In other words, the proposed method recognizes all images satisfying $\frac{1}{4}\sum_{i=0}^{1}\sum_{j=0}^{1} f_{org}(2(x-1)+i, 2(y-1)+j) = \frac{1}{4}\sum_{i=0}^{1}\sum_{j=0}^{1} f'(2(x-1)+i, 2(y-1)+j)$ as being the original image. Therefore, if the users do not wish such images to be recognized as the same as the original image, our method is not applicable.

3.3. Difference between the signature generation system and fractal block coding

Fractal block coding selects the best matched domain block as the range block (Section 2, Procedure 3). Therefore, different domain blocks might be selected by a range block, or different domain blocks selected by different range blocks might overlap each other. Actually, if $T_{\min} = 0$ in Eq. (5), the proposed method has the same situation. In other words, depending on the selection of D_l^{opt}, $\cup_{l=1}^{m} D_l^{opt}$ might cover only a part of the original image [an example is shown in Fig. 3(a-1) for the case of $T_{\min} = 0$)]. For the proposed authentication, the extracted signature image consists of the blocks generated by processing the target image blocks specified by the authentication parameters. Therefore, if the target blocks not specified by the authentication parameters are replicas of the original image, the authentication system cannot detect it. In order to overcome this kind of problem, we introduce the parameter $T_{\min}$ into our method. The parameter $T_{\min}$ controls the covered area of the original image as follows: a larger $T_{\min}$ causes more different D_l^{opt} to be selected, and finally the whole image is covered by the selected blocks D_l^{opt} with much larger $T_{\min}$.

Furthermore, if the original image is a portrait, the area corresponding to the person is more important than the other areas, such as the background. In this case, the author naturally desires to protect this area more strongly than the others. However, if the blocks selected by the authentication parameters are mainly placed in the background, only the background is modified, and the important area is used unaltered; our method cannot authenticate the image as belonging to the author even though it is the original image, because the extracted signature image is much different from the registered signature image. This is a problem for the application of the proposed method to authentication.

Therefore, although fractal image coding selects the domain block best matched to the range block from all of the domain blocks in Section 3.1 Procedure 2 of our method selects it from only the area desired by the author, that is, the copy-prohibited area. By this modification, the proposed method can select the original image blocks from the specified area of the original image for generation of the extracted signature image.

4. Confirmation of the Suitability of the Proposed System for Authentication

In order to apply the proposed system to the image authentication problem, we have to prove that in the proposed method a set of authentication parameters produces only one extracted signature image, that is, a signature extracted from an image different from the original image by using the authentication parameters is always different from the registered signature image.

Before proving the above, let us clarify the following two characteristics of the proposed method. First, from Section 3.1 Procedure 4, if half-scale versions of some images are the same as the half-scale original image, they are recognized as being the same as the original image. Second, if the authentication area is specified based on Section 3.1 Procedure 2, a target image, whose area other than the specified area is different from the original image, is recognized as being the same image as the original one.

Let us prove that the proposed method retains the above denoted characteristics. The extracted signature image generated in the authentication system f_{ext} consists of the extracted signature blocks R_i^{ext} computed by Procedure 3 in Section 3.2. Further, the pixel intensities of each extracted signature block are obtained by processing the pixel intensities of the target image block D_j^o specified by the location parameter. Therefore, to prove that the proposed method retains the above characteristic is identical to proving that an extracted signature block is not generated from any different target block. Now, the relationship between $f'_{D_k^o}(x', y')$, which is obtained by substituting the pixel intensities of the target image block D_j^o for the intensities of Eq. (9), and $f_{R_i^{ext}}(x, y)$ is described by rewriting Eq. (8) as

$$A = \begin{pmatrix} \cos\theta & -\lambda\sin\theta & 0 \\ \sin\theta & \lambda\cos\theta & 0 \\ 0 & 0 & s \end{pmatrix}, C = \begin{pmatrix} e \\ f \\ o \end{pmatrix} \quad (10)$$

as follows:

$$\begin{pmatrix} \hat{x} \\ \hat{y} \\ f_{R_i^{ext}}(\hat{x}, \hat{y}) \end{pmatrix} = A \begin{pmatrix} x' \\ y' \\ f'_{D_k^o}(x', y') \end{pmatrix} + C \quad (11)$$

In Eq. (10), the case of $s = 0$, where s is computed in the signature generation system as stated before, is

(i) the case in which the block specified by the location parameter is like a block D_k^{org} whose pixel intensities are $f'_{D_k^{org}}(x, y) = c(x = 1, \ldots, B, y = 1, \ldots, B)$, where c is a constant:

(ii) the case of $f_{R_i^{sig}}(x, y) = c(x = 1, \ldots, B, y = 1, \ldots, B)$;

or

(iii) a case other than (i) and (ii) in which a block D_k^{org} satisfying $\sum_{x=1}^{B} \sum_{y=1}^{B} f_{R_i^{sig}}(x, y) f'_{D_k^{org}}(x, y) = \frac{1}{B^2} \sum_{x=1}^{B} \sum_{y=1}^{B} f_{R_i^{sig}}(x, y) \sum_{x=1}^{B} \sum_{y=1}^{B} f'_{D_k^{org}}(x, y)$ is selected as D_i^{opt}.

In case (i), if the signature blocks satisfying (i) are selected in computing s, we replace them by blocks of the others, or compute the signature block by using only the parameter o with $s \neq 0$. Further, case (ii) means that all of the pixel intensities of R_i^{sig} are the same. Therefore, when using the proposed method, we do not select such an image as the original signature image, or do not evaluate such a block to compute the authentication criterion. Finally, in case (iii), we replace the selected block D_k^{org} with a block of the others, or modify one or more of its pixel intensities slightly. The above countermeasures assure for all kinds of extracted signature images that $s \neq 0$. Therefore, it can be ascertained that $\det A = -\lambda s$. When A^{-1} exists, it is guaranteed that the extracted signature blocks are never generated from different target blocks. Consequently, since it is proved that our method does not extract an extracted signature image from different target images, it is applicable to the authentication problem.

5. Simulations

5.1. Selection of the original image blocks and the registered signature image

Let us confirm by simulations that the parameter $T_{\min}$ [Eq. (5)] can control the area not specified by the authentication parameters as stated in Section 3.3. For the simulations, Girl, shown in Fig. 2(a), is utilized as the original image, and (b) is used as the original signature image. Their sizes are 256 × 256 pixels and their maximum gray level is 255. In the signature generation system, the size of the original signature block ($B \times B$) is 8×8 pixels, and that of the original image block is 16×16 pixels. These sizes are usually adopted in fractal image coding. When the proposed method is used, they should be determined by consideration of the data size of the authentication parameters to be registered with the authentication agency, the quality of the registered signature image, and so on. The size of the data to be registered is increased by using blocks of smaller sizes, and simultaneously the registered signature image generated in the signature generation system approximates the original signature image much more closely.

The simulation results with $T_{\min} = 0$, 500, and 1000 are shown in (a-1), (b-1), and (c-1) of Fig. 3. In these figures, the selected original image blocks show the original intensities. From (a-1), (b-1), and (c-1), we can see that the selected original image blocks can cover a larger area of the original image to be authenticated with larger $T_{\min}$, which corresponds to the control explained in Section 3.3.

The registered signatures generated with these $T_{\min}$ are also shown in (a-2), (b-2), and (c-2). For the comparison between each of the registered signatures and the original signature, the following SNR is utilized:

$$\mathrm{SNR} = 10 \log_{10} \frac{\sum_{x=1}^{256} \sum_{y=1}^{256} (f_{sig}(x, y))^2}{\sum_{x=1}^{256} \sum_{y=1}^{256} (f_{sig}(x, y) - f_{reg}(x, y))^2} \quad (12)$$

From the simulation results, with increasing $T_{\min}$, such as $T_{\min} = 0$, 500, and 1000, the SNR of the registered signature deteriorates, such as 22.04, 21.20, and 20.36 dB. However, even in the case of $T_{\min} = 1000$, in which 80% of the

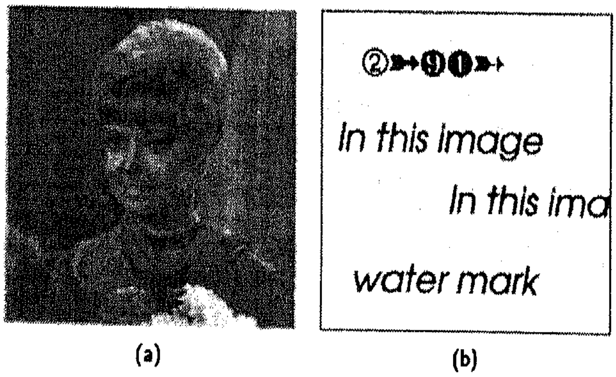
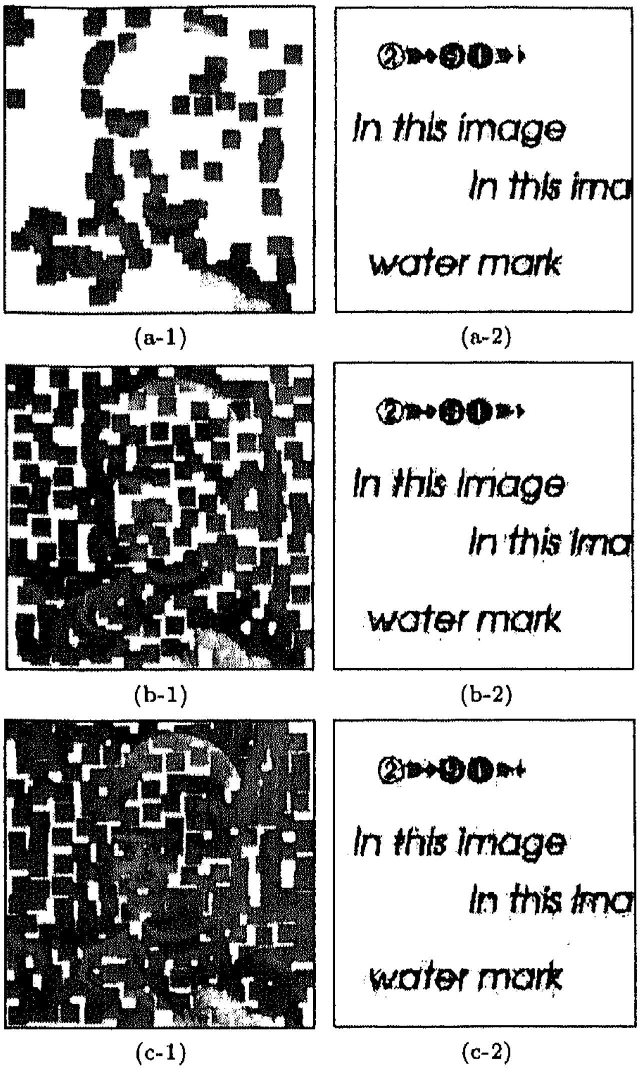


Fig. 2. (a) Original image; (b) reference signature image.



(a-1) (a-2)
(b-1) (b-2)
(c-1) (c-2)

Fig. 3. Selected original image blocks and registered signature images.

original image is covered, the result shown in (c-2) remains over 20 dB; therefore, we can confirm that an image much different from the original signature image is not registered in our method.

We tried to apply our method to several different original images and original signature images with different combinations, and obtained similar results to the above. Although we cannot guarantee that an image much different from the original signature image is not registered at all; it does not present a major problem for the accuracy of authentication in our method, because the registered signature is actually registered with the authentication agency and is used for authentication.

5.2. Robustness of the proposed method to signal processing

The robustness of the proposed method is tested with images which are processed by different types of manipulations. In these simulations, when Fig. 2(a) is utilized as the original image and Fig. 2(b) as the registered signature image in the signature generation system, the registered signature is compared with the extracted signature image from the original image contaminated by several signal processing methods. For the comparison, we use the SNR defined by substituting $f_{reg}(x, y)$ for $f_{sig}(x, y)$ and $f_{ext}(x, y)$ for $f_{reg}(x, y)$ in Eq. (12). Further, the original image blocks are selected from the entire original image by using $T_{\min} = 1000$; thus, the registered signature image is the image shown in Fig. 3(c-2). The signal processing methods applied to the original image are the following six:

(a) Smoothing (1)

As an example of smoothing by linear filters, the average filter with a size of 3 × 3 pixels is applied to the original image, using the mask

$$\frac{1}{16}\begin{pmatrix} 1 & 2 & 1 \\ 2 & 4 & 2 \\ 1 & 2 & 1 \end{pmatrix}$$

(b) Smoothing (2)

As an example of smoothing by nonlinear filters, a median filter with a size of 3 × 3 pixels is applied to the original image.

(c) Sharpening

A sharpening filter with a size of 3 × 3 pixels, whose coefficients are as follows, is applied to the original image:

$$\begin{pmatrix} 0 & -1 & 0 \\ -1 & 5 & -1 \\ 0 & -1 & 0 \end{pmatrix}$$

(d) JPEG compression

A JPEG with 25% quality parameter is applied to the original image.

(e) Scaling

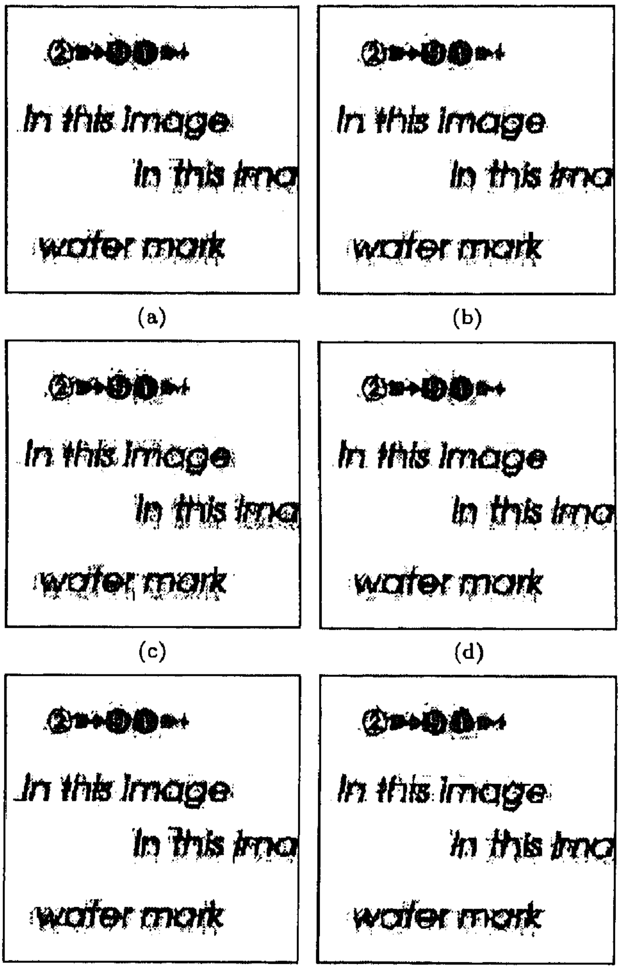
The original image is scaled down to half its original size, that is, a size of 128 × 128 pixels. In order to apply the proposed method to the scaled image, it is rescaled to the original size, and the scaled image is enlarged by a simple interpolation procedure with a weighting of 1 applied to the neighbor pixels.

(f) Random geometric distortions

With the software Stirmark (Version 3.1, http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/), which is often used as a benchmark, the original image is contaminated by random geometric distortion.

The signature images extracted from the contaminated images by the above signal processing methods are shown in Figs. 4(a) to 4(f). Panels (a) to (f) correspond to the images contaminated by the above signal processing manipulations (a) to (f), where (f) is the extracted signature which maintains the most approximate quality on average in 100 trials. The SNRs of the extracted signature images are as follows: (a) 35.1 dB; (b) 31.3 dB; (c) 23.6 dB; (d) 31.5 dB; (e) 29.9 dB; and (f) 17.67 dB, where the average of 100 trials is 17.7 dB.

From Fig. 4, we can see that after the signal processing, extracted signature images of high quality whose SNRs are greater than 17 dB can be obtained. Also we obtained some other simulation results: the results of JPEG compression with quality = 70% and 50% are SNR 37.07 and 34.7 dB, respectively; and for the use of the image enlarged to double the original size, the result is an SNR of 29.9 dB, where the enlarged image is scaled down to half of the enlarged size by down-sampling after low-pass filtering.



(a) (b)

(c) (d)

(e) (f)

Fig. 4. Extracted signature images after signal processing operations.

In particular, Figs. 4(d) and 4(f) show the following important points: First, Fig. 4(d) shows that the proposed method can extract a signature with a quality of over 30 dB from the original image contaminated by JPEG compression, which is often used for the data storage and transmission. Based on these results, the proposed method is effective for the authentication of compressed images. Second, the result (f) obtained with Stirmark, which is an example of numerous programs recently developed, exceeds 17.7 dB. This shows that the proposed method should be useful for several applications.

6. Conclusions

In this paper, an authentication method without signature insertion is proposed, which is different from the previous digital watermarking methods presented for image copyright protection. Since the proposed method does not insert any signatures into the original image, by using the proposed method the author can distribute the original image, at its original quality, without any contamination. Further, compared with the method which directly registers the original image with the authentication agency, the proposed method registers a smaller amount of data. By using the proposed method, the authors or owners of artworks can distribute their products at the original quality while the copyrights are properly protected. In Section 5, based on the simulation results, it is verified that the proposed method is not affected by signal processing operations.

However, before the practical use of the proposed method, the following points must be discussed. First, since the proposed method extracts the signature image by using the original image blocks specified by the location parameter, if the target image is an image clipped from the original one, the proposed method needs the original image to fix the location parameter. This problem must be overcome before practical use. Second, since the proposed method must register the signature and the authentication parameters with the authentication agency, the agency must maintain large amounts of data. In the case of numerous images to be registered, the agency has a major problem; it must be overcome by controlling the word length of the authentication parameters, etc. Finally, in Procedure 5 of Section 3.2, comparing the extracted signature image with the registered signature image, we apply a threshold to the distance between the two images, which is one possible approach. In the use of the threshold, we must avoid authentication of images similar to the original one, which are not the same as the original. Therefore, before practical use, a reliable method of setting the threshold must be derived.

Acknowledgments. The authors are grateful to Dr. Akio Miyazaki of the Graduate School of Information Science and Electrical Engineering, Kyushu University, for useful suggestions. This work was supported by a grant from the Japan Society for the Promotion of Science [Grant-in-Aid for Scientific Research (C) 14550343].

REFERENCES

1. Matsui K. A base of digital watermark. Morikita Press; 1998.
2. Jacquin AE. Image coding based on fractal theory of iterated contractive image transformation. IEEE Trans Image Process 1992;1:18–30.
3. Barnsley MF, Sloan A. Method and apparatus for processing. United States Patent 5,065,447, 1991.
4. Ejima M, Miyazaki A. Digital watermark technique using one-dimensional image signal obtained by raster scanning. Trans IEICE 1999;J82-A:1083–1091.
5. Saito T, Cheong CK. A new image coding technique, focusing on fractal theory. J IEICE 1992;75:1343–1355.
6. Piva P, Barni M, Vartolini F, Cappelini V. DCT-based watermarking recovering without resorting to the uncorrupted original image. Int Conf Image Processing, 1997;1:520–523.

AUTHORS (from left to right)

Miki Haseyama (member) received her M.S. and D.Eng. degrees in electronic engineering from Hokkaido University in 1988 and 1993. From 1989 to 1993, she was a research associate at the Hokkaido University Research Institute of Applied Electricity. Since 1995, she has been an associate professor at Hokkaido University. Her research interests include digital signal processing and image processing.

Isao Kondo (student member) is a student in the M.E. program at Hokkaido University. His research interest is image processing.