Phase-Only Correlation Based Matching in Scrambled Domain for Preventing Illegal Matching

Izumi Ito and Hitoshi Kiya

Graduate School of System Design, Tokyo Metropolitan University
6-6 Asahigaoka, Hino-shi, Tokyo, Japan
kiya@sd.tmu.ac.jp

Abstract. We herein propose an image matching in the scrambled domain for preventing illegal image matching, which is defined as a malicious and intentional act conducted in order to deduce the content of images. The phase of discrete Fourier transform (DFT) coefficients of images is scrambled for visual protection. In addition, the magnitude of DFT coefficients is scrambled for preventing illegal image matching. Phase-only correlation (POC) or phase correlation can be applied directly to images in the scrambled domain for alignment and similarity. The accuracy of POC in the scrambled domain is the same as that in the non-scrambled domain. Simulations are presented to confirm the appropriateness and effectiveness of the proposed scrambling.

Keywords: phase-only correlation, image matching, visual protection, illegal image matching.

1 Introduction

Phase-only correlation or phase correlation, which is referred to as POC in the present paper, is used to estimate the similarity and translation between two signals. POC in terms with Fourier transform was developed as PHAse Transform in [1] and POC in terms with discrete Fourier transform (DFT) was proposed by Kuglin and Hines in [2]. The concept of the POC is based on the Fourier shift property, and the estimation of translation is extended to the estimation of rotated and scaled values between two images by log-polar coordinate change [3]. A number of subpixel estimation methods have been proposed [4]-[8], and high-accuracy techniques for POC have been developed [9]. The estimation of geometrically converted values enables POC to be an effective method for image matching [10]-[13]. In POC-based image matching, images are stored in the form of images or their DFT coefficients as templates in a database. As a result, if templates were leaked, unlike templates that consist of statistical feature of images, the contents of the templates are revealed. Generally, encrypting is used for protection [14]-[16]. However, encrypted images require decrypting before image matching. In addition, decrypting of a multitude of templates requires enormous

Y.Q. Shi (Ed.): Transactions on DHMS V, LNCS 6010, pp. 51–69, 2010.

computational complexity, and after image matching, decrypted images have to be discarded so as not to cause a security problem. Therefore, signal processing in an encrypted domain is desired [17] [18].

Based on this background, we previously proposed phase scrambling that protects the information of the original image visually [19] [20] for POC and DCT sign phase correlation [21]. However, since phase scrambling protects only the phase information, the phase scrambling does not prevent the templates from being deduced by the magnitude of DFT coefficients (DFT magnitude) of the templates.

In the present paper, we propose a matching system in which both the phase information and the magnitude of DFT coefficients of templates are protected. First, direct DFT magnitude scrambling is considered in order to show the problem of scrambling of the DFT magnitude. Next, based on the processes of image matching, we propose a scrambling method for the DFT magnitude, in which the phase information of the log-polar transformed DFT magnitude is scrambled. In typical image matching system using POC, after alignment for rotation and scaling, the matching score is calculated. In the proposed scrambling method, not only rotated and scaled values for alignment are estimated by POC without descrambling but also the matching score can be calculated by POC without descrambling. Moreover, the values estimated by POC between signals which are scrambled with the same key are mathematically ensured to be the same as those estimated by POC between non-scrambled signals. Also, since the proposed scrambling disperse the correlation peak in the case of different key, the proposed scrambling has the effectiveness of preventing illegal image matching, which is the malicious and intentional deduction of the content of the template by POC. The experimental results of preventing illegal image matching show the effectiveness and appropriateness of the proposed method.

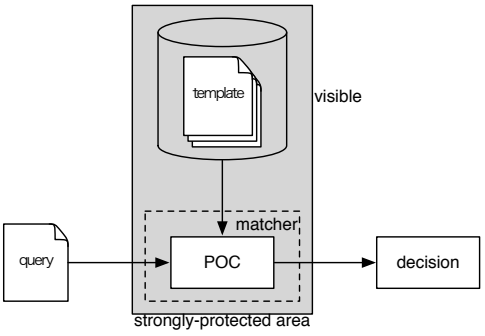
2 Preliminary

In this section, phase-only correlation and phase scrambling are explained. Single-dimensional notation is used for the sake of brevity. Integer values, n, n_1, and n_2 denote the indices of signals in the space domain, and integer values, k, k_1, and k_2 denote the indices of signals in the frequency domain.

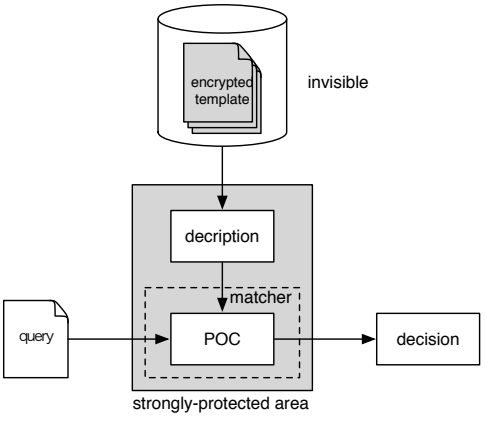
2.1 Goal of the Present Study

In an image matching system composed of a multitude of templates, template security is an important consideration. Specifically, the matching system using POC requires templates to be hidden from view, because the POC requires the templates to be either original images or phase information of original images.

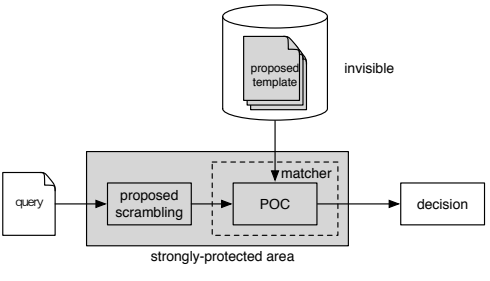
Figure 1 illustrates the relationship between the strongly protected area and matching systems using POC. Figure 1(a) shows a typical matching system using POC, in which the templates are visible, and a broad area that includes the database should be strongly protected. If the templates were leaked, the original image will be revealed. Figure 1(b) shows an encrypted template matching



(a) typical matching system using POC.



(b) encrypted template matching system using POC.



(c) proposed matching system using POC.

Fig. 1. Relationship between strongly protected area and matching systems using POC. (a) Typical matching system, in which the templates are visible and result in compromise. A broad area that includes the database should be strongly protected. (b) Encrypted template matching system, in which the templates are encrypted and invisible. However, the decryption of each template is required in the matching process. (c) Proposed matching system, in which the templates are scrambled and invisible. Instead of descrambling of each template, the proposed scrambling is required for a query in the matching process. The strongly protected area can be narrowed as suitably as the encrypted template matching system.

system using POC, in which each template for a query is decrypted, and after image matching, decrypted images should be removed, although the templates are invisible due to encryption and the strongly protected area can be narrowed. Figure 1(c) shows the proposed matching system using POC, in which templates are invisible and which can narrow the strongly protected area as suitably as the encrypted template matching system shown in Fig. 1(b). In addition, the proposed matching system can handle the protected templates directly. As a result, compared to the encrypted template matching system, the proposed matching system has high processing efficiency, because the number of the scrambling operations for a query is less than the number of the decrypting operations for a multitude of templates generally, and the removal of decrypted images is not required.

Figure 2 illustrates phase scrambling, which we proposed previously [19] [20], for visual protection. The DFT coefficients of an image are composed of the phase information and the magnitude. Once the inverse DFT is applied to either the DFT coefficients or the phase information, the information of the image is exposed, while the inverse DFT of the magnitude of DFT coefficients is invisible and does not expose the information. Based on these considerations, phase scrambling protects the templates from important information being revealed visually by distorting the phase information. However, since the DFT magnitude is untouched, the system cannot prevent the information of templates from being deduced based on the DFT magnitude.

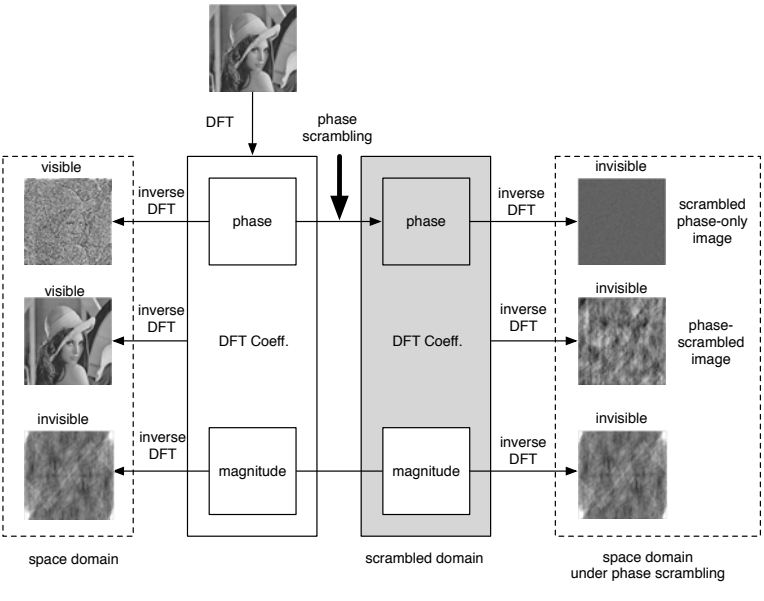


Fig. 2. Phase scrambling for visual protection. Phase scrambling protects the visual content of the original image.

In the present paper, we consider the scrambling of the DFT magnitude and an image matching system in which templates are invisible and POC can be applied without descrambling. We assume that the other levels of attacks are strongly protected, except for the case in which leakage of templates occurs.

2.2 Phase-Only Correlation (POC)

Translation. Let $G_i(k)$ be the N-point DFT coefficients of the N-point signal $g_i(n)$ which are real numbers. The phase term, $\phi_{G_i}(k)$, is defined as

$$\phi_{G_i}(k) = G_i(k)/|G_i(k)| = e^{j\theta_i(k)} \tag{1}$$

where $|G_i(k)|$ denotes the magnitude of $G_i(k) = |G_i(k)|e^{j\theta_i(k)}$, j denotes $\sqrt{-1}$, and if $|G_i(k)| = 0$, then $\phi_{G_i}(k) = e^{j\theta_i(k)}$ is replaced by zero.

Let $G_1(k)$ and $G_2(k)$ be N-point DFT coefficients of the N-point signals $g_1(n)$ and $g_2(n)$ which are real numbers, respectively. The normalized cross spectrum, $R_\phi(k)$, is defined as

$$R_\phi(k) = \phi^*_{G_1}(k) \cdot \phi_{G_2}(k) \tag{2}$$

where $\phi^*_{G_1}(k)$ denotes the complex conjugate of $\phi_{G_1}(k)$. The POC is defined by the inverse DFT of $R_\phi(k)$ as

$$r_\phi(n) = \frac{1}{N} \sum_{k=0}^{N-1} R_\phi(k) W_N^{-nk} \tag{3}$$

where W_N denotes $\exp(-j2\pi/N)$. The translation between $g_1(n)$ and $g_2(n)$ are estimated by the location n of the maximum correlation value $\gamma = \max_n (r_\phi(n))$ [2].

Rotation and scaling. In the estimation of rotated and scaled values, the magnitude of DFT coefficients (DFT magnitude) is regarded as an image in the space domain, and the coordinates of the DFT magnitude are mapped in log-polar order so that the rotated and scaled values reduce to the horizontal and vertical translations, respectively.

Let $|G_i(k_1, k_2)|$ be the $N \times N$-point DFT magnitude of the $N \times N$-point image $g_i(n_1, n_2)$. The DFT magnitude $|G_i(k_1, k_2)|$ is altered into a new image, $g_{i_{LP}}(n_1, n_2)$, consisting of the same intensity values, but arranged in new positions:

$$g_{i_{LP}}(n_1, n_2) = \mathrm{LP}\left[|G_i(k_1, k_2)|\right] \tag{4}$$

where LP denotes log-polar mapping. In the present paper, $g_{i_{LP}}(n_1, n_2)$ is referred to as the log-polar image. In practice, the intensity of the DFT magnitude is interpolated in order to convert a digital image into an analog image in the process of log-polar mapping.

Let $g_{1_{LP}}(n_1, n_2)$ and $g_{2_{LP}}(n_1, n_2)$ be log-polar images of $g_1(n_1, n_2)$ and $g_2(n_1, n_2)$, respectively. In addition, let $G_{1_{LP}}(k_1, k_2)$ and $G_{2_{LP}}(k_1, k_2)$ be the DFT coefficients of $g_{1_{LP}}(n_1, n_2)$ and $g_{2_{LP}}(n_1, n_2)$, respectively. The rotated and

scaled values are estimated from the location of the maximum correlation value, γ_{LP}, of the POC, $r_{\phi_{LP}}(n_1, n_2)$, between $g_{1_{LP}}(n_1, n_2)$ and $g_{2_{LP}}(n_1, n_2)$, that is,

$$r_{\phi_{LP}}(n_1, n_2) = \frac{1}{N^2} \sum_{k_1=0}^{N-1} \sum_{k_2=0}^{N-1} R_{\phi_{LP}}(k_1, k_2) W_N^{-n_1 k_1} W_N^{-n_2 k_2} \tag{5}$$

where

$$R_{\phi_{LP}}(k_1, k_2) = \phi^*_{G_{1_{LP}}}(k_1, k_2) \cdot \phi_{G_{2_{LP}}}(k_1, k_2) \ . \tag{6}$$

The locations n_1 and n_2 of $\gamma_{LP} = \max_{n_1, n_2} r_{\phi_{LP}}(n_1, n_2)$ correspond to the rotated and scaled values between $g_1(n_1, n_2)$ and $g_2(n_1, n_2)$, respectively [3].

2.3 Phase Scrambling

Visual protection. Phase scrambling is accomplished by multiplying N-point DFT coefficients of an N-point signal by the phase term of an N-point key sequence, $\theta_{\alpha_i}(k)$, i.e.,

$$\widetilde{G}_i(k) = G_i(k) \cdot e^{j\theta_{\alpha_i}(k)} \ . \tag{7}$$

Replacing $G_i(k)$ in Eq. (7) by its polar form yields

$$\widetilde{G}_i(k) = |G_i(k)| \phi_{G_i}(k) \cdot e^{j\theta_{\alpha_i}(k)} \ . \tag{8}$$

Therefore, phase scrambling affects only the phase of DFT coefficients,

$$\widetilde{\phi}_{G_i}(k) = \phi_{G_i}(k) \cdot e^{j\theta_{\alpha_i}(k)} \ . \tag{9}$$

The phase scrambling in Eq. (9) protects the visual information of the original image. In [19] [20], the element of a key sequence is either 0 or π, which corresponds to $\exp(j0) = 1$ or $\exp(j\pi) = -1$, respectively.

Image matching in the scrambled domain. From Eqs. (2) and (9), the normalized cross spectrum, $\widetilde{R}_\phi(k)$, under phase scrambling is given as

$$\begin{aligned} \widetilde{R}_\phi(k) &= \phi^*_{G_1}(k) \cdot \phi_{G_2}(k) \\ &= \phi^*_{G_1}(k) e^{-j\theta_{\alpha_1}(k)} \cdot \phi_{G_2}(k) e^{j\theta_{\alpha_2}(k)} \ . \end{aligned} \tag{10}$$

If $\theta_{\alpha_1}(k) = \theta_{\alpha_2}(k)$, then

$$e^{-j\theta_{\alpha_1}(k)} \cdot e^{j\theta_{\alpha_2}(k)} = 1 \ . \tag{11}$$

Therefore, from Eqs. (2), (10), and (11), we obtain

$$\widetilde{R}_\phi(k) = R_\phi(k) \ . \tag{12}$$

There is no effect of scrambling on the normalized cross spectrum in the case of the same key sequences. That is, mathematically, the translation and the maximum correlation value estimated by the POC between non-scrambled signals can be obtained from the POC between two signals which are scrambled with the same key sequences.

2.4 A Key Sequence and Its Update

A key sequence. The length of a key sequence is required the length of a signal, i.e., N-point key sequence is required for scrambling of an N-point signal. The N-point key sequence, $\theta_{\alpha_i}(k)$, $k = 0, 1, \cdots, N-1$, is determined from a set $U_{x_1}^M$ that consists of M-member, x_1,x_2,$\cdots$,x_M, $(M \leq N)$, i.e.,

$$\theta_{\alpha_i}(k) \in U_{x_1}^M, \quad U_{x_1}^M = \{x_1, x_2, \cdots, x_M\} \ . \tag{13}$$

In two-dimensional expression, $N \times N$-point key sequence, $\theta_{\alpha_i}(k_1, k_2)$, $k_1 = 0, 1, \cdots, N-1$, $k_2 = 0, 1, \cdots, N-1$ is required for scrambling an $N \times N$-point signal. In [19] [20], the element of a key sequence is in $U_0^2 = \{0, \pi\}$, which corresponds to $\exp(j0) = 1$ or $\exp(j\pi) = -1$. Generally, the element of a key sequence can be set using random numbers with a key, α_i. In the case of using random numbers, phase scrambling is analogous to a stream cipher [22]. The key space of the key sequence is determined from the size of image, $N \times N$, the number of members, M, and how to generate random numbers. If true random numbers are generated, the key space is $M^{N \times N}$.

The effectiveness of preventing illegal image matching is considered in terms of probability. A large number of the cases in which the value of an element of a key sequence is different from the value of the corresponding element of another key sequence increases the effectiveness of preventing illegal image matching. Let two key sequences be $\theta_{\alpha_1}(k)$ and $\theta_{\alpha_2}(k)$, where $\theta_{\alpha_i}(k) \in U_{x_1}^2$ and $U_{x_1}^2 = \{x_1, x_2\}$. Let q_{x_1} be the occurrence probability of x_1 per element. The probability, $Q_2(q_{x_1}, q_{x_2})$, that satisfies $\theta_{\alpha_1}(k) = \theta_{\alpha_2}(k)$ for any k is given as

$$Q_2(q_{x_1}, q_{x_2})|_{q_{x_1}=1-q_{x_2}} = q_{x_1}^2 + (1-q_{x_1})^2 = 2\left(q_a - \frac{1}{2}\right)^2 + \frac{1}{2} \ . \tag{14}$$

Therefore, $Q_2(q_{x_1}, q_{x_2})$ gives the minimum value of $1/2$ when $q_{x_1} = 0.5$. The effectiveness of preventing illegal image matching with $q_{x_1} = 0.5$ will be shown in Section 4.

Next, a set with M-member $U_{x_1}^M$ is considered. We assume that each occurrence probability q_{x_i}, $i = 1, 2, \cdots, M$ is the same. The probability, $Q_M(q_{x_1}, q_{x_2}, \cdots, q_{x_M})$, that satisfies $\theta_{\alpha_1}(k) = \theta_{\alpha_2}(k)$ for any k is given as

$$Q_M(q_{x_1}, q_{x_2}, \cdots, q_{x_M})\big|_{q_{x_1}=q_{x_2}=\cdots=q_{x_M}} = M\frac{1}{M^2} = \frac{1}{M} \ . \tag{15}$$

A large number of members in a set enhances the effectiveness of preventing illegal image matching with respect to coincident probability [23].

Update of a key sequence. The key sequence is renewable. At regular intervals or when the database has been accessed illegally, the key sequence can be renewed, and the templates can be updated without descrambling. The updated key sequence $\theta'_{\alpha_i}(k)$ is given by the addition of new key sequence $\eta_{\alpha_i}(k)$ as

$$\theta'_{\alpha_i}(k) = \theta_{\alpha_i}(k) + \eta_{\alpha_i}(k) \ . \tag{16}$$

For instance, the phase term protected by scrambling with key sequence $\theta_{\alpha_i}(k)$ can be updated directly by multiplying $\widetilde{\phi}_i(k) = \phi_i(k)e^{j\theta_{\alpha_i}(k)}$ by $\exp(j\eta_{\alpha_i}(k))$:

$$\begin{aligned}\widetilde{\phi}'_i(k) &= \phi_i(k)e^{j\theta_{\alpha_i}(k)} \cdot e^{j\eta_{\alpha_i}(k)} \\ &= \phi_i(k)e^{j\theta'_{\alpha_i}(k)} \ . \end{aligned} \tag{17}$$

The updated key sequence, $\theta'_{\alpha_i}(k)$, is used for a query in the matching process after updating the templates.

3 Scrambling for the DFT Magnitude

We propose a scrambling method for the DFT magnitude, in which the phase information of log-polar image is scrambled, in order to prevent illegal image matching.

3.1 Direct DFT Magnitude Scrambling

In order to clarify the problem of scrambling of the DFT magnitude, direct DFT magnitude scrambling is introduced. Direct DFT magnitude scrambling is based on an analogy of phase scrambling. Direct DFT magnitude scrambling is accomplished by multiplying the $N \times N$-point key sequence $r_{\beta_i}(k_1, k_2)$ by the DFT magnitude, where $r_{\beta_i}(k_1, k_2) \in \mathbb{R}$ and $\mathbb{R}$ denotes a set of real numbers.

In direct DFT magnitude scrambling, the scrambled DFT magnitude, $\widetilde{G}_i(k_1, k_2)$, is given as

$$\widetilde{G}_i(k_1, k_2) = |G_i(k_1, k_2)| \cdot r_{\beta_i}(k_1, k_2) \ . \tag{18}$$

From Eq. (4), the scrambled log-polar image $\widetilde{g}_{i_{LP}}(n_1, n_2)$ is given as

$$\widetilde{g}_{i_{LP}}(n_1, n_2) = \mathrm{LP}\left[|G_i(k_1, k_2)|\, r_{\beta_i}(k_1, k_2)\right] \ . \tag{19}$$

If $r_{\beta_i}(k_1, k_2)$ is a constant, C_i, for all k_1 and k_2, then $\widetilde{g}_{i_{LP}}(n_1, n_2)$ is expressed as

$$\widetilde{g}_{i_{LP}}(n_1, n_2) = C_i g_{i_{LP}}(n_1, n_2) \ . \tag{20}$$

In this case, the normalized cross spectrum $\widetilde{R}_{\phi_{LP}}(k_1, k_2)$ between $\widetilde{g}_{1_{LP}}(n_1, n_2)$ and $\widetilde{g}_{2_{LP}}(n_1, n_2)$ is equal to $R_{\phi_{LP}}(k_1, k_2)$. In other words, illegal image matching is not prevented. Moreover, if $r_{\beta_i}(k_1, k_2)$ is not a constant, then $\widetilde{g}_{i_{LP}}(n_1, n_2)$ cannot be expressed by the non-scrambled log-polar image, $g_{i_{LP}}(n_1, n_2)$, because of the practical limitation that occurs as a result of the interpolation applied during transformation into log-polar coordinates. Even if interpolation does not affect the log-polar mapping, the scrambling of a log-polar image cannot be canceled by the scrambling with the same key sequence. Namely, the rotation angle and scale factor cannot be estimated correctly by POC under scrambling. Therefore, direct DFT magnitude scrambling is not useful in achieving our goal.

3.2 Phase Scrambling of Log-Polar Image

We propose a scrambling method for the DFT magnitude, which involves scrambling the phase information of a log-polar image that is converted from the DFT magnitude. Theoretically, the proposed method not only ensures the same values estimated by POC between non-scrambled images but also reduces the computational load for descrambling of templates in a system.

Let $G_{i_{LP}}(k_1, k_2)$ be the $N \times N$-point DFT coefficients of $N \times N$-point log-polar image $g_{i_{LP}}(n_1, n_2)$. The scrambled DFT coefficients, $\widetilde{G}_{i_{LP}}(k_1, k_2)$, are obtained by multiplying $G_{i_{LP}}(k_1, k_2)$ by the phase term of an $N \times N$-point key sequence $\theta_{\beta_i}(k_1, k_2)$:

$$\widetilde{G}_{i_{LP}}(k_1, k_2) = G_{i_{LP}}(k_1, k_2) \cdot e^{j\theta_{\beta_i}(k_1, k_2)} \ . \tag{21}$$

The normalized cross spectrum $\widetilde{R}_{\phi_{LP}}(k_1, k_2)$ between $\widetilde{G}_{1_{LP}}(k_1, k_2)$ and $\widetilde{G}_{2_{LP}}(k_1, k_2)$ is given as

$$\widetilde{R}_{\phi_{LP}}(k_1, k_2) = \phi^*_{G_{1_{LP}}}(k_1, k_2) e^{-j\theta_{\beta_1}(k_1, k_2)} \cdot \phi_{G_{2_{LP}}}(k_1, k_2) e^{j\theta_{\beta_2}(k_1, k_2)} \ . \tag{22}$$

If $\theta_{\beta_1}(k_1, k_2) = \theta_{\beta_2}(k_1, k_2)$, then

$$\widetilde{R}_{\phi_{LP}}(k_1, k_2) = R_{\phi_{LP}}(k_1, k_2) \ . \tag{23}$$

As long as the same interpolation method is used, the relative rotated and scaled values are preserved. In addition, the proposed method protects templates from illegal image matching.

The proposed scrambling is to scramble both phase information and DFT magnitude of an image. Figure 3 summarizes the steps of the proposed scrambling.

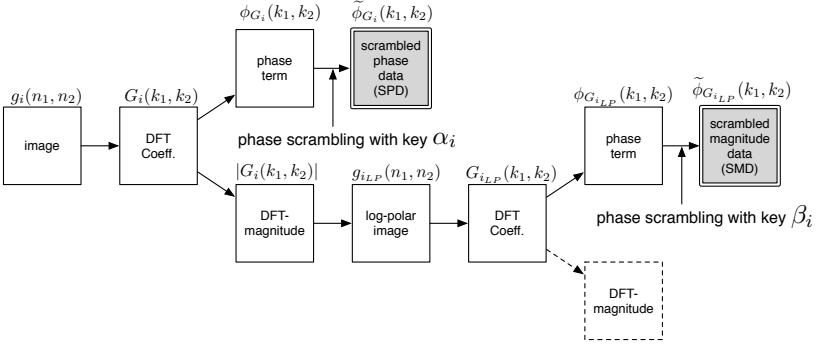


Fig. 3. Proposed scrambling. The DFT coefficients of an image are separated into the phase term and the DFT-magnitude. The phase term is directly phase-scrambled to obtain the scrambled phase data (SPD) with a key, α_i, while the DFT magnitude is transformed into a log-polar image, and the phase term of the log-polar image is phase-scrambled to obtain the scrambled magnitude data (SMD) with a key, β_i. The SPD and SMD can be used for POC.

3.3 System Model

Figure 4 shows a model of a system. The system has two main processes, namely, the template generation process and the image matching process. The steps of these two main processes are explained below.

Template generation process. Images are stored as templates in a database through the proposed scrambling. All templates registered in the database are scrambled by independent key sequences. Note that an independent key may be managed by individual.

The steps are as follows:

1. The DFT is applied to an image to obtain the DFT coefficients.
2. The phase term of the DFT coefficients is phase-scrambled with a key, α_i, to obtain the scrambled phase data (SPD).
3. The DFT magnitude, as shown in Fig. 5(b), is converted into a log-polar image (see Fig. 5(c)).
4. The DFT is applied to the log-polar image to obtain the DFT coefficients.

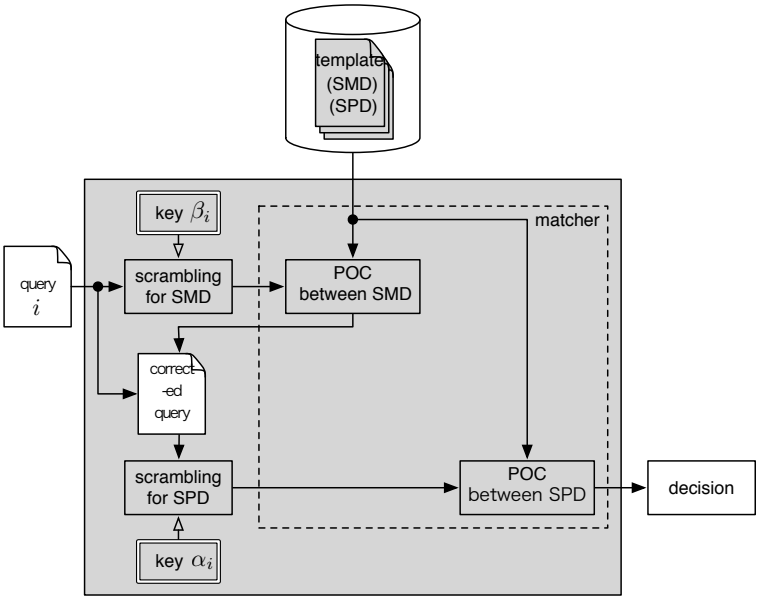
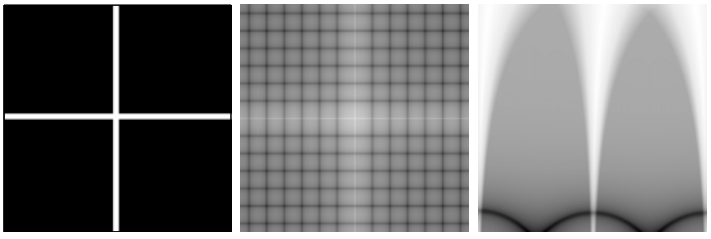
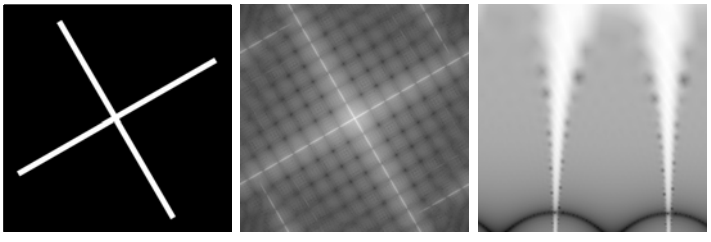


Fig. 4. System model (correction of rotation and scaling is required). When the database is queried, the scrambling for SMD is applied to a query, and POC between the SMD of the query and that of a template is calculated for correction of rotation and scaling of the query. After the corrected query is scrambled to obtain the SPD, the POC between the SPD of the corrected query and that of the template is calculated to obtain the matching score.



(a) original image (b) DFT-magnitude of the original image (c) log-polar image of the original image



(d) rotated image (e) DFT magnitude of the rotated image (f) log-polar image of the rotated image

Fig. 5. Rotated image and log-polar image. (a) 512×512 monochrome image. (b) DFT magnitude of (a). (c) Log-polar image of (b). (d) Rotated image of (a). (e) DFT magnitude of (d). (f) Log-polar image of (e).

5. The phase term of the DFT coefficients of the log-polar image is phase-scrambled with a key, β_i, to obtain the scrambled magnitude data (SMD).
6. The SPD and SMD are stored as a template.

Image matching process. The image matching process consists of alignment steps and matching steps. The alignment steps are performed in order to align a query or to call a template for matching steps in the database. The matching steps are performed in order to obtain the maximum correlation value used as a matching score.

Alignment steps

1. The DFT is applied to a query to obtain a DFT magnitude (see Fig. 5 (e)).
2. The DFT magnitude is transformed into a log-polar image (see Fig. 5 (f)).
3. The DFT is applied to the log-polar image to obtain the phase term of the DFT coefficients of the log-polar image.
4. The phase term is phase-scrambled with key β_i to obtain the SMD.
5. The POC between the SMD of the query and that of a template is calculated to estimate the rotated and scaled values.
6. The query is aligned by the estimated values to generate the corrected query.

In a typical matching system using POC, after alignment for rotation and scaling, the matching score is calculated. Therefore, among the alignment steps

mentioned above, Step 4 is the only additional step for the proposed scrambling.

Matching steps

1. The DFT is applied to the corrected query to obtain the DFT coefficients.
2. The phase term of the DFT coefficients is scrambled with key α_i to obtain the SPD of the corrected query.
3. The POC between the SPD of the corrected query and that of the template is performed to obtain the maximum correlation value.

As compared to a typical matching system using POC, Step 2 is the only additional step for the proposed scrambling.

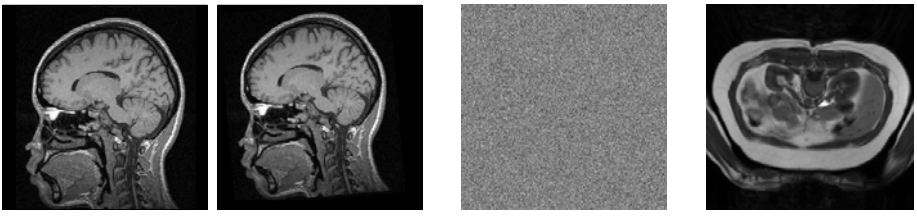
4 Simulation

In the following simulations, $N \times N$-point key sequences $\theta_{\alpha_i}(k_1, k_2)$ and $\theta_{\beta_i}(k_1, k_2)$ were determined from a two-member set $U^2_{\pi/2} = \{\pi/2, -\pi/2\}$ in Eq. (13). The occurence probability $x_{\pi/2}$ was 0.5.

4.1 Image Matching under the Proposed Scrambling

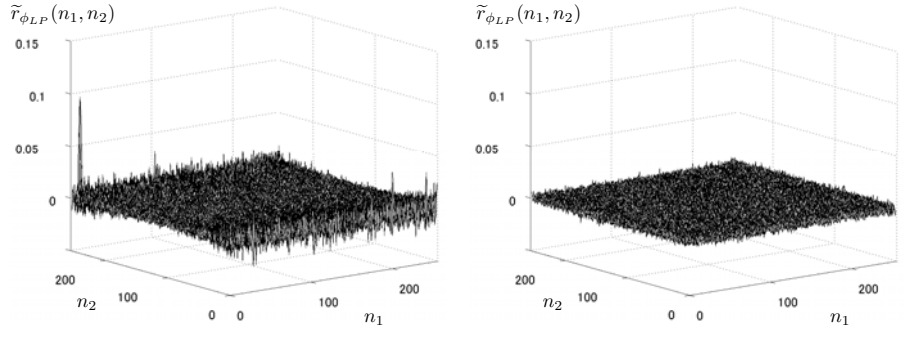
Image matching between two images, namely, a template and a query, was performed using POC. The query shown in Fig. 6(b) is generated from the template, which is the 256×256 8-bit monochrome image shown in Fig. 6(a), by translation, rotation and scaling, in which the rotation angle, φ, was five degrees and the scale factor, s, was 0.95. The POC between the template and the query was calculated in order to estimate the rotation angle and the scale factor. The estimated rotation angle, $\hat{\phi}$, and scale factor, $\hat{s}$, were 4.941 and 0.947, respectively. After correcting the query using $\hat{\phi}$ and $\hat{s}$, the POC between the template and the corrected query was calculated in order to obtain the maximum correlation value. The maximum correlation value, γ, was 0.495.

Next, the template was scrambled to obtain the SPD by Eq. (7) and SMD by Eq. (21) with the key sequences $\theta_{\alpha_1}(k_1, k_2)$ for SPD and $\theta_{\beta_1}(k_1, k_2)$ for SMD. Figure 6(c) shows the scrambled phase-only image of the template that is the inverse DFT of the SPD of the template. We can confirm that the original information of the template cannot be deduced by SPD. After the query was scrambled with the key sequence $\theta_{\beta_2}(k_1, k_2)$ to obtain the SMD, the POC between the SMD of the template and the SMD of the query was performed. Figures 7(a) and 7(b) show the POC surface between the SMDs with the same key sequences and the POC surface between the SMDs with different key sequences, respectively. In the case of using the same key sequences, i.e., $\theta_{\beta_1}(k_1, k_2) = \theta_{\beta_2}(k_1, k_2)$, the estimated rotation angle under scrambling, $\widetilde{\varphi}$, and the estimated scale factor under scrambling, $\widetilde{s}$, were 4.941 and 0.947, respectively, i.e., $\widetilde{\varphi} = \hat{\varphi}$ and $\widetilde{s} = \hat{s}$. We confirmed that the POC surface between the SMD of the template and the SMD of the query and the POC surface between non-scrambled images were



(a) template (b) query (head) (c) scrambled phase-only image of image (a) (d) query (liver)

Fig. 6. Test images. (a) 256×256 8-bit monochrome image. (b) Image generated from (a) by translation by five pixels in the horizontal and vertical directions, rotation by five degrees about the center of the image, and scaling by 0.95. (c) Scrambled phase-only image of (a). (d) 256×256 8-bit monochrome image.



(a) with the same key sequences (b) with different key sequences.

Fig. 7. POC surface between the SMDs with the same key sequences and the SMDs with different key sequences. (a) When $\theta_{\beta_1}(k_1, k_2) = \theta_{\beta_2}(k_1, k_2)$, a distinct peak appears on the POC surface. (b) When $\theta_{\beta_1}(k_1, k_2) \neq \theta_{\beta_2}(k_1, k_2)$, no distinct peak appears on the POC surface.

identical as derived in Eq. (23). In the case of using different key sequences, i.e., $\theta_{\beta_1}(k_1, k_2) \neq \theta_{\beta_2}(k_1, k_2)$, $\widetilde{\varphi}$ and $\widetilde{s}$ were 32.4 and 3.03, respectively, i.e., $\widetilde{\varphi} \neq \hat{\varphi}$ and $\widetilde{s} \neq \hat{s}$. The rotation angle and scale factor could not be estimated correctly in the different key sequences. On the other hand, when only the phase information was scrambled, the POC surface under scrambling and the POC surface under non-scrambling were identical, although different key sequences were used.

After the query was corrected by $\widetilde{\varphi}$ and $\widetilde{s}$, the corrected query was scrambled with the key sequence, $\theta_{\alpha_2}(k_1, k_2)$, to obtain the SPD. The POC between the SPD of the template and the SPD of the corrected query was then performed. Figure 8 shows the POC surface between the SPDs with the same key sequences, in which the maximum correlation value under scrambling $\widetilde{\gamma}$ was 0.495, i.e., $\widetilde{\gamma} = \gamma$. The POC surface between the SPDs shown in Fig. 8 and the POC surface between non-scrambled images after correcting were identical. The proposed

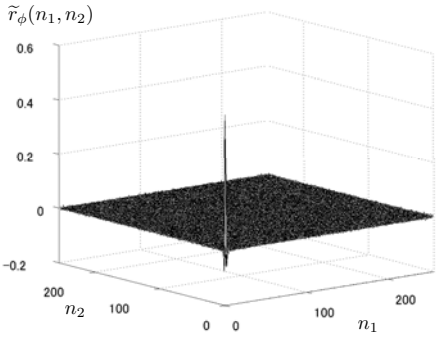


Fig. 8. POC surface between the SPDs with the same key sequences. A distinct peak appears on the POC surface. The POC surface between the SPDs and the POC surface between non-scrambled images after correcting were identical.

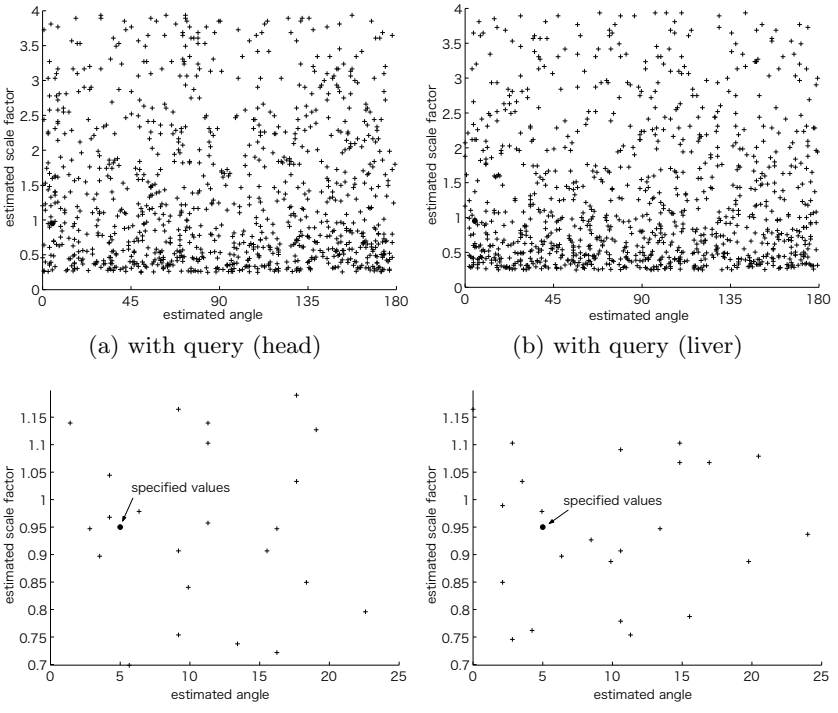
scrambling does not affect the values estimated by POC as derived in Eq. (12) mathematically, and has the effectiveness of preventing illegal image matching. The time for single scrambling was 18.7% of the time for single POC between two images, where the time was the average of 100 operations.

4.2 Effectiveness of Preventing Illegal Image Matching

The rotation angle and the scale factor were estimated by the POC between the SMD of the template and the SMD of the query. A total of 1000 different key sequences were used. The template shown in Fig. 6(a) was scrambled with $\theta_{\beta_0}(k_1, k_2)$ to obtain the SMD of the template. The query was rotated by φ degrees, scaled by s and scrambled with $\theta_{\beta_i}(k_1, k_2)$, $i = 1, 2, \cdots, 1000$ where $\theta_{\beta_0}(k_1, k_2) \neq \theta_{\beta_i}(k_1, k_2)$ to obtain the SMD of the query. $\widetilde{\varphi}$ and $\widetilde{s}$ are calculated from the location of the maximum correlation value under scrambling, $\widetilde{\gamma_{LP}}$.

Figure 9(a) shows 1000 sets of $\widetilde{\varphi}$ and $\widetilde{s}$ when Fig. 6(b) was used as the query where $\varphi = 5$ and $s = 0.95$, and Fig. 9(b) shows 1000 sets of $\widetilde{\varphi}$ and $\widetilde{s}$ when Fig. 6(d) was used as the query where $\varphi = 5$ degree and $s = 0.95$. The dispersion of 1000 sets shown in Fig. 9(a) in which the query was the same as the template was similar to the dispersion of 1000 sets shown in Fig. 9(b) in which the query was different from the template. Therefore, we can conclude that the proposed scrambling has the effect of preventing illegal image matching by POC in order to deduce the template. Figures 9(c) and 9(d) show the magnification of Figs 9(a) and 9(b), respectively. There was no point in which $\widetilde{\varphi} = \hat{\varphi}$ and $\widetilde{s} = \hat{s}$. In addition, $\widetilde{\gamma_{LP}}$ around the specified values (φ and s) were less than 25 % of the maximum correlation value under non-scrambling, γ_{LP}.

Figures 10(a) and 10(b) show the magnification of 1000 sets of $\widetilde{\varphi}$ and $\widetilde{s}$ estimated by the POC of the SMD of the template with the SMD of the query (head) and with the SMD of the query (liver), respectively, where $\varphi = 10$ and $s = 1.05$. Figures 10(c) and 10(d) show the magnification of 1000 sets of $\widetilde{\varphi}$ and $\widetilde{s}$ estimated



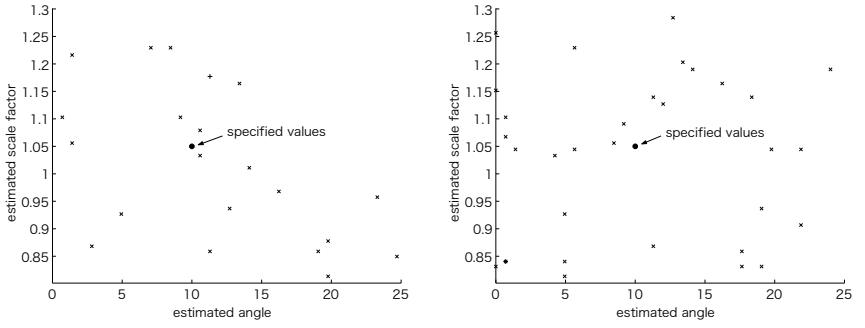
(a) with query (head) (b) with query (liver)

(c) magnification of (a) (d) magnification of (b)

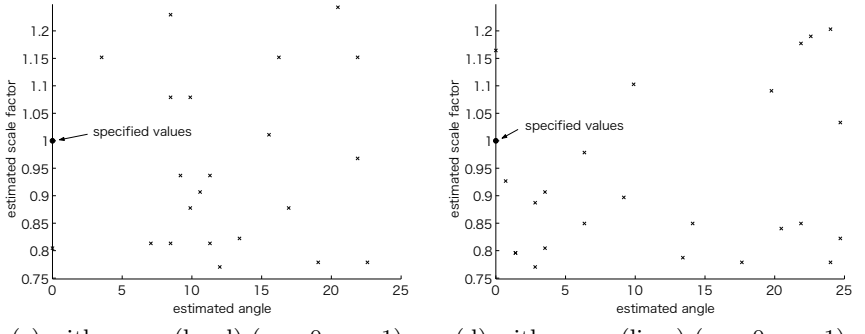
Fig. 9. Effectiveness of preventing illegal image matching ($\varphi = 5$ and $s = 0.95$). A total of 1000 different key sequences are used. The '+' plots denote that $\widetilde{\gamma_{LP}}$ is greater than or equal to 10% of γ_{LP} and less than 25% of γ_{LP}. (a) 1000 sets of $\widetilde{\varphi}$ and $\widetilde{s}$ estimated by the POC of the SMD of the template with the SMD of the query (head). (b) 1000 sets of $\widetilde{\varphi}$ and $\widetilde{s}$ estimated by the POC of the SMD of the template with the SMD of the query (liver). (c) Magnification of (a). (d) Magnification of (b).

by POC of the SMD of the template with the SMD of the query (head) and with the SMD of the query (liver), respectively, where $\varphi = 0$ and $s = 1$.

The histograms of $\widetilde{\varphi}$ and $\widetilde{s}$ in Figs. 9(a), 10(a), and 10(c) are shown in Figs 11(a), 11(b), and 11(c), respectively. When $\varphi = 5$, the mean and variance of the estimated rotation angle are 91.6 degrees and 2817.5, respectively. When $s = 0.95$, the mean and variance of the estimated scale factor are 1.41 and 1.0869, respectively. When $\varphi = 10$, the mean and variance of estimated rotation angle were 90.0 degrees and 2709.6, respectively. When $s = 1.05$, the mean and variance of estimated scale factor are 1.34 and 0.9972, respectively. When $\varphi = 0$, the mean and variance of the estimated rotation angle are 101.4 degrees and 2625.5, respectively. When $s = 1$, the mean and variance of the estimated scale factor are 1.30 and 0.9436, respectively. From these results, the mean and variance resemble the other mean and variance, and have no outstanding



(a) with query (head) ($\varphi = 10$, $s = 1.05$) (b) with query (liver) ($\varphi = 10$, $s = 1.05$)



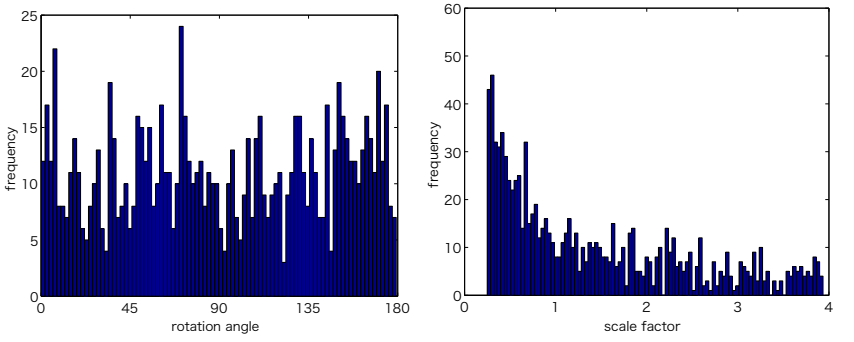
(c) with query (head) ($\varphi = 0$, $s = 1$) (d) with query (liver) ($\varphi = 0$, $s = 1$)

Fig. 10. Effectiveness of preventing illegal image matching ($\varphi = 10$, $s = 1.05$ and $\varphi = 0$, $s = 1$). A total of 1000 different key sequences are used. The 'x' plots denote that $\widetilde{\gamma_{LP}}$ is less than 10% of γ_{LP}. The '+' plots denote that $\widetilde{\gamma_{LP}}$ is greater than or equal to 10% of γ_{LP} and less than 25% of γ_{LP}. (a) Magnification of 1000 sets of $\widetilde{\varphi}$ and $\widetilde{s}$ estimated by the POC between the SMD of the template and the SMD of the query (head) ($\varphi = 10$, $s = 1.05$). (b) Magnification of 1000 sets of $\widetilde{\varphi}$ and $\widetilde{s}$ estimated by the POC between the SMD of the template and the SMD of the query (liver) ($\varphi = 10$, $s = 1.05$). (c) Magnification of 1000 sets of $\widetilde{\varphi}$ and $\widetilde{s}$ estimated by the POC between the SMD of the template and the SMD of the query (head) ($\varphi = 0$, $s = 1$). (d) Magnification of 1000 sets of $\widetilde{\varphi}$ and $\widetilde{s}$ estimated by the POC between the SMD of the template and the SMD of the query (liver) ($\varphi = 0$, $s = 1$).

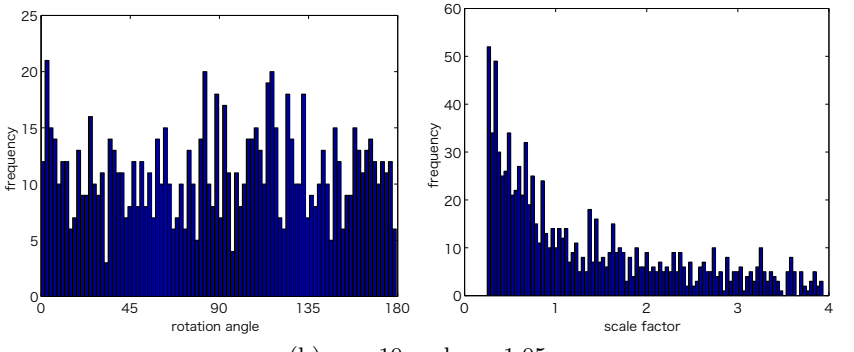
characteristic. Therefore, it is difficult to deduce the template by POC using local images. We can confirm the effectiveness of preventing illegal image matching of the proposed method.

4.3 Histogram of the DFT Magnitude

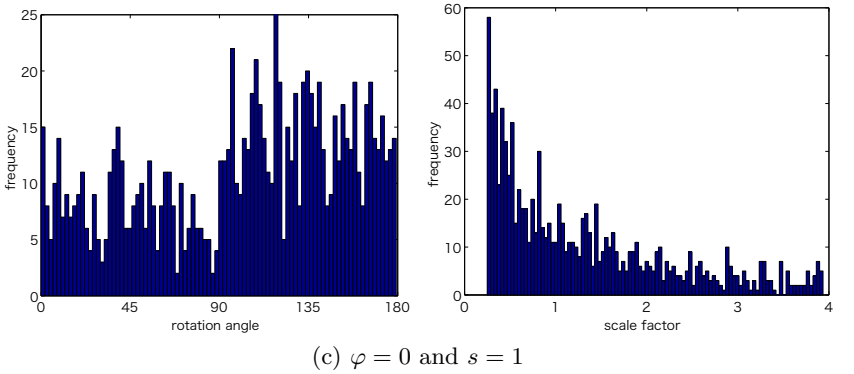
Figure 12 shows three histograms for the process of generating SMD. The intensity is normalized. Figure 12(a) shows the histogram of the DFT magnitude of the image shown in Fig. 6(a). Figure 12(b) shows the histogram of the log-polar image mapped from 12(a). The histogram is changed by log-polar mapping, in which



(a) $\varphi = 5$ and $s = 0.95$

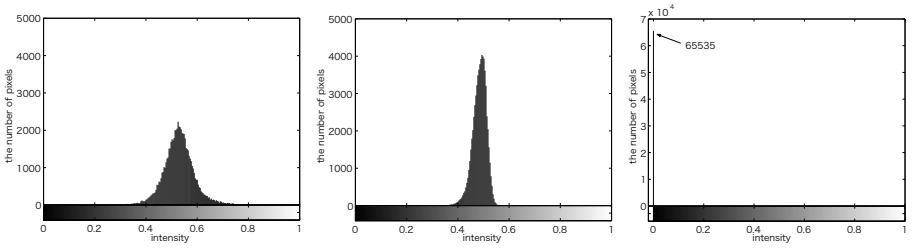


(b) $\varphi = 10$ and $s = 1.05$



(c) $\varphi = 0$ and $s = 1$

Fig. 11. Histograms of $\widetilde{\varphi}$ and $\widetilde{s}$ estimated by the POC between the SMD of the template and the SMD of the query (head). (a) $\varphi = 5$ and $s = 0.95$. The mean and variance of the estimated rotation angle are 91.6 degrees and 2817.5, respectively. The mean and variance of the estimated scale factor are 1.41 and 1.0869, respectively. (b) $\varphi = 10$ and $s = 1.05$. The mean and variance of estimated rotation angle are 90.0 degrees and 2709.6, respectively. The mean and variance of estimated scale factor are 1.34 and 0.9972, respectively. (c) $\varphi = 0$ and $s = 1$. The mean and variance of the estimated rotation angle are 101.4 degrees and 2625.5, respectively. The mean and variance of the estimated scale factor are 1.30 and 0.9436, respectively.



(a) DFT magnitude (b) Log-polar image (c) Inverse DFT of the absolute value of the SMD

Fig. 12. Histograms for the process of generating SMD. The intensity is normalized. (a) DFT magnitude of the template. (b) Log-polar image. When DFT magnitude is mapped into a log-polar image, the histogram is changed due to interpolation and unused points. (c) Inverse DFT of the absolute value of the SMD. Since the SMD is generated from the phase information of the log-polar image, it is difficult to deduce (a) from (c).

interpolation is performed and a number of points in the DFT-magnitude are not used. Figure 12(c) shows the histogram of the inverse DFT of the absolute value of the SMD. Since the SMD is generated from the phase information of the log-polar image, the characteristics of the DFT magnitude is hidden, and it is difficult to deduce Fig. 12(a) from Fig. 12(c) except for phase-based matching. The proposed scrambling is confirmed to protect the DFT magnitude of an image.

5 Conclusion

We have proposed a scrambling method for the DFT magnitude and an image matching system. After describing the problem of scrambling for the DFT magnitude by direct DFT magnitude scrambling, we have shown that the scrambling of the transformed DFT magnitude is effective in preventing illegal image matching. We have shown mathematically that POC can be directly applied to images in the proposed scrambled domain and that the same values under non-scrambling are obtained from the proposed scrambled domain. The prevention of illegal image matching was evaluated through simulations to show the effectiveness of the proposed method.

References

1. Knapp, C.H., Carter, G.C.: The Generalized Correlation Method for Estimation of Time Delay. IEEE Trans. Acoust., Speech, Signal Process. ASSP-24(4), 320–327 (1976)
2. Kuglin, C.D., Hines, D.C.: The Phase Correlation Image Alignment Method. In: Proc. Int. Conf. Cybernetics and Society, pp. 163–165 (1975)
3. Chen, Q., Defrise, M., Deconinck, F.: Symmetric Phase-only Matched Filtering of Fourier-Mellin Transforms for Image Registration and Recognition. IEEE Trans. Pattern Anal. Mach. Intell. 16(2), 1156–1168 (1994)

4. Thévenaz, P., Ruttimann, U.E., Unser, M.: A Pyramidal Approach to Subpixel Registration Based on Intensity. IEEE Trans. Image Process. 7(1), 27–41 (1998)
5. Foroosh, H., Zerubia, J., Berthod, M.: Extension of Phase Correlation to Sub-pixel Registration. IEEE Trans. Image Process. 11(3), 188–200 (2002)
6. Hoge, W.S.: A Subspace Identification Extension to the Phase Correlation Method. IEEE Trans. Med. Imag. 22(2), 277–280 (2003)
7. Foroosh, H., Balci, M.: Sub-pixel Registration and Estimation of Local Shifts Directly in the Fourier Domain. In: Proc. IEEE Int. Conf. Image Process. vol. 3, pp. 1915–1918 (2004)
8. Balci, M., Foroosh, H.: Subpixel Estimation of Shifts Directly in the Fourier Domain. IEEE Trans. Image Process. 15(7), 1965–1972 (2006)
9. Takita, K., Aoki, T., Sasaki, Y., Higuchi, T., Kobayashi, K.: High-accuracy Subpixel Image Registration Based on Phase-Only Correlation. IEICE Trans. Fundamentals E86-A(8), 1925–1934 (2003)
10. Ito, K., Nakajima, H., Kobayashi, K., Aoki, T., Higuchi, T.: A Fingerprint Matching Algorithm Using Phase-Only Correlation. IEICE Trans. Fundamentals E87-A(3), 682–691 (2004)
11. Ito, K., Nikaido, A., Aoki, T., Kosuge, E., Kawamata, R., Kashima, I.: A Dental Radiograph Recognition System Using Phase-Only Correlation for Human Identification. IEICE Trans. Fundamentals E91-A(1), 298–305 (2008)
12. Ito, K., Aoki, T., Nakajima, H., Kobayashi, K., Higuchi, T.: A Palmprint Recognition Algorithm Using Phase-Only Correlation. IEICE Trans. Fundamentals E91-A(4), 1023–1030 (2008)
13. Miyazawa, K., Ito, K., Aoki, T., Kobayashi, K., Nakajima, H.: An Effective Approach for Iris Recognition Using Phase-based Image Matching. IEEE Trans. Pattern Anal. Mach. Intell. 30(10), 1741–1756 (2008)
14. Jain, A.K., Ross, A., Pankanti, S.: Biometrics: A Tool for Information Security. IEEE Trans. Inf. Forensics Security 1(2), 125–143 (2006)
15. Fujiyoshi, M., Saitou, W., Watanabe, O., Kiya, H.: Hierarchical Encryption of Multimedia Contents for Access Control. In: Proc. IEEE Int. Conf. Image Process., pp. 1977–1980 (2006)
16. Kuroiwa, K., Fujiyoshi, M., Kiya, H.: Codestream Domain Scrambling of Moving Objects Based on DCT Sign-Only Correlation for Motion JPEG Movies. In: Proc. IEEE Int. Conf. Image Process., vol. V, pp. 157–160 (2007)
17. Bianchi, T., Piva, A., Barni, M.: Implementing the Discrete Fourier Transform in the Encrypted Domain. In: Proc. IEEE Int. Conf. Acoust., Speech Signal Process., pp. 1757–1760 (2008)
18. Bianchi, T., Piva, A., Barni, M.: Comparison of Different FFT Implementations in the Encrypted Domain. In: Proc. 16^{th} European Signal Process. Conf. (2008)
19. Kiya, H., Ito, I.: Image Matching between Scrambled Images for Secure Data Management. In: Proc. 16^{th} European Signal Process. Conf. (2008)
20. Ito, I., Kiya, H.: A New Class of Image Registration for Guaranteeing Secure Data Management. In: Proc. IEEE Int. Conf. Image Process., pp. 269–272 (2008)
21. Ito, I., Kiya, H.: DCT Sign-Only Correlation with Application to Image Matching and the Relationship with Phase-Only Correlation. In: Proc. IEEE Int. Conf. Acoust., Speech Signal Process., vol. 1, pp. 1237–1240 (2007)
22. Schneier, B.: Applied Cryptography. John Wiley & Sons, Inc., Chichester (1996)
23. Ito, I., Kiya, H.: Phase scrambling for blind image matching. In: Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing, pp. 1521–1524 (2009)