20

Phase Scrambling for Image Matching in the Scrambled Domain

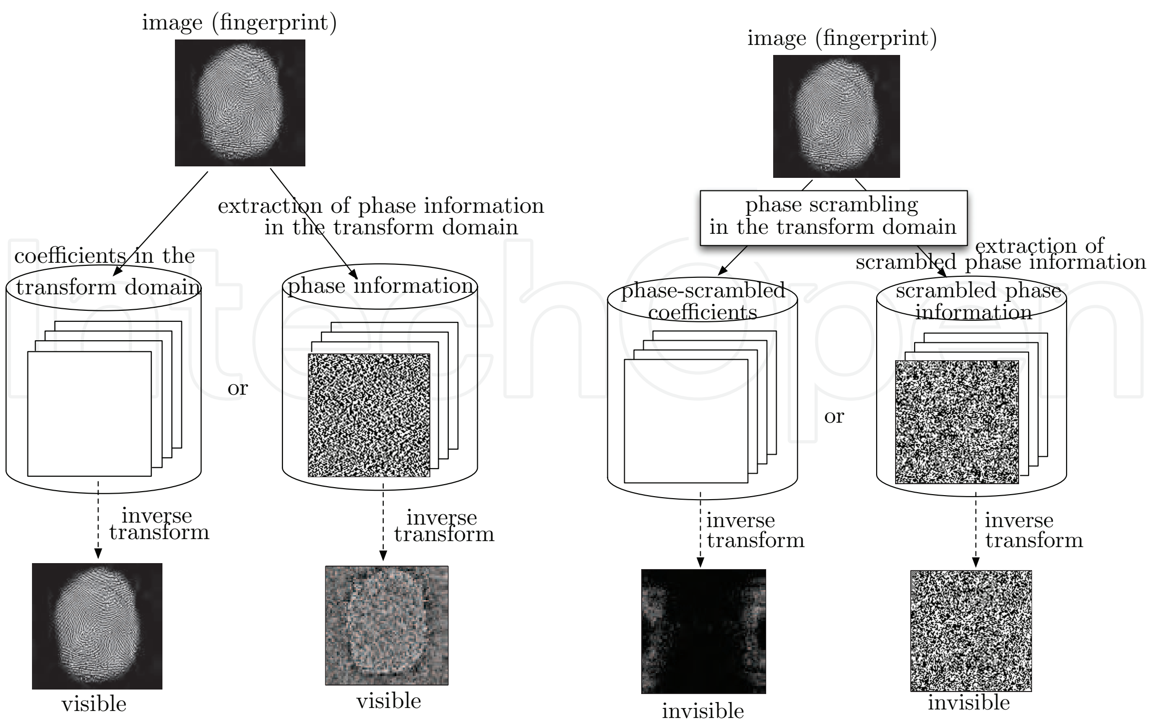
Hitoshi Kiya and Izumi Ito
Graduate School of System Design, Tokyo Metropolitan University
6-6 Asahigaoka, Hino-shi, Tokyo, Japan

1. Introduction

In recent years, signal matching has been required in many fields. A number of matching methods have been developed, and an appropriate method should be selected for each application in order to obtain the desired performance (1)(2). Phase-only correlation (POC), phase correlation or PHAse Transform (PHAT) (3)-(17), which is referred to herein as POC, is a phase-based correlation that is used for various applications, such as delay estimation (3)(4), motion estimation (5), registration (6)(7), video detection (8)(9), and biometrics authentication (10)(11). Phase-only correlation with Fourier transform was developed as PHAT in sound/sonar processing literature (3), and POC with discrete Fourier transform was proposed by Kuglin and Hines (12). The concept of POC is based on the fact that the information related to the displacement of two signals resides in the phase of the cross spectrum. Combining POC with various techniques, such as interpolation and curve fitting, provides highly accurate estimation (13)-(17). In special cases, the normalized cross spectrum corresponds to the product of the signs of discrete cosine transform (DCT) coefficients. Previously, we derived this relationship mathematically and proposed DCT sign phase correlation (DCT-SPC) based on this relationship (18). DCT-SPC is a phase-based correlation and has properties that are similar to those of POC.

Images, particularly in the fields of biometrics, medicine, and surveillance camera require extreme security in order to avoid the risk of identity theft and invasion of privacy (19). Generally, encrypting and scrambling are used to protect information (20) (21). However, these protected images require decrypting or descrambling before image matching. In other words, neither POC nor DCT-SPC can be directly applied to conventional encrypted and scrambled images. Based on privacy concerns, secure multi-party techniques were applied to vision algorithms such as Blind Vision in (22). However, in (22), neither the registration nor the estimation of the geometric relationship between two images was discussed.

In this chapter, for POC and DCT-SPC, we present phase-scrambled signals and a matching method that can be directly applied to phase-scrambled signals without descrambling. The presented methods are motivated by secure data management. The phase scrambling distorts only the phase information, which contains significant information of signals. Phase scrambling protects against the exposure of the information in the signal. Synchronized phase scrambling yields the relationship between non-scrambled signals. Therefore, POC and DCT-SPC can be directly applied to phase-scrambled signals. Moreover, the presented scrambling



(a) conventional templates (b) secure templates by phase scrambling.

Fig. 1. Stored templates for phase-based correlation. (a) Conventional templates: If the templates in a database were to be stolen, information about the original images would be vulnerable. (b) Secure templates: A template is stored in either a phase-scrambled coefficients form or a scrambled phase information form in order to guarantee secure data management. Phase scrambling prevents templates from putting at risk the information about the original images.

has no effect on image matching. That is, the same accuracy is obtained from phase-scrambled signals without descrambling (23)(24).

This chapter is organized as follows. In Section 2, we describe the motivations and important considerations of the present study. In Section 3, POC and DCT-SPC are explained. In Section 4, the phase-scrambled signals and image matching for POC are described. We explain the reason why the POC between phase-scrambled signals has the same accuracy as that between the non-scrambled signals. In Section 5, the sign phase-scrambled signals and image matching for DCT-SPC are described. In Section 6, various simulations are presented for the purpose of confirming the effectiveness and appropriateness of the scrambled signals and image matching. Finally, Section 7 concludes this chapter.

2. Image matching between visually protected images

Image matching for authentication requires several templates that have been registered previously. Generally, the management of these templates requires a great deal of labor. Countermeasures to prevent theft and refusal of cross-references [1] are required. Phase-based correlation uses the phase information of signals. Specifically, POC and DCT-SPC require the phase

[1] Templates registered in a particular system being diverted to another system without the permission of a registrant.

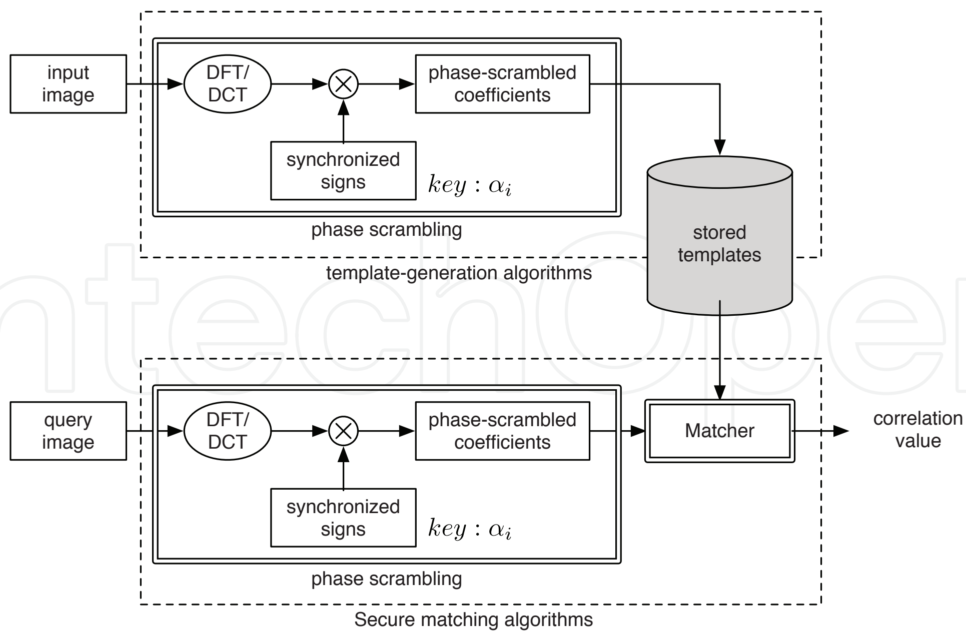


Fig. 2. Model of template-generation and matching algorithms for secure data management

factors of DFT coefficients (DFT phase factors) and the signs of DCT coefficients (DCT signs) respectively, for translation estimation. In addition, both correlations require the magnitude of DFT coefficients for rotation and scaling estimation (6). When the effect of rotation and scaling are small and can be ignored, only phase information is used for matching. Therefore, the conventional template for phase-based correlation is stored in either the coefficients in the transformed domain or in a phase information form. If the template stored in the coefficients were to be stolen, the information in the original signal may be compromised. Even in the case of the templates stored in the phase information form, the information in the original signal may be exposed by the inverse transform of the phase information, as shown in Fig. 1 (a). In addition, neither the templates stored in the coefficients form nor the phase information form is considered for cross-referencing. Moreover, the templates stored in either the coefficients form or the phase information form may be modified or removed. Alternately, new templates may be introduced to the database. In order to address these problems, we focus on secure data management.

In this chapter, we present phase-scrambled signals and a matching method for these signals using POC and DCT-SPC. The presented method is motivated by the need to guarantee secure data management. The template is stored in either phase-scrambled coefficients or a scrambled phase information form, as shown in Fig. 1 (b), and the complete information about the original signal is protected by phase scrambling. In addition, the templates are used for image matching without descrambling. Synchronized scrambling by the same key allows estimation of the translated, rotated, and scaled values between an image and the template by phase-based correlation. Desynchronized scrambling using different keys prevents cross-referencing of templates, thereby guaranteeing secure data management. Note that, in the presented method, phase scrambling has no effect on matching using POC and DCT-SPC. That is, the estimation value between the phase-scrambled signals is obtained with the same accuracy as that between non-scrambled signals.

3. Phase-based correlation

Two phase-based correlations, POC and DCT-SPC, are explained. Single-dimensional notation is used for the sake of brevity. Let $\mathbb{C}$, $\mathbb{R}$, and $\mathbb{Z}$ denote the sets of complex, real, and integer numbers, respectively.

3.1 Phase-only correlation (POC)

Let the N-point DFT of the N-point real signal $g_i(n)$, $(i = 1, 2)$ $(n = 0, 1, \cdots N-1)$ be $G_i(k)$, $(k = 0, 1, \cdots, N-1)$. $G_i(k)$ is expressed in polar form as

$$G_i(k) = |G_i(k)| e^{j\theta_{ik}} \tag{1}$$

$$= |G_i(k)| \phi_{G_i}(k) \tag{2}$$

where $j = \sqrt{-1}$. The quantities $|G_i(k)|$ and θ_{ik} are the magnitude and phase, respectively. $\phi_{G_i}(k) = e^{j\theta_{ik}}$ is referred to as the phase factor.
The normalized cross spectrum is given as

$$R_\phi(k) = \phi_{G_1}(k) \cdot \phi^*_{G_2}(k), \tag{3}$$

where $\phi^*_{G_2}(k)$ denotes the complex conjugate of $\phi_{G_2}(k)$.
The POC is defined as the inverse DFT of $R_\phi(k)$ in (10)-(12), i.e.,

$$r_\phi(n) = \frac{1}{N} \sum_{k=0}^{N-1} R_\phi(k) W_N^{-nk}, \quad n = 0, 1, \cdots, N-1, \tag{4}$$

where W_N denotes $e^{-j2\pi/N}$. The integer displacement value between signals is estimated using (4).

3.2 DCT sign phase correlation (DCT-SPC)

Let the N-point DCT of the N-point real signal $g_i(n)$ be $G_{iC}(k)$. The DCT-II is defined as

$$G_{iC}(k) = \sqrt{\frac{2}{N}} C_k \sum_{n=0}^{N-1} g_i(n) \cos\left(\frac{\pi(n+1/2)k}{N}\right) \tag{5}$$

where

$$C_k = \begin{cases} 1/\sqrt{2}, & k = 0 \\ 1, & k \neq 0 \end{cases}. \tag{6}$$

$G_{iC}(k)$ is expressed as the absolute value, $|G_{iC}(k)|$, and the sign, $\sigma_{Gi}(k)$, i.e.,

$$G_{iC}(k) = |G_{iC}(k)| \sigma_{Gi}(k). \tag{7}$$

The DCT sign product is given as

$$R_\sigma(k) = \sigma_{G_1}(k) \cdot \sigma_{G_2}(k), \quad k = 0, 1, \cdots, N-1, \tag{8}$$

where $\sigma_{G_i}(k)$ is the sign of $G_{iC}(k)$. If $G_{iC}(k)$ is zero, $\sigma_{G_i}(k)$ is replaced by zero. DCT-SPC is defined in (18) as

$$r_\sigma(n) = \frac{1}{N} \sum_{k=0}^{N-1} K_k R_\sigma(k) \cos\left(\frac{\pi n k}{N}\right), \quad n = 0, 1, \cdots, N-1 \tag{9}$$

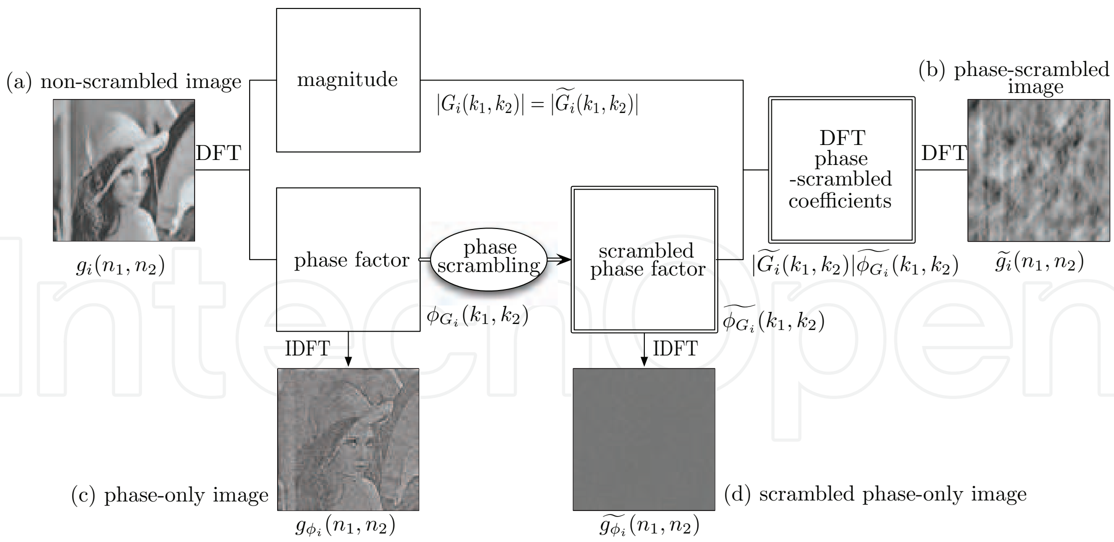


Fig. 3. Images derived from a non-scrambled image and their relationships: The non-scrambled image is composed of the magnitude $|G_i(k_1,k_2)|$ and the phase factor $\phi_{G_i}(k_1,k_2)$, while the phase-scrambled image is composed of the magnitude $|\widetilde{G_i}(k_1,k_2)|$, which is identical to $|G_i(k_1,k_2)|$, and the scrambled phase factor $\widetilde{\phi_{G_i}}(k_1,k_2)$.

where K_k is the weight, which is generally given as

$$K_k = (C_k)^2. \tag{10}$$

The integer displacement value is estimated using (9). The advantages of DCT-SPC over POC are computational complexity and memory complexity, because the DCT-SPC uses only the DCT signs to estimate translation between signals. The translation with non-integer numbers can be estimated by DCT-SPC with fitting function as well as POC (25).

4. Phase-scrambled signals and matching using POC

4.1 Template-generation and matching algorithms for secure data management

Figure 2 shows a model of the template-generation and matching algorithms. In the template-generation algorithms, either the DFT or the DCT coefficients of an input image are calculated and multiplied by the synchronized signs in order to generate the phase-scrambled coefficients. Either the phase-scrambled coefficients or the scrambled phase information, which is extracted from the phase-scrambled coefficients, is stored as a template in a database. In the secure matching algorithms, when a query image, which is not scrambled, is input, the DFT or the DCT coefficients of the query image are calculated and multiplied by the synchronized signs to generate the phase-scrambled coefficients. The matcher executes phase-based correlation between the phase-scrambled coefficients and templates.

In this section, we explain scrambled signals for POC and an image-matching method using POC. We demonstrate that scrambling has no effect on the accuracy of matching.

4.2 Phase-scrambled signals

Let us first consider scrambling of the N-point signal $g_i(n)$ for POC. First, N-point signs, $s_{\alpha_i}(k)$, are generated in random order by a random number generator with a key, α_i, i.e.,

$$s_{\alpha_i}(k) \in \{1, -1\} \tag{11}$$

$$k = 0, 1, \cdots, N-1. \tag{12}$$

In this chapter, the key corresponds to a seed that initializes the random number generator. Multiplying the DFT coefficients, $G_i(k)$, of $g_i(n)$ by the N-point signs, $s_{\alpha_i}(k)$, yields the scrambled DFT coefficients $\widetilde{G_i}(k)$; i.e.,

$$\widetilde{G_i}(k) = G_i(k) \cdot s_{\alpha_i}(k) \tag{13}$$

$$= G_i(k) \cdot e^{-j(s_{\alpha_i}(k)-1)\pi/2}$$

$$= |G_i(k)| e^{j\theta_{ik}} e^{-j(s_{\alpha_i}(k)-1)\pi/2} \tag{14}$$

where $s_{\alpha_i}(k) = e^{-j(s_{\alpha_i}(k)-1)\pi/2}$. $\widetilde{G_i}(k)$ is expressed in polar form as

$$\widetilde{G_i}(k) = |\widetilde{G_i}(k)| e^{j\widetilde{\theta_{ik}}}. \tag{15}$$

Comparing (14) and (15) yields the relationship between the non-scrambled coefficients and the phase-scrambled coefficients:

$$|\widetilde{G_i}(k)| = |G_i(k)| \tag{16}$$

and

$$\widetilde{\theta_{ik}} = \begin{cases} \theta_{ik} + \pi, & s_{\alpha_i}(k) = -1 \\ \theta_{ik}, & s_{\alpha_i}(k) = 1 \end{cases}. \tag{17}$$

We can conclude that scrambling has no effect on the magnitude. Therefore, the phase-scrambled coefficients $\widetilde{G_i}(k)$ are expressed in terms of the DFT magnitude, $|G_i(k)|$, of the original signal and the scrambled phase factor, $\widetilde{\phi_{G_i}}(k)$, as

$$\widetilde{G_i}(k) = |G_i(k)| \widetilde{\phi_{G_i}}(k). \tag{18}$$

The phase-scrambled signal $\widetilde{g_i}(n)$ is the inverse transform of the phase-scrambled coefficients:

$$\widetilde{g_i}(n) = \frac{1}{N} \sum_{k=0}^{N-1} \widetilde{G_i}(k) W_N^{-nk}. \tag{19}$$

Let us consider the two-dimensional version of the signals as images. Figure 3 shows the limited images derived from a non-scrambled image $g_i(n_1, n_2)$, the DFT coefficients of which are $G_i(k_1, k_2) = |G_i(k_1, k_2)| \phi_{G_i}(k_1, k_2)$. The phase-scrambled image $\tilde{g}_i(n_1, n_2)$ protects the visual information of the non-scrambled image, as shown in Fig. 3 (b). The DFT magnitude of the non-scrambled image and that of the phase-scrambled image are identical. The phase factor of the non-scrambled image and that of the phase-scrambled image are different. The phase-only image $g_{\phi_i}(n_1, n_2)$, as shown in Fig. 3 (c), which is derived from the phase factors of the non-scrambled image, exposes information about the non-scrambled image, whereas the

scrambled phase-only image $\widetilde{g}_i(n_1, n_2)$, as shown in Fig. 3 (d), protects the visual information about the non-scrambled image.
These limited images are expressed as follows:

$$g_{\phi_i}(n_1, n_2) = \frac{1}{N^2} \sum_{k_1=0}^{N-1} \sum_{k_2=0}^{N-1} \phi_{G_i}(k_1, k_2) W_N^{-n_1 k_1} W_N^{-n_2 k_2}. \quad (20)$$

$$\widetilde{g}_i(n_1, n_2) = \frac{1}{N^2} \sum_{k_1=0}^{N-1} \sum_{k_2=0}^{N-1} |G_i(k_1, k_2)| \widetilde{\phi_{G_i}}(k_1, k_2) W_N^{-n_1 k_1} W_N^{-n_2 k_2}. \quad (21)$$

$$\widetilde{g_{\phi_i}}(n_1, n_2) = \frac{1}{N^2} \sum_{k_1=0}^{N-1} \sum_{k_2=0}^{N-1} \widetilde{\phi_{G_i}}(k_1, k_2) W_N^{-n_1 k_1} W_N^{-n_2 k_2}. \quad (22)$$

where $\widetilde{\phi_{G_i}}(k_1, k_2)$ denotes the scrambled-phase factor.
The phase-scrambled signal and the phase-scrambled coefficients are the space domain representation and the frequency domain representation, respectively. In the following sections, we generally do not distinguish the phase-scrambled signal from the phase-scrambled coefficients, except where confusion may occur. We refer to the phase-scrambled coefficients as the phase-scrambled signal for one-dimensional expression or the phase-scrambled image for two-dimensional expression.

4.3 Matching using POC between phase-scrambled signals

From (3), the normalized cross spectrum, $\widetilde{R_\phi}(k)$, between $\widetilde{\phi_{G_1}}(k)$ and $\widetilde{\phi_{G_2}}(k)$ is given as

$$\begin{aligned} \widetilde{R_\phi}(k) &= \widetilde{\phi_{G_1}}(k) \cdot \widetilde{\phi^*_{G_2}}(k) \\ &= s_{\alpha_1}(k) \cdot \phi_{G_1}(k) \cdot s^*_{\alpha_2}(k) \cdot \phi^*_{G_2}(k) \end{aligned} \quad (23)$$

where, if the same key is used, i.e., $s_{\alpha_1}(k) = s_{\alpha_2}(k)$, for any k, then

$$s_{\alpha_1}(k) \cdot s^*_{\alpha_2}(k) = s_{\alpha_1}(k) \cdot s_{\alpha_2}(k) = 1 \quad (24)$$

and

$$\widetilde{R_\phi}(k) = R_\phi(k). \quad (25)$$

If the keys are different, i.e., $\alpha_1 \neq \alpha_2$, then $\widetilde{R_\phi}(k) \neq R_\phi(k)$. We conclude that the normalized cross spectrum of phase-scrambled signals and that of non-scrambled signals are identical if the key is the same, and we can therefore obtain the estimation values with the same accuracy.

4.4 Scrambling and image matching steps for POC

4.4.1 Scrambling

Scrambling proceeds as follows:

Step 1 The DFT coefficients are calculated from an image.

Step 2 The signs $s_{\alpha_i}(k)$ are generated by a key α_i.

Step 3 The DFT coefficients are multiplied by the signs according to (13).

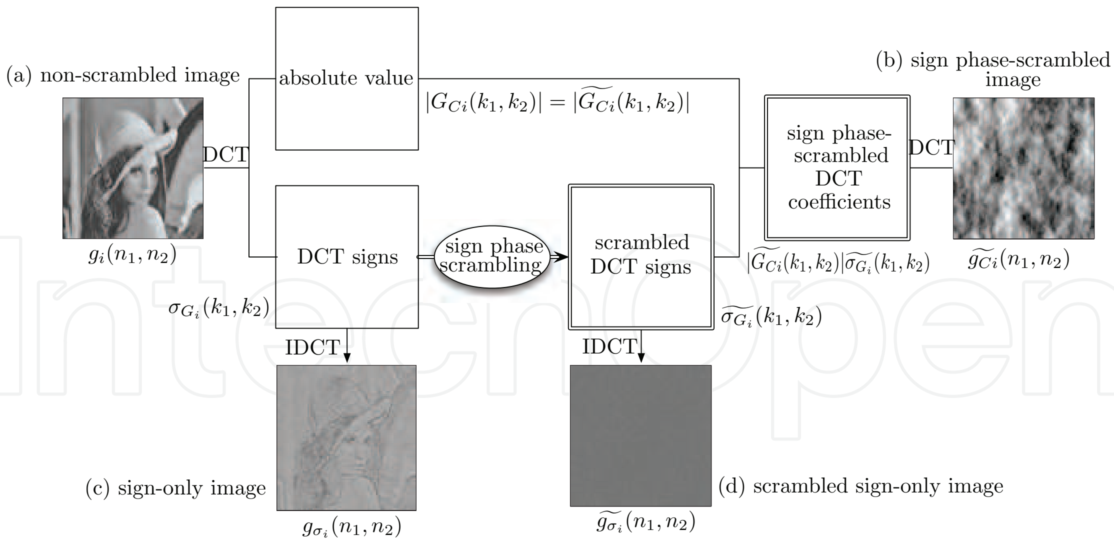


Fig. 4. Images derived from a non-scrambled image and their DCT relationships: The non-scrambled image is composed of the absolute value $|G_C(k_1,k_2)|$ of DCT coefficients and the DCT signs $\sigma_{G_i}(k_1,k_2)$, while the sign phase-scrambled image is composed of the absolute value $|\widetilde{G_{Ci}}(k_1,k_2)|$, which is identical to $|G_{Ci}(k_1,k_2)|$, and the scrambled DCT signs $\widetilde{\sigma_{G_i}}(k_1,k_2)$.

4.4.2 Image matching for translation

Image matching using POC for estimating translation between a query and a template is accomplished according to the following steps:

Step 1 The query is scrambled by the signs that are used for scrambling of the template.

Step 2 The DFT phase factors are extracted.

Step 3 The normalized cross spectrum is calculated using (3).

Step 4 The inverse DFT is applied to the result of Step 3 using (4).

Scrambling has no effect on the accuracy of image matching, because the effect of scrambling is canceled when the normalized cross spectrum is calculated.

4.4.3 Image matching for rotation and scaling

The DFT magnitude is used for the estimation of the rotated and scaled values between images (6). The phase scrambled method does not distort the DFT magnitude. Therefore, the DFT magnitude can be directly used for estimation. The steps for phase-scrambled images are the same as those for non-scrambled images.

5. Sign phase-scrambled signals and DCT-SPC

In this section, we explain sign phase-scrambled signals and their matching for DCT-SPC. The DCT signs express the phases of signals in the transform domain (18). We show that scrambling has no effect on the accuracy of image matching.

5.1 Sign phase-scrambled signal

Let us consider sign phase scrambling of $g_i(n)$ for DCT-SPC. Multiplying $s_{\alpha_i}(k)$ in (17) by $G_{Ci}(k)$ yields the sign phase-scrambled DCT coefficients, $\widetilde{G_{Ci}}(k)$, i.e.,

$$\begin{aligned}\widetilde{G_{Ci}}(k) &= G_{Ci}(k) \cdot s_{\alpha_i}(k) \\ &= |G_{Ci}(k)|\sigma_{G_i}(k) \cdot s_{\alpha_i}(k) \quad (26)\\ &= |\widetilde{G_{Ci}}(k)|\widetilde{\sigma_{G_i}}(k) \quad (27)\end{aligned}$$

where the quantities $|\widetilde{G_{Ci}}(k)|$ and $\widetilde{\sigma_{G_i}}(k)$ are the absolute value and sign, respectively. Combining (26) and (27) gives the quantitative relationships between the sign phase-scrambled DCT coefficients, $\widetilde{G_{Ci}}(k)$, and the non-scrambled DCT coefficients, $G_{Ci}(k)$:

$$|\widetilde{G_{Ci}}(k)| = |G_{Ci}(k)| \quad (28)$$

and

$$\widetilde{\sigma_{G_i}}(k) = \sigma_{G_i}(k) \cdot s_{\alpha_i}(k). \quad (29)$$

Therefore, the sign phase-scrambled DCT coefficient, $\widetilde{G_{Ci}}(k)$, is expressed in terms of the absolute value, $|G_{Ci}(k)|$, of the non-scrambled signal and the scrambled DCT sign, $\widetilde{\sigma_{G_i}}(k)$, as

$$\widetilde{G_{Ci}}(k) = |G_{Ci}(k)|\widetilde{\sigma_{G_i}}(k) \quad (30)$$

The sign phase-scrambled signal is the inverse transform of the sign phase-scrambled DCT coefficients, i.e.,

$$\widetilde{g_{C_i}}(n) = \sqrt{\frac{2}{N}} \sum_{k=0}^{N-1} C_k |G_{C_i}(k)| \widetilde{\sigma_{G_i}}(k) \cos\left(\frac{\pi(n+\frac{1}{2})k}{N}\right). \quad (31)$$

The sign phase-scrambled signals are real numbers. The DCT-SPC uses the DCT signs, which are extracted from the transform of the sign phase-scrambled signals.
Figure 4 shows the images derived from a non-scrambled image, as shown in Fig. 4 (a), and the relationships between these images. As shown in Fig. 4 (b), the sign phase-scrambled image protects the information about the non-scrambled image. The DCT signs of the non-scrambled image and that of the sign phase-scrambled image are different. The sign-only image, as shown in Fig. 4 (c), which is derived from the DCT signs of the non-scrambled image, exposes the information of the non-scrambled image, while the scrambled sign-only image, as shown in Fig. 4 (d), protects the information about the non-scrambled image.

5.2 Matching using DCT-SPC between sign-scrambled signals

In the case of the sign phase-scrambled DCT coefficients, the DCT sign product is also invariant if the same key is used. From (8), the DCT sign product, $\widetilde{R_\sigma}(k)$, between $\widetilde{\sigma_{G_1}}(k)$ and $\widetilde{\sigma_{G_2}}(k)$ is given as

$$\widetilde{R_\sigma(k)} = \widetilde{\sigma_{G_1}}(k) \cdot \widetilde{\sigma_{G_2}}(k). \quad (32)$$

From (8),

$$\widetilde{R_\sigma(k)} = \sigma_{G_1}(k) s_{\alpha_1}(k) \cdot \sigma_{G_2}(k) s_{\alpha_2}(k). \quad (33)$$

If the same key is used, we obtain the same result under scrambling, i.e.,

$$\widetilde{R_\sigma}(k) = R_\sigma(k). \quad (34)$$

If the keys are different, the result is $\widetilde{R_\sigma}(k) \neq R_\sigma(k)$. This can help prevent illegal use of the image matching.

We can thus conclude that there is no effect of scrambling on registration accuracy.

5.3 Scrambling and image matching steps for DCT-SPC

5.3.1 Sign phase scrambling

Scrambling proceeds as follows:

Step 1 The DCT coefficients are calculated from an image.

Step 2 The signs $s_{\alpha_i}(k)$ are generated by a key α_i.

Step 3 The DCT coefficients are multiplied by the signs $s_{\alpha_i}(k)$ according to (26).

5.3.2 Image matching for translation

Image matching using DCT-SPC for estimating translation between a query and a template is accomplished according to the following steps:

Step 1 The query is scrambled by the signs that are used for scrambling of the template.

Step 2 The DCT signs are extracted.

Step 3 The DCT sign product is calculated using (8).

Step 4 The inverse transform is applied to the result of Step 3 using (9).

Scrambling does not affect the accuracy of image matching, because the effect of scrambling is canceled when the DCT sign product is calculated.

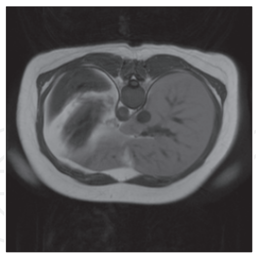
6. SIMULATION

6.1 Translation (synchronized phase scrambling)

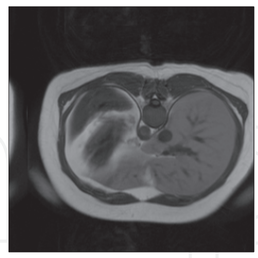
Translation estimation experiments were performed using non-scrambled images and synchronized phase-scrambled images. Figure 5 shows the test images: (a) is a 256 $\times$ 256 non-scrambled image, (b) is the shifted image of (a) by 20 pixels in both the horizontal and vertical directions, and (c) and (d) are the phase-scrambled images of (a) and (b), respectively. Note that the phase-scrambled images were generated with the same key, which initializes the random number generator, i.e., $\alpha_1 = \alpha_2$, $s_{\alpha_1}(k) = s_{\alpha_2}(k)$, for any k. We refer to the use of the same key as synchronized phase scrambling. We executed POC between the two non-scrambled images, (a) and (b), and POC between the two phase-scrambled images, (c) and (d), as shown in Fig. 5. Figure 6 shows that the POC surface between phase-scrambled images in (21) was the same as the POC surface between non-scrambled images in the case of synchronized phase scrambling. Phase scrambling has no effect on the accuracy of image matching.

We also performed DCT-SPC between the two non-scrambled images and DCT-SPC between the corresponding sign phase-scrambled images. Note that the sign phase-scrambled images were generated using the same key. Figure 7 shows the DCT-SPC surface between sign phase-scrambled images and that between non-scrambled images. Sign phase scrambling was confirmed to have no effect on the accuracy of image matching.

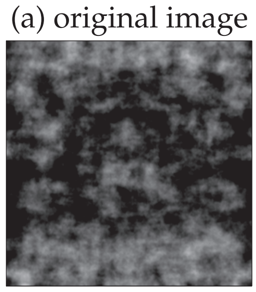
We also confirmed the estimation of translation with subpixel accuracy. The same accuracy was obtained for phase-scrambled images as that for non-scrambled images. (Details are omitted due to space limitations.)



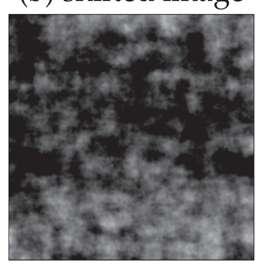
(a) original image



(b) shifted image

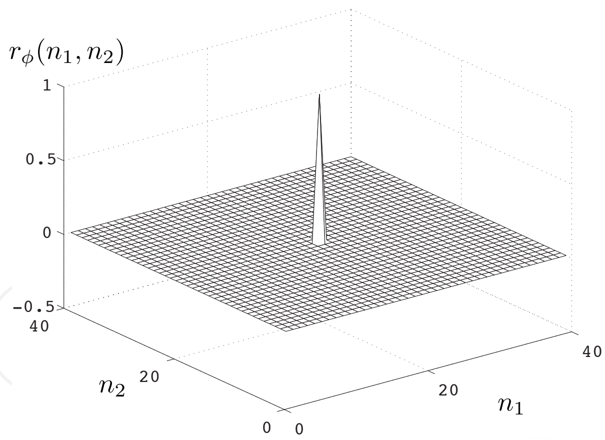


(c) phase-scrambled image of (a)

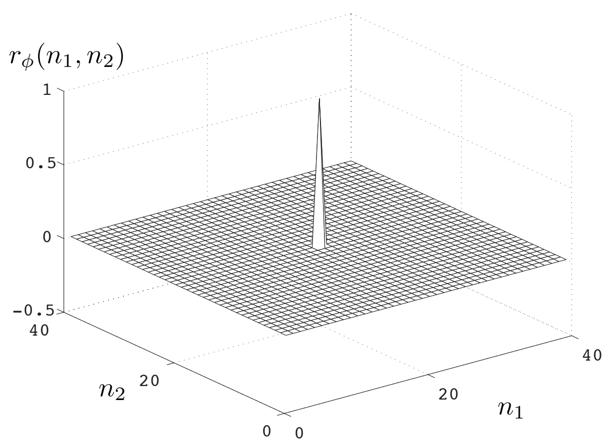


(d) phase-scrambled image of (b)

Fig. 5. Test images (256×256): (a) is the original image, and (b) is the shifted image of (a). (c) and (d) are the phase-scrambled images of (a) and (b), respectively.

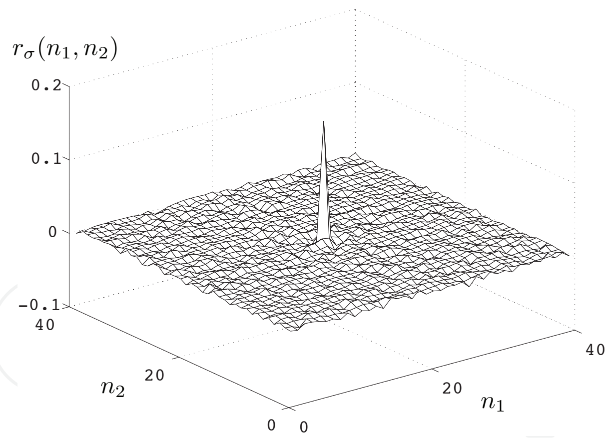


(a) non-scrambled image

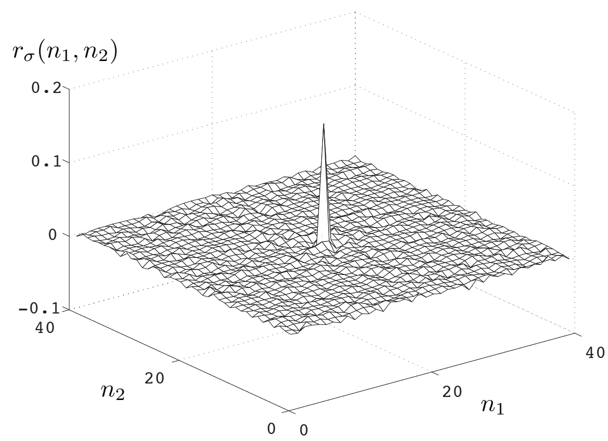


(b) scrambled image with the same key, $\alpha_1 = \alpha_2$

Fig. 6. Estimation of translation using POC: (a) is the POC surface between the non-scrambled images, and (b) is the POC surface between the phase-scrambled images. (a) and (b) are identical, and an acute peak appears at the location expressing the translational displacement.



(a) non-scrambled image



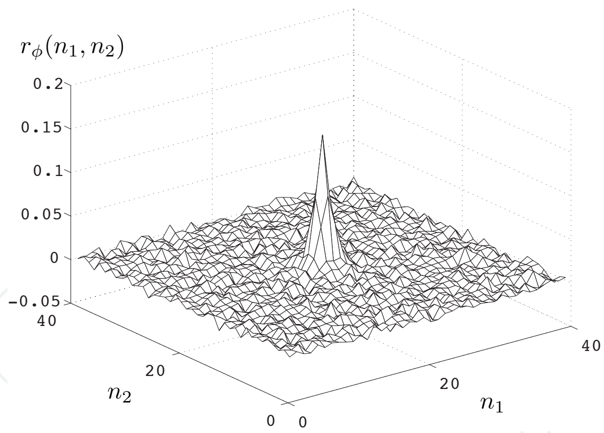
(b) scrambled image with the same key, $\alpha_1 = \alpha_2$

Fig. 7. Estimation of translation using DCT-SPC: (a) is the DCT-SPC surface between the non-scrambled images, and (b) is the DCT-SPC surface between the sign phase-scrambled images. (a) and (b) are identical, and an acute peak appears at the location expressing the translational displacement.

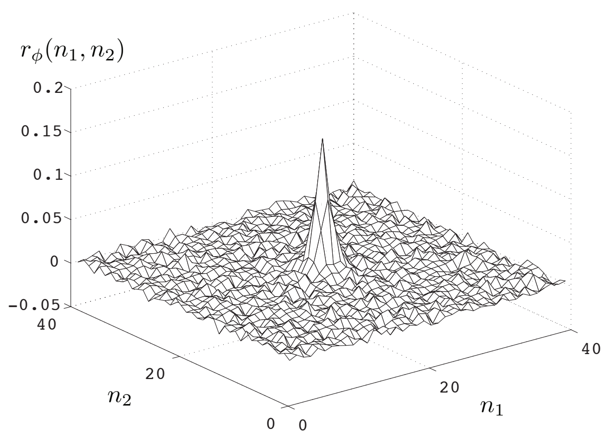
6.2 Effect of noise on image matching (synchronized phase scrambling)

Figure 8 shows the effect of noise on image matching. The test image is shown in Fig. 5 (a), and the shifted image is shown in Fig. 5 (b). First, the noise, which consisted of Gaussian random numbers with zero mean and a standard deviation of 25, was added to the shifted image in the space domain. Figure 8 (a) shows the POC surface between the image and the shifted image with noise. Compared with Fig. 6 (a), the effect of noise on the POC surface is clear.

Next, we scrambled these two images and performed POC. Figure 8 (b) shows the results. We confirmed that (a) and (b) in Fig. 8 were identical. We can conclude that scrambling has no effect on image matching.



(a) POC between the non-scrambled image and the non-scrambled shifted image with noise

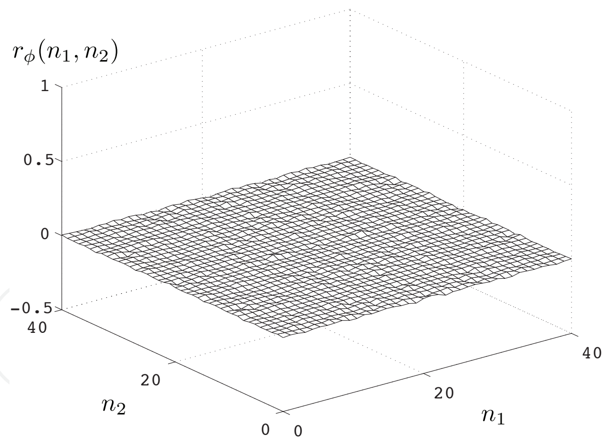


(b) POC between the phase-scrambled image and the phase-scrambled shifted image with noise

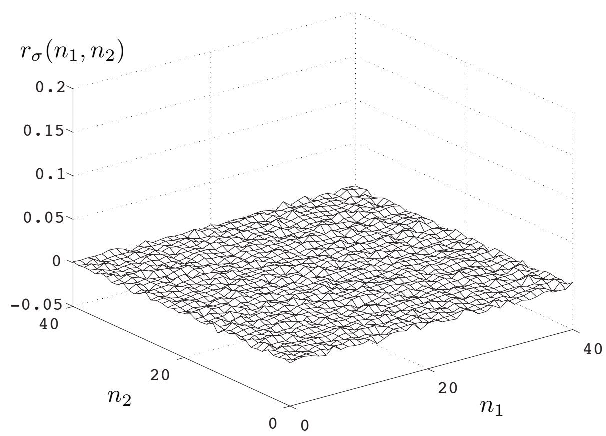
Fig. 8. POC with noise: Gaussian random number with zero mean and a standard deviation of 25. (a) and (b) are identical.

6.3 Translation (desynchronized phase scrambling)

Translation estimation experiments were performed between the desynchronized phase-scrambled images and desynchronized sign phase-scrambled images. That is, the phase-scrambled images were generated with different keys, i.e., $\alpha_1 \neq \alpha_2$. The sign phase-scrambled images were also generated with different keys, i.e., $\alpha_1 \neq \alpha_2$. Figure 9 shows both the POC surface between phase-scrambled images and the DCT-SPC surface between sign phase-scrambled images. A distinct peak expressing the translational displacement did not appear on either the POC surface and the DCT-SPC surface. The properties of phase-scrambled images with different keys provides a countermeasure against cross-referencing.



(a) POC with different key $\alpha_1 \neq \alpha_2$



(b) DCT-SPC with different key $\alpha_1 \neq \alpha_2$

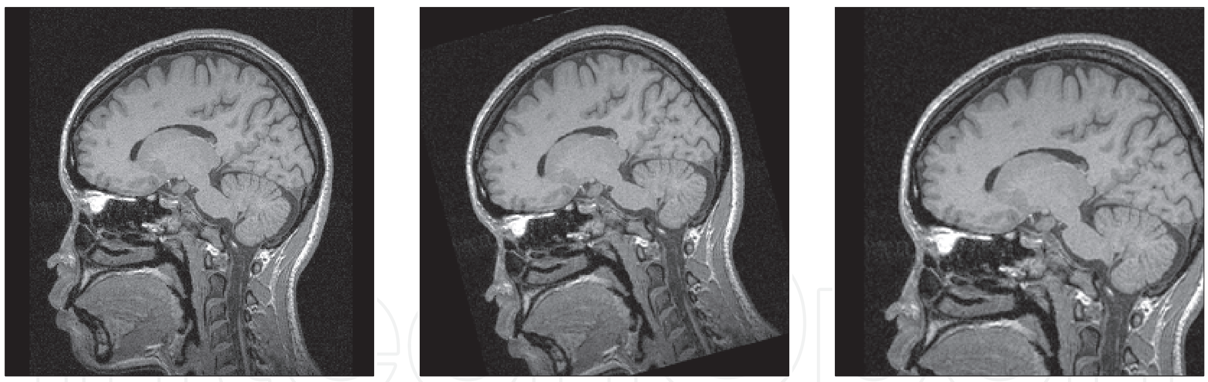
Fig. 9. Estimation of translation with different key, $\alpha_1 \neq \alpha_2$ (a) is the POC surface between phase-scrambled images with different keys, (b) is the DCT-SPC surface between sign phase-scrambled images with different keys. A distinct peak expressing the translational displacement did not appear in (a) or (b).

6.4 Rotation and Scaling

Rotated and scaled values are generally estimated using the DFT magnitude. This is based on the fact that the DFT magnitude contains information related to the rotated and scaled values, which are independent of translation. Note that the log-polar transform is applied to the DFT magnitude in order to reduce the rotated and scaled values to vertical and horizontal translations, respectively (6).

The rotated and scaled values between two images, as shown in Fig. 10, were estimated under two conditions: non-scrambling and phase scrambling with the same key. We confirmed that the POC surface between phase-scrambled images with the same key and that between non-scrambled images were identical. This result is trivial, however, because the presented phase scrambling does not distort the DFT magnitude, as shown in (16).

The phase scrambling does not affect the image matching, and we can perform image matching without descrambling.



(a) original image (b) rotated image, angle: 15°. (c) scaled image, scale factor: 1.2

Fig. 10. Estimation of the rotated and scaled values. Log-polar transform is used to reduce rotated and scaled values to translational values (6).

7. Conclusion

The presented scrambling enables image matching using invisible images. In addition, image matching between phase-scrambled images is performed with the same accuracy as that between non-scrambled images. We have explained how to generate phase-scrambled signals that protect the information in the original image and demonstrated that the presented synchronized phase-scrambling maintains the relative relationship between two signals mathematically. We have shown that the presented scrambling is applicable to both DFT and DCT coefficients, and therefore secure image matching for phase-based correlation is achieved.
In particular, DCT-SPC is closely related to the image compression method. Application of the presented scrambling in areas such as image communications and image compression appears promising.
In the presented scrambling, the management of keys depends on desired systems. Meanwhile, for visual protection, there is one-time key based phase scrambling which does not require the management of keys (26; 27).

8. References

[1] B. V. K. V. Kumar, A. Mahalanobis and R. Juday, *Correlation pattern recognition,* Cambridge University Press. UK, Nov. 2005

[2] C. H. Chen and P. S. P. Wang, *Hand book of pattern recognition and computer vision (3rd edition),* World Scientific Publishing. 2005

[3] C. H. Knapp and G. C. Carter, "The generalized correlation method for estimation of time delay," *IEEE trans. Acoust., Speech, Signal Process.*, vol. ASSP-24, no. 4, Aug. 1976

[4] O. S. Jahromi and P. Aarabi, "Theory and design of multirate sensor array," *IEEE trans. Signal Process.*, vol. 53, no. 5, May 2005

[5] C. A. Wilson and J. A.Theriot, "A correlation-based approach to calculate rotation and translation of moving cells," *IEEE Trans. Image Process.*, vol. 15, no. 7, pp. 1939–1951, July 2006

[6] Q. Chen, M. Defrise, and F. Deconinck, "Symmetric phase-only matched filtering of Fourier-Mellin transforms for image registration and recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 16, no. 2, pp. 1156–1168, Dec. 1994

[7] B. S. Reddy and B. N. Chatterji, "An FFT-based technique for translation, rotation, and scale-invariant image registration," *IEEE Trans. Image Process.*, vol. 5, no. 8, pp. 1266-1271, Aug. 1996

[8] O. Urhan, M. K. Güllü, and S. Ertürk, "Modified phase-correlation based robust hard-cut detection with application to archive Film," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 16, no. 6, pp. 753–770, June 2006

[9] T. Vlachos, "Cut detection in video sequences using phase correlation," *IEEE Signal Process. Lett.*, vol. 7, no. 7, pp. 173–175, Jul. 2000

[10] K. Ito, A. Morita, T. Aoki, T. Higuchi, H. Nakajima, and K. Kobayashi, "A fingerprint recognition algorithm using phase-based image matching for low-quality Fingerprints," in *Proc. IEEE Int. Conf. Image Process.*, vol. 2, pp. 33–36, Sept. 2005

[11] K. Miyazawa, K. Ito, T. Aoki, K. Kobayashi, and H. Nakajima, "An efficient iris recognition algorithm using phase-based image matching," in *Proc. IEEE Int. Conf. Image Process.*, vol. 2, pp. 49–52, Sept. 2005

[12] C. D. Kuglin and D. C. Hines, "The phase correlation image alignment method," in *Proc. Int. Conf. Cybernetics and Society*, pp. 163–165, Sept. 1975

[13] M. Balci and H. Foroosh, "Subpixel estimation of shifts directly in the Fourier domain," *IEEE Trans. Image Process.*, vol. 15, no. 7, pp. 1965–1972, July 2006

[14] H. Foroosh and M. Balci, "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, Oct. 2004

[15] H. Foroosh, J. Zerubia, and M. Berthod, "Extension of phase correlation to sub-pixel registration," *IEEE Trans. Image Process.*, vol. 11, no. 3, pp. 188-200, Mar. 2002

[16] W. S. Hoge, "A subspace identification extension to the phase correlation method," *IEEE Trans. Med. Imag.*, vol. 22, no. 2, pp. 277-280, Feb. 2003

[17] P. Thévenaz. U. E. Ruttimann, and M. unser, "A pyramidal approach to subpixel registration based on intensity," *IEEE Trans. Image Process.*, vol. 7, no. 1, pp. 27-41, Jan. 1998

[18] I. Ito and H. Kiya, "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, Apr. 2007

[19] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 2, pp. 125–143, June 2006

[20] M. Fujiyoshi, W. Saitou, O. Watanabe, and H. Kiya, "Hierarchical encryption of multimedia contents for access control," in *Proc. IEEE Int. Conf. Image Process.*, pp. 1977–1980, Oct. 2006

[21] K. Kuroiwa, M. Fujiyoshi, and H. Kiya, "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, Sept. 2007

[22] S. Avidan and M. Butman, "Blind Vision," in *Proc. ECCV 2006*, Part III, LNCS 3953, pp. 1–13, Springer-Verlag, 2006

[23] H. Kiya and I. Ito, "Image matching between scrambled images for secure data management," in *Proc. EURASIP* 16^{th} *European Signal Process. Conf.*, Aug. 2008

[24] I. Ito and H. Kiya, "A new class of image registration for guaranteeing secure data management," in *Proc. 2008 IEEE Int. Conf. Image Process.*, pp. 269–272, Oct. 2008

[25] I. Ito and H. Kiya, "Multiple-peak model fitting function for DCT sign phase correlation with non-integer shift precision," in *Proc. 2009 IEEE Int. Conf. Acoustics, Speech and Signal Process.*, pp. 449–452, Apr. 2009.

[26] I. Ito and H. Kiya, "Image matching between visually protected images with one-time key based phase scrambling," in *Proc. EURASIP* 17^{th} *Europian Signal Processing Conf.*, pp. 1314-1318, Aug. 2009.
[27] I. Ito and H. Kiya, "One-time key based phase scrambling for phase-only correlation between visually protected images," EURASIP Journal on Information Security, to be published.

Signal Processing

Edited by Sebastian Miron

ISBN 978-953-7619-91-6
Hard cover, 528 pages
Publisher InTech
Published online 01, March, 2010
Published in print edition March, 2010

This book intends to provide highlights of the current research in signal processing area and to offer a snapshot of the recent advances in this field. This work is mainly destined to researchers in the signal processing related areas but it is also accessible to anyone with a scientific background desiring to have an up-to-date overview of this domain. The twenty-five chapters present methodological advances and recent applications of signal processing algorithms in various domains as telecommunications, array processing, biology, cryptography, image and speech processing. The methodologies illustrated in this book, such as sparse signal recovery, are hot topics in the signal processing community at this moment. The editor would like to thank all the authors for their excellent contributions in different areas of signal processing and hopes that this book will be of valuable help to the readers.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821