16th European Signal Processing Conference (EUSIPCO 2008), Lausanne, Switzerland, August 25-29, 2008, copyright by EURASIP

IMAGE MATCHING BETWEEN SCRAMBLED IMAGES FOR SECURE DATA MANAGEMENT

Hitoshi KIYA and Izumi ITO

Graduate School of System Design, Tokyo Metropolitan University
6-6, Asahigaoka, Hino-shi, Tokyo, Japan, 191-0065
phone: +81 42 585 8419, fax: +81 42 583 5119, email: kiya@eei.metro-u.ac.jp

ABSTRACT

We propose a scrambling method for image matching using phase-only correlation (POC) or discrete cosine transform sign phase correlation (DCT-SPC). The proposed scrambling method distorts only the phase, which has significant information of images. The information in each image is protected by the distorted phase information. In addition, synchronized scrambling keeps the relative relation between images. Therefore, either POC or DCT-SPC can be directly applied to the scrambled images in order to estimate the translated, rotated, and scaled values. Moreover, the proposed scrambling does not affect the accuracy of estimation values.

1. INTRODUCTION

In recent years, image matching has been required for many fields. A lot of matching methods have been developed, and an appropriate method should be selected for each application to obtain the desired performance [1, 2]. As one of correlation-based matching methods, phase-only correlation (POC) [3, 4, 5, 6, 7] is used for biometrics [8], such as iris [6] and fingerprinting [7]. POC or phase correlation is first proposed by Kuglin and Hines [3]. The concept of POC is based on the fact that the information related to the displacement of two images resides in the phase of the cross power spectrum. POC gives highly accurate displacement values by using some techniques, interpolation and curve fitting. In a specific case, the phase of the cross power spectrum corresponds to the product of the sign of discrete cosine transform (DCT) coefficients. DCT sign phase correlation (DCT-SPC) was proposed based on the fact [9, 10]. DCT-SPC has similar properties of POC, and the conciseness of time and space complexities of DCT-SPC is of advantage.

Images, particularly in biometrics [8] and in medical field, require extreme care to avoid the risk of identity theft and invasion of privacy. Generally, encrypting and scrambling are used for protecting information [11, 12]. However, these protected images require decrypting or descrambling before image matching. In other words, both POC and DCT-SPC cannot be directly applied to the conventional encrypted and scrambled images.

In this paper, we propose a scrambling method for image matching using either POC or DCT-SPC in order to address these threats. The proposed scrambling method distorts only the phase. Exposure of personal information can be prevented by scrambled images. The correlation and displacement values can be directly calculated without descrambling. Moreover, there is no effect of scrambling on image matching at all. That is, the exactly same accuracy is obtained from scrambled images without descrambling.

The rest of this paper is organized as follows: We show our motivations and explained the POC and DCT-SPC as preliminary in Section 2. The proposed scrambling and an image matching method between them are explained in Section 3. Some simulations are presented in Section 4. We conclude this paper in Section 5.

2. PRELIMINARY

Our concerns are expressed to clarify our motivations. Phase-only correlation (POC) and DCT sign phase correlation (DCT-SPC) are explained.

The single-dimensional notation is used for brevity.

2.1 Concerns

Generally, the management of data demands a lot of attention. Measure for theft and refusal of cross-reference[1] are required. The data for reference using DCT-SPC or POC should be stored in either raw data or feature data such as DFT coefficients, their phase information, and DCT signs. If the raw data should be stolen, the information is leaked out. If the feature data should be stolen, the information is exposed by the inverse transform of either DCT signs or DFT phase information as shown in Fig. 1. In addition, both raw data and feature data are not considered about cross-reference.

Our motivations are to propose a scrambling method for image registration using DCT-SPC or POC, and to show that the proposed scrambling method does not affect registration.

2.2 Phase-only correlation (POC)

Let N-point DFT of N-point 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

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

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

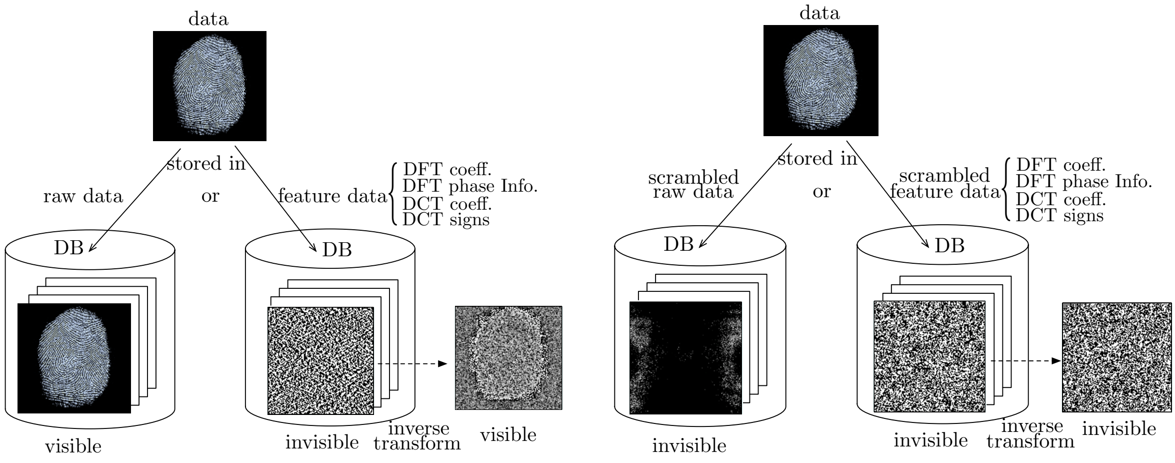
The quantities $|G_i(k)|$ and θ_{ik} are the magnitude and the phase, respectively. $G_i'(k) = e^{j\theta_{ik}}$ is referred to as phase factor in this paper.

The normalized cross spectrum is given as

$$R(k) = G_1'(k)\cdot\overline{G_2'(k)}, \tag{3}$$

where $G_i'(k)$ denotes the phase factor, and $\overline{G_2'(k)}$ denotes the complex conjugate of $G_2'(k)$.

[1] The data registered in a system is diverted in another system without a permission of a registrant.



(a) risk of compromise.

(b) secure data management for compromise.

Figure 1: (a) Risk of compromise: If raw data in a database should be stolen, the information is leaked out. If feature data in a database should be stolen, the information is exposed by the inverse transform of either DCT signs or DFT phase information. (b) Secure data management for compromise: Data is stored in either scrambled raw data or scrambled feature data for guaranteeing secure data management.

The POC is defined as the inverse DFT of $R(k)$ in [3, 6, 7], i.e.,

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

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

2.3 DCT sign phase correlation (DCT-SPC)

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

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

where

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

The DCT sign product is given as

$$R_C(k) = G'_{C_1}(k)\cdot G'_{C_2}(k), \quad k=0,1,\cdots,N-1, \tag{7}$$

n where $G'_{C_i}(k)$ is the sign of $G_{C_i}(k)$. If $G_{C_i}(k)$ is zero, the $G'_{C_i}(k)$ is replaced by zero. The DCT-SPC is defined in [9, 10] as

$$r_C(n) = \frac{1}{N}\sum_{k=0}^{N-1} K_k R_C(k)\cos\left(\frac{\pi nk}{N}\right), \quad n=0,1,\cdots,N-1 \tag{8}$$

where K_k is weight, and generally given as

$$K_k = (C_k)^2. \tag{9}$$

The integer displacement value is estimated according to Eq. (8).

3. IMAGE MATCHING BETWEEN SCRAMBLED IMAGES

In this section, the proposed scrambling method is explained. Moreover, it is shown that there is no effect of scrambling on the accuracy of image matching. Single-dimensional notation is continuously used for brevity.

3.1 Scrambling images

Let us first consider scrambling for POC. DFT coefficients are changed by scrambling. Let N-point DFT of N-point signal, $g_i(n)$, $(i=1,2)$, $(n=0,1,\cdots N-1)$ be $G_i(k)$, $(k=0,1,\cdots,N-1)$. First, N-point signs, $s_{\alpha_i}(k)$, are generated in a random order by using a random number generator with a key, α_i, i.e.,

$$s_{\alpha_i}(k) \in \{1,-1\} \tag{10}$$

$$k = 0,1,\cdots,N-1 \tag{11}$$

Then, the scrambled DFT coefficients $\widetilde{G}_i(k)$ is obtained by the product $s_{\alpha_i}(k)$ and $G_i(k)$. i.e.,

$$\begin{aligned}\widetilde{G}_i(k) &= s_{\alpha_i}(k)\cdot G_i(k) \\ &= e^{-j(s_{\alpha_i}(k)-1)\pi/2}G_i(k).\end{aligned} \tag{12}$$

$\widetilde{G}_i(k)$ is expressed in polar form as

$$\widetilde{G}_i(k) = |\widetilde{G}_i(k)|e^{j\widetilde{\theta_{ik}}} \tag{13}$$

where $e^{j\widetilde{\theta_{ik}}} = s_{\alpha_i}\cdot G'_i(k)$. Comparing Eq. (1) with Eq. (13) provides that only the phase is changed by scrambling, i.e.,

$$|\widetilde{G}_i(k)| = |G_i(k)| \tag{14}$$

and

$$\widetilde{\theta_{ik}} = \begin{cases} \theta_{ik}+\pi, & s_{\alpha_i}(k)=-1 \\ \theta_{ik}, & s_{\alpha_i}(k)=1 \end{cases}. \tag{15}$$

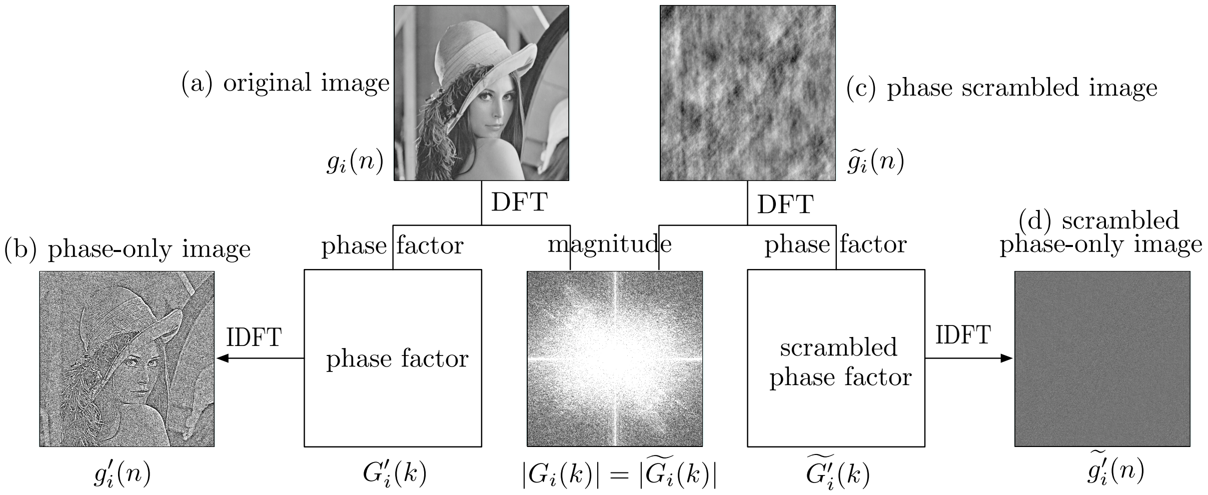


Figure 2: DFT relation between non-scrambled and scrambled images.

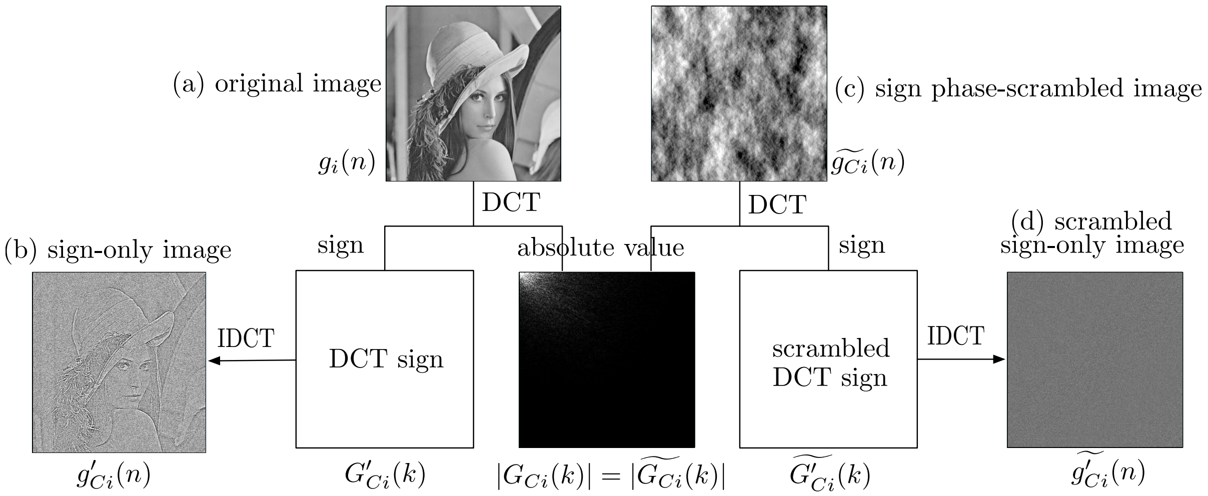


Figure 3: DCT relation between non-scrambled and scrambled images.

There is no effect of scrambling on the magnitude. Figure 2 shows the DFT relation between non-scrambled and scrambled images. The DFT magnitude of scrambled image is exactly the same as that of non-scrambled one. If the inverse DFT (IDFT) is applied to the phase factor of a non-scrambled image, the phase-only image shown in (b) is obtained and results in exposure of information. When the IDFT, on the other hand, is applied to the phase factor of a scrambled image, the scrambled phase-only image shown in (d) is obtained and the information about the original image is protected. The phase-scrambled image shown in (c) is generated by the IDFT of $\widetilde{G}_i(k)$.

Let us next consider scrambling for DCT-SPC. Let DCT coefficients be $G_{Ci}(k)$, $(i = 1,2)$, $(k = 0,1,\cdots,N-1)$. By multiplying $s_{\alpha_i}(k)$ in Eq. (15) by $G_{Ci}(k)$, the scrambled DCT coefficients, $\widetilde{G_{Ci}}(k)$, is obtained. i.e.,

$$\begin{aligned}\widetilde{G_{Ci}}(k) &= s_{\alpha_i}(k)\cdot G_{Ci}(k)\\ &= s_{\alpha_i}(k)\cdot |G_{Ci}(k)|G'_{Ci}(k) \qquad (16)\\ &= |\widetilde{G_{Ci}}(k)|\widetilde{G'_{Ci}}(k) \qquad (17)\end{aligned}$$

where the quantities $|\widetilde{G_{Ci}}(k)|$ and $\widetilde{G'_{Ci}}(k)$ are the absolute value and the sign, respectively. From Equations (16) and (17), the relation between $\widetilde{G'_{Ci}}(k)$ and $G'_{Ci}(k)$ is given as

$$\widetilde{G'_{Ci}}(k) = s_{\alpha_i}(k)\cdot G'_{Ci}(k) \qquad (18)$$

and the relation between $|\widetilde{G_{Ci}}(k)|$ and $|G_{Ci}(k)|$ is

$$|\widetilde{G_{Ci}}(k)| = |G_{Ci}(k)|. \qquad (19)$$

We can conclude that DCT signs are changed and the absolute values are invariant. Figure 3 shows the DCT relation between non-scrambled and scrambled images. We can see that the original information is protected by scrambling.

3.2 Image matching under scrambling

According to Eq. (3), the normalized cross spectrum, $\widetilde{R}(k)$, between $\widetilde{G_1'}(k)$ and $\widetilde{G_2'}(k)$ is given as

$$\begin{aligned}\widetilde{R}(k) &= \widetilde{G_1'}(k) \cdot \overline{\widetilde{G_2'}(k)} \\ &= s_{\alpha_1}(k) \cdot G_1'(k) \cdot \overline{s_{\alpha_2}(k) \cdot G_2'(k)} \qquad (20)\end{aligned}$$

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

$$s_{\alpha_1}(k) \cdot s_{\alpha_2}(k) = 1 \qquad (21)$$

and

$$\widetilde{R}(k) = R(k). \qquad (22)$$

If the keys are different, i.e., $s_{\alpha_1} \neq s_{\alpha_2}$, then $\widetilde{R}(k) \neq R(k)$. In the case of scrambled DCT coefficients, the DCT sign product is also invariant if the common key is used. The proposed scrambling has no effect on registration accuracy.

3.3 Scrambling and image matching steps for secure data management

3.3.1 Scrambling

Scrambling proceeds as follows:

1. The DFT / DCT coefficients are obtained from an image.
2. The signs with random order are generated by a key.
3. The DFT / DCT coefficients are scrambled according to Eq. (12) / Eq. (16).

The scrambled data is directly stored, or transformed and stored as an image with scrambled either phase or sign.

3.3.2 Translation

Image matching for estimation of translation between scrambled images using POC or DCT-SPC is accomplished according to the following steps:

1. The DFT phase factors / the DCT signs are extracted.
2. The normalized cross spectrum / the DCT sign product is calculated according to Eq. (3) / Eq. (7).
3. The inverse transform is applied to the result of step 2 according to Eq. (4) / Eq. (8).

These steps are the same as those in non-scrambled images. The proposed scrambling affects neither the steps nor the accuracy of image matching, because the effect of scrambling is canceled when the normalized cross spectrum or the DCT sign product is calculated.

4. SIMULATION

A. Translation (synchronized scrambling)

We estimated the translational displacement between images in Fig. 4: (b) is created from (a) shifted by 20 pixels in the horizontal and the vertical directions, respectively, and (c) and (d) are the corresponding phase-scrambled images that correspond to the IDFT of scrambled DFT coefficients. Figures 5 (a) and (b) show the POC surface between the non-scrambled images and that between the phase-scrambled images, respectively. A peak appears at the location that corresponds to the translational displacements. We confirmed that the POC surface of non-scrambled images and that of phase-scrambled images were identical.

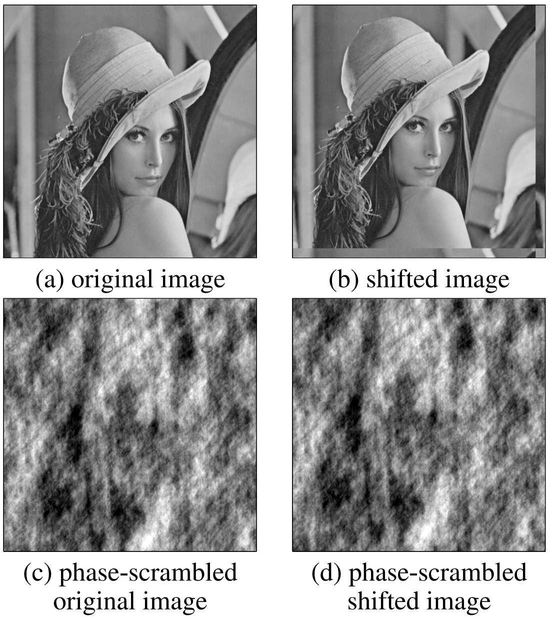

(a) original image
(b) shifted image
(c) phase-scrambled original image
(d) phase-scrambled shifted image

Figure 4: Estimation of translational displacement. (256 × 256)

Estimation of translation between images with noise was performed. 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. Figures 6 (a) and (b) show the POC surface between non-scrambled images and that between phase-scrambled images, respectively. We confirmed that the POC surface between non-scrambled image and that between phase-scrambled images were identical.

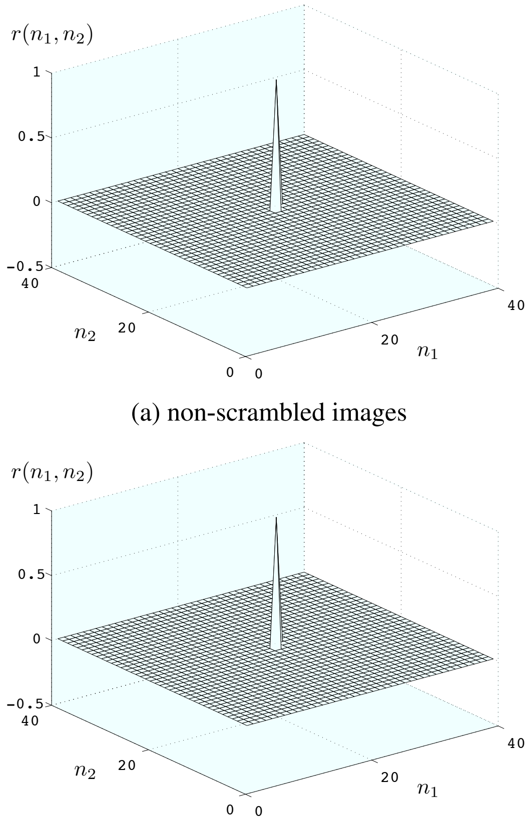
We also performed the estimation of translation with subpixel accuracy between images. We confirmed that the estimation value between the phase-scrambled images was obtained with the same accuracy as that between non-scrambled images. Details are omitted due to space limitation.

5. CONCLUSION

We have proposed a scrambling method for image matching. The method can be utilized for either POC or DCT-SPC. We have explained how to generate scrambled images so that the effect of scrambling is canceled when both POC and DCT-SPC is carried out. It is shown that the proposed method protects the information in each image keeping relative relations and that POC and DCT-SPC therefore can be directly applied in order to estimate the values between scrambled images without descrambling. There is no effect of scrambling on the accuracy of image matching. Some simulations has been presented to confirm that exactly the same accuracy is obtained and to show the appropriateness and the effectiveness of the proposed method.

Acknowledgment

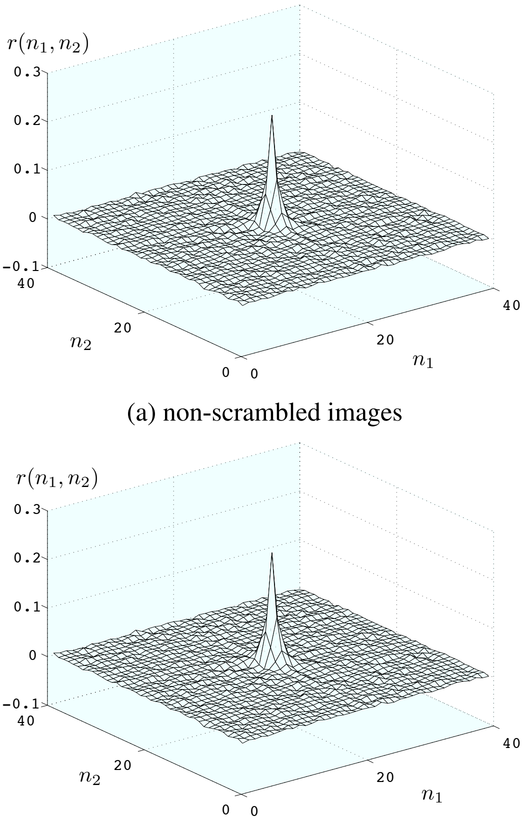
This work has been supported in part by a Grant-in-Aid for Scientific Research C No.20560361 from the Japan Society



(a) non-scrambled images

(b) scrambled images

Figure 5: Estimation of translation using POC



(a) non-scrambled images

(b) scrambled images

Figure 6: Effect of noise: Noise consists of Gaussian random numbers with 0 mean and a standard deviation of 25.

for the Promotion of Science (JSPS).

REFERENCES

[1] B. V. K. V. Kumar, A. Mahalanobis, and R. Juday, *Correlation Pattern Recognition*, Cambridge University Press. UK, 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. D. Kuglin and D. C. Hines, “The phase correlation image alignment method,” in *Proc. Int. Conf. Cybernetics and Society*, pp.163-165, Sept. 1975

[4] Q. Chen, M. Defrise, and F. Deconinck, “Symmetric phase-only matched filtering of Fourier-Mellin transforms for image registration and recognition”, *IEEE Trans. Pattern Analysis and machine intelligence*, vol.16, no.2, pp.1156-1168, Dec. 1994

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

[6] 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 Processing*, vol.II, pp.49–52, Sept. 2005

[7] 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 Processing*, vol.II, pp.33–36, Sept. 2005

[8] 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

[9] 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. Acoustics, Speech and Signal Processing*, Vol.1, pp.1237-1240, Apr. 2007

[10] I. Ito and H. Kiya, “DCT sign phase correlation and its application to estimation of translation between signals,” *Trans. IEEE Signal Processing*, submitted for publication

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

[12] K. Kuroiwa, M. Fujiyoshi, H. Kiya, “Codestream domain scrambling of moving objects based on DCT sign-only correlation for motion JPEG movies, ” in *Proc. IEEE Int. Conf. Image Processing*, vol.V, pp.157–160, Sept. 2007