# IMAGE MATCHING BETWEEN VISUALLY PROTECTED IMAGES WITH ONE-TIME KEY BASED PHASE SCRAMBLING

*Izumi Ito and Hitoshi Kiya*

Graduate School of System Design, Tokyo Metropolitan University
6-6 Asahigaoka, Hino-shi, 191-0065, Tokyo, Japan
phone: + (81)-42-585-8454, fax: + (81)-42-583-8119, email:ito-izumi@sd.tmu.ac.jp, kiya@sd.tmu.ac.jp

## ABSTRACT

We propose an image matching method using one-time key based phase scrambling. The phase scrambling is used for protection of the original information of templates visually in order to secure privacy. In the proposed method, a key is used to scramble an image once, but the key is not required in the image matching. An appropriately determined key allows image matching for visually protected images without the key. In the previously proposed image matching technique, a key was required for both scrambling and image matching.

## 1. INTRODUCTION

A number of approaches to image matching such as correlation in the space domain using features as typified by corners and edges have been investigated. Phase-only correlation (POC) is a frequency domain approach to image matching. POC with discrete Fourier transform (DFT) was first proposed by Kuglin and Hines [1]. The translation between signals and the direct measure of the degree of signal congruence can be simultaneously estimated by POC based on the Fourier shift property. In addition, the rotation and scaling can be estimated using the magnitude of DFT coefficients that are mapped into the log-polar coordinates [2]. High-accuracy estimation by POC has been developed [3, 4].

Generally, image matching using POC requires visual information protection of templates in order to secure privacy [5]. Typically, encryption is used for the protection of signals [6]. However, decryption is required before image matching using POC. In order to address these problems, we previously proposed the image matching method using phase scrambling for POC [7, 8]. The previously proposed method enables direct image matching between protected images. However, a key is required for both scrambling and image matching.

In the proposed image matching method, one-time key based phase scrambling is used for POC. A key is used once for scrambling, but is not required for image matching. The parameters that control the effect of visual information protection and image matching are discussed. A key for which parameters are chosen appropriately enables the phase scrambling to perform keyless image matching. As a result, the proposed method eliminates the need to save the key. Independent keys are used for scrambling of all templates.

## 2. PRELIMINARY

The goal of the proposed image matching method is described in this section. POC and phase scrambling for POC, which are elements of the proposed method, are then explained. One-dimensional expression is used for the sake of brevity.

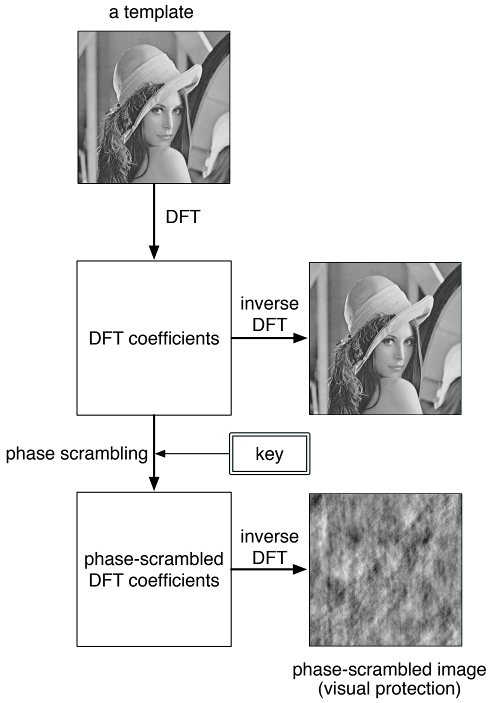
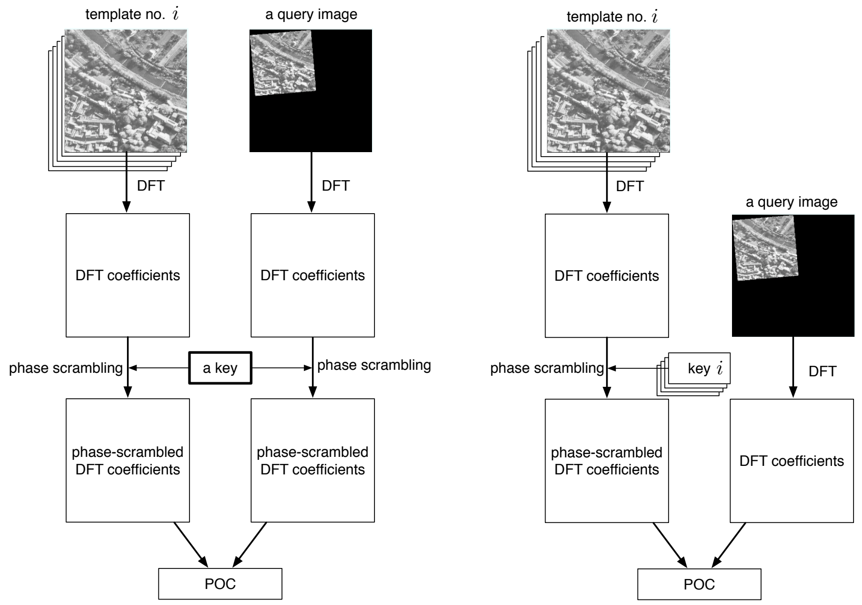

a template
DFT
DFT coefficients
inverse DFT
phase scrambling
key
phase-scrambled DFT coefficients
inverse DFT
phase-scrambled image (visual protection)

Figure 1: Phase scrambling. The phase scrambling is accomplished in the frequency domain. The inverse DFT of the DFT coefficients reveals the information of the template. Conversely, the inverse DFT of the scrambled DFT coefficients does not reveal the information of the template.

### 2.1 Goal of the proposed image matching

Phase scrambling protects the original information of images visually, as shown in Fig. 1. The phase scrambling for POC is performed in the frequency domain. The DFT coefficients of a signal are scrambled by multiplying them by random phase terms. The inverse DFT of the scrambled DFT coefficients does not reveal the original information of the image, whreas the inverse DFT of the DFT coefficients reveals the information of the original image.

The proposed image matching uses phase scrambling in order to protect the original information of templates visually in case leakage of the templates occurs. Even if the sensed



(a) previous image matching (b) proposed image matching

Figure 2: Difference between the previously proposed image matching and image matching proposed herein. (a) Previously proposed image matching. A key is required for scrambling of both templates and query images. (b) Image matching proposed herein. A key is only used for scrambling of templates. All templates are scrambled by independent keys.

image that is used as a query has translation, rotation, and scaling for the corresponding template, image matching between the phase-scrambled template and the query can be performed by POC.

Figure 2 shows the difference between the image matching that we proposed previously and the image matching proposed herein. In the previous image matching, the key that is used for phase scrambling of templates must be saved safely and used again in the image matching using POC. On the other hand, in the proposed image matching, the key that is used for phase scrambling of templates need not to be saved and is not required for image matching. Independent keys are used for all templates. The management of keys is not required.

## 2.2 POC

### 2.2.1 *Translation*

Let $G_i(k)$, $k = 0, 1, \cdots, N-1$, be the $N$-point DFT coefficients of $N$-point signal, $g_i(n)$, $n = 0, 1, \cdots, N-1$. The phase term $\phi_{G_i}(k)$ is defined as

$$\phi_{G_i}(k) = G_i(k)/|G_i(k)| \tag{1}$$

where $|G_i(k)|$ denotes the absolute value of $G_i(k)$. If $|G_i(k)| = 0$, then $\phi_{G_i}(k)$ is replaced by 0.

Let $g_2(n)$ be the shifted signal of $g_1(n)$. The normalized cross spectrum, $R_\phi(k)$, between $g_1(n)$ and $g_2(n)$ is defined in terms of their corresponding phase term $\phi_{G_1}(k)$ and $\phi_{G_2}(k)$ as follows:

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

where $\phi^*_{G_1}(k)$ denotes the complex conjugate of $\phi_{G_1}(k)$. The POC function, $r_\phi(n)$, 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 $\exp(-j2\pi/N)$ and $j$ denotes $\sqrt{-1}$. The translation between two signals is estimated by the location of the peak of $r_\phi(n)$ in Eq. (3) [1].

### 2.2.2 *Rotation and Scaling*

Rotation and scaling between two images are estimated by POC using the magnitude of DFT coefficients that are mapped into the log-polar coordinates [2]. Log-polar transform reduces the rotation angle and scale factor in the Cartesian coordinates to horizontal and vertical translation in the log-polar coordinates.

## 2.3 Phase scrambling for POC

Phase scrambling for POC is performed in the frequency domain. When $N$-point DFT coefficients, $G_i(k)$, $k = 0, 1, \cdots, N-1$, are scrambled, a key sequence, $\theta_{\alpha_i}(k)$, $k = 0, 1, \cdots, N-1$, is determined, and the corresponding phase terms are then multiplied by the DFT coefficients. Namely, the phase-scrambled DFT coefficients, $\widetilde{G}_i(k)$, are defined as

$$\widetilde{G}_i(k) = G_i(k) \cdot e^{j\theta_{\alpha_i}(k)} \ . \tag{4}$$

Replacing $G_i(k)$ in Eq. (4) by its polar form yields

$$\widetilde{G}_i(k) = |G_i(k)|\phi_{G_i}(k) \cdot e^{j\theta_{\alpha_i}(k)} \ . \tag{5}$$

The absolute value $|\widetilde{G}_i(k)|$ and the phase term $\widetilde{\phi}_{G_i}(k)$ of $\widetilde{G}_i(k)$ are related to the original absolute value $|G_i(k)|$ and the original phase term $\phi_{G_i}(k)$, respectively, as

$$|\widetilde{G_i}(k)| = |G_i(k)| \tag{6}$$

and

$$\widetilde{\phi}_{G_i}(k) = \phi_{G_i}(k) \cdot e^{j\theta_{\alpha_i}(k)} \quad . \tag{7}$$

Thus, phase scrambling affects only the phase of DFT coefficients.

The phase-scrambled signal, $\widetilde{g_i}(n)$ is defined by the inverse DFT of $\widetilde{G_i}(k)$ as

$$\widetilde{g_i}(n) = \frac{1}{N}\sum_{k=0}^{N-1}\widetilde{G_i}(k)W_N^{-nk} \quad . \tag{8}$$

The phase-scrambled image is a two-dimensional expression of the phase-scrambled signal.

In image matching, the normalized cross spectrum $\widetilde{R_\phi}(k)$ between phase scrambled DFT coefficients $\widetilde{G_1}(k)$ and $\widetilde{G_2}(k)$ is directly calculated as

$$\widetilde{R_\phi}(k) \quad = \quad \widetilde{\phi}^*_{G_1}(k) \cdot \widetilde{\phi}_{G_2}(k) \quad . \tag{9}$$

The POC function $\widetilde{r_\phi}(n)$ is then obtained from the inverse DFT of $\widetilde{R_\phi}(k)$.

## 3. PROPOSED IMAGE MATCHING

In one-time key based phase scrambling, a key is used once for scrambling of template, and the key is not required for image matching.

Let $g_1(n)$ be a template, which will be scrambled and stored in a database, and let $g_2(n)$ be a sensed signal, which will be used as a query.

### 3.1 Key parameters

A template is scrambled by $\theta_{\alpha_1}(k)$ according to Eq. (4), where $\theta_{\alpha_1}(k)$ is determined from a set $U^M_{x_1}$ that consists of $M$ members, $x_1, x_2, \cdots, x_M$:

$$\theta_{\alpha_i}(k) \in U^M_{x_1}, \quad U^M_{x_1} = \{x_1, x_2, \cdots, x_M\} \quad . \tag{10}$$

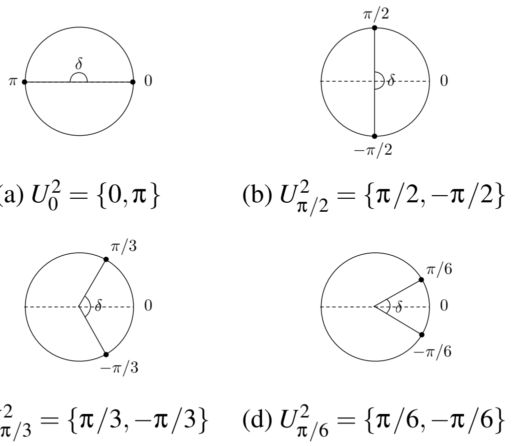
Let $q_{x_i}$ be the occurrence probability of $x_i$ and let $\delta$ be the difference of phases of members. Figure 3 shows examples of $\delta$ in two-member set. Here $q_{x_i}$ and $\delta$ affect the visual information protection in the template and the peak value of POC in image matching.

A key sequence can be generated using a random number generator, in which the random numbers are related to each member of $U^M_{x_1}$. In one-time key based phase scrambling for POC, the key sequence $\theta_{\alpha_i}(k)$ should be determined from a set appropriately, in which the occurrence probability and the difference of phases of members are considered.

### 3.2 Keyless image matching

The DFT coefficients of the query are multiplied by $\exp(jx_1)$, which is the phase term of a member of $U^M_{x_1}$:

$$\widetilde{G_2}(k) = G_2(k) \cdot e^{jx_1} \quad . \tag{11}$$



(a) $U^2_0 = \{0, \pi\}$ (b) $U^2_{\pi/2} = \{\pi/2, -\pi/2\}$

(c) $U^2_{\pi/3} = \{\pi/3, -\pi/3\}$ (d) $U^2_{\pi/6} = \{\pi/6, -\pi/6\}$

Figure 3: Difference of phases of members ($M = 2$).

According to Eq. (9), $\widetilde{R_\phi}(k)$ between $\widetilde{G_1}(k)$ and $\widetilde{G_2}(k)$ is given as

$$\begin{aligned}\widetilde{R_\phi}(k) &= \widetilde{\phi}^*_{G_1}(k) \cdot \widetilde{\phi}_{G_2}(k) \\ &= \phi^*_{G_1}(k) \cdot e^{-j\theta_{\alpha_1}(k)} \cdot \phi_{G_2}(k) \cdot e^{jx_1} \\ &= R_\phi(k) \cdot e^{j(x_1 - x_i)}.\end{aligned} \tag{12}$$

If $x_i = x_1$, then

$$\widetilde{R_\phi}(k) = R_\phi(k), \tag{13}$$

otherwise,

$$\widetilde{R_\phi}(k) \neq R_\phi(k). \tag{14}$$

Obviously, the probability of Eq. (13) corresponds to the occurrence probability of $x_1$. If $q_{x_1}$ exceeds the value of the occurrence probability of the other members in $U^M_{x_1}$, we can estimate the translation and the measure of the degree of image congruence from $\widetilde{r_\phi}(n)$, which is the inverse DFT of $\widetilde{R_\phi}(k)$.

### 3.3 Effect on the peak value of POC

In the case of two-memger set, $U^2_{x_1}$, the peak value of $\widetilde{r_\phi}(n)$ between the signals in which one-time key based phase scrambling is applied with $\delta = \pi$ is derived analytically as

$$\max_n \left(|\widetilde{r_\phi}(n)|\right) \approx |\gamma(2q_{x_1} - 1)| \tag{15}$$

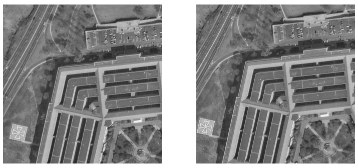
where $\gamma$ is the peak value of $r_\phi(n)$ between the non-scrambled signals. The detail derivation is omitted due to space limitation. From Eq. (15), if $q_{x_1} = 1$, then the peak value is $\gamma$. If $q_{x_1} = 0.5$, then the peak value is 0, i.e., a peak does not appear at the location $n$ that expresses the translation.

## 4. SIMULATION

The key sequence is determined from a two-member set.

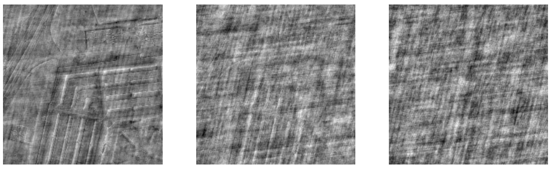
### 4.1 Occurrence probability and difference of phases

The image shown in Fig. 4(a) was scrambled. Figure 5 shows the phase-scrambled images with different occurrence probability. The key sequence is determined from $\{\pi/2, -\pi/2\}$.



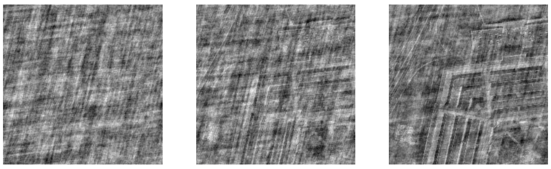
(a) template (b) query

Figure 4: Template and query. (a) Template. 512 × 512, 8 bits/pixel. (b) Query is generated by translation from (a) by 20 pixels in the horizontal and vertical directions.



$q_{\pi/2} = 0.9$ $q_{\pi/2} = 0.7$ $q_{\pi/2} = 0.5$

Figure 5: Phase-scrambled images with the occurrence probability $q_{\pi/2}$, where $\theta_{\alpha_i}(k_1,k_2) \in \{\pi/2, -\pi/2\}$. The closer $q_{\pi/2}$ to 0.5, the stronger the visual protection becomes.



$\{\pi/2, -\pi/2\}$ $\delta = \pi$ $\{\pi/3, -\pi/3\}$ $\delta = 2\pi/3$ $\{\pi/4, -\pi/4\}$ $\delta = \pi/2$

Figure 6: Phase-scrambled images with the difference of phases $\delta = 2a$, where $\theta_{\alpha_i}(k_1,k_2) \in \{a, -a\}$, $q_a = 0.5$, a = $\pi/2$, $\pi/3$, and $\pi/4$. The smaller the difference of phases in a set, the weaker the visual protection becomes.

The closer $q_{\pi/2}$ to 0.5, the stronger the visual protection becomes. Figure 6 shows the phase-scrambled images with the difference of phases $\delta$. The smaller the difference of phases in a set, the weaker the visual protection becomes. The parameters $q_{x_i}$ and $\delta$ control the visual effect of images and the peak value of POC as shown in Eq. (15).

### 4.2 Translation estimation

Image matching experiments were performed. The two images shown in Fig. 4 are translated by 20 pixels in the horizontal and vertical directions. We assume that rotation and scaling are normalized in advance. The template was scrambled by the key sequence $\theta_{\alpha_i}(k_1,k_2) \in \{\pi/2, -\pi/2\}$ with $q_{\pi/2} = 0.7$, 0.6, and 0.5, respectively.

#### *4.2.1 Without noise*

The DFT coefficients of the query were multiplied by $\exp(j\pi/2)$. Figure 7(a), (b), and (c) show the POC surface between the two images in the cases of $q_{\pi/2} = 0.7$, 0.6, and 0.5, respectively. In the cases of $q_{\pi/2} = 0.7$ and 0.6, the translation can be correctly estimated from the location of the peak value of $\tilde{r}_\phi(n)$.

Figure 8 shows the estimated locations in different key sequences. A total of 1,000 different key sequences $\theta_{\alpha_i}(k_1,k_2)$, $i = 1, \cdots, 1{,}000$ are used for the phase scrambling of the template. For the case in which $\theta_{\alpha_i}(k_1,k_2) \in \{\pi/2, -\pi/2\}$ with $q_{\pi/2} = 0.5$, the translation was not estimated correctly, as shown in Fig. 8(a). The mean and the variance of the peak values were 0.0090 and $2.53 \times 10^{-7}$, respectively. In contrast, for the case in which $\theta_{\alpha_i}(k_1,k_2) \in \{\pi/3, -\pi/3\}$ with $q_{\pi/3} = 0.5$, the translation was estimated correctly, as shown in Fig. 8(b). The mean and the variance of the peak values were 0.2065 and $1.87 \times 10^{-6}$, respectively. We also confirmed that for the case in which $\theta_{\alpha_i}(k_1,k_2) \in \{\pi/2, -\pi/2\}$ with $q_{\pi/2} = 0.7$, the translation was estimated correctly. The mean and the variance of the peak values were 0.3306 and $2.73 \times 10^{-6}$, respectively.

#### *4.2.2 With noise*

Figure 9(a) shows the POC surface between the template and the query that was corrupted by additive noise. The noise is Gaussian random numbers with zero mean and a standard deviation of 25. Figure 9(b) shows the POC surface between the template and the query that was corrupted by JPEG quantization noise. The Q-factor[1] was 200. In both cases, when $q_{\pi/2} = 0.7$, the translation can be estimated correctly.

### 4.3 Identification

Identification between a query image and templates was performed. A total of 1,000 images [9] were scrambled by $\theta_{\alpha_i}(k_1,k_2) \in \{\pi/2, -\pi/2\}$ with $q_{\pi/2} = 0.7$ and stored as templates. A query was generated from one of the images by translation, rotation, and scaling. After rotation and scaling of the query were normalized for the template, the peak value of the POC between the query and the template was calculated. We confirmed that the peak value of the POC between the query and the corresponding template was the maximum value of the peak value of all templates.

## 5. CONCLUSION

We have proposed one-time key based phase scrambling for image matching. In addition to protecting the original information of template visually for privacy and security, the proposed method enables keyless image matching. The occurrence probability and the difference of phases were introduced for the one-time key based phase scrambling. These parameters control the effect of visual information protection and the peak value of POC. Experimental results revealed the effectiveness and the appropriateness of the proposed method.

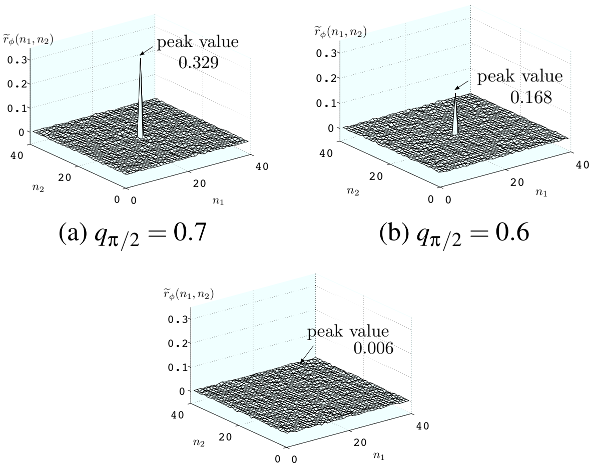
### Acknowledgment

This work has been supported in part by a Grant-in-Aid for Scientific Research C No.20560361 from the Japan Society for the Promotion of Science (JSPS).

## REFERENCES

[1] C. D. Kuglin and D. C. Hines, “The phase correlation image alignment method,” in *Proc. Int. Conf. Cybernetics and Society*, pp.163–165, September 1975

[1] 8 × 8 DCT coefficients are divided by the quantization step $Q(k_1,k_2)$. $Q(k_1,k_2)$ is generated by $Q_T(k_1,k_2) \cdot Q_F/50$, where $Q_T(k_1,k_2)$ and $Q_F$ denote a predefined quantization table and a Q-factor, respectively.

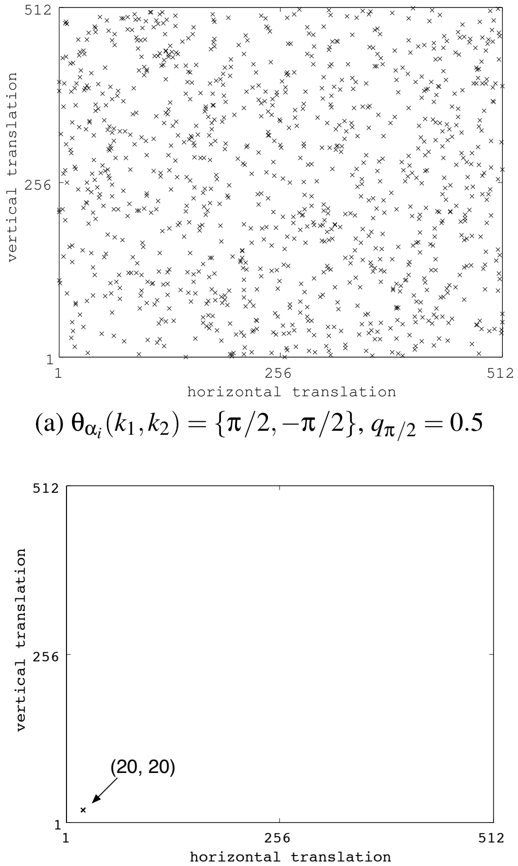


(a) $q_{\pi/2} = 0.7$

(b) $q_{\pi/2} = 0.6$

(c) $q_{\pi/2} = 0.5$

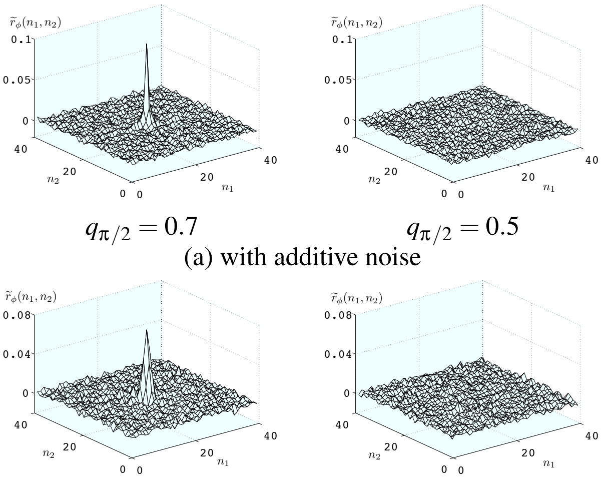
Figure 7: POC surface without noise. $\theta_{\alpha_i}(k_1,k_2) \in \{\pi/2, -\pi/2\}$. The peak value decreases according to Eq. (15).



(a) $\theta_{\alpha_i}(k_1,k_2) = \{\pi/2, -\pi/2\}$, $q_{\pi/2} = 0.5$

(b) $\theta_{\alpha_i}(k_1,k_2) = \{\pi/3, -\pi/3\}$, $q_{\pi/3} = 0.5$

Figure 8: Translation estimation without noise with a total of 1,000 different key sequences. The 'x' plots denote the estimated translation that is the location of the peak value of the POC surface.



$q_{\pi/2} = 0.7$ $q_{\pi/2} = 0.5$

(a) with additive noise

$q_{\pi/2} = 0.7$ $q_{\pi/2} = 0.5$

(b) with JPEG quantization noise

Figure 9: POC surface with noise. $\theta_{\alpha_i}(k_1,k_2) \in \{\pi/2, -\pi/2\}$. (a) The query is corrupted by additive noise (Gaussian random numbers with zero mean and a standard deviation of 25). (b) The query is corrupted by JPEG quantization noise (Q-factor = 200).

[2] 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.12, Dec. 1994

[3] 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.

[4] K. Takita, T. Aoki, Y. Sasaki, T. Higuchi, and K. Kobayashi, "High-accuracy subpixel image registration based on phase-only correlation," *IEICE Trans. Fundamentals,* vol.E86-A, no.8, pp.1925–1934, Aug. 2003

[5] 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

[6] M. Fujiyoshi, W. Saitou, O. Watanabe, and H.Kiya, "Hierarchical encryption of multimedia contents for access control," in *Proc. IEEE ICIP 2006*, pp.1977–1980, Atlanta, USA, Oct. 8-11, 2006

[7] I. Ito and H. Kiya, "Image matching between scrambled images for secure data management," in *Proc. EUSIPCO 2008*, Lausanne, Switzerland, August 25-29, 2008.

[8] I. Ito and H. Kiya, "Phase scrambling for blind image matching," in *Proc. IEEE ICASSP 2009*, pp.1521-1524, Taipei, R.O.C., April 19-24, 2009.

[9] G. Schaefer and M. Stich "UCID - An uncompressed colour image database," in *Proc. SPIE, Storage and Retrieval Methods and Applications for Multimedia*, pp. 472-480, San Jose, USA. 2004