Hindawi Publishing Corporation
EURASIP Journal on Information Security
Volume 2009, Article ID 841045, 11 pages
doi:10.1155/2009/841045

Research Article

One-Time Key Based Phase Scrambling for Phase-Only Correlation between Visually Protected Images

Izumi Ito (EURASIP Member) and Hitoshi Kiya (EURASIP Member)

Graduate School of System Design, Tokyo Metropolitan University, 6-6 Asahigaoka, Hino-shi, Tokyo 191-0065, Japan

Correspondence should be addressed to Hitoshi Kiya, kiya@sd.tmu.ac.jp

Received 24 March 2009; Revised 18 August 2009; Accepted 23 October 2009

Recommended by Sen-Ching Samson Cheung

One-time key based phase scrambling is proposed for privacy-protected image matching. The image matching is performed using invisible templates that are protected by phase scrambling. A key for phase scrambling is not required for the image matching, and the key can even be discarded after scrambling if the template does not need to be reconstructed. Theoretical analyses are presented to provide guidelines for designing key parameters that affect the visual effect and image matching. Experimental results demonstrate the effectiveness and appropriateness of the proposed method.

1. Introduction

A number of approaches to image matching, such as correlation in the space domain and using features as typified by corners and edges, have been investigated. Phase-only correlation (POC) is a frequency domain approach to image matching. Phase-only correlation 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 log-polar coordinates [2]. High-accuracy estimation by POC has been developed [3–5].

Generally, image matching using POC requires visual protection of templates in order to secure privacy [6, 7]. Typically, encryption is used for the protection of signals [8]. However, decryption is required before image matching using POC. In order to address these problems, we previously proposed a method for image matching that used synchronized phase scrambling [9, 10]. The previously proposed method enables direct image matching between protected images. However, a key is required for both scrambling and image matching, and the key must be kept secret from attackers.

In one-time key based phase scrambling, a key is used once for scrambling but is not required for image matching. Moreover, after scrambling, the key can be discarded if the template does not need to be reconstructed. Under the limited two-member set, the effect of scrambling on POC values and the visual effect are analyzed theoretically, and these analyses provide a guideline for designing key parameters. A key for which the parameters have been chosen appropriately enables keyless image matching to be performed by phase scrambling. Finally, experimental results demonstrate the effectiveness and appropriateness of the proposed scrambling.

2. Preliminary

The goal of the proposed image matching method is described in this section. Phase-only correlation and phase scrambling for POC, which are elements of the proposed method, are then explained. In the present paper, for the sake of brevity, the one-dimensional case is considered. Let $\mathbb{C}$, $\mathbb{R}$, and $\mathbb{Z}$ denote the sets of complex, real, and integer numbers, respectively.

2.1. Goal of the Proposed Image Matching. Phase scrambling protects the original information of images visually, as shown in Figure 1. The phase scrambling for POC is performed in

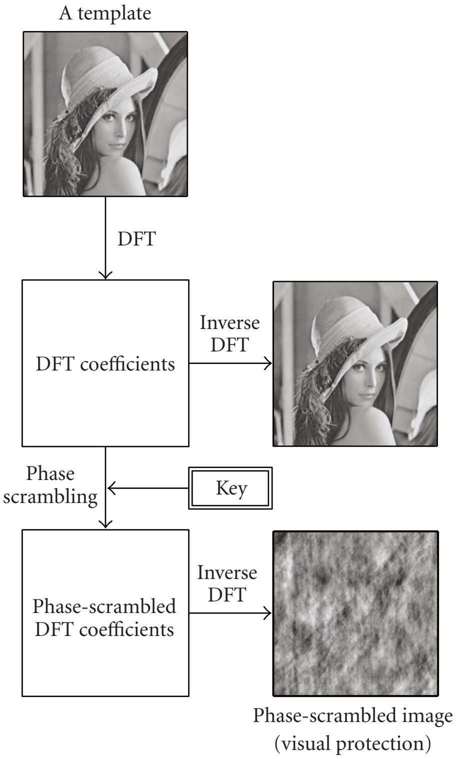


Figure 1: Phase scrambling. The phase scrambling is accomplished in the frequency domain. The inverse DFT of the DFT coefficients reveals the information of the template. Conversely, the inverse DFT of the scrambled DFT coefficients does not reveal the information of the template.

the frequency domain. The DFT coefficients of a signal are scrambled by multiplying the coefficients with random phase terms. The inverse DFT of the scrambled DFT coefficients does not reveal the original information of the image, whereas 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 there is leakage of the template. Image matching between the phase-scrambled template and the query can be performed by POC even if the sensed image that is used as a query has translation, rotation, and scaling for the corresponding template.

The difference between the previously proposed image matching and the image matching proposed herein is shown in Figure 2. In the previous method, the key used for the phase scrambling of templates must be saved securely and reused in the image matching by POC. On the other hand, in the proposed method, the key used for phase scrambling of templates is not required for image matching and does not need to be saved. Independent keys are used for all templates and the key is a one-use key.

2.2. POC

2.2.1. Translation. Let $G_i(k)$, $k = 0, 1, \ldots, N-1$, $i \in \mathbb{Z}$ be the N-point DFT coefficients of N-point signal, $g_i(n) \in \mathbb{R}$, $n = 0, 1, \ldots, N-1$. The phase term $\phi_{G_i}(k)$ is defined as

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

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 terms $\phi_{G_1}(k)$ 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 $\sqrt{-1}$ [1]. The translation between two signals is estimated by the location of the peak of $r_\phi(n)$ in (3). In addition, the value of the peak is used as a measure of the signal congruence.

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 log-polar coordinates [2]. Log-polar transform reduces the rotation angle and scale factor in the Cartesian coordinates to horizontal and vertical translation in log-polar coordinates.

2.3. Phase Scrambling for POC

2.3.1. Phase Scrambling and Phase-Scrambled Signal. Phase scrambling for POC is performed in the frequency domain. The phase-scrambled DFT coefficients, $\widetilde{G}_i(k)$, are defined as

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

where $\theta_{\alpha_i}(k)$ denotes a key sequence and α_i denotes an identifier for the key sequence. Phase scrambling affects only the phase term, that is, the scrambled phase term, $\widetilde{\phi_{G_i}}(k)$, is given as

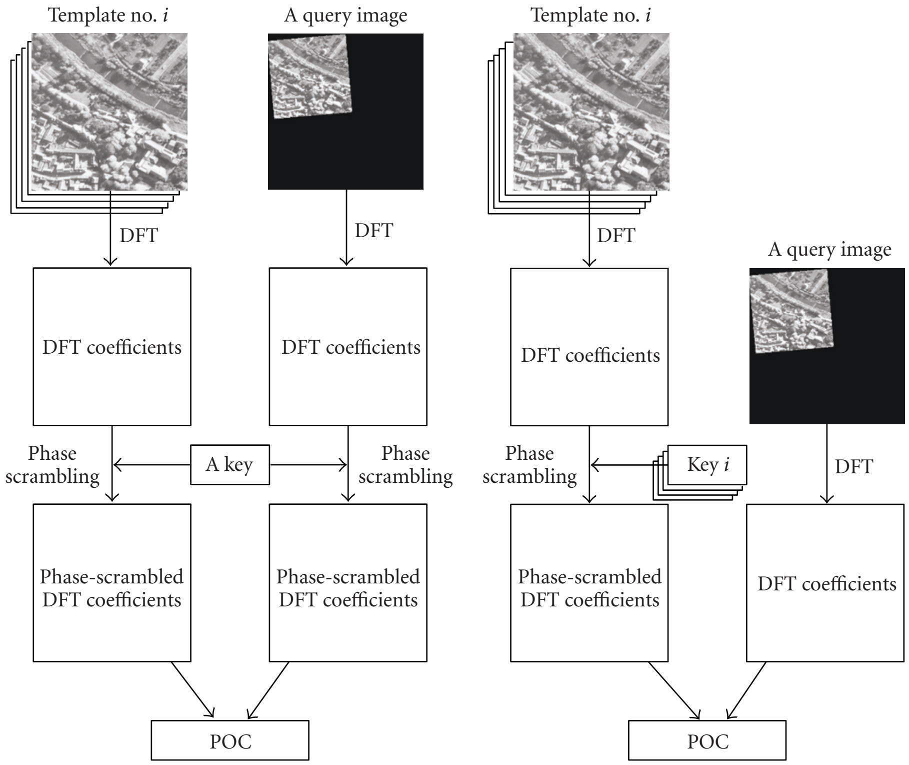
$$\widetilde{\phi_{G_i}}(k) = \phi_{G_i} \cdot e^{j\theta_{\alpha_i}(k)}. \tag{5}$$

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

$$\widetilde{g}_i(n) = \frac{1}{N}\sum_{k=0}^{N-1} \widetilde{G}_i(k) W_N^{-nk}. \tag{6}$$

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

A key sequence is constructed from a set of M members, $x_1, x_2, \ldots, x_M \in \mathbb{R}$, and the length of the key sequence is



(a) previous image matching

(b) proposed image matching

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

the same as that of the DFT coefficients. That is, an M-ary key sequence, $\theta_{\alpha_i}(k)$, is expressed with a set, $U_{x_1}^M$, as

$$\theta_{\alpha_i}(k) \in U_{x_1}^M, \quad \forall k,$$
$$U_{x_1}^M = \{x_1, x_2, \ldots, x_M\}, \tag{7}$$

where, for convenience, the superscript and subscript of the term $U_{x_1}^M$ denote the number of members and the first member, respectively. A key sequence can be generated using a cryptographically secure pseudorandom number generator, in which the random numbers are related to each member of $U_{x_i}^M$ specified by the users. As M increases, the key space increases, whereas the determination of members becomes more complicated.

2.3.2. Image Matching under Synchronized Phase Scrambling. The phase scrambled signal can be used directly for image matching using POC.

Let $g_1(n)$ and $g_2(n)$ be a template and a query, respectively. According to (4), $g_1(n)$ is scrambled by $\theta_{\alpha_1}(k)$ and then stored in the form of phase-scrambled DFT coefficients in a system. When the system is queried with respect to $g_2(n)$, $g_2(n)$ is scrambled by $\theta_{\alpha_2}(k)$, and the POC between $\widetilde{G_1}(k)$ and $\widetilde{G_2}(k)$ is then performed. In other words, $\widetilde{G_1}(k)$ and $\widetilde{G_2}(k)$ are given as

$$\widetilde{G_1}(k) = G_1(k) \cdot e^{j\theta_{\alpha_1}(k)},$$
$$\widetilde{G_2}(k) = G_2(k) \cdot e^{j\theta_{\alpha_2}(k)}. \tag{8}$$

The normalized cross spectrum $\widetilde{R}_\phi(k)$ is calculated as

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

The POC function $\widetilde{r}_\phi(n)$ is then obtained as

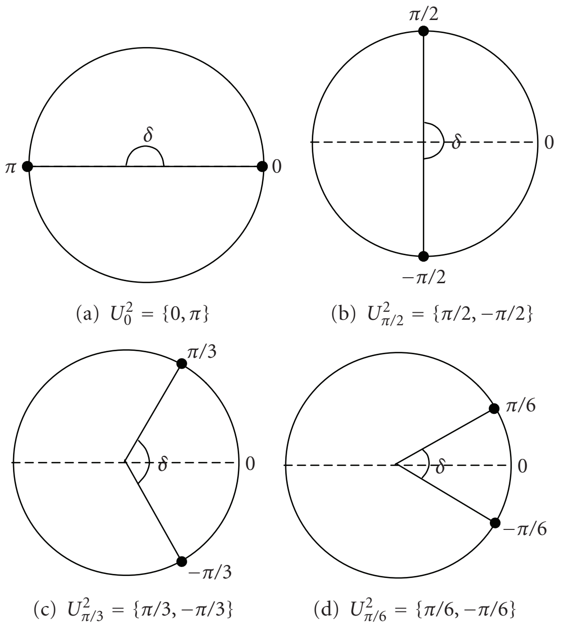
$$\widetilde{r}_\phi(n) = \frac{1}{N}\sum_{k=0}^{N-1} \widetilde{R}_\phi(k) W_N^{-nk}. \tag{10}$$

When the key sequence for the template and that for the query are the same, the POC under phase scrambling and the POC between nonscrambled signals are identical. Namely, if for all k, $\theta_{\alpha_1}(k) = \theta_{\alpha_2}(k)$, then by substituting (5) into (9), we obtain the following:

$$\widetilde{R_\phi}(k) = \phi^*_{G_1}(k)e^{-j\theta_{\alpha_1}(k)} \cdot \phi_{G_2}(k)e^{j\theta_{\alpha_1}(k)} = R_\phi(k). \tag{11}$$

From (3), (10), and (11), we therefore obtain

$$\widetilde{r_\phi}(n) = r_\phi(n). \tag{12}$$



(a) $U_0^2 = \{0, \pi\}$

(b) $U_{\pi/2}^2 = \{\pi/2, -\pi/2\}$

(c) $U_{\pi/3}^2 = \{\pi/3, -\pi/3\}$

(d) $U_{\pi/6}^2 = \{\pi/6, -\pi/6\}$

Figure 3: Difference of phases.

Thus, a key sequence is used for both the template and the query, and these two key sequences are synchronized. In the proposed method, a key sequence is used for a template only.

3. Proposed Image Matching and Visual Information Protection

One-time key based phase scrambling is proposed and analyzed statistically. In the present paper, the set for key sequences is limited to a two-member set.

3.1. One-Time Key Based Phase Scrambling for POC. A binary key sequence is used only once for scrambling a template and is not required for image matching.

The binary key sequence is constructed from a set of only two members, x_1 and x_2, that is,

$$\theta_{\alpha_1}(k) \in U_{x_1}^2 = \{x_1, x_2\}. \tag{13}$$

For an N-point signal, a binary key sequence of length N is generated using a cryptographically secure pseudo random number generator, the output of which belongs to either x_1 or x_2. Let q_{x_1} be the occurrence probability of x_1, and let δ be the difference of phases, $x_1 - x_2$, examples of which are shown in Figure 3.

Let $g_1(n)$ and $g_2(n)$ be a template and a query, respectively. In a system, $g_1(n)$ is scrambled by $\theta_{\alpha_1}(k) \in U_{x_1}^2$ according to (4) and is stored in the form of $\widetilde{G_1}(k)$. When the system is queried with respect to $g_2(n)$, its DFT coefficients, $G_2(k)$, are multiplied by a constant, that is,

$$\widetilde{G_1}(k) = G_1(k) \cdot e^{j\theta_{\alpha_1}(k)}, \tag{14}$$

$$\widetilde{G_2}(k) = G_2(k) \cdot e^{jx_1(k)}. \tag{15}$$

The POC between $\widetilde{G_1}(k)$ and $\widetilde{G_2}(k)$ is calculated according to (9) and (10).

Although (12) is not satisfied under one-time key based phase scrambling, the peak value of $r_\phi(n)$, which is used as a measure of signal congruence, is estimated from $\widetilde{r_\phi}(n)$ using parameters that are explained in the following section.

3.2. Effect of One-Time Key Based Phase Scrambling. The effect on the peak value of POC is considered in terms of the average value of POC under the proposed scrambling.

From (5), (9), (14) and (15), $\widetilde{R_\phi}(k)$ is expressed as

$$\begin{aligned}\widetilde{R_\phi}(k) &= \widetilde{\phi}^*_{G_1}(k) \cdot \widetilde{\phi}_{G_2}(k) \\ &= \phi^*_{G_1}(k) e^{-j\theta_{\alpha_1}(k)} \cdot \phi_{G_2}(k) e^{jx_1} \\ &= R_\phi(k) e^{j(x_1 - \theta_{\alpha_1}(k))}.\end{aligned} \tag{16}$$

Here, we assume that the key sequence is a single value, that is, if for all k, $\theta_{\alpha_i}(k) = x_C$, then

$$\widetilde{R_\phi}(k) = R_\phi(k) e^{j(x_1 - x_C)} \tag{17}$$

and since $e^{j(x_1 - x_C)}$ is a constant, from (10), $\widetilde{r_\phi}(n)$ can be obtained as

$$\widetilde{r_\phi}(n) = e^{j(x_1 - x_C)} r_\phi(n). \tag{18}$$

Under the above assumption, if $x_C = x_1$, then

$$\widetilde{r_\phi}(n) = r_\phi(n), \tag{19}$$

and if $x_C = x_2$, then

$$\widetilde{r_\phi}(n) = e^{j(x_1 - x_2)} r_\phi(n). \tag{20}$$

From (19) and (20), the average value of $\widetilde{r_\phi}(n)$, that is, $\widetilde{r}_{\phi_{\text{ave}}}(n)$, is defined in terms of q_{x_1} as follows:

$$\widetilde{r}_{\phi_{\text{ave}}}(n) = q_{x_1} \cdot r_\phi(n) + (1 - q_{x_1}) \cdot e^{j\delta} \cdot r_\phi(n). \tag{21}$$

Since $\widetilde{r}_{\phi_{\text{ave}}}(n)$ is a complex number, the real and imaginary parts of $\widetilde{r}_{\phi_{\text{ave}}}(n)$ can be expressed as

$$\begin{aligned}\operatorname{Re}\left(\left[\widetilde{r}_{\phi_{\text{ave}}}(n)\right]\right) &= q_{x_1} r_\phi(n) + (1 - q_{x_1}) \cdot \cos(\delta) \cdot r_\phi(n), \\ \operatorname{Im}\left(\left[\widetilde{r}_{\phi_{\text{ave}}}(n)\right]\right) &= (1 - q_{x_1}) \cdot \sin(\delta) \cdot r_\phi(n),\end{aligned} \tag{22}$$

where Re[·] and Im[·] denote the operations to obtain the real and imaginary parts, respectively, of signals, and their peak values can be given as

$$\max_n\left(\left|\operatorname{Re}\left[\widetilde{r}_{\phi_{\text{ave}}}(n)\right]\right|\right) = |q_{x_1} p + (1 - q_{x_1}) \cdot \cos(\delta) \cdot p|, \tag{23}$$

$$\max_n\left(\left|\operatorname{Im}\left[\widetilde{r}_{\phi_{\text{ave}}}(n)\right]\right|\right) = |(1 - q_{x_1}) \cdot \sin(\delta) \cdot p|, \tag{24}$$

where p denotes the peak value of $r_\phi(n)$, which is referred to as the original peak value.

The peak value of POC under one-time key based phase scrambling is approximated by the average value of POC under one-time key based phase scrambling. That is,

$$\begin{aligned} \max_n\left(\left|\mathrm{Re}\left[\tilde{r}_\phi(n)\right]\right|\right) &\approx \max_n\left(\left|\mathrm{Re}\left[\tilde{r}_{\phi_{\mathrm{ave}}}(n)\right]\right|\right), \\ \max_n\left(\left|\mathrm{Im}\left[\tilde{r}_\phi(n)\right]\right|\right) &\approx \max_n\left(\left|\mathrm{Im}\left[\tilde{r}_{\phi_{\mathrm{ave}}}(n)\right]\right|\right). \end{aligned} \tag{25}$$

Based on the above consideration, we observe the following.

Adjustment of the Peak Value. The peak value of $\tilde{r}_\phi(n)$ can be controlled using the occurrence probability, q_{x_1}, and the difference of phases, δ, as parameters. If queries are expected to contain noise, which causes a lower peak value, the peak value can be adjusted using parameters q_{x_1} and δ to be higher within (23) and (24).

Invalid Parameters for the Proposed Scrambling. There is a set of invalid parameters for one-time key based phase scrambling. From (24), we obtain $\delta = \pi + 2\pi l$, $l \in \mathbb{Z}$ such that, for $q_{x_1} \neq 0$, $\max_n(|\mathrm{Im}[\tilde{r}_{\phi_{\mathrm{ave}}}(n)]|) = 0$. From (23), we obtain $q_{x_1} = 0.5$ such that, for $\delta = \pi + 2\pi l$, $\max_n(|\mathrm{Re}[\tilde{r}_{\phi_{\mathrm{ave}}}(n)]|) = 0$. The set of invalid parameters is thus given as

$$(q_{x_1}, \delta) = (0.5, \pi + 2\pi l), \quad l \in \mathbb{Z}. \tag{26}$$

Estimation of the Original Peak Value. The original peak value, p, can be estimated from $\tilde{r}_\phi(n)$ using parameters q_{x_1} and δ, and thereby the effect of scrambling can be practically avoided. From (23) and (24), the original peak value, p, can be estimated from the observed peak value using the above parameters as follows:

$$\begin{aligned} p &\approx \frac{\max_n\left(\left|\mathrm{Re}\left[\tilde{r}_\phi(n)\right]\right|\right)}{\left(q_{x_1} + \left(1 - q_{x_1}\right) \cdot \cos(\delta)\right)}, \\ p &\approx \frac{\max_n\left(\left|\mathrm{Im}\left[\tilde{r}_\phi(n)\right]\right|\right)}{\left(\left(1 - q_{x_1}\right) \cdot \sin(\delta)\right)}. \end{aligned} \tag{27}$$

3.3. Effect on Visual Information. We consider the error energy between the phase scrambled signal and the non-scrambled signal, in which the larger error energy provides greater visual protection.

Let $\tilde{g}_i(n)$ be the scrambled signal of the original signal, $g_i(n)$, obtained using the key sequence $\theta_{\alpha_i}(k)$, that is,

$$\tilde{g}_i(n) = \frac{1}{N}\sum_{k=0}^{N-1} G_i(k) e^{j\theta_{\alpha_i}(k)} W_N^{-nk}. \tag{28}$$

Here, we assume that the key sequence is a single value, that is, if for all k, $\theta_{\alpha_i}(k) = x_C$, then

$$\begin{aligned} \tilde{g}_i(n) &= \frac{1}{N}\sum_{k=0}^{N-1} G_i(k) e^{jx_C} W_N^{-nk} \\ &= e^{jx_C} \frac{1}{N}\sum_{k=0}^{N-1} G_i(k) W_N^{-nk} \\ &= e^{jx_C} g_i(n). \end{aligned} \tag{29}$$

Under the above assumption, since $\tilde{g}_i(n)$ is a complex number, the real and imaginary parts of $\tilde{g}_i(n)$ are expressed accordingly as

$$\mathrm{Re}[\tilde{g}_i(n)] = \cos(x_C) \cdot g_i(n), \tag{30}$$

$$\mathrm{Im}[\tilde{g}_i(n)] = \sin(x_C) \cdot g_i(n). \tag{31}$$

The real part of the error energy, E_r, between the original signal and the real part of the phase scrambled signal is defined as

$$E_r = \sum_{n=0}^{N-1} \left| g_i(n) - \mathrm{Re}[\tilde{g}_i(n)] \right|^2. \tag{32}$$

Under the above assumption, from (30), (32) is expressed as

$$\begin{aligned} E_r &= \sum_{n=0}^{N-1} |1 - \cos(x_C)|^2 \left| g_i(n) \right|^2 \\ &= |1 - \cos(x_C)|^2 \cdot C_{g_i}, \end{aligned} \tag{33}$$

where

$$C_{g_i} = \sum_{n=0}^{N-1} \left| g_i(n) \right|^2. \tag{34}$$

If $x_C = x_1$, then

$$E_r = |1 - \cos(x_1)|^2 \cdot C_{g_i} \tag{35}$$

and if $x_C = x_2$, then

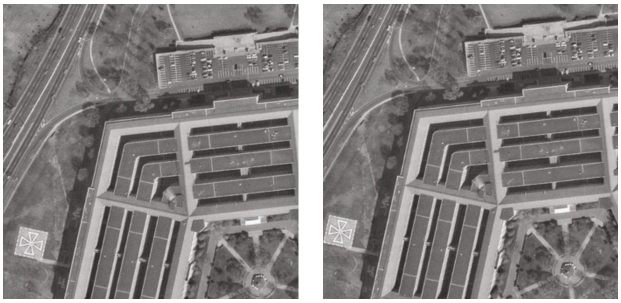
$$E_r = |1 - \cos(x_2)|^2 \cdot C_{g_i}. \tag{36}$$

The average, $\overline{E}_r$, of the real part of the error energy, E_r, is defined in terms of the occurrence probability, q_{x_1}, as

$$\overline{E}_r = q_{x_1} |1 - \cos(x_1)|^2 \cdot C_{g_i} + \left(1 - q_{x_1}\right) |1 - \cos(x_2)|^2 \cdot C_{g_i}. \tag{37}$$

The average of the imaginary part of the error energy is defined in a similar manner. The imaginary part of the error energy, E_i, between the original signal and the imaginary part of phase scrambled signal is defined as

$$E_i = \sum_{n=0}^{N-1} \left| g_i(n) - \mathrm{Im}[\tilde{g}_i(n)] \right|^2. \tag{38}$$



(a) template (b) query

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

The average, $\overline{E}_i$, of E_i is defined with q_{x_1} as

$$\overline{E}_i = q_{x_1}|1-\sin(x_1)|^2 \cdot C_{g_i} + (1-q_{x_1})|1-\sin(x_2)|^2 \cdot C_{g_i}. \tag{39}$$

The visual effect of phase-scrambled signals can be estimated from (37) and (39), as will be shown in Section 4.2.

The parameters for key sequence are selected based on both the average error energy and the effect on the peak value discussed in Section 3.2.

3.4. Security Consideration. A key sequence based on a user-specified key is generated using a cryptographically secure pseudorandom number generator. A key sequence is used only once for scrambling a template. If the scrambled template does not need to be reconstructed in a system, the key sequence can be discarded after scrambling, and, consequently, its protection is not required. In the following, we focus on the known-plaintext attack and the ciphertext-only attack.

3.4.1. Known-Plaintext Attack. This model assumes that an attacker has samples of both a plaintext and its ciphertext and uses them to reveal further secret information, such as secret keys and code books.

In a system using the proposed scrambling, each template is scrambled by an independent key sequence. Accordingly, even if an attacker obtains sets of a plaintext and its ciphertext, the other key sequences cannot be inferred by these sets.

3.4.2. Ciphertext-Only Attack. This model assumes that an attacker accesses only a ciphertext.

In this model, there are two approaches by which to deduce the original template:

(1) using a local image possessed by an attacker.

(2) guessing a key sequence.

With respect to the former approach, although the original template can be inferred using the signal congruence from the POC between a scrambled template and a local image possessed by an attacker, or through other methods using such a local image, even if an attack is successful, the attacker has already had access to a closely related image; the contents of which are already known to the attacker prior to the attack. Namely, the situation is considered as a case in which the information has been already leaked. The aim of the proposed scrambling is to prevent the information leakage from a template itself. The inference by using a local image is therefore excluded from the scope of the protection of the proposed scrambling.

With respect to the latter approach, theoretically, even if in the case of a brute force attack, as in the case of the one-time pad, which is unconditionally secure and theoretically unbreakable, it is impossible to confirm whether an inferred key sequence is correct. Since not a binary bit but a coherent unit of phase is changed, the scrambled template can be practically inferred by brute force attack although complete restoration is impossible for the above-described reason. Consequently, the proposed scrambling protects the visual information of the original template within the scope of key space and completely protects the original template. If the size of a template is $N \times N$, the key space is $2^{N\times N}$. We assume the size of a template to be adequate.

When a system requires much higher security, the proposed scrambling can be combined with other cryptographic techniques. Even if decryption is required for image matching, the effect of the proposed scrambling remains valid.

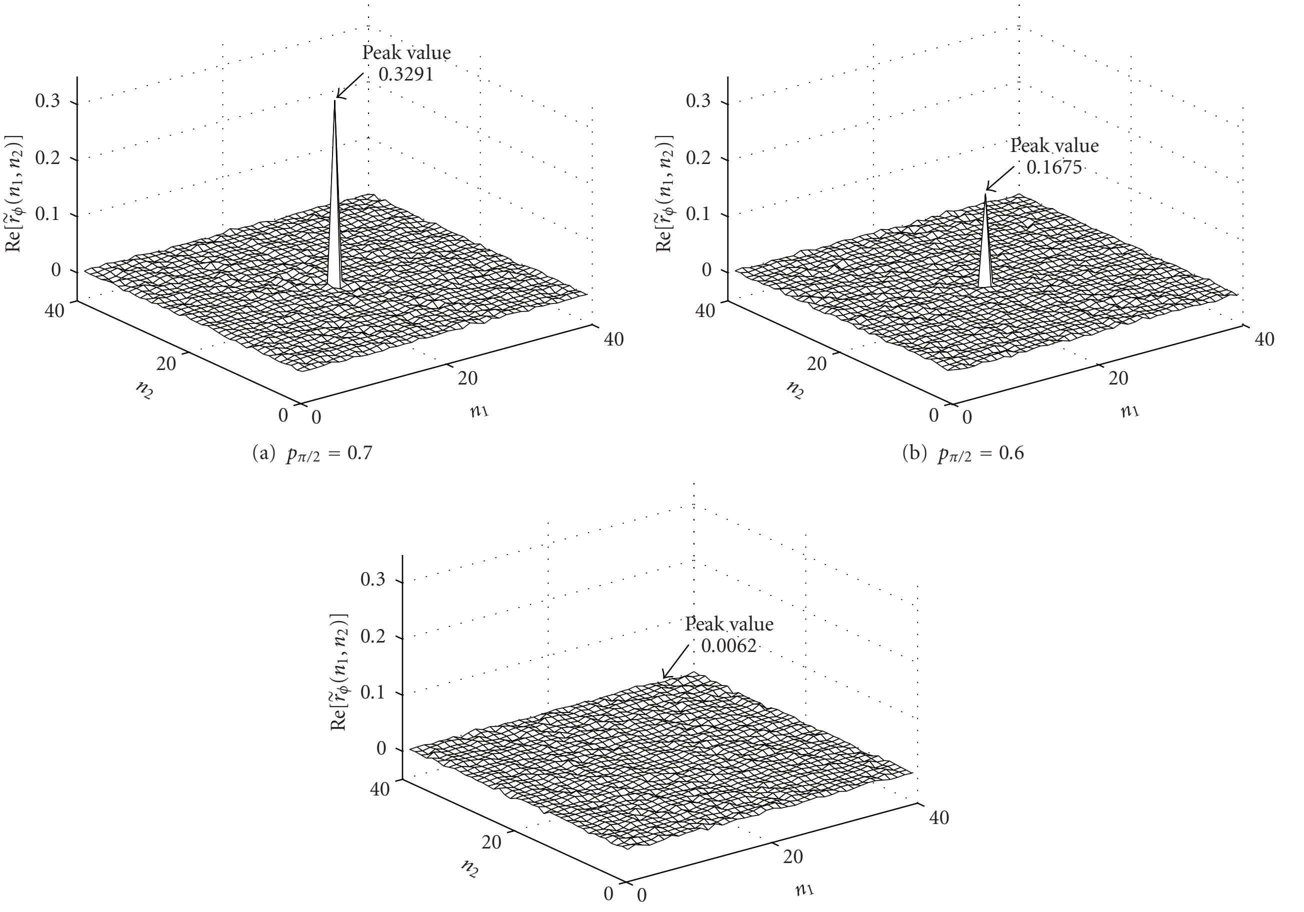
4. Simulations

4.1. POC under the Proposed Scrambling. We performed POC between two images under one-time key based phase scrambling to show that both translation and signal congruence can be estimated even under scrambling.

In the following simulations, we used a 512×512 section of a $1,024 \times 1,024$, 8-bits/pixel image called "pentagon", as a template and a query, as shown in Figure 4. The template and query were translated by 20 pixels in the horizontal and vertical directions. The template was scrambled by a key sequence, $\theta_{\alpha_i}(k_1,k_2)$, according to (4). After the query was processed according to (15), POC was performed between the template and the query. The translation and signal congruence were then estimated from the observed peak of the POC surface.

4.1.1. Without Noise. First, we evaluated the peak value by controlling the parameters for key sequences. The key sequence $\theta_{\alpha_i}(k_1,k_2)$ was generated using the sets of $\{\pi/2,-\pi/2\}$, that is, $\delta = \pi$ with $q_{\pi/2} = 0.5$ to 0.95, and $\{a,-a\}$, $a = \pi/8$ to $\pi/2$ with $q_a = 0.5$, respectively. The original peak value, p, which is the peak value of the POC between the non-processed template and query, was 0.8264.

The real parts of POC surfaces for the cases in which $\theta_{\alpha_i}(k_1,k_2) \in \{\pi/2,-\pi/2\}$ with $q_{\pi/2} = 0.7$, 0.6, and 0.5, are shown in Figures 5(a), 5(b), and 5(c), respectively. Peaks appeared on the POC surfaces, and the observed peak values were 0.3291, 0.1675, and 0.0062, respectively. The observed

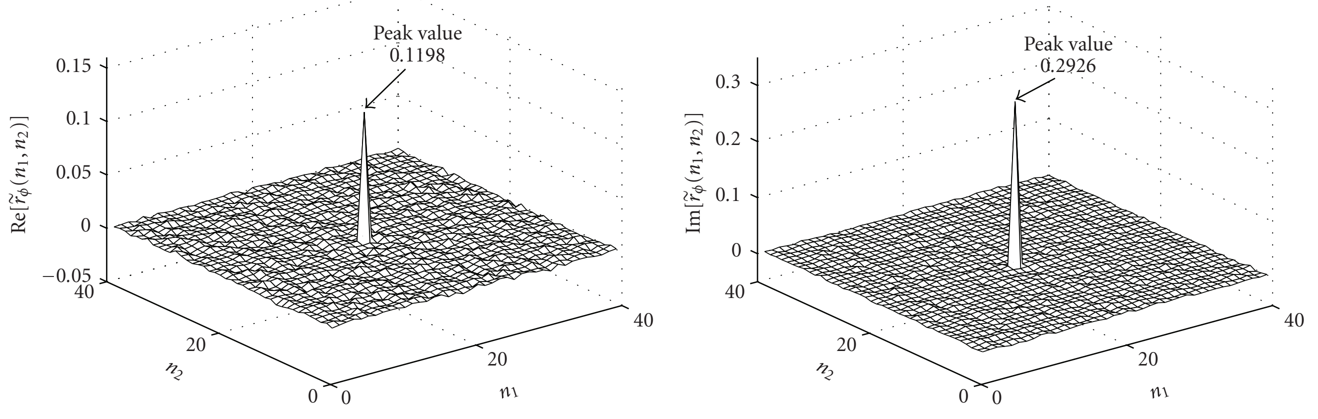


(a) $p_{\pi/2} = 0.7$

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

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

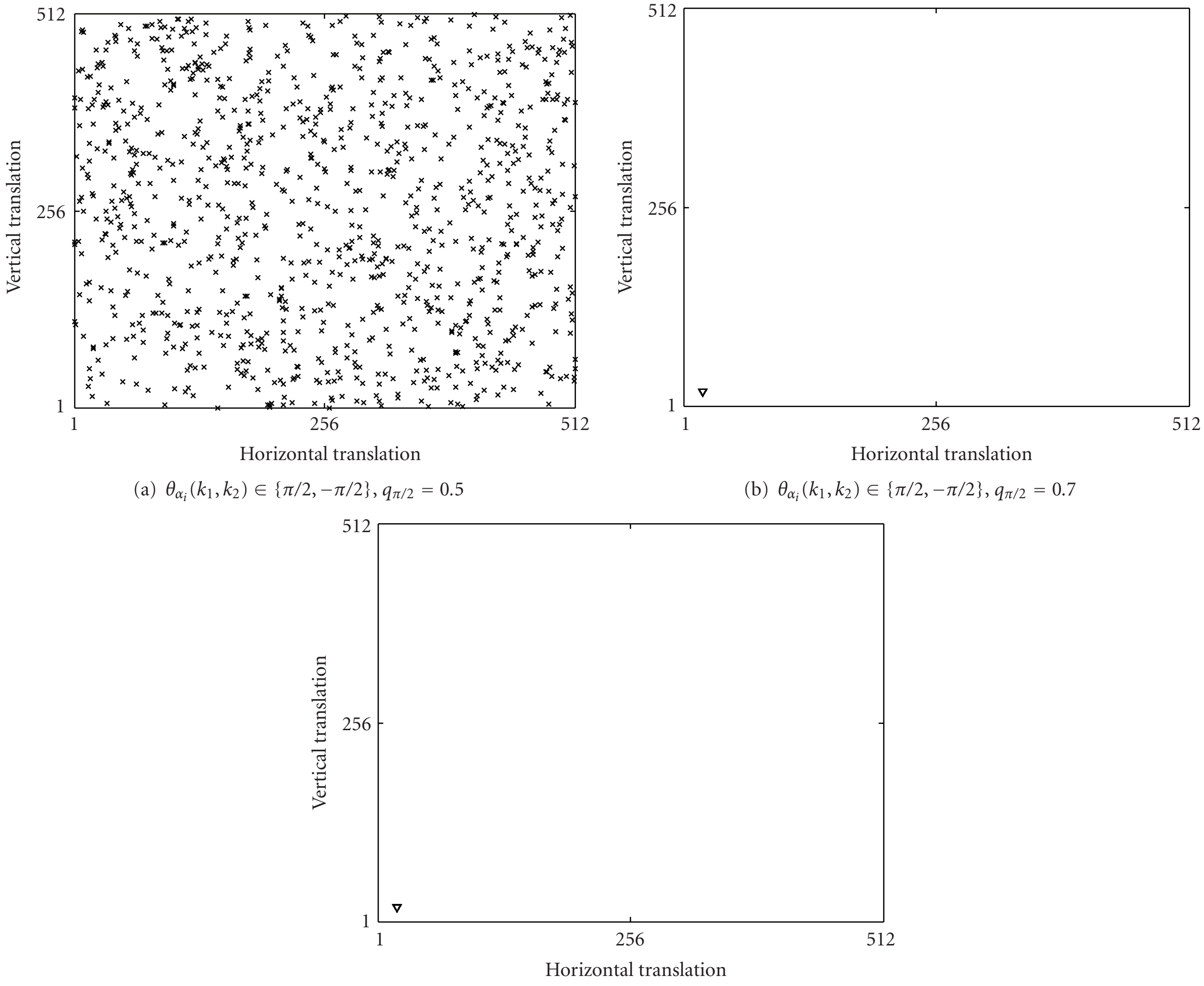
FIGURE 5: Real part of the POC surface without noise. $\theta_{\alpha_i}(k_1,k_2) \in \{\pi/2, -\pi/2\}$, $(\delta = \pi)$. The peak value decreases according to (23) as $q_{\pi/2}$ approaches 0.5.



(a) real part

(b) imaginary part

FIGURE 6: Real and imaginary parts of the POC surface without noise. $\theta_{\alpha_i}(k_1,k_2) \in \{3\pi/8, -3\pi/8\}$, $(\delta = 3\pi/4)$ with $q_{3\pi/8} = 0.5$.



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

(b) $\theta_{\alpha_i}(k_1, k_2) \in \{\pi/2, -\pi/2\}$, $q_{\pi/2} = 0.7$

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

Figure 7: Translation estimation without noise using a total of 1,000 different key sequences. The "×" symbols denote the estimated translation, which is the peak location on the POC surface. The "∇" symbols denote the degeneracy of the "×" plots. The translation can be estimated correctly for all but the set of invalid parameters.

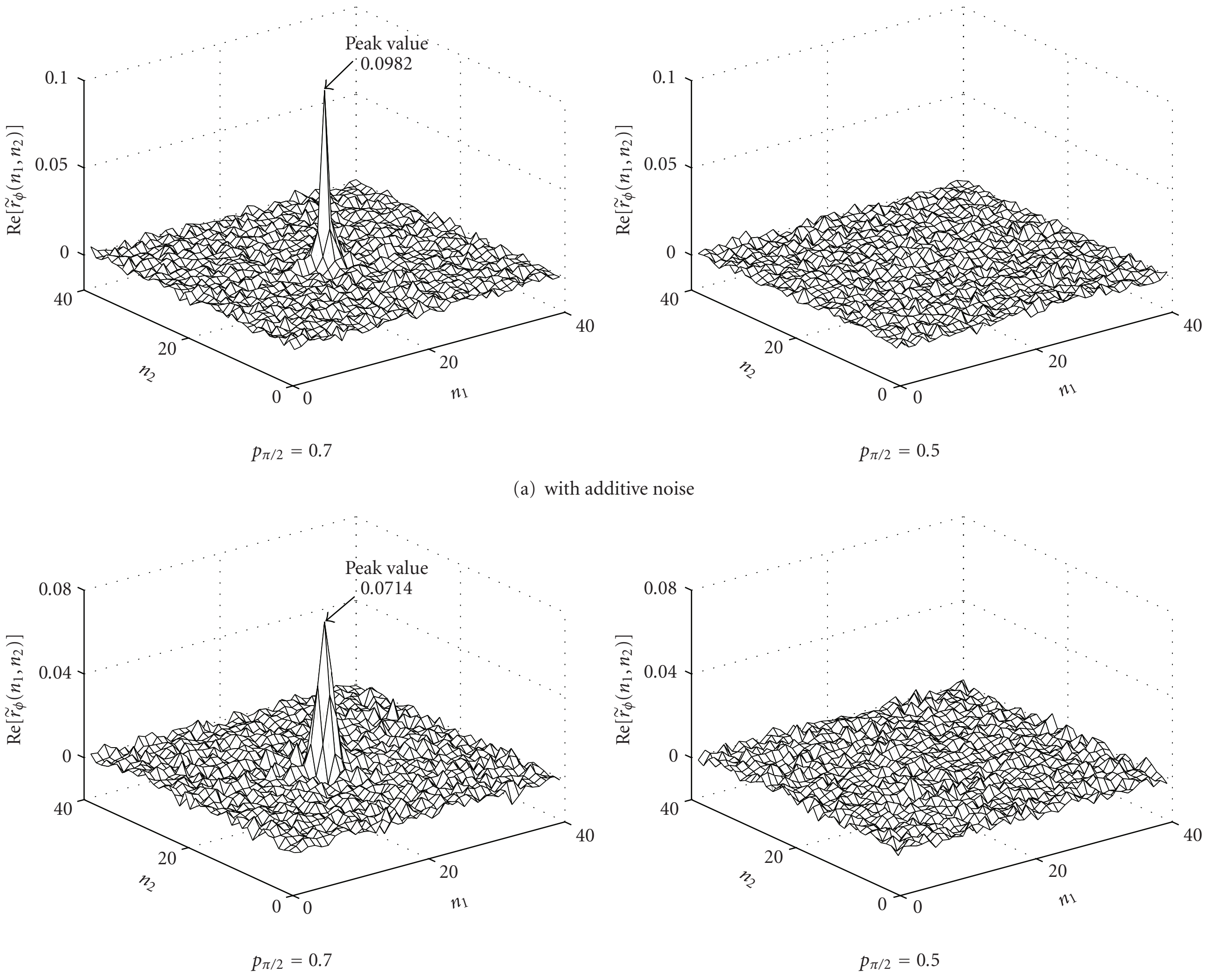
peak value was confirmed to decrease according to (23) as $q_{\pi/2}$ approaches 0.5 for $\delta = \pi$, and, for the case in which $\delta = \pi$ and $q_{\pi/2} = 0.5$, that is, the set of invalid parameters, a distinct peak did not appear on the POC surface.

The real and imaginary parts are shown in Figures 6(a) and 6(b), respectively, of the POC surface for the case in which $\theta_{\alpha_i}(k_1, k_2) \in \{3\pi/8, -3\pi/8\}$, that is, $\delta = 3\pi/4$, with $q_{3\pi/8} = 0.5$. A peak appears in both the real and imaginary parts of the POC surface.

The error between the observed and calculated peak values are presented in Tables 1 and 2. The observed peak values in the tables denote the average peak values observed on the POC surface for a total of 20 different key sequences. The peak value of POC under the proposed scrambling can be adjusted by controlling the parameters according to (23) and (24), which also means that the original peak value can be estimated from the observed peak value using the parameters according to (27).

Next, we investigated the peak location on the POC surface. A total of 1,000 different key sequences, which were generated using the sets of $\{\pi/2, -\pi/2\}$ with $q_{\pi/2} = 0.5$, $\{\pi/3, -\pi/3\}$ with $q_{\pi/3} = 0.5$, and $\{\pi/2, -\pi/2\}$ with $q_{\pi/2} = 0.7$, were considered.

The estimated locations for different key sequences are shown in Figure 7. For the case in which $\theta_{\alpha_i}(k_1, k_2) \in \{\pi/2, -\pi/2\}$ with $q_{\pi/2} = 0.5$, that is, the set of invalid parameters, the translation was not estimated correctly, as shown in Figure 7(a). For the cases in which $\theta_{\alpha_i}(k_1, k_2) \in \{\pi/2, -\pi/2\}$ with $q_{\pi/2} = 0.7$ and $\theta_{\alpha_i}(k_1, k_2) \in \{\pi/3, -\pi/3\}$ with $q_{\pi/3} = 0.5$, the translation was estimated correctly, as shown in Figures 7(b) and 7(c), respectively. Estimation of the translation from POC under the proposed scrambling



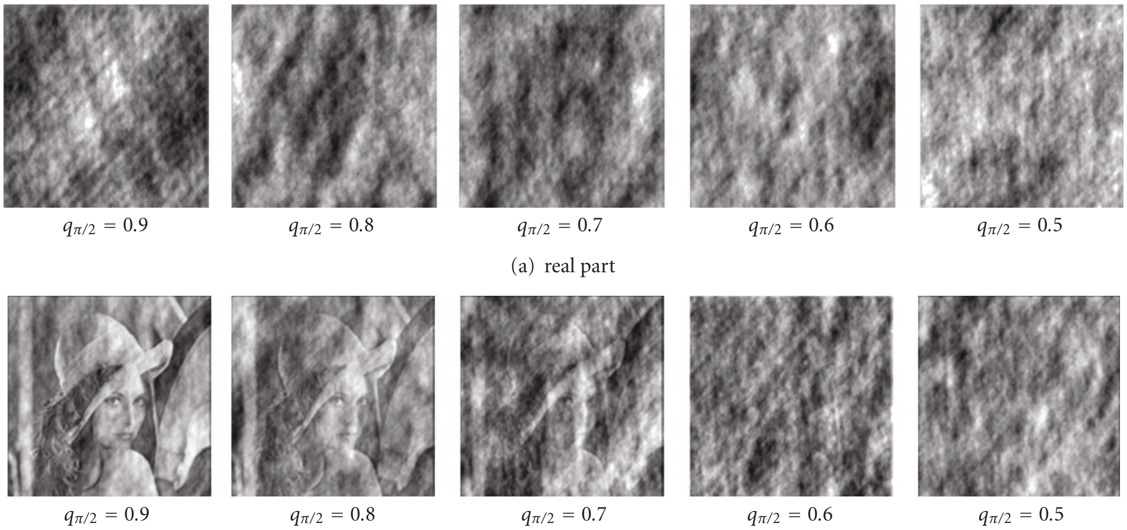
(a) with additive noise

(b) with JPEG quantization noise

Figure 8: Real part of 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).

Table 1: Error between the observed and calculated peak values of the real part of the POC surface. $\theta_{\alpha_i}(k_1,k_2) \in \{\pi/2, -\pi/2\}$, that is, $\delta = \pi$, with $q_{\pi/2} = 0.55$ to 0.95.

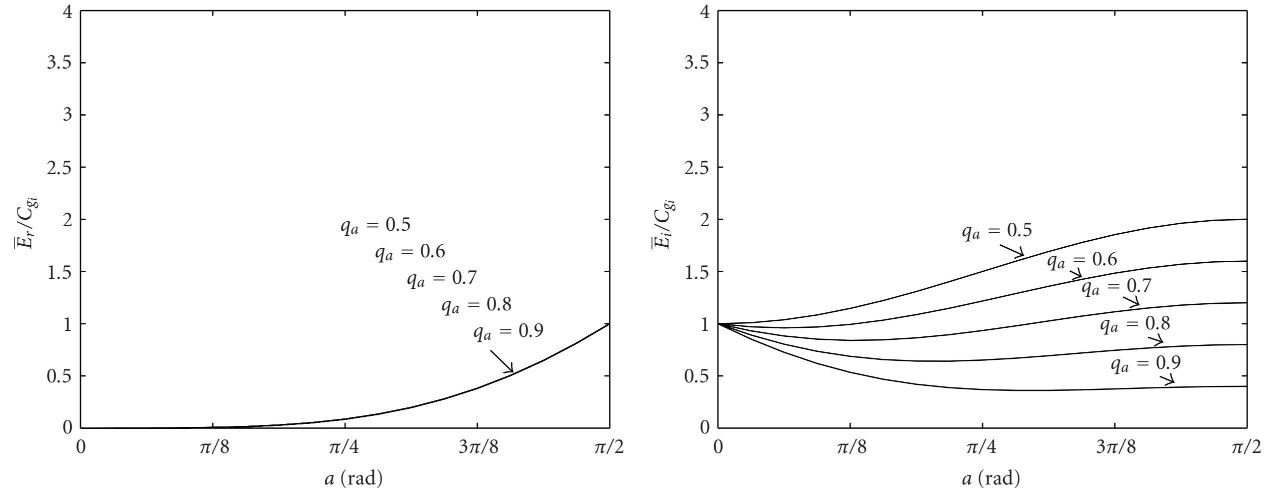
$q_{\pi/2}$	Observed peak value	Calculated peak value	Error
0.55	0.0829	0.0826	0.0003
0.60	0.1653	0.1652	−0.0001
0.65	0.2482	0.2478	0.0004
0.70	0.3307	0.3304	0.0003
0.75	0.4136	0.4130	0.0006
0.80	0.4954	0.4956	−0.0002
0.85	0.5785	0.5782	0.0003
0.90	0.6614	0.6608	0.0006
0.95	0.7440	0.7434	0.0006



(a) real part

(b) imaginary part

FIGURE 9: Real and imaginary parts of phase-scrambled images. Image "Lena" (512 × 512, 8 bits/pixel) is scrambled by $\theta_{\alpha_i}(k_1, k_2) \in \{\pi/2, -\pi/2\}$, that is, $\delta = \pi$ with occurrence probability $q_{\pi/2} = 0.5, 0.6, 0.7, 0.8$, and 0.9.



(a) real part

(b) imaginary part

FIGURE 10: Average error energy over C_{g_i}. Image "Lena" (512 × 512, 8 bits/pixel) is scrambled by $\theta_{\alpha_i}(k_1, k_2) \in \{\pi/2, -\pi/2\}$, that is, $\delta = \pi$ with occurrence probability $q_{\pi/2} = 0.5, 0.6, 0.7, 0.8$, and 0.9.

TABLE 2: Error between the observed and calculated peak values of the real and imaginary parts of the POC surface. $\theta_{\alpha_i}(k_1, k_2) \in \{a, -a\}$, that is, $\delta = 2a$, with $q_a = 0.5$.

a	Part	Observed peak value	Calculated peak value	Error
$\pi/2$	Real	0.0064	0.0000	0.0064
$\pi/2$	Imaginary	0.0064	0.0000	0.0064
$3\pi/8$	Real	0.1212	0.1210	0.0002
$3\pi/8$	Imaginary	0.2924	0.2922	0.0002
$\pi/4$	Real	0.4132	0.4132	0.0000
$\pi/4$	Imaginary	0.4131	0.4132	−0.0001
$\pi/8$	Real	0.7055	0.7054	0.0001
$\pi/8$	Imaginary	0.2922	0.2922	0.0000

has been demonstrated to be possible for all but the set of invalid parameters.

4.1.2. With Noise. We evaluated the noise version of POC under the proposed scrambling. The key sequence was generated by the set of $\{\pi/2, -\pi/2\}$ with $q_{\pi/2} = 0.7$ and 0.5. The POC surface between the template and the query that was corrupted by additive noise is shown in Figure 8(a). The noise consists of Gaussian random numbers with zero mean and a standard deviation of 25. Under this condition, the original peak value was 0.2433. The POC surface between the template and the query that was corrupted by JPEG quantization noise is shown in Figure 8(b). The Q-factor was 200.(8×8 DCT coefficients are divided by the quantization step $Q(k_1, k_2)$, which is generated by $Q_T(k_1, k_2) \cdot Q_F/50$, where $Q_T(k_1, k_2)$, and Q_F denotes a predefined quantization table and a Q-factor, resp.). Under this condition, the original peak value was 0.1779. When $q_{\pi/2} = 0.7$, a peak that expresses the translation appeared on the POC surface at the location (20, 20) in both conditions and the peak values were 0.0982 and 0.0714, respectively. We confirmed that even when the query is corrupted by noise, the original peak value under the condition can be estimated from the observed peak value on the POC surface under the proposed scrambling.

4.2. Visual Effect and the Average Error Energy. We compared the visual effect of a phase-scrambled image with the average error energy in order to demonstrate the validity of the discussion in Section 3.3. We used a 512×512, 8 bits/pixel image called "Lena". The key sequence was generated from the set of $\{\pi/2, -\pi/2\}$, with $q_{\pi/2} = 0.5, 0.6, 0.7, 0.8$, and 0.9. The average error energy was calculated according to (37) and (39) using the parameters $\{a, -a\}$, that is, $\delta = 2a$, for $a = 0$ to $\pi/2$ and $q_{\pi/2} = 0.5, 0.6, 0.7, 0.8$, and 0.9.

The real and imaginary parts of the phase-scrambled images are shown in Figures 9(a) and 9(b), respectively. The real part of the phase-scrambled images is invisible and shows almost no variation, whereas the imaginary part of the phase-scrambled images is degraded as the occurrence probability approaches 0.5. The real and imaginary parts of the average error energy calculated from (37) and (39) are shown in Figures 10(a) and 10(b), respectively. When $a = \pi/2$, the average of the real part of the error energy is constant regardless of the occurrence probability, whereas the average of the imaginary part of the error energy increases as the occurrence probability approaches 0.5. The average error energy is confirmed to coincide with the visual effect of the phase-scrambled image.

If templates are required to be invisible, the parameters should be set as close to the set of invalid parameters as possible.

5. Conclusion

We have proposed one-time key based phase scrambling for image matching. Protecting the original information of the template visually for privacy and security, the proposed method enables keyless image matching. The occurrence probability of a member and the difference of phases were discussed for the one-time key based phase scrambling. These parameters can control the effect of visual protection and the peak value of POC. The effectiveness of visual protection has been demonstrated by the error energy between the phase-scrambled image and the original image. The peak value of one-time key based phase scrambling for the case of the two-member set has been explained theoretically. Experimental results revealed the effectiveness and appropriateness of the proposed method. In the future, a theoretical explanation for the case of a multiple-member set and the degree of robustness against attacks will be considered.

Acknowledgment

This study was 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 *Proceedings of the International Conference on Cybernetics and Society*, pp. 163–165, September 1975.

[2] Q. Chen, M. Defrise, and F. Deconinck, "Symmetric phase-only matched filtering of Fourier-Mellin transforms for image registration and recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 16, no. 12, pp. 1156–1168, 1994.

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

[4] W. S. Hoge, "A subspace identification extension to the pulse correlation method," *IEEE Transactions on Medical Imaging*, vol. 22, no. 2, pp. 277–280, 2003.

[5] K. Takita, T. Aoki, Y. Sasaki, T. Higuchi, and K. Kobayashi, "High-accuracy subpixel image registration based on phase-only correlation," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E86-A, no. 8, pp. 1925–1934, 2003.

[6] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 125–143, 2006.

[7] K. Miyazawa, K. Ito, T. Aoki, K. Kobayashi, and H. Nakajima, "An effective approach for Iris recognition using phase-based image matching," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 30, no. 10, pp. 1741–1756, 2008.

[8] M. Fujiyoshi, W. Saitou, O. Watanabe, and H. Kiya, "Hierarchical encryption of multimedia contents for access control," in *Proceedings of the International Conference on Image Processing (ICIP '06)*, pp. 1977–1980, Atlanta, Ga, USA, October 2006.

[9] H. Kiya and I. Ito, "Image matching between scrambled images for secure data management," in *Proceedings of the 16th European Signal Processing Conference (EUSIPCO '08)*, Lausanne, Switzerland, August 2008.

[10] I. Ito and H. Kiya, "Phase scrambling for blind image matching," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '09)*, pp. 1521–1524, Taipei, Taiwan, April 2009.