HOKKAIDO UNIVERSITY

Title	A Theoretical Analysis of One-time Key Based Phase Scrambling for Phase-only Correlation between Visually Protected Images
Author(s)	Ito, Izumi; Kiya, Hitoshi
Description	APSIPA ASC 2009: Asia-Pacific Signal and Information Processing Association, 2009 Annual Summit and Conference. 4-7 October 2009. Sapporo, Japan. Poster session: Image, Video, and Multimedia Signal Processing 1 (5 October 2009).
Citation	Proceedings : APSIPA ASC 2009 : Asia-Pacific Signal and Information Processing Association, 2009 Annual Summit and Conference, 250-253
Issue Date	2009-10-04
Doc URL	https://hdl.handle.net/2115/39684
Type	conference paper
File Information	MP-P2-1.pdf

Hokkaido University Collection of Scholarly and Academic Papers : HUSCAP

A Theoretical Analysis of One-time Key Based Phase Scrambling for Phase-only Correlation between Visually Protected Images

Izumi Ito and Hitoshi Kiya
Tokyo Metropolitan University, Hino-shi 191-0065 Tokyo Japan
E-mail: {ito-izumi, kiya}@sd.tmu.ac.jp Tel: +81-42-585-8454

***Abstract*—We present a theoretical analysis of one-time key based phase scrambling for image matching using phase-only correlation (POC). Phase scrambling is used for visual information protection of templates. The effect of scrambling on POC values is analyzed. As a result, the peak value, which is used as a measure of signal congruence, of the POC between non-scrambled signals can be estimated by observed POC values with key parameters. In addition, we indicate a condition in which the peak value of the POC between non-scrambled signals estimated by observed POC values with one parameter.**

I. Introduction

Translation between signals and the direct measure of the degree of signal congruence can be simultaneously estimated by phase correlation [1] also known as phase-only correlation (POC). The rotation and scaling between images can be estimated by POC using the magnitude of DFT coefficients that are mapped into the log-polar coordinates [2]. Moreover, high-accuracy estimation techniques for POC have been developed [3][4]. As a result, POC is used as an image matching methods [5]. However, since POC requires images themselves, the visual information of the templates in an image matching system must be protected for privacy and security [6].

Phase scrambling for POC is developed by the authors to protect the visual information of templates and to perform POC directly in the scrambled templates [7]-[10]. If the key that is used for scrambling of template is used for image matching, phase scrambling does not affect POC values [7]-[9]. On the other hand, in one-time key based phase scrambling, the key is used only once for the scrambling of templates, and is not required for image matching [10]. Therefore, one-time key based phase scrambling eliminates the need to save the key. However, one-time key based phase scrambling affects POC values. The peak value, which is used as a measure of signal congruence, of POC generally decreases.

In the present paper, we analyze the effect of one-time key based phase scrambling on POC values. The key determined from a multi-member set is discussed as a general expression. The analysis allows estimation of the peak value of the POC between non-scrambled signals using key parameters. Based on the general expression, we deduce a condition in which the peak value of the POC between non-scrambled signals can be estimated by the POC under one-time key based phase scrambling with one parameter.

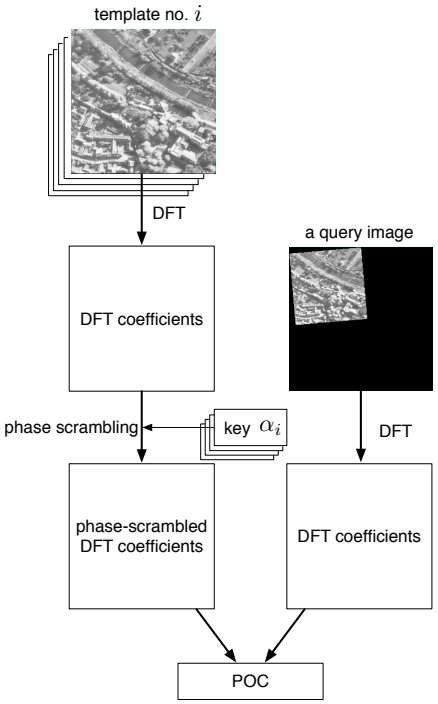


Fig. 1. Image matching using one-time key based phase scrambling for POC. All templates are scrambled by independent keys in order to protect the original information. Without descrambling, the scrambled templates are directly used for POC.

II. Preliminary

In one-time key based phase scrambling, the POC between the phase-scrambled template and a query can be directly performed to obtain a measure of signal congruence, as shown in Fig. 1. In this section, POC, phase scrambling, and image matching under phase scrambling are explained. Let $\mathbb{C}$, $\mathbb{R}$, and $\mathbb{Z}$ denote the sets of complex, real, and integer numbers, respectively.

A. POC

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

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

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

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

where $\phi^*_{G_1}(k)$ denotes the complex conjugate of $\phi_{G_1}(k)$. The POC function $r_\phi(n) \in \mathbb{R}$ 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 and the measure of the degree of signal congruence are estimated by the location and the value of the peak of $r_\phi(n)$ in (3), respectively [1].

B. Phase scrambling for visual information protection

Phase scrambling is performed in the frequency domain. Let $g_i(n)$ be an N-point signal which is used as a template. Phase-scrambled DFT coefficients, $\widetilde{G}_i(k)$, of $g_i(n)$ are given as

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

where $\theta_{\alpha_i}(k)$ denotes an N-point key sequence and α_i denotes a key.

Here, $\theta_{\alpha_i}(k)$, for all k belongs a set $U^M_{x_1}$ that consists of M members, $x_1, x_2, \cdots, x_M \in \mathbb{R}$, i.e.,

$$\theta_{\alpha_i}(k) \in U^M_{x_1}, \quad U^M_{x_1} = \{x_1, x_2, \cdots, x_M\}. \tag{5}$$

Note that the superscript and subscript of U denote the number of members and the first member, respectively, for the sake of convenience. Let q_{x_i} be the occurrence probability of x_i. The q_{x_i} and the difference of phases are key parameters which will be discussed in Section III.

Phase scrambling affects only the phase of signals. Replacing $G_i(k)$ in Eq. (4) by its polar form yields

$$\widetilde{G}_i(k) = |G_i(k)|\phi_{G_i}(k) \cdot e^{j\theta_{\alpha_i}(k)}. \tag{6}$$

From (6), 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

$$|\widetilde{G}_i(k)| = |G_i(k)|, \tag{7}$$

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

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

$$\widetilde{g}_i(n) = \frac{1}{N} \sum_{k=0}^{N-1} \widetilde{G}_i(k) W_N^{-nk}. \tag{9}$$

The phase-scrambled image, which is a two-dimensional expression of the phase-scrambled signal, does not reveal the original information as shown in Fig. 2. Therefore, rather than the DFT coefficients, the phase-scrambled DFT coefficients are stored as a template in case leakage of the template occurs.

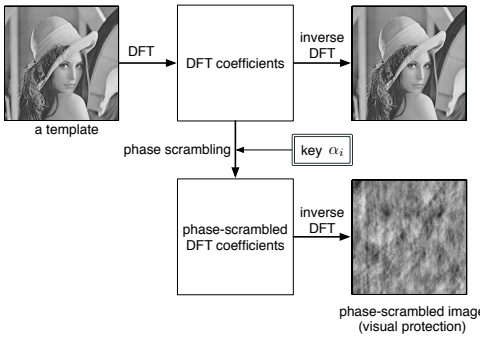


Fig. 2. Phase scrambling for visual protection. The original information of a template is protected visually by phase scrambling

C. Image matching under phase scrambling

Phase-scrambled DFT coefficients are used for image matching without descrambling.

Let $g_1(n)$ and $g_2(n)$ be a template and a query, respectively, and let $\widetilde{G}_1(k)$ be the phase-scrambled DFT coefficients of $g_1(n)$ by a key sequence $\theta_{\alpha_1}(k)$. In image matching, $\widetilde{G}_2(k)$ is generated from the query according to (4) where $\theta_{\alpha_2}(k)$ is the same key sequence that is used for scrambling of the template, i.e. for all k,

$$\theta_{\alpha_2}(k) = \theta_{\alpha_1}(k). \tag{10}$$

The normalized cross spectrum $\widetilde{R}_\phi(k)$ between $\widetilde{G}_1(k)$ and $\widetilde{G}_2(k)$ is calculated as

$$\widetilde{R}_\phi(k) \quad = \quad \widetilde{\phi}^*_{G_1}(k) \cdot \widetilde{\phi}_{G_2}(k). \tag{11}$$

The POC function $\widetilde{r}_\phi(n) \in \mathbb{C}$ is then obtained from the inverse DFT of $\widetilde{R}_\phi(k)$, as follows:

$$\widetilde{r}_\phi(n) = \frac{1}{N} \sum_{k=0}^{N-1} \widetilde{R}_\phi(k) W_N^{-nk}. \tag{12}$$

From (8) and (10), $\widetilde{R}_\phi(k)$ is given as

$$\widetilde{R}_\phi(k) = \phi^*_{G_1} e^{-j\theta_{\alpha_1}(k)} \cdot \phi_{G_2} e^{j\theta_{\alpha_2}(k)} = R_\phi(k).$$

Therefore, the POC function between phase-scrambled signals and that between non-scrambled signals are identical under the condition (10).

On the other hand, in one-time key based phase scrambling, a key sequence that is used for scrambling of a template is not used for a query [10]. Rather than scrambling of a query by a key sequence, $\widetilde{G}_2(k)$ is generated by multiplying $G_2(k)$ by the phase term of x_1:

$$\widetilde{G}_2(k) = G_2(k) \cdot e^{jx_1} \tag{13}$$

where x_1 is a member of $U^M_{x_1}$. Note that Fig. 1 is the special case in which $x_1 = 0$, that is, $\widetilde{G}_2(k) = G_2(k)$. According

to (11), $\widetilde{R}_\phi(k)$ between $\widetilde{G}_1(k)$ and $\widetilde{G}_2(k)$ is calculated. The POC function $\widetilde{r}_\phi(n)$ is then obtained by the inverse DFT of $\widetilde{R}_\phi(k)$. $\widetilde{r}_\phi(n)$ is not equivalent to $r_\phi(n)$ due to the effect of scrambling,

III. Theoretical analysis

The effect of one-time key based phase scrambling on POC values is analyzed theoretically.

A. General expression of one-time key based phase scrambling

The DFT coefficients $G_1(k)$ of $g_1(n)$ are scrambled by $\theta_{\alpha_1}(k) \in U_{x_1}^M$. The DFT coefficients $G_2(k)$ of $g_2(n)$ are multiplied by e^{jx_1}, i.e.,

$$\widetilde{G}_1(k) = G_1(k) \cdot e^{j\theta_{\alpha_1}(k)} \tag{14}$$

$$\widetilde{G}_2(k) = G_2(k) \cdot e^{jx_1}. \tag{15}$$

$\widetilde{R}_\phi(k)$ between $\widetilde{G}_1(k)$ and $\widetilde{G}_2(k)$ is given as

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

If $\theta_{\alpha_1}(k) = x_1$, then

$$\widetilde{R}_\phi(k) = R_\phi(k), \tag{17}$$

otherwise,

$$\widetilde{R}_\phi(k) \neq R_\phi(k). \tag{18}$$

Therefore, $\widetilde{r}_\phi(n)$ that is the inverse DFT of $\widetilde{R}_\phi(k)$ consists of following M values with their occurrence probability.

$$\widetilde{r}_\phi(n) = \begin{cases} r_\phi(n), & (q_{x_1}) \\ r_\phi(n) \cdot e^{j(x_1 - x_2)} & (q_{x_2}) \\ \vdots & \vdots \\ r_\phi(n) \cdot e^{j(x_1 - x_M)} & (q_{x_M}) \end{cases} \tag{19}$$

where q_{x_i} denotes the occurrence probability of x_i.

The peak value of POC under one-time key based phase scrambling is expressed in terms of statistical basis. From (19), the average, λ, of the peak values of $\widetilde{r}_\phi(n)$ is defined as

$$\lambda = q_{x_1} p + q_{x_2} p \cdot e^{j(x_1 - x_2)} + \cdots + q_{x_M} p \cdot e^{j(x_1 - x_M)} \tag{20}$$

where p denotes the original peak value (the peak value of the POC between non-scrambled signals), i.e.,

$$p = \max_n (r_\phi(n)). \tag{21}$$

Since λ is a complex number, the real part, λ_{re}, and imaginary part, λ_{im} of λ are given as

$$\lambda_{re} = p\{q_{x_1} + q_{x_2} \cos(x_1 - x_2) + \cdots + q_{x_M} \cos(x_1 - x_M)\}, \tag{22}$$

$$\lambda_{im} = p\{q_{x_2} \sin(x_1 - x_2) + \cdots + q_{x_M} \sin(x_1 - x_M)\}. \tag{23}$$

The real part, Re[·], and the imaginary part, Im[·], of the peak value of $\widetilde{r}_\phi(n)$ can be expressed as

$$\max_n (|\mathrm{Re}[\widetilde{r}_\phi(n)]|) \approx |\lambda_{re}|, \tag{24}$$

$$\max_n (|\mathrm{Im}[\widetilde{r}_\phi(n)]|) \approx |\lambda_{im}|. \tag{25}$$

Thus, if key parameters that are the occurrence probability, q_{x_i}, and the difference of phases, $(x_1 - x_i)$, of all members are known, then the original peak value, p, can be estimated.

For example, in a two-member set for the case in which $x_1 - x_2 = \pi$, the peak value of $\widetilde{r}_\phi(n)$ is given with the occurrence probability, q_{x_1}, as

$$\max_n (|\mathrm{Re}[\widetilde{r}_\phi(n)]|) \approx |p \cdot (2q_{x_1} - 1)|. \tag{26}$$

That is, p is estimated as

$$|p| \approx \max_n (|\mathrm{Re}[\widetilde{r}_\phi(n)]|)/|2q_{x_1} - 1|. \tag{27}$$

B. Estimation using one parameter

A condition in which the original peak value, p, can be estimated by POC under one-time key based phase scrambling with one parameter, q_{x_1} is described in the following.

When the occurrence probability except for q_{x_1} is the same, i.e.,

$$q_{x_2} = q_{x_3} = \cdots = q_{x_M}, \tag{28}$$

(20) is rewritten as

$$\lambda = q_{x_1} p + (M-1) \cdot q_{x_2} p \cdot \underbrace{(e^{j(x_1 - x_2)} + e^{j(x_1 - x_3)} + \cdots + e^{j(x_1 - x_M)})}_{A}. \tag{29}$$

Suppose that A in (29) is 0, we can estimate the original peak value, p, from $\widetilde{r}_\phi(n)$ with q_{x_1} even if the other parameters are unknown:

$$\max_n (|\widetilde{r}_\phi(n)|) \approx |p \cdot q_{x_1}|. \tag{30}$$

The condition in which A in (29) is 0 is such that A is an $(M-1)$-term geometrical series which satisfies

$$\begin{aligned} x_1 - x_2 &= \delta \\ x_1 - x_3 &= 2\delta \\ &\vdots \\ x_1 - x_M &= (M-1)\delta \end{aligned} \tag{31}$$

and

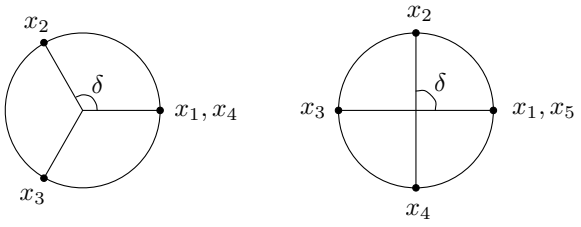
$$\delta = 2\pi/(M-1). \tag{32}$$

Under (31) and (32), it follows that

$$A = e^{j2\pi/(M-1)} \cdot \frac{1 - (e^{j2\pi/(M-1)})^{(M-1)}}{1 - e^{j2\pi/(M-1)}} = 0. \tag{33}$$

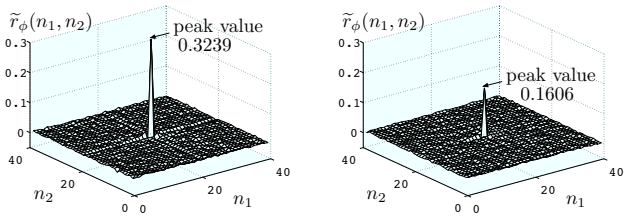
Note that $\exp(jx_1) = \exp(jx_M)$ from (31) and (32).

Therefore, (28), (31), and (32) are the condition for (30). Figures 3(a) and 3(b) show examples of members which satisfy the condition for (30). The effect of scrambling on the POC values can be avoided by estimating the original peak value from the peak value of the POC under one-time key based phase scrambling according to (30).



(a) $M = 4$ (b) $M = 5$

Fig. 3. Examples of members that satisfy the condition for (30). (a) $M = 4$, i.e., $\{x_1, x_2, x_3, x_4\} = \{0, 2\pi/3, 4\pi/3, 2\pi\}$. (b) $M = 5$, i.e., $\{x_1, x_2, x_3, x_4, x_5\} = \{0, \pi/2, \pi, 3\pi/2, 2\pi\}$.



(a) $q_{\pi/2} = 0.7$ (b) $q_{\pi/2} = 0.6$

Fig. 4. POC surface under one-time key based phase scrambling, where the template is scrambled by $\theta_{\alpha_1}(k_1, k_2) \in \{\pi/2, -\pi/2\}$ with $q_{\pi/2}$ = 0.7 and 0.6, respectively. The peak value decreases according to (26).

IV. Simulations

POC between two images, a template and a query, was performed. The template and the query, which are 400×400 area of image Lena (512×512, 8bits/pixel), were translated by 20 pixels in both the horizontal and vertical directions.

Figures 4(a) and 4(b) show the POC surface under one-time key based phase scrambling, where the template was scrambled by $\theta_{\alpha_1}(k_1,k_2) \in \{\pi/2, -\pi/2\}$ with $q_{\pi/2} = 0.7$ and 0.6, respectively. The peak value of the POC surface decreases according to (26). In [10], this decrease was not analyzed and was limited to a two-member set where $x_1 - x_2 = \pi$. The decrease is analyzed in the present paper as a general expression.

We evaluated the effectiveness of the condition for (30) including (26). A total of 50 one-time keys were used for evaluation. Table I shows the original peak value estimated from the peak value of the POC under one-time key based phase scrambling with $\theta_{\alpha_1}(k_1, k_2) \in U^M_{x_1}$, $M = 3$, 4, and 5, in which members satisfy the condition for (30). When $M = 3$, the members were $\{0, \pi, 2\pi\}$, when $M = 4$, the members were $\{0, 2\pi/3, 4\pi/3, 2\pi\}$, and when $M = 5$, the members were $\{0, \pi/2, \pi, 3\pi/2, 2\pi\}$. We can confirm that the original peak value, p, can be estimated from the peak value of the POC surface under one-time key based phase scrambling with q_{x_1} when the members satisfy the condition for (30). We also performed noise version and confirmed that the original peak value can be estimated from the POC under one-time key based phase scrambling.

TABLE I
Estimation of the original peak value.

A total of 50 one-time keys were used for evaluation. The original peak value, p, was estimated from the observed values using (30). $p = 0.8074$.

M	q_{x_1}	observed value		estimated value		error
		mean	variance	mean $\hat{p}$	variance	$\lvert\hat{p} - p\rvert$
3	1/2	0.4035	3.90E-06	0.8071	7.80E-06	0.0003
	1/3	0.2687	3.45E-06	0.8061	1.03E-05	0.0013
	1/4	0.2020	4.31E-06	0.8080	1.73E-05	0.0006
4	1/2	0.4033	3.08E-06	0.8065	6.16E-06	0.0008
	1/3	0.2687	2.64E-06	0.8062	7.91E-06	0.0011
	1/4	0.2016	2.69E-06	0.8062	1.07E-05	0.0011
5	1/2	0.4035	3.16E-06	0.8070	6.32E-06	0.0004
	1/3	0.2691	3.54E-06	0.8073	1.06E-05	0.0001
	1/4	0.2017	3.60E-06	0.8068	1.44E-05	0.0006

V. Conclusions

We have presented a theoretical analysis of one-time key based phase scrambling for POC. We have indicated a general expression which shows the difference between the peak value of POC in non-scrambling and that in one-time key based phase scrambling with parameters. As a result, the peak value of POC in non-scrambling can be estimated by POC under one-time key based phase scrambling with all the parameters. In addition, we have described a condition in which the peak value of POC in non-scrambling can be estimated by POC with one parameter. The effect of scrambling on the POC values can be avoided in one-time key based phase scrambling.

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

[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, pp.1156–1168, 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] K. Miyazawa, K. Ito, T. Aoki, K. kobayashi, and H. Nakajima, "An effective approach for iris recognition using phase-based image matching," *IEEE Trans. Pattern Anal. Mach. Intell.,* vol.30, no.10, pp.1741–1756, Oct. 2008

[6] 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

[7] H. Kiya and I. Ito, "Image matching between scrambled images for secure data management," in *Proc. EURASIP EUSIPCO*, Aug. 2008.

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

[9] I. Ito and H. Kiya, "Phase scrambling for blind image matching," in *Proc. IEEE ICASSP*, pp.1521–1524, Apr. 2009.

[10] I. Ito and H. Kiya, "Image matching between visually protected images with one-time key based phase scrambling," in *Proc. EURASIP EUSIPCO*, Aug. 2009. in press.