

We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900

Open access books available

186,000

International authors and editors

200M

Downloads

Our authors are among the

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com



High-Accuracy and High-Security Individual Authentication by the Fingerprint Template Generated Using the Fractional Fourier Transform

Reiko Iwai and Hiroyuki Yoshimura
*Graduate School of Engineering, Chiba University
 Japan*

1. Introduction

The personal identities by the biological information have been increasing everywhere, e.g. on ATM of the bank, at the airport, and so on. In particular, the fingerprint authentication or handwriting analysis has been used as the simplest way, because the biological information does not have to be remembered and there is no worry to be lost like a password. Most of the methods, whole fingerprint images or handwriting data were stored as templates on paper without modification. When the authentication is needed, the biological information and the template were matched manually.

Recently, the fingerprint images or handwriting data have been stored as templates on the database of the computer. The authentication method, where the biological information and the template on the database are matched automatically, is becoming mainstream on the background that the computer technology has rapidly been developed.

The generation methods of the templates of the fingerprint images are classified into two major categories. One generation method is to use a priori extracted features of the images, such as minutiae (Maltoni et al., 2003). The other is to use the spatial frequency data of the one-dimensional (1D) data extracted from the two-dimensional (2D) original fingerprint image in a specific direction (Takeuchi et al., 2007).

However, there are some problems related to storing the templates; 1) the unfair use is possible when the information leaks out; 2) the biological information cannot keep the same condition forever so that it could not be always verified accurately when matching.

We have to consider the following points to solve these problems. For the former, the information on the fingerprint images should be hidden in order not to be used unfairly by unauthorized persons when the information leaks out. For the latter, the high accuracy of the authentication should be demanded even if there are some hurt and dirty on the fingerprint images.

To solve these problems, in this manuscript, the templates are generated using the fractional Fourier transform (FRT) (Ozaktas et al., 2001) which is the generalization of the conventional Fourier transform (FT). The FRT has a feature that the FRT's orders can be changed to arbitrary real numbers. Therefore, we could generate the templates solving the above-mentioned problems when the FRT is applied to the 1D data extracted from the 2D original fingerprint image in a specific direction. In addition, recently, research on a high-speed

optical arithmetic processing of the FRT has been developed (Lohmann, 1993; Moreno et al., 2003; Ozaktas et al., 2001). Therefore, under the assumption of realizing the high-speed optical arithmetic processing of the FRT in the near future, the templates are stored as the intensity FRT in our study.

In this manuscript, we introduce the templates generated by the FRT of the fingerprint images. Moreover, we indicate the authentication accuracy by use of the templates and the robustness for unauthorized third persons. Specifically, we analyze from the following three perspectives: 1) the behavior of peak value of cross-correlation function between the original fingerprint image and the generated template expressed in terms of the intensity FRT; 2) the behavior of peak value of cross-correlation function between the original fingerprint image and the intensity inverse FRT (IFRT) of generated template; 3) derivation of the minimum error rate (MER) and authentication threshold on the basis of the false acceptance rate (FAR) and the false rejection rate (FRR) (Mansfield et al., 2001).

These analyses allow us to show the difference between the template and the original fingerprint image and that between the intensity IFRT of the template and the original image, quantitatively. This fact means that we cannot identify the original fingerprint image as the difference between them becomes greater and greater. In addition, the high authentication accuracy can be obtained by the analysis using the FAR and FRR which are the criterion of authentication accuracy.

2. Definition of the Fractional Fourier Transform (FRT)

The FRT is the generalization of a conventional FT. The FRT of 1D input data $u(x)$ is defined as (Ozaktas et al., 2001; Bultheel & Martinez Sulbaran, 2004a)

$$u_p(x_p) = F^{(p)}[u(x)] = \int u(x) \exp[i\pi(x_p^2 + x^2) / s^2 \tan \phi] \times \exp[-2i\pi x_p x / s^2 \sin \phi] dx, \quad (1)$$

where a constant factor has been dropped; $\phi = p\pi / 2$, where p is the FRT's order; s is a constant. In particular, in the optical FRT, s is called a scale parameter expressed in terms of $s = \sqrt{\lambda f_s}$ where λ is the wavelength and f_s is an arbitrarily fixed focal length (Ozaktas et al., 2001). In this manuscript, the value of s was fixed at 1.0.

When p takes a value of $4n+1$, n being any integer, the FRT corresponds to the conventional FT. The intensity distribution of the FRT, $I_p(x_p)$, which is named intensity FRT in our study, is obtained by calculating $|u_p(x_p)|^2$. In addition, $u_p(x_p)$ can be decoded to $u(x)$ by the IFRT with the order $-p$ as follows:

$$u(x) = F^{(-p)}[u_p(x_p)]. \quad (2)$$

In this manuscript, we call p in Eq. (2) the IFRT's order. "Disfrft.m" (Bultheel & Martinez Sulbaran, 2004b) was used in our numerical calculation of the FRT.

2.1 Modeling waveform pattern of the fingerprint

In this subsection, as a 1D modeled fingerprint image, we used the finite rectangular wave which is regarded as the simplification of the grayscale distribution in an arbitrary scanned

line of the 2D original fingerprint images. We make clear the charactererisc of the amplitude, phase and intensity distributions of the FRT.

First, Fig. 1 (a) shows the cross-sectional waveform that isn't modeled in an arbitrary scanned line of the 2D original fingerprint images. Although the grayscale levels are composed of intermediate values between 0 and 255 at the actual scanned lines in the case of 2D black and white image of 8 bits, in order to highlight the FRT as our method together with its feasibility, a finite rectangular wave is assumed to be the simplification of the grayscale distribution of the fingerprint image as shown in Fig. 1 (b). Horizontal axis is intentionally composed of 1024 (2^{10}) pixels to be smoothly illustrated the results of the FT and the FRT. We premise the application of the FRT to the 2D original fingerprint image which has multiple lines with random FRT's orders. In addition, the FRT's orders can be used as arbitrary real numbers.

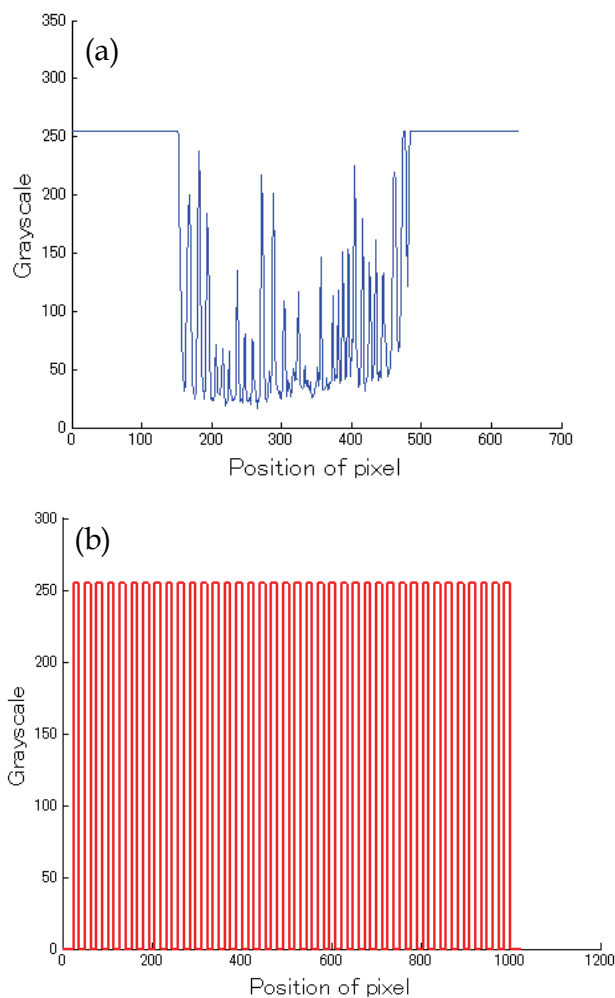


Fig. 1. (a) Cross-sectional waveform of a 2D original fingerprint image and (b) the finite rectangular wave as a modeled fingerprint image

2.2 Application of the FRT

The algorithm of the FRT has been intensively studied (Marinho & Bernardo, 1998; Yang et al., 2004; Bailey & Swarztrauber, 1991). Alternatively, the FRT was also applied to the fake finger detection (Lee et al., 2009).

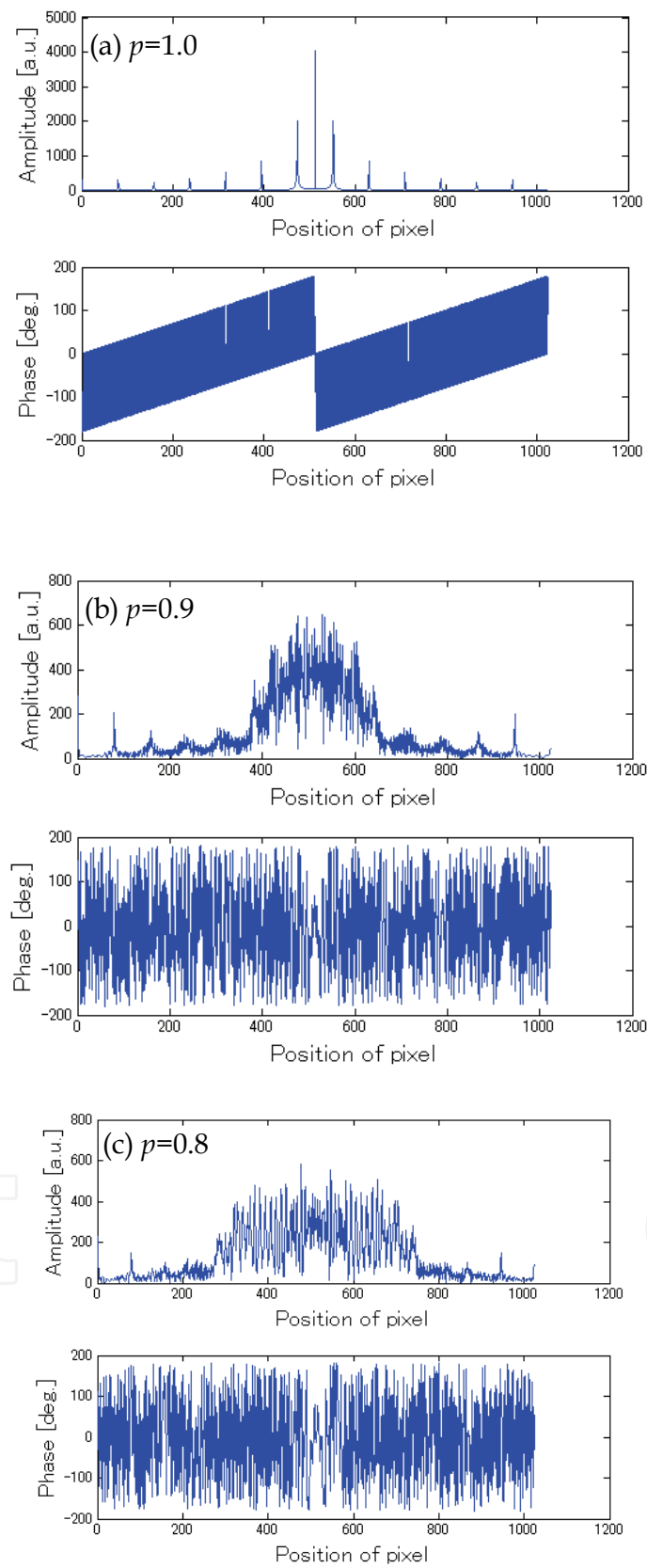


Fig. 2. Examples of the amplitude and phase distributions of the FRTs applied to the finite rectangular wave, when p s= (a) 1.0, (b) 0.9 and (c) 0.8

In this subsection we apply the FRT to the 1D finite rectangular wave data shown in Fig. 1 (b) as a modeled fingerprint image. Basically, the FRT with the order p is applied to the finite rectangular wave in Eq. (1). The FRT with the order p can be decoded to the finite rectangular wave by the IFRT with the same order p as already explained in Eq. (2). Fig. 2 demonstrates the results of the FRTs in comparison with the conventional FT (i.e., the FRT with $p=1.0$). Namely, Fig. 2 (a) shows the result of the FT as the amplitude distribution at the upper portion and the phase distribution at the lower portion. Figs. 2 (b) and 2 (c) are the results of the FRTs with $p=0.9$ and 0.8 , respectively. As a result, the peak values of the amplitude distributions in Figs. 2 (a), 2 (b) and 2 (c) are 4.04×10^3 , 6.59×10^2 and 5.80×10^2 , respectively.

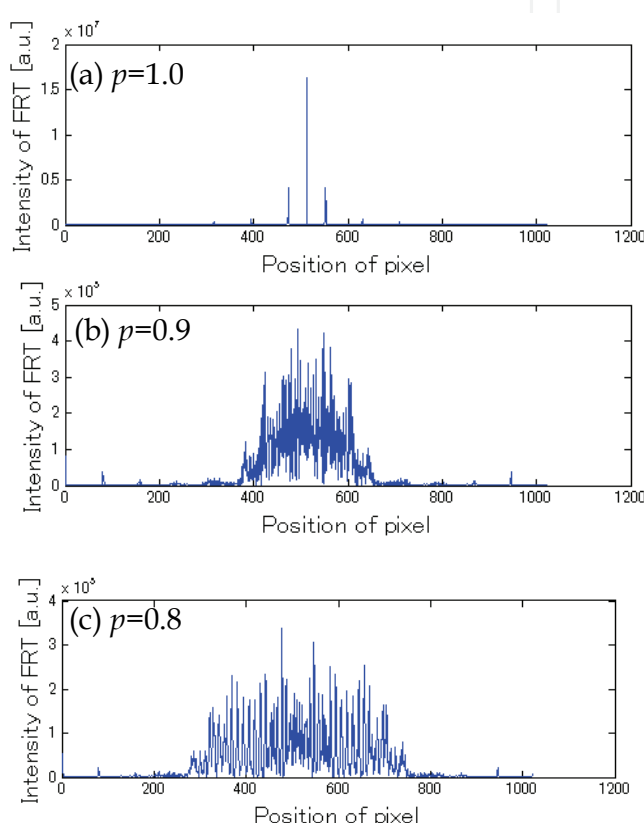


Fig. 3. The intensity distributions of the FRTs of the finite rectangular wave shown in Fig. 1, when p s= (a) 1.0, (b) 0.9 and (c) 0.8

It is found that the peak value of the amplitude distribution falls remarkably and the width of spread increases when the value of the FRT's order p decreases. It is also found that there is little difference in phase distributions between Figs. 2 (b) and 2 (c). In the case of FT shown in Fig. 2 (a), the order p can be identified through the waveforms of the amplitude and phase distributions. However, in the case of FRT, the order p may not be identified through them. In particular, it is difficult to identify the FRT's orders p s through the waveforms of the phase distributions shown in Figs. 2 (b) and 2 (c). Therefore, this fact led us the new method safer than the conventional method using the FT, because the FRT's order has highly-confidential in the applied FRT condition.

In this way, we focused on the intensity distribution of the FRT from a viewpoint of the security of individual information, because the intensity FRT may not be completely

decoded to the original fingerprint image by the IFRT. Fig. 3 depicts the intensity FT of Fig. 2 (a) and the intensity FRTs of Figs. 2 (b) and 2 (c). The peak values of the intensity distributions in Figs. 3 (a), 3 (b) and 3 (c) are 1.63×10^7 , 4.34×10^5 and 3.37×10^5 , respectively. It is found from the comparison between Figs. 2 and 3 that the peak value of the wave pattern of the intensity distribution is very high.

3. How to generate the fingerprint template by use of the FRT and its characteristics

Fingerprint images provided by the Biometric System Laboratory (Maltoni & Maio., 2004) were used as original raw data. As an example, the data in the TIF format with 480 vertical and 640 horizontal pixels (480×640 pixels) is visualized in Fig. 4. In this manuscript, as shown in Fig. 4, height and width of the images are called ‘line’ and ‘column,’ respectively. The templates were generated by the FRT of the cross-sectional waveform with an arbitrary random order in every longitudinally (or transversally) scanned line of the original fingerprint images.

Fig. 4 illustrates an example where the FRTs with the random orders of $p_1, p_2, p_3, \dots, p_m$ and p_n are conducted in transversally-scanned lines from the top to the bottom of the fingerprint image. Therefore, the information on the FRT’s order in every transversally-scanned line is needed to be decoded to the original fingerprint image by use of the IFRT. For that reason, there is almost no possibility of the unfair use by the unauthorized third persons.

Fig. 5 depicts an example of the template expressed in terms of the intensity FRT. The reason why we used the intensity FRT as the template is that we would use a high-speed optical processing system of the FRT (Lohmann, 1993; Moreno et al., 2003; Ozaktas et al., 2001) to generate the templates in the near future. In this case, the template can be produced at higher speed because of no need of calculation by a computer. As shown in Fig. 5, the information on the original fingerprint image cannot be known from the template which was generated by the FRT with a random order in every transversally-scanned line.

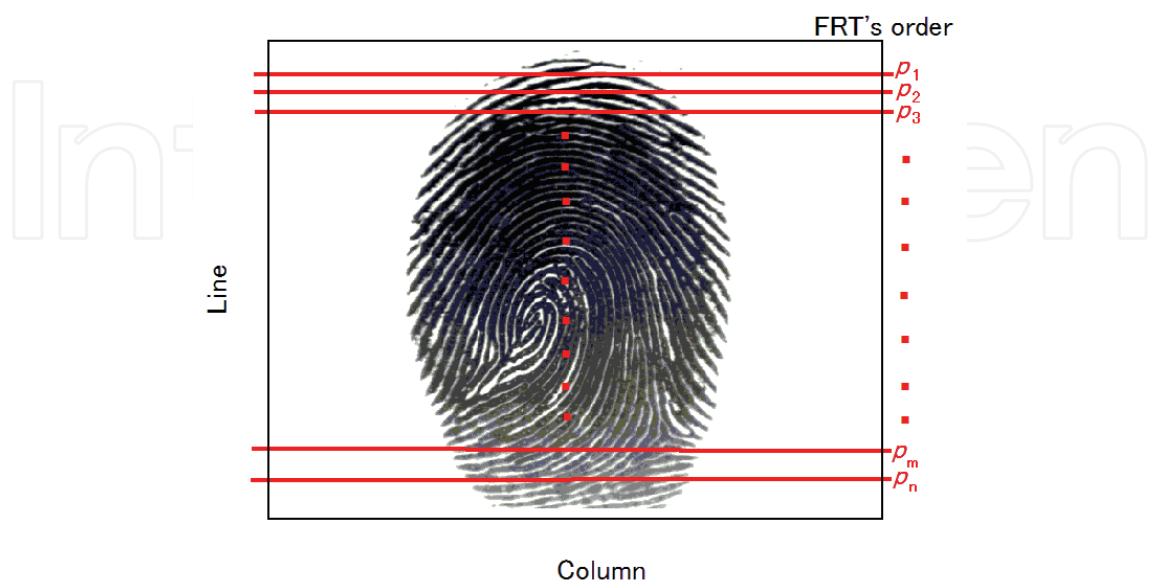


Fig. 4. Fingerprint image

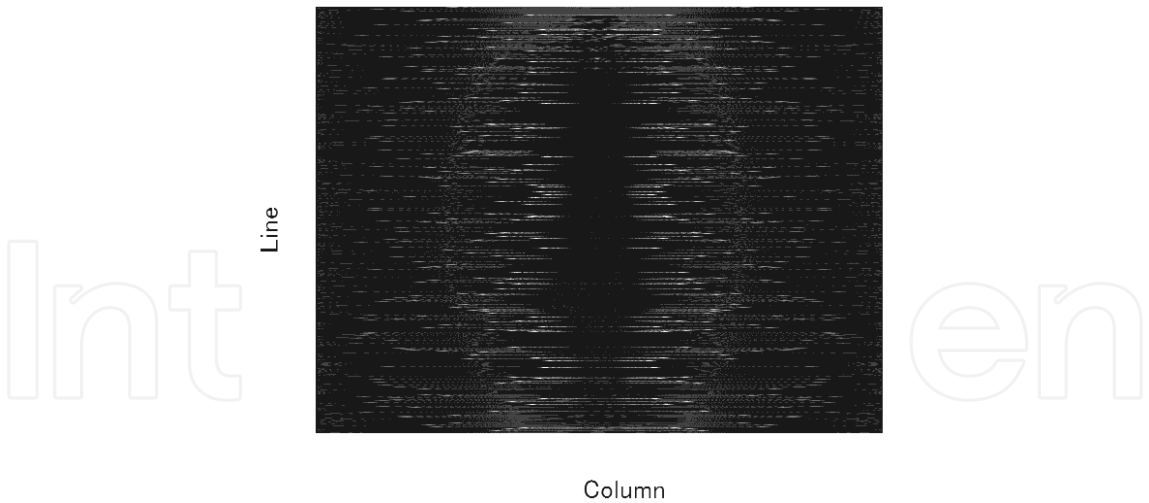


Fig. 5. Template

4. Characteristics of the fingerprint authentication

Next, 100 kinds of fingerprint images were prepared, and the fingerprint images with 200 lines and 200 columns (200×200 pixels) were extracted from a central part of the original fingerprint images. Two examples of extracted fingerprint images are depicted in Fig. 6 and the real size is 10.2 mm by 10.2 mm. The blank space was deleted from the original fingerprint images so that more accurate authentication could be conducted by use of the extracted fingerprint images. For this reason, the matching speed can be expected to be faster because the matching range is small.

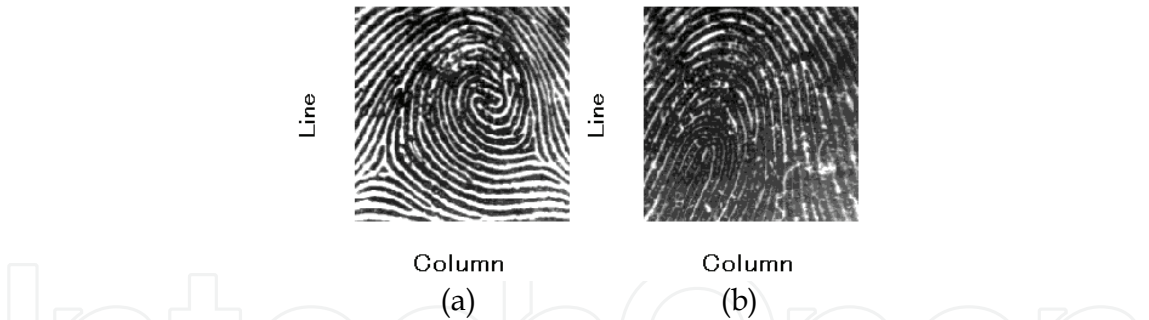


Fig. 6. Fingerprint images with 200 lines and 200 columns extracted at a center of the original fingerprint images

4.1 Difference between the template and the extracted fingerprint image

We analyzed the behavior of the peak value of the normalized cross-correlation function between the template generated by the FRT with a different order in every line and the extracted fingerprint image shown in Fig. 6. The templates were generated for 100 kinds of extracted fingerprint images with 200 lines and 200 columns. The behavior was analyzed for the FRT’s order ranges of 4 kinds of 0.1-0.9, 0.1-1.9, 0.1-2.9 and 0.1-3.9. Fig. 7 gives the result. In Fig. 7, the vertical and horizontal axes denote the peak value of the normalized cross-correlation function and the FRT’s order range, respectively. In the figure, the symbol of circle and the bar denote the averaged peak value and the standard deviation of the peak value, respectively. The averaged peak values for the FRT’s

order ranges of 0.1-0.9, 0.1-1.9, 0.1-2.9 and 0.1-3.9 are 0.636, 0.420, 0.443 and 0.429, respectively. Additionally, the standard deviations of the peak values for the FRT's order ranges of 0.1-0.9, 0.1-1.9, 0.1-2.9 and 0.1-3.9 are 0.0484, 0.0474, 0.0592 and 0.0533, respectively. The averaged peak value of 0.420 is the smallest of them when the FRT's order range is 0.1-1.9. It is found that the template has a great difference between the extracted fingerprint image and the template under the condition that the FRT's order range is 0.1-1.9, 0.1-2.9 or 0.1-3.9.

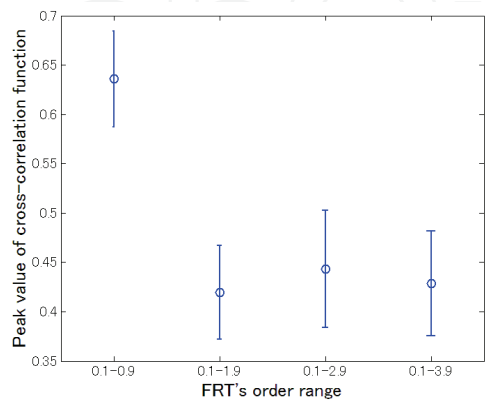


Fig. 7. Peak value of the normalized cross-correlation function between the template and the extracted fingerprint image for every FRT's order range

4.2 Robustness of the template for the IFRT

Next, we analyzed the behavior of the peak value of the normalized cross-correlation function between the intensity IFRT of the template and the extracted fingerprint image shown in Fig. 6. The IFRT of the template was generated by the IFRT with a different order in every line of the template generated in Subsection 4.1. In the analysis, 100 kinds of fingerprint images with 200 lines and 200 columns were used.

The behavior was analyzed for the IFRT's order ranges of 4 kinds of 0.1-0.9, 0.1-1.9, 0.1-2.9 and 0.1-3.9. Fig. 8 gives the result. In Fig. 8, the vertical and horizontal axes denote the peak value of the normalized cross-correlation function and the IFRT's order range, respectively. In the figure, the symbol of square and the bar denote the averaged peak value and the standard deviation of the peak value, respectively. The averaged peak values for the IFRT's order ranges of 0.1-0.9, 0.1-1.9, 0.1-2.9 and 0.1-3.9 are 0.340, 0.215, 0.211 and 0.205, respectively. Additionally, the standard deviations of the peak values for the IFRT's order ranges of 0.1-0.9, 0.1-1.9, 0.1-2.9 and 0.1-3.9 are 0.0406, 0.0365, 0.0436 and 0.0351, respectively. The averaged peak value of 0.205 is the smallest of them when the IFRT's order range is 0.1-3.9. It is found that the template has a great difference between the extracted fingerprint image and the intensity IFRT of the template under the condition that the order range is 0.1-1.9, 0.1-2.9 or 0.1-3.9. Therefore, the unauthorized third persons who are unapprised of the information on the FRT's order in every line cannot retrieve the extracted fingerprint data from the template.

5. Authentication accuracy based on the FAR and FRR

Fig. 9 illustrates the basic concept of the FAR and FRR. In the figure, the left-hand curve is the imposter distribution and the right-hand curve is the authentic distribution. The authentication threshold is decided by a value satisfied with the condition that the FAR and

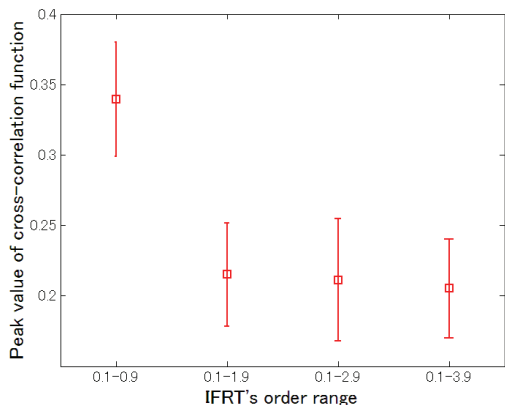


Fig. 8. Peak value of the normalized cross-correlation function between the intensity IFRT of the template and the extracted fingerprint image for every IFRT’s order range

FRR take the same value corresponding to the MER. The FAR is the probability of accepting other person erroneously. As shown in the figure, it corresponds to an area of the impostor distribution higher than the authentication threshold. On the other hand, the FRR is the probability of rejecting identical person and corresponds to the area of the authentic distribution lower than the authentication threshold. In our analysis, the horizontal axis in Fig. 9 corresponds to the peak value of the 2D normalized cross-correlation function of the intensity FRTs for the two sets of fingerprint images.

In order to obtain the imposter and authentic distributions, 100 kinds of templates were used. For each of them, 10 kinds of templates were prepared to obtain the imposter distribution. On the other hand, for each of the templates, 10 kinds of templates, which were produced by the FRT of the extracted fingerprint images superimposed by random noise (average $\mu=0$, standard deviation $\sigma=25.5$), were prepared to obtain the authentic distribution. Figs. 10 and 11 are the results showing the behavior of peak value of the normalized cross-correlation function of the FRT intensity by changing the FRT’s order range for the imposter distribution and the authentic distribution, respectively. As same as Fig. 7 in the Subsection 4.1, in Figs. 10 and 11, the vertical and horizontal axes denote the peak value of normalized cross-correlation function and the FRT’s order range, respectively.

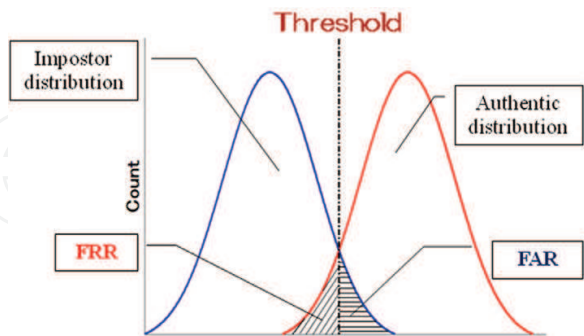


Fig. 9. Basic concept of the FAR and FRR

In Fig. 10 related to the impostor distribution, the symbol of cross and the bar denote the averaged peak value and the standard deviation of the peak value, respectively. The averaged peak values for the FRT’s order ranges of 0.1-0.9, 0.1-1.9, 0.1-2.9 and 0.1-3.9 are 0.658, 0.735, 0.764 and 0.732, respectively. Additionally, the standard deviations of the peak values for the FRT’s order ranges of 0.1-0.9, 0.1-1.9, 0.1-2.9 and 0.1-3.9 are 0.0928, 0.0868, 0.0650 and 0.0861, respectively. On the other hand, in Fig. 11 related to the authentic

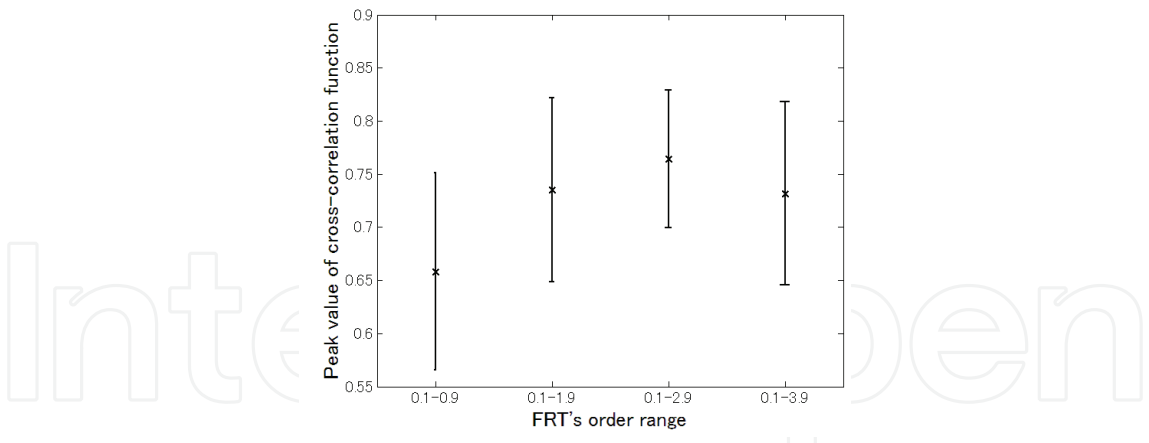


Fig. 10. Behavior of peak value of the normalized cross-correlation function related to the impostor distribution

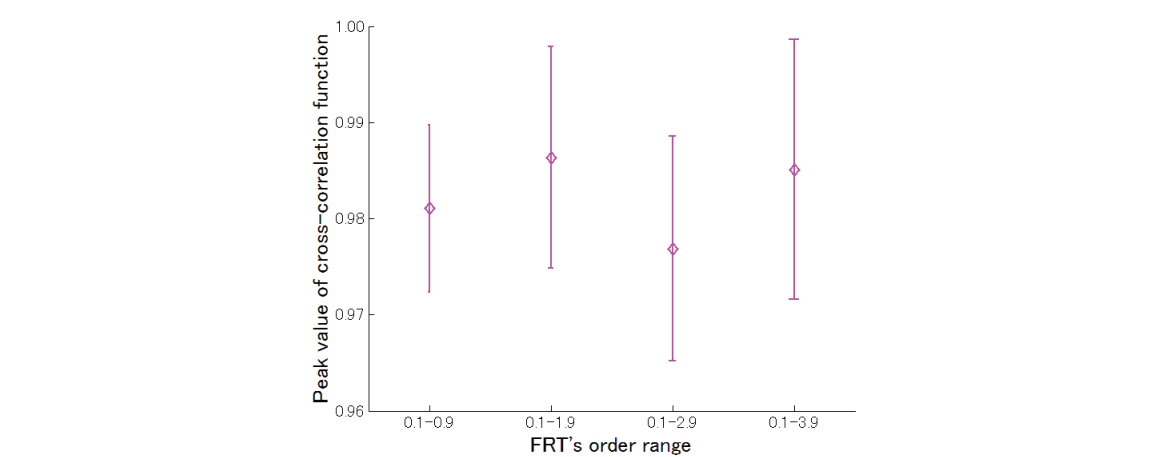


Fig. 11. Behavior of peak value of the normalized cross-correlation function related to the authentic distribution

distribution, the symbol of diamond shape and the bar denote the averaged peak value and the standard deviation of the peak value, respectively. The averaged peak values for the FRT's order ranges of 0.1-0.9, 0.1-1.9, 0.1-2.9 and 0.1-3.9 are 0.981, 0.986, 0.977 and 0.985, respectively. Additionally, the standard deviations of the peak values for the FRT's order ranges of 0.1-0.9, 0.1-1.9, 0.1-2.9 and 0.1-3.9 are 0.00869, 0.0115, 0.0117 and 0.0135, respectively.

Moreover, Fig. 12 depicts histograms that correspond to the impostor and authentic distributions, when the FRT's order range is 0.1-0.9. The left-hand curve in Fig. 12 corresponds to the impostor distribution related to Fig. 10, when the FRT's order range is 0.1-0.9. The right-hand curve in Fig. 12 corresponds to the authentic distribution related to Fig. 11, when the FRT's order range is 0.1-0.9. In this case, the MER is $7.36 \times 10^{-4}\%$ and the authentication threshold is 0.95.

Furthermore, Fig. 13 illustrates histograms that correspond to the impostor and authentic distributions, when the FRT's order range is 0.1-1.9. The MER is $5.31 \times 10^{-3}\%$ and the authentication threshold is 0.96. As we can see from the comparison between Figs. 12 and 13, the peak of the impostor distribution shifts to right and the peak of the authentic distribution becomes high, when the FRT's range is changed from 0.1-0.9 to 0.1-1.9.

The recent available specification sheets of major fingerprint authentication systems in the market indicate that the matching accuracy is from 0.001 % to 1.0 % in the FAR and from 0.0001 % to 0.1 % in the FRR. As summarized in Table 1, the MER takes a value of $7.36\times10^{-4}\%$ when $p=0.1-0.9$, $5.31\times10^{-3}\%$ when $p=0.1-1.9$, $2.80\times10^{-3}\%$ when $p=0.1-2.9$, and $5.51\times10^{-3}\%$ when $p=0.1-3.9$. As a result, we found that the fingerprint authentication by use of the FRT has the high matching accuracy.

From the results shown in Figs. 7, 8, 10 and 11 and Table 1 and our final objective to realize the FRT by the optical system, we can say that the suitable FRT's order range is 0.1-1.9 in our method.

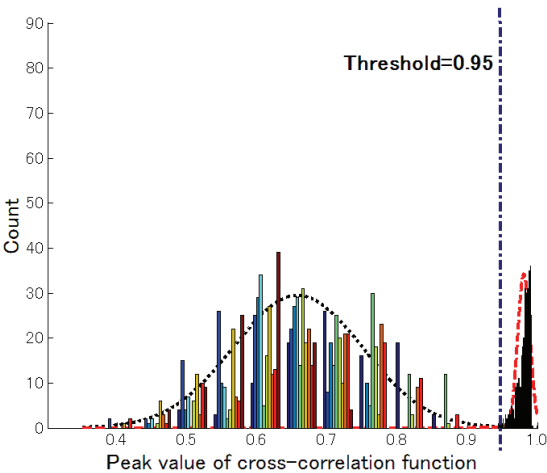


Fig. 12. A set of histograms corresponding to the impostor and authentic distributions (FRT's order range=0.1-0.9)

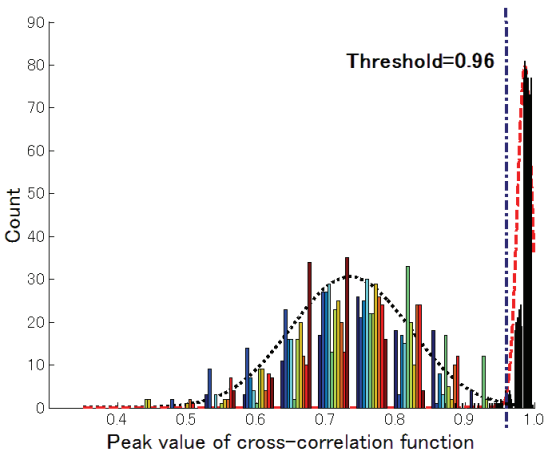


Fig. 13. A set of histograms corresponding to the impostor and authentic distributions (FRT's order range=0.1-1.9)

FRT's order range	MER (FAR / FRR)	Threshold
0.1~0.9	7.36×10^{-4}	0.95
0.1~1.9	5.31×10^{-3}	0.96
0.1~2.9	2.80×10^{-3}	0.94
0.1~3.9	5.51×10^{-3}	0.95

Table 1. MERs and authentication thresholds for various FRT's order ranges

6. Effects of size reduction of the extracted fingerprint image on the authentication

In Section 5, we analyzed the authentication accuracy by use of the templates generated by the FRT of the extracted fingerprint images with the size of 200×200 pixels. In this section, the authentication accuracy is analyzed by changing the size of the extracted fingerprint image, for example, 50×200, 100×200 and 150×200 pixels, when the FRT's order range is 0.1-1.9. The analysis method is the same as that in Section 5.

First, Fig. 14 illustrates the result related to the impostor distribution which is the behavior of peak value of the normalized cross-correlation function of the intensity FRTs of two different extracted fingerprint images, by changing the extracted line number. The vertical and horizontal axes denote the peak value of normalized cross-correlation function and the extracted line number, respectively. In the figure, the symbols of diamond shape, cross and circle denote the averaged peak values when the FRT's orders are 1.0, 0.0 and random between 0.1 and 1.9, respectively. Additionally, the bar denotes the standard deviation of the peak value.

When the extracted line numbers are 50, 100, 150 and 200, the averaged peak values for $p=1.0$ are 0.967, 0.949, 0.931 and 0.916, respectively. For $p=0.0$, the averaged peak values are 0.749, 0.751, 0.757 and 0.764, respectively, and for $p=\text{random}$, they are 0.734, 0.732, 0.732 and 0.735, respectively.

From these results, it is found that the probability of the accepting other person erroneously is low when $p=\text{random}$ in comparison with those when $p=1.0$ and 0.0. Moreover, there is little effect for the variation of the extracted line number when $p=\text{random}$ in comparison with that when $p=1.0$.

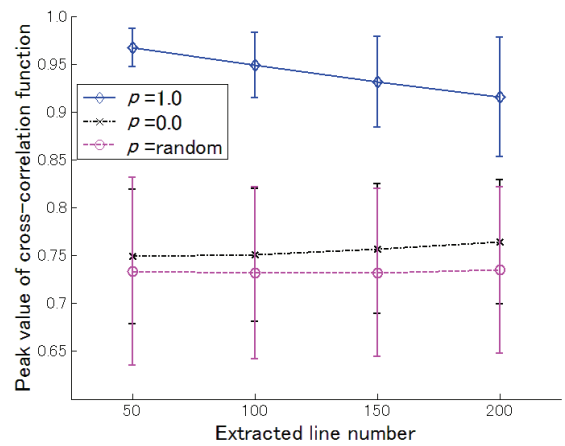


Fig. 14. Peak value of the normalized cross-correlation function of the intensity FRTs by changing the extracted line number (Impostor distribution)

Next, Fig. 15 illustrates the result related to the authentic distribution which is the behavior of peak value of the normalized cross-correlation function of the intensity FRTs of the extracted fingerprint images with and without random noise, by changing the extracted line number. The vertical and horizontal axes denote the peak value of normalized cross-correlation function and the extracted line number, respectively. In the figure, the symbols of diamond shape, circle and cross denote the averaged peak values when the FRT's orders are 1.0, random between 0.1 and 1.9, and 0.0, respectively. Additionally, the bar denotes the standard deviation of the peak value.

When the extracted line numbers are 50, 100, 150 and 200, the averaged peak values for $p=1.0$ are 0.989, 0.993, 0.995 and 0.995, respectively. For $p=\text{random}$, the averaged peak values are 0.976, 0.982, 0.984 and 0.986, respectively, and for $p=0.0$, they are 0.967, 0.972, 0.975 and 0.977, respectively.

From these results, it is found that the probabilities of the rejecting identical person erroneously are more-or-less identical for $ps=1.0$, 0.0 and random. Moreover, there is little effect for the variation of the extracted line number for $ps=1.0$, 0.0 and random.

Table 2 illustrates the MERs for the variation of the extracted line number, which were obtained from Figs. 14 and 15. From the table, it is found that the effect of the variation of the extracted line number on the authentication accuracy is very little because the values of MERs are fully small as shown in Table 2.

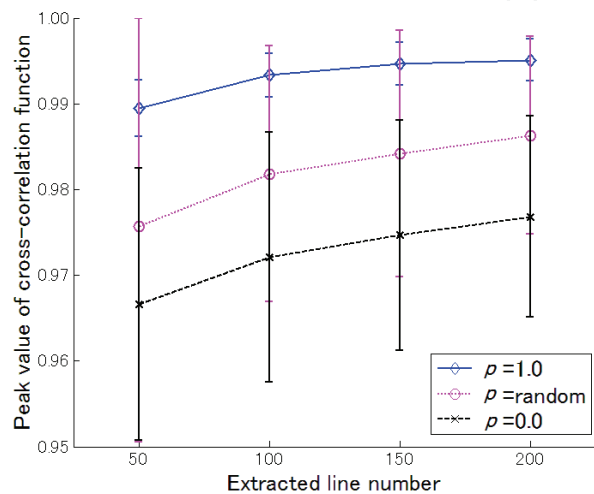


Fig. 15. Peak value of the normalized cross-correlation function of the intensity FRTs by changing the extracted line number (Authentic distribution)

Extracted line number	MER, $p=1.0$ (FAR / FRR)	MER, $p=0.0$ (FAR / FRR)	MER, $p=\text{random}$ (FAR / FRR)
50	0.165	5.83×10^{-3}	2.49×10^{-2}
100	0.111	4.22×10^{-3}	8.49×10^{-3}
150	0.104	3.79×10^{-3}	6.72×10^{-3}
200	0.110	2.81×10^{-3}	5.31×10^{-3}

Table 2. MERs for variations of the extracted line number and the FRT’s order

7. Conclusions

First, we generated the templates of many original fingerprint images by use of the FRT. As a result from comparisons between the generated templates and the original fingerprint images, it was found that the templates are fully different from the original fingerprint images when the templates were generated by changing randomly the FRT’s order in every line of the original fingerprint images. It was also found that the generated templates are very high secure, because the templates could not be decoded to the original fingerprint images by the unauthorized third persons who are unapprised of the information on the FRT’s order in every line.

Additionally, the authentication accuracy of the templates generated by the FRT of the extracted fingerprint images with 200×200 pixels was analyzed by changing the FRT’s order

range. We found that the suitable FRT's order range for the generation of the template in our method is 0.1-1.9.

The authentication accuracy was also analyzed by changing the size of the extracted fingerprint image, concretely, 150×200, 100×200 and 50×200 pixels. As a result, it was found that the authentication accuracy is fully high even if the size of the extracted fingerprint image is small, so that the authentication is possible at higher speed.

8. References

- Bailey, D. H. & Swartztrauber, P. N. (1991). The fractional Fourier transform and applications, *SIAM Review*, Vol. 33, No. 3, pp. 389-404, ISSN: 0036-1445
- Bultheel, A. & Martinez Sulbaran, H. E. (2004a). Computation of the fractional Fourier transform, *Applied and Computational Harmonic Analysis*, Vol. 16, No. 3, pp. 182-202, ISSN: 1063-5203
- Bultheel, A. & Martinez Sulbaran, H. E. (2004b). <http://nalag.cs.kuleuven.be/research/software/FRFT/>
- Lee, H.; Maeng, H. & Bae, Y. (2009). Fake finger detection using the fractional Fourier transform, In: *Biometric ID Management and Multimodal Communication*, Fierrez, J.; Ortega-Garcia, J.; Esposito, A.; Drygajlo, A. & Faundez-Zanuy, M. (Eds.), pp. 318-324, Springer, ISBN: 978-3-642-04390-1, Heidelberg
- Lohmann, A. W. (1993). Image rotation, Wigner rotation, and the fractional Fourier transform, *Journal of the Optical Society of America A*, Vol. 10, No. 10, pp.2181-2186, ISSN: 0740-3232
- Maltoni, D.; Maio, D.; Jain, A.K. & Prabhakar, S. (2003). *Handbook of Fingerprint Recognition*, Springer, 2003, ISBN : 0-387-95431-7, New York
- Maltoni, D. & Maio, D.; (2004). Download Page of FVC2004, Biometric System Laboratory, University of Bologna, Italy (<http://bias.csr.unibo.it/fvc2004/download.asp>)
- Mansfield, T.; Kelly, G.; Chandler, D. & Kane, J. (2001). Biometric Product Testing Final Report, Issue 1.0, In: *CESG/BWG Biometric Test Programme*, Centre for Mathematics and Scientific Computing, National Physical Laboratory
- Marinho, F. J. & Bernardo, L. M. (1998). Numerical calculation of fractional Fourier transforms with a single fast-Fourier-transform algorithm, *Journal of the Optical Society of America A*, Vol. 15, No. 8, pp. 2111-2116, ISSN: 0740-3232
- Moreno, I.; Davis, J. A. & Crabtree, K. (2003). Fractional Fourier transform optical system with programmable diffractive lenses, *Applied Optics*, Vol. 42, No. 32, pp. 6544-6548, ISSN: 0003-6935
- Ozaktas, H. M. ; Zalevsky, Z. & Kutay, M. A. (2001). *The Fractional Fourier Transform*, John Wiley & Sons., 2001, ISBN: 0-471-96346-1, Chichester
- Takeuchi, H. ; Umezaki, T. ; Matsumoto, N. & Hirabayashi, K.. (2007). Evaluation of low-quality images and imaging enhancement methods for fingerprint verification, *Electronics and Communications in Japan, Part 3*, Vol. 90, No. 10, pp. 40-53, Online ISSN : 1520-6424
- Yang, X.; Tan, Q.; Wei, X.; Xiang, Y.; Yan, Y. & Jin, G. (2004). Improved fast fractional-Fourier-transform algorithm, *Journal of the Optical Society of America A*, Vol. 21, No. 9, pp. 1677-1681, ISSN: 1084-7529



Fourier Transforms - Approach to Scientific Principles

Edited by Prof. Goran Nikolic

ISBN 978-953-307-231-9

Hard cover, 468 pages

Publisher InTech

Published online 11, April, 2011

Published in print edition April, 2011

This book aims to provide information about Fourier transform to those needing to use infrared spectroscopy, by explaining the fundamental aspects of the Fourier transform, and techniques for analyzing infrared data obtained for a wide number of materials. It summarizes the theory, instrumentation, methodology, techniques and application of FTIR spectroscopy, and improves the performance and quality of FTIR spectrophotometers.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Reiko Iwai and Hiroyuki Yoshimura (2011). High-Accuracy and High-Security Individual Authentication by the Fingerprint Template Generated Using the Fractional Fourier Transform, *Fourier Transforms - Approach to Scientific Principles*, Prof. Goran Nikolic (Ed.), ISBN: 978-953-307-231-9, InTech, Available from: <http://www.intechopen.com/books/fourier-transforms-approach-to-scientific-principles/high-accuracy-and-high-security-individual-authentication-by-the-fingerprint-template-generated-usin>

INTECH
open science | open minds

InTech Europe

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

InTech China

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

© 2011 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the [Creative Commons Attribution-NonCommercial-ShareAlike-3.0 License](https://creativecommons.org/licenses/by-nc-sa/3.0/), which permits use, distribution and reproduction for non-commercial purposes, provided the original is properly cited and derivative works building on this content are distributed under the same license.

IntechOpen

IntechOpen