Figure 3(b) shows the histogram of the PV in case of $0.7 \le p_i(=q_i) \le 1.0$. The APV is 0.456 and the SDPVs is 3.55×10^{-2}. In Table 4, the APVs and the SDPVs are summarized in cases of $0.5 \le p_i(=q_i) \le 1.0$, $0.6 \le p_i(=q_i) \le 1.0$, $0.7 \le p_i(=q_i) \le 1.0$, $0.8 \le p_i(=q_i) \le 1.0$ and $0.9 \le p_i(=q_i) \le 1.0$. From this table, it was found that the APV takes the largest value in case of $0.5 \le p_i \le 1.0$. However, the SDPV takes the smallest value in case of $0.8 \le p_i \le 1.0$. The condition that the APV takes the largest value and the SDPV takes the smallest value is desired to achieve the high recognition accuracy. Therefore, we can say that the most suitable condition of p_i in our template generating
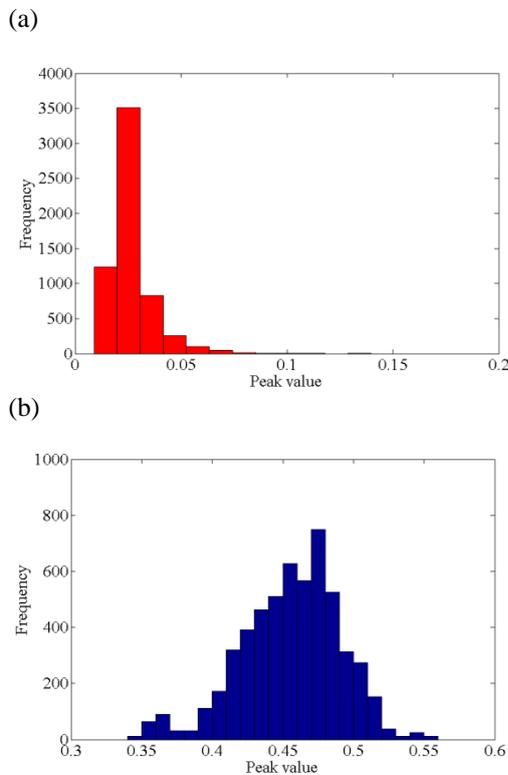
(a)

(b)

Figure 3. (a) Histogram of the PV of the NCF between the templates of two different fingerprint images in case of $0.7 \le p_i(=q_i) \le 1.0$. The APV is 2.65×10^{-2} and the SDPV is 9.92×10^{-3}. (b) Histogram of the PV of the NCF between the templates of the fingerprint images with and without random noise, in case of $0.7 \le p_i(=q_i) \le 1.0$. The APV is 0.456 and the SDPV is 3.55×10^{-2}.

Table 3. APVs and SDPVs of the NCFs between the templates obtained from two different fingerprint images, in cases of $0.5 \le p_i(=q_i) \le 1.0$, $0.6 \le p_i(=q_i) \le 1.0$, $0.7 \le p_i(=q_i) \le 1.0$, $0.8 \le p_i(=q_i) \le 1.0$ and $0.9 \le p_i(=q_i) \le 1.0$.

Range of p_i $(=q_i)$	APV	SDPV
0.5-1.0	2.91×10^{-2}	1.41×10^{-2}
0.6-1.0	2.73×10^{-2}	1.15×10^{-2}
0.7-1.0	2.65×10^{-2}	9.92×10^{-3}
0.8-1.0	2.74×10^{-2}	9.37×10^{-3}
0.9-1.0	3.51×10^{-2}	1.03×10^{-2}

Table 4. APVs and SDPVs of the NCFs between the templates obtained from the fingerprint images with and without random noise, in cases of $0.5 \le p_i(q_i) \le 1.0$, $0.6 \le p_i(=q_i) \le 1.0$, $0.7 \le p_i(=q_i) \le 1.0$, $0.8 \le p_i(=q_i) \le 1.0$ and $0.9 \le p_i(=q_i) \le 1.0$.

Range of p_i $(=q_i)$	APV	SDPV
0.5-1.0	0.516	4.17×10^{-2}
0.6-1.0	0.487	3.79×10^{-2}
0.7-1.0	0.456	3.55×10^{-2}
0.8-1.0	0.427	3.50×10^{-2}
0.9-1.0	0.407	3.64×10^{-2}

method cannot be decided only from the viewpoint of the genuine distribution

5.3 ROC curve

As an example, in case of $0.7 \le p_i(=q_i) \le 1.0$, the impostor and genuine distributions could be obtained from Figures 3(a) and 3(b) by fitting the normalized Gaussian distributions. Figure 4 shows the result. The left-side and right-side curves correspond to the impostor and genuine distributions, respectively. By changing the threshold level corresponding to the PV, the ROC curve could be obtained as shown in Figure 5(a). The results in cases of $0.5 \le p_i(=q_i) \le 1.0$, $0.6 \le p_i(=q_i) \le 1.0$, $0.8 \le p_i(=q_i) \le 1.0$ and $0.9 \le p_i(=q_i) \le 1.0$ are also shown in Figures 5(b), 5(c), 5(d) and 5(e), respectively. From these figures, we can understand that the values of the FAR and FRR are the smallest in case of $0.7 \le p_i(=q_i) \le 1.0$.
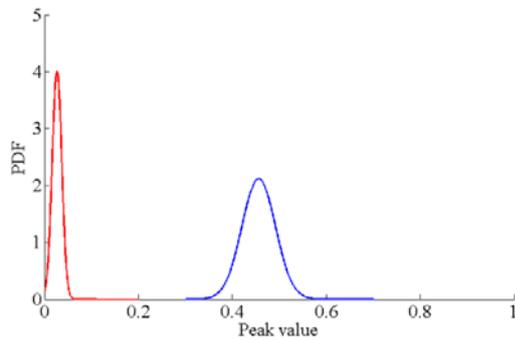
Figure 4. Impostor distribution (left-side curve) and genuine distribution (right-side curve) obtained from Figures 3(a) and 3(b), respectively. PDF means the probability density function.

5.4 MER

From the ROC curves shown in Figure 5, we can obtain the MERs. In Table 5, the MERs are summarized in cases of $0.5 \leq p_i(=q_i) \leq 1.0$, $0.6 \leq p_i(=q_i) \leq 1.0$, $0.7 \leq p_i(=q_i) \leq 1.0$, $0.8 \leq p_i(=q_i) \leq 1.0$ and $0.9 \leq p_i(=q_i) \leq 1.0$. From this table, it was found that the MER takes the smallest value of 1.60×10^{-19} % in case of $0.7 \leq p_i(=q_i) \leq 1.0$. Therefore, we can say that $0.7 \leq p_i(=q_i) \leq 1.0$ is the most suitable condition of p_i and q_i in our template generating method, and our templates can realize the extremely high recognition accuracy, because the smallest values of the FARs and the FRRs of the commercially available fingerprint recognition systems are 0.001% and 0.1%, respectively, as summarized in Table 2 in [19].

6. Robustness of our proposed templates

In this section, the robustness of our proposed fingerprint templates is analyzed by use of the 110 fingerprint images which were used in the previous section. First, for each fingerprint image, 50 templates were generated by changing p_i in different transverse lines of the image in $0.7 \leq p_i \leq 1.0$. Therefore, we investigated 5,500 cases. Next, the inverse DFSTs (IDFSTs) of the generated templates were performed under the same values of p_i which were used in the generating process of the templates. This condition of p_i was assumed to be the most serious case that an adversary could get both the template itself and the information about the transforms' orders, p_i.
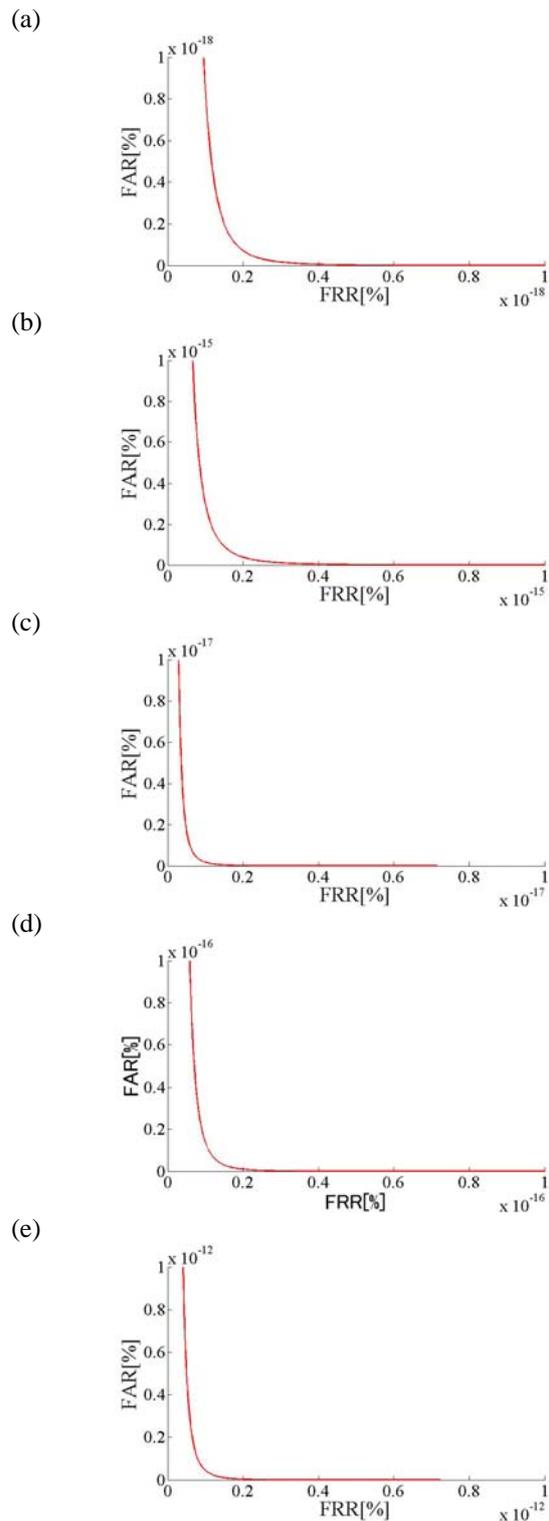
(a)

(b)

(c)

(d)

(e)

Figure 5. ROC curves in cases of (a) $0.7 \leq p_i(=q_i) \leq 1.0$ (b) $0.5 \leq p_i(=q_i) \leq 1.0$ (c) $0.6 \leq p_i(=q_i) \leq 1.0$ (d) $0.8 \leq p_i(=q_i) \leq 1.0$ and (e) $0.9 \leq p_i(=q_i) \leq 1.0$.

Finally, we derived the APV and the SDPV of the NCFs between the input data of the DFSTs of the fingerprint images and the obtained IDFST data. As an example, Figure 6(a) shows the input data of the DFST of the fingerprint image shown in Figure 1(a) and Figure 6(b) shows an example of the fingerprint template, i.e., the PDs of the DFSTs. Figure 6(c) shows the obtained IDFST data.

As a result, the APV and the SDPV for 5,500 templates were 4.76×10^{-2} and 1.08×10^{-2}, respectively. For other ranges of p_i, the APVs and the SDPVs were also obtained and are summarized in Table 6. From this table, it was understood that our templates could not be easily restored to the original input data because the APVs of the NCFs are extremely small. In this way, it was found that our proposed fingerprint templates have fully high robustness.

7. Conclusions

In this paper, we have proposed a new method for generating fingerprint templates with high recognition accuracy and high security by use of the DFST. Specifically, the fingerprint template corresponds to the PDs of the DFSTs with different transforms' orders for the grayscale distributions in different transverse

Table 5. MERs obtained from the ROC curves shown in Figure 5.

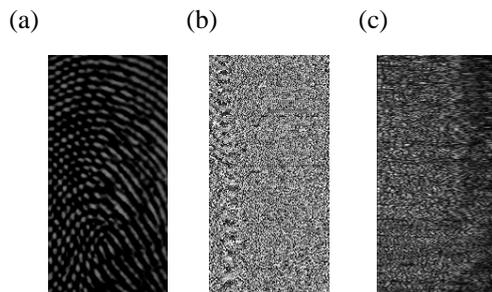| Range of p_i	MER (%)
0.5-1.0	1.32×10^{-16}
0.6-1.0	6.66×10^{-19}
0.7-1.0	1.60×10^{-19}
0.8-1.0	1.07×10^{-17}
0.9-1.0	8.36×10^{-14}

(a)   (b)   (c)

Figure 6. (a) original input data of the DFST of the fingerprint image shown in Figure 1(a), (b) an example of the fingerprint template, i.e., the PDs of the DFSTs and (c) an example of the obtained IDFST data in case of $0.7 \leq p_i \leq 1.0$.

Table 6. APVs and SDPVs of the NCFs between the input data of the DFSTs of the fingerprint images and the obtained IDFST data in cases of $0.5 \leq p_i \leq 1.0$, $0.6 \leq p_i \leq 1.0$, $0.7 \leq p_i \leq 1.0$, $0.8 \leq p_i \leq 1.0$ and $0.9 \leq p_i \leq 1.0$.

Range of p_i	APV	SDPV
0.5-1.0	5.24×10^{-2}	1.05×10^{-2}
0.6-1.0	4.95×10^{-2}	1.06×10^{-2}
0.7-1.0	4.76×10^{-2}	1.08×10^{-2}
0.8-1.0	4.69×10^{-2}	1.11×10^{-2}
0.9-1.0	4.87×10^{-2}	1.19×10^{-2}

lines of the original fingerprint image. As a result, it was made clear that (i) the recognition accuracy of our fingerprint templates is extremely high, i.e., MER= 1.60×10^{-19} %, when $0.7 \leq p_i \leq 1.0$; (ii) the robustness, i.e., the security, of our templates is also extremely high.

As a further study, the effects of the misalignment in the recognition process should be analyzed in detail.

8. References

[1] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, New York, 2003.

[2] U. Uludag and A. Jain, "Securing fingerprint template: Fuzzy vault with helper data," in *Proceedings of 2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06)*, 2006, pp. 163-170.

[3] A. Nagar, K. Nandakumar, and A. K. Jain, "Securing fingerprint template: Fuzzy vault with minutiae descriptors," in *Proceedings of 19th International Conference on Pattern Recognition, 2008 (ICPR2008)*, 2008, pp.1-4.

[4] K. Xi and J. Hu, "Biometric mobile template protection: A composite feature based fingerprint fuzzy valut," in *Proceedings of IEEE International Conference on Communications, 2009 (ICC'09)*, 2009, pp. 1-5.

[5] R. Wang, X. Yang, X. Liu, S. Zhou, P. Li, K. Cao, and J. Tian, "A novel fingerprint template protection scheme based on distance projection coding," in *Proceedings of 2010 20th International Conference on Pattern Recognition (ICPR)*, 2010, pp. 886-889.

[6] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 29, No. 4, 2007, pp. 561-572.

[7] C. Lee, J. –Y. Choi, K. –A. Toh, S. Lee, and J. Kim, "Alignment-free cancelable fingerprint templates based on local minutiae information," *IEEE Transactions on Systems, Man, and Cybernetics. Part B: Cybernetics*, Vol. 37, No. 4, 2007, pp. 980-992.

[8] H. Yang, X. Jiang, and A. C. Kot, "Generating secure cancelable fingerprint templates using local and global features," in *Proceedings of 2nd IEEE International Conference on Computer Science and Information Technology, 2009 (ICCSIT 2009)*, 2009, pp. 645-649.

[9] B. Yang, C. Busch, P. Bours, and D. Gafurov, "Non invertible geometrical transformation for fingerprint minutiae template protection," in *Proceedings of the First International Workshop on Information Forensics and Security, 2009 (WIFS 2009)*, 2009, pp. 81-85.

[10] Z. Jin, A. B. J. Teoh, T. S. Ong, and C. Tee, "Generating revocable fingerprint template using minutiae pair representation," *Proceedings of 2010 2nd International Conference on Education Technology and Computer (ICETC)*, Vol. 5, 2010, pp. V5-251-V5-255.

[11] H. M. Ozaktas, Z. Zalevsky, and M. A. Kutay, *The fractional Fourier transform*, John Wiley & Sons., New York, 2001.

[12] R. Iwai and H. Yoshimura, "Matching accuracy analysis of fingerprint templates generated by data processing method using the fractional Fourier transform," *International Journal of Communications, Network and System Sciences*, Vol. 4, No. 1, 2011, pp. 24-32. Available: http://www.scirp.org/journal/ PaperInformation.aspx?paperID=3692

[13] R. Iwai and H. Yoshimura, "High-accuracy and high-security individual authentication by the fingerprint template generated using the fractional Fourier transform," in *Fourier Transforms - Approach to Scientific Principles*, (Goran Nikolic, Ed.). InTech, Croatia, 2011, Chapter 15, pp. 281-294. Available: http://www.intechweb.org/books/show/title/fourier-transforms-approach-to-scientific-principles

[14] S. –C. Pei and M. –H. Yeh, "The discrete fractional cosine and sine transform," *IEEE Transactions on Signal Processing,* Vol. 49, No.6, 2001, pp. 1198-1207.

[15] T. Mansfield, G. Kelly, D. Chandler, and J. Kane, "Biometric Product Testing Final Report, Issue 1.0," in *CESG/BWG Biometric Test Programme, Centre for Mathematics and Scientific Computing*, National Physical Laboratory, 2001. Available: http://www.lgiris. com/download/brochure/ uk_report.pdf

[16] V. Namias, "The fractional Fourier transform and its application in quantum mechanics," *IMA Journal of Applied Mathematics,* Vol. 25, No.3, 1980, pp. 241-265.

[17] F. J. Marinho and L. M. Bernardo, "Numerical calculation of fractional Fourier transforms with a single fast-Fourier-transform algorithm," *Journal of the Optical Society of America,* Vol. 15, No.8, 1998, pp. 2111-2116.

[18] A. W. Lohmann, "Image rotation, Wigner rotation, and the fractional Fourier transform," *Journal of the Optical Society of America A,* Vol. 10, No.10, 1993, pp. 2181-2186.

[19] H. Yoshimura, "Optical spatial-frequency correlation system for fingerprint recognition," in *State of the Art in Biometrics*, (Jucheng Yang and Loris Nanni, Eds.). InTech, Croatia, 2011, Chapter 4, pp. 85-104. Available: http://www.intechweb.org/books/show/title/state-of-the-art-in-biometrics