Zen Chen (*Institute of Computer Science & Information Engineering, National Chiao Tung University, Hsinchu, Taiwan, Republic of China*)

Yi-Ping Hung: corresponding author

Cheng-Yuan Tang: also with the Institute of Computer Science & Information Engineering, National Chiao Tung University

References

1 BEAUCHMIN, S.S., and BARRON, J.L.: 'The computation of optical flow', *ACM Comput. Surv.*, 1995, **27**, (3), pp. 433–467

2 HUANG, H.C., and HUNG, Y.P.: 'Adaptive early-jump-out technique for fast motion estimation in video coding', *Graph. Models Image Process.*, 1997, **59**, (6), pp. 388–394

3 MEER, P., MINTZ, D., ROSENFELD, A., and KIM, D.: 'Robust regression methods for computer vision: A review', *Int. J. Comput. Vision*, 1991, **6**, pp. 59–70

4 ROUSSEEUW, P.J., and LEROY, A.M.: 'Robust regression & outlier detection' (Wiley, New York, 1987)

5 SINGH, A.: 'Optical flow computation: A unified perspective' (IEEE Computer Society Press, 1992)

Shape recognition using DRFT-based correlator

Neng-Chung Hu and Kuo-Kan Yu

The proposed approach uses two types of correlator. The first is a correlator using DFT to detect the positions of peak values, while the second is a correlator using the discrete rotational Fourier transform (DRFT) to display the correlated images. The purpose of this scheme is to recognise multiple different targets simultaneously.

Introduction: Correlators are among the most powerful techniques for locating multiple objects. Several schemes have been proposed [1 – 3]. These conventional correlators, based on DFT, cannot handle multiple different targets. For example, if both reference and input have many different objects, the DFT-based correlator of the reference and input will generate many peak values. It is difficult to recognise the images of the input objects from these peaks. However this problem can be easily solved if we use the DRFT-based correlator in our proposed approach, for the DRFT [4] contains both time and frequency information.

DRFT and DRFT-based correlator: The DRFT is given by [4]

$$X_\alpha[n,k]=a_0(\alpha)x[n]+a_1(\alpha)X[k]+a_2(\alpha)x[-n]+a_3(\alpha)X[-k] \quad (1)$$

where the rotational angle α relates to the fractional order P of the DFT by

$$\alpha = P\cdot(\pi/2) \quad (2)$$

and the coefficients corresponding to each component are

$$a_0(\alpha) = 0.5(1+e^{j\alpha})\cos\alpha \quad (3)$$

$$a_1(\alpha) = 0.5(1-je^{j\alpha})\sin\alpha \quad (4)$$

$$a_2(\alpha) = 0.5(e^{j\alpha}-1)\cos\alpha \quad (5)$$

$$a_3(\alpha) = 0.5(-1-je^{j\alpha})\sin\alpha \quad (6)$$

Based on this, we borrow the definition from the 1D DRFT and define the two-dimensional DRFT of an $N\times N$ square image as

$$X_\alpha[n_1,n_2,k_1,k_2] = a_0(\alpha)x[n_1,n_2]+a_1(\alpha)X[k_1,k_2] +a_2(\alpha)x[-n_1,-n_2]+a_3(\alpha)X[-k_1,-k_2] \quad (7)$$

where $X[k_1,k_2]$ is the two-dimensional DFT of $x[n_1,n_2]$. Like the 1D DRFT, the 2D DRFT contains both time and frequency domain information.

The correlation of $x[n_1,n_2]$ and $h[n_1,n_2]$ is given by

$$x[n_2,n_2]^\circ h[n_1,n_2] = \frac{1}{N}\sum_{k_1=0}^{N-1}\sum_{k_2=0}^{N-1} x[k_1,k_2]h[k_1-n_1,k_2-n_2] \quad n_1,n_2=0,1,2,...,N-1 \quad (8)$$

The correlation value is the overlapped area of $x[n_1,n_2]$ and $h[n_1,n_2]$ divided by N. The correlation can be implemented by the DFT transform domain as $X[k_1,k_2]H^*[k_1,k_2]$, where '*' denotes the complex conjugate. Thus the DRFT-based correlator is given by $X_\alpha[n_1,n_2,k_1,k_2]$ $H_\alpha^*[n_1,n_2,k_1,k_2]$, where $X_\alpha[n_1,n_2,k_1,k_2]$ and $H_\alpha[n_1,n_2,k_1,k_2]$ are the DRFT of $x[n_1,n_2]$ and $h[n_1,n_2]$, respectively. The product is then taken by the inverse DRFT given by $a_0(-\alpha)x[n_1,n_2]$ + $a_1(-\alpha)X[k_1,k_2]$ + $a_2(-\alpha)x[-n_1,-n_2]$ + $a_3(-\alpha)X[-k_1,-k_2]$, yielding 64 terms. Among these 64 terms, only two kinds of information are significant: correlation and product results. The correlation results are generated by the following terms: $a_1(-\alpha)a_0(\alpha)a_0^*(\alpha)X[k_1,k_2]^\circ H^*[k_1,k_2]$, $a_3(-\alpha)a_2(\alpha)a_2^*(\alpha)X[k_1,k_2]^\circ H^*[k_1,k_2]$, $a_1(-\alpha)a_2(\alpha)a_2^*(\alpha)X[-k_1,-k_2]^\circ H^*[-k_1,-k_2]$, $a_3(-\alpha)a_0(\alpha)a_0^*(\alpha)X[-k_1,-k_2]^\circ H^*[-k_1,-k_2]$, $a_3(-\alpha)a_1(\alpha)a_1^*(\alpha)x[n_1,n_2]^\circ h^*[n_1,n_2]$, $a_1(-\alpha)a_3(\alpha)a_3^*(\alpha)x[n_1,n_2]^\circ h^*[n_1,n_2]$, $a_1(-\alpha)a_1(\alpha)a_1^*(\alpha)x[-n_1,-n_2]^\circ h^*[-n_1,-n_2]$ and $a_3(-\alpha)a_3(\alpha)a_3^*(\alpha)x[-n_1,-n_2]^\circ h^*[-n_1,-n_2]$, while the product results are generated by $a_0(-\alpha)a_0(\alpha)a_0^*(\alpha)x[n_1,n_2]h^*[n_1,n_2]$, $a_2(-\alpha)a_2(\alpha)a_2^*(\alpha)x[n_1,n_2]h^*[n_1,n_2]$, $a_0(-\alpha)a_2(\alpha)a_2^*(\alpha)x[-n_1,-n_2]h^*[-n_1,-n_2]$ and $a_2(-\alpha)a_0(\alpha)a_0^*(\alpha)x[-n_1,-n_2]h^*[-n_1,-n_2]$. The former generates correlation peaks, while the latter generates the correlated images. If the images in the input have exactly the same positions as the images in the reference, the DRFT-based correlator can generate the correlation peaks from the correlation results. Moreover, it can display the correlated images owing to the product results. The displayed images are our targets. Because of this, we are able to obtain from the peak values the images corresponding to the peaks. In the proposed shape recognition scheme, we first use the conventional correlator to generate the peak values and their locations, and then, according to these locations, we shift the reference images to the correct positions. Finally, we use the DRFT-based correlator to display the correlated images.

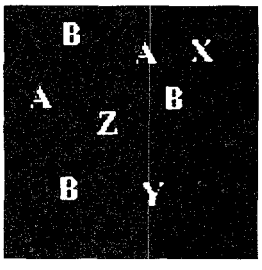

Fig. 1 *Input image*

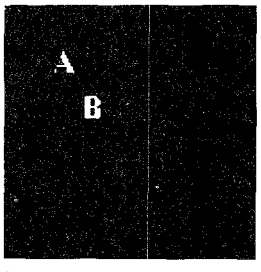

Fig. 2 *Reference image*

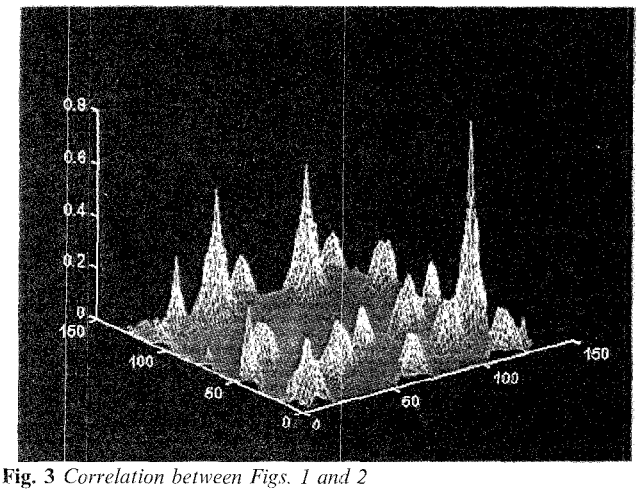

Fig. 3 *Correlation between Figs. 1 and 2*

Computer simulations and discussions: Figs. 1 and 2 are used as the input and reference respectively. The conventional correlator

generates several peaks (shown in Fig. 3), and it is difficult to distinguish which peaks are generated by which images of the input. However, the peak values and their corresponding positions shown in Table 1 indicate only four significant peaks. To obtain the images corresponding to these four peaks, the DRFT-based correlator is applied. To see which image in both the reference and the input generates the first peak, we move Fig. 2 40 pixels in the X-direction and 124 pixels in the Y-direction. The moved image is correlated with the input object by the DRFT-based correlator, resulting in the displayed image shown in Fig. 4*a*, which is the 'A and B' image in the top righthand corner of Fig. 1. By applying the same procedures to the second, third, and fourth peaks, we obtain two single Bs and one single A, shown in Fig. 4*b–d*. The conclusion of the DRFT-based correlation between Figs. 1 and 2 is that Fig. 1 contains four patterns; 'A and B', two single Bs, and one single A.

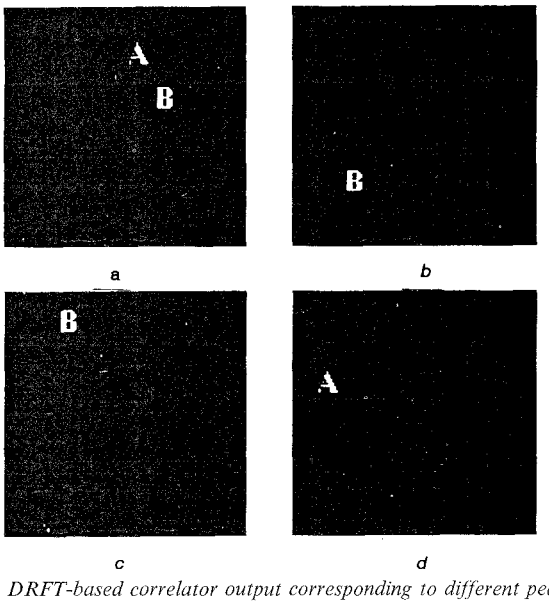

Fig. 4 *DRFT-based correlator output corresponding to different peaks*

a 1st peak
b 2nd peak
c 3rd peak
d 4th peak

Table 1: Seven larger peak values of Fig. 3

Peak number	Peak value	Co-ordinate (*x*, *y*)	Corresponding input object	Matching reference object	Detected input object		
					Position	Area (pixels): 128×(peak value)	DRFT-based correlator output
1	0.7969	(40, 124)	Upper right A, B	A, B	A(73.30) B(82.46)	102	Fig. 4*a*
2	0.5078	(116, 40)	Lower left B	B	(32.98)	65	Fig. 4*b*
3	0.5078	(117, 91)	Upper left B	B	(38.18)	65	Fig. 4*c*
4	0.2891	(116, 18)	Left A	A	(17.50)	37	Fig. 4*d*
5	0.2578	(8, 8)	Z	B	(55.59)	33	
6	0.2188	(54, 100)	X	B	(97.20)	28	
7	0.2031	(31, 43)	Y	B	(73.94)	26	

Conclusion: The DRFT contains both time and frequency information. Thus, the DRFT-based correlator can not only generate correlation peaks, but also display the corresponding correlated images. With this property, the DRFT-based correlator can be used to recognise multiple different objects.

10 April 1998
Electronics Letters Online No: 19980738

Neng-Chung Hu and Kuo-Kan Yu (*Electronic Engineering Department, National Taiwan University of Science and Technology, 43, Keelung Road, Sec. 4, Taipei, Taiwan, Republic of China*)

References

1 HORNER, J.L., and BARTELT, H.O.: 'Two-bit correlation', *Appl. Opt.*, 1985, **24**, (18), pp. 2889–2893
2 MAHALANOBIS, A., KUMAR, B.V.K.V., and CASASENT, D.: 'Minimum average correlation energy filters', *Appl. Opt.*, 1987, **26**, (17), pp. 3633–3640
3 JAVIDI, B., WANG, J., and TANG, Q.: 'Multiple-object binary joint transform correlation using multiple-level threshold crossing', *Appl. Opt.*, 1991, **30**, (29), pp. 4234–4244
4 SANTHANAM, B., and McCLELLAN, J.H.: 'The discrete rotational Fourier transform', *IEEE Trans. Signal Process.*, 1996, **SP-44**, (4), pp. 994–998

Improvement of Saeednia's self-certified key exchange protocols

Tzong-Chen Wu, Yuh-Shihng Chang and Tzouh-Yi Lin

In 1997, two self-certified key exchange protocols were proposed by Saeednia. It is shown that Saeednia's self-certified key exchange protocols are insecure in that an adversary may impersonate any legitimate user in key exchange. An improvement against the impersonation attack is described.

Introduction: Saeednia [1] presented two key exchange protocols based on Girault's self-certified public key system [2]. In Saeednia's key exchange protocols, there exists a trusted third party (TTP) for system setup and user registration; however, the TTP does not know the secret key of any user during user registration. Saeednia's key exchange protocols preserve the merits inherent in both the identity-based system and the self-certified system, and hence allow a considerable reduction in communication complexity. In this Letter, we first show that Saeednia's self-certified key exchange protocols are insecure. An adversary may impersonate any legitimate user in running these protocols. We also present an improvement that can withstand the impersonation attack.

Saeednia's key exchange protocol: In the setup of this system, the TTP chooses an integer n as the product of two large distinct primes p and q of almost the same size, such that $p = 2p' + 1$ and $q = 2q' + 1$, where p' and q' are also primes, a base $g \neq 1$ of order $r = p'q'$, a large integer $u < r$, and a one-way hash function f. The TTP makes g, u, f and n public, keeps r secret and discards p and q afterwards. Next, any user U_i can register with the TTP by performing the following steps:

(i) U_i randomly chooses a secret key $x_i \in Z_u$, computes the public key $y_i = g^{x_i} \bmod n$ and gives it to the TTP.

(ii) The TTP prepares a string I_i associated with U_i's personal information (name, address, etc.) and computes U_i's identity $ID_i = f(I_i)$.

(iii) The TTP computes $w_i = y_i^{ID_i^{-1}} \bmod n$ as a witness and sends $\{I_i, w_i\}$ to U_i.

(iv) U_i verifies the identity and the witness by checking that $y_i = w_i^{f(I_i)} \bmod n$.

Saeednia claimed that forging a valid witness w_i for U_i is equivalent to breaking an instance of the RSA cryptosystem [3]. Suppose that U_i and U_j want to exchange a secret key to be used for secure communication. They can perform the following protocols. These protocols are based on the well-known Diffie-Hellman key distribution system [4]. Note that the secret key exchanged in protocol 1 is invariant, while it is time-variant in protocol 2.

Protocol 1

(i) U_i sends $\{I_i, w_i\}$ to U_j

(ii) U_j sends $\{I_j, w_j\}$ to U_i

(iii) U_i computes the secret key shared with U_j as $k = w_j^{f(I_j) \cdot x_i} \bmod n$

(iv) U_j computes the secret key shared with U_i as $k = w_i^{f(I_i) \cdot x_j} \bmod n$

Protocol 2

(i) U_i randomly chooses a secret integer $t_i \in Z_u$, computes $v_i = g^{t_i} \bmod n$ and sends $\{I_i, w_i, v_i\}$ to U_j

(ii) U_j randomly chooses a secret integer $t_j \in Z_u$, computes $v_j = g^{t_j} \bmod n$ and sends $\{I_j, w_j, v_j\}$ to U_i

(iii) U_i computes the secret key shared with U_j as $k = w_j^{f(I_j) \cdot t_i} \cdot v_j^{x_i} \bmod n$

(iv) U_j computes the secret key shared with U_i as $k = w_i^{f(I_i)} \cdot t_j \cdot v_i^{x_j} \bmod n$.