SPATIAL FREQUENCY DOMAIN IMAGE PROCESSING FOR BIOMETRIC RECOGNITION

B.V.K. Vijaya Kumar, Marios Savvides, Krithika Venkataramani,and Chunyan Xie

Dept. of ECE, Carnegie Mellon University, Pittsburgh, PA 15213, USA

ABSTRACT

Biometric recognition refers to the process of matching an input biometric to stored biometric information. In particular, biometric verification refers to matching the live biometric input from an individual to the stored biometric template about that individual. Examples of biometrics include face images, fingerprint images, iris images, retinal scans, etc. Thus, image processing techniques prove useful in the biometric recognition. In this paper, we discuss spatial frequency domain image processing methods useful for biometric recognition.

1. INTRODUCTION

Verifying a user's identity is critical for e-commerce and access control. Most current authentication systems are password based making them susceptible to problems such as forgetting the password and passwords being stolen. One way to overcome these problems is to employ biometrics (e.g., fingerprints, face, iris pattern, etc.) for authentication. Another important application is to match an individual's biometrics against a database of biometrics. An example application of biometric identification is the matching of fingerprints found at a crime scene to a set of fingerprints in a database. Authentication problem has narrower scope, but the matching technologies are applicable to both verification and identification problems. We will refer to these problems loosely as biometric recognition.

Many biometric sensors output images and thus image processing plays an important role in biometric authentication. Image preprocessing is important since the quality of a biometric input can vary significantly. For example, the quality of a face image depends very much on illumination type, illumination level, detector array resolution, noise levels, etc. Preprocessing methods that take into account sensor characteristics must be employed prior to attempting any matching of the biometric images. However, this paper will focus on spatial frequency domain image processing technologies that can be used for matching biometric images. Processing in spatial frequency domain is nothing but 2-D filtering and we will refer to this approach as correlation filtering.

As we will see, correlation filter offer several advantages over model-based approaches. First is the built-in shift-invariance. If the input image is translated with respect to training images, that shift is usually easy to determine and correct when correlation filters are used. Second, correlation filters are based on integration operation and thus offer graceful degradation in that impairments to the test image cause only gradual degradation in the quality of the output. Third, correlation filters can be designed to exhibit attributes such as noise tolerance, high discrimination, etc. Finally, correlation filter designs offer closed form expressions.

The rest of this paper is organized as follows. Section 2 provides some background for correlation filters. Section 3 illustrates the application of correlation filters to face verification and Section 4 contains our conclusions.

2. CORRELATION FILTERS

Object recognition is performed by cross-correlating an input image with a synthesized template or filter and processing the resulting correlation output. Figure 1 shows schematically how the cross-correlation is obtained using Fast Fourier Transforms (FFTs). The correlation output is searched for peaks, and the relative heights of these peaks are used to determine whether the object of interest is present or not. The locations of the peaks indicate the position of the objects.

Correlation filters have been investigated mostly for automatic target recognition (ATR) [1] applications. The most basic correlation filter is the matched filter (MF), which performs well at detecting a reference image corrupted by additive white noise. But it performs poorly

when the reference image appears with distortions (e.g., rotations, scale changes). In biometric verification, the input biometric is bound to have some differences from the reference biometric because of normal variations. Then, one MF will be needed for each appearance of a biometric. Clearly this is computationally impractical. Hester and Casasent [2] addressed this challenge with the introduction of the synthetic discriminant function (SDF) filter. The SDF filter is a linear combination of MFs where the combination weights are chosen so that the correlation outputs corresponding to the training images would yield pre-specified values at the origin. For example, the correlation peak values corresponding to the training images of authentics can be set to 1, and the peak values due to the impostor training images can be set to zero. It is hoped that the resulting correlation filter would yield correlation peak values close to 1 for non-training images from the authentic class and correlation peak values close to zero for non-training images from the impostor class.

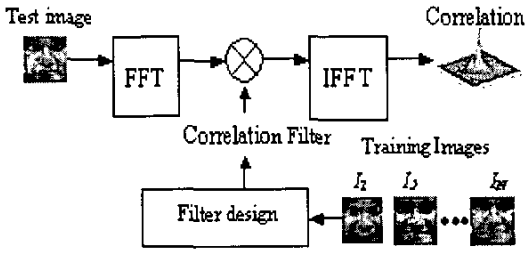

Figure 1 Block diagram of correlation process

Although the original SDF filter produces pre-specified correlation peak values, it also results in large sidelobes. Sometimes these sidelobes are larger than the pre-specified peak values leading to misclassifications. The peak sharpness can be improved by using minimum average correlation energy (MACE) filters [3] designed to produce correlation peaks that approximate impulse functions. We will show in Section 3 results for face verification using MACE filters.

Several advances have been made in the design of correlation filters. We give below short summaries of two important approaches to correlation filter design.

2.1 Optimal Tradeoff Filters (OTF)

In the OTF method [4], the training biometric images from a single user are used to construct a single spatial frequency filter that discriminates that user from others. This single filter captures the essence of the fingerprint images from an authentic user while tolerating the variability within that set. The OTF is designed using a multi-criteria optimization procedure to optimally tradeoff a distortion tolerance figure of merit against a discrimination figure of merit [5]. This multi-criteria optimization procedure provides us the ability to tune the filter behavior as needed to achieve a desired tradeoff between false acceptance rate (FAR) and false rejection rate (FRR).

2.2 Distance Classifier Correlation Filters (DCCF)

Another method to design the correlation filters is based on the concept of distance between a test image and the training images [6]. One can imagine each fingerprint image (with dxd pixels) to be a point in a d^2-dimensional space where each axis corresponds to a different pixel in the image. Then the training fingerprint images from a person represent a few points in this image space. Figure 2 shows the case of 3 classes. The DCCF method determines a transform **H** such that the training sets are maximally separated after the transform. When a test input **z** appears, it is subject to the same transform **H** and its distances to all three classes in the transformed domain are estimated and the input is assigned to the class with the smallest distance. These distances can be obtained using correlation [6].

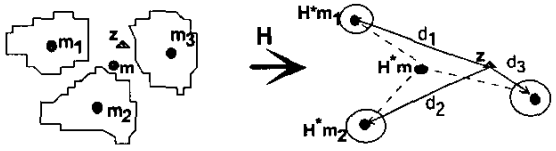

Figure 2 Transformation of 3 clusters in DCCF

Once the correlation filter $H(u,v)$ is determined, an input biometric image $f(x,y)$ is tested for its authenticity by forming the correlation output $c(x,y)$ as follows.

$$c(x,y) = \mathrm{FT2}^{-1}\left\{\mathrm{FT2}\left[\, f(x,y)\right] \bullet H^*(u,v)\right\}$$

where FT2 refers to the 2-D Fourier transform (efficiently implemented using FFT) and $\mathrm{FT2}^{-1}$ refers to the inverse 2-D FT operation. The resulting 2-D output $c(x,y)$ is next processed to determine various soft metrics such as correlation peak value, peak-to-sidelobe ratio, correlation plane energy, etc. These correlation performance metrics [5] can be used to provide a more reliable authentication decision.

Correlation-based verification has several advantages over other biometric verification methods. In feature

based methods, the designer needs to make somewhat arbitrary decisions about which features to use. In correlation based methods, no information is lost as all image pixels are used. Also, correlation methods are more graceful in their degradation due to the underlying integration operation. Finally, neural network based methods cannot handle fingerprint images directly because of the number of neurons is as large as the number of image pixels. In contrast, correlation methods exhibit the needed speed because of the underlying FFT efficiency. Also, the correlation filters can be recursively updated as new images are acquired instead of having to re-compute these filters from scratch. Another major advantage of using the correlation filter approach is the resulting shift-invariance. If the test biometric image is shifted from its nominal center, correlation peak moves by the same amount and thus correlation metrics do not change. However, input shift can be a big problem for feature-based methods since they require centering before computing the features.

3. FACE VERIFICATION

In this section, we briefly illustrate the application of correlation filters for face verification. More details can be found elsewhere [7].

3.1 Face Database

We use a facial expression database collected at the Advanced Multimedia Processing (AMP) Lab at the Electrical and Computer Engineering Department of CMU [8]. The database consists of 13 subjects, whose facial images were captured with varying expressions. Each subject in the database has 75 images of varying facial expressions. The faces were captured in a video sequence where a face tracker [9] tracked the movement of the user's head and based upon an eye localization routine and extracted registered face images of size 64x64. Example images are shown in Fig. 4.

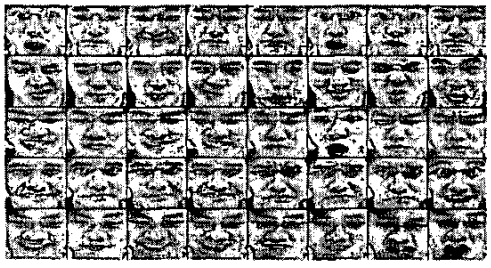

Figure 4. Sample images from the facial expression database.

3.2 Face Verification using MACE Filters

We have evaluated, using the above facial expression database, the performance of MACE filter for face verification. A single MACE filter was synthesized for each of the 13 persons using a variable number of training images from that person. In the test stage, for each filter, we performed cross correlations with all the face images from all the people (i.e., 13 x 75 = 975 images). For authentics, the correlation output should be sharply peaked and it should not exhibit such strong peaks for impostors. Peak to sidelobe ratio (PSR) defined below is used to measure the peak sharpness.

$$\mathrm{PSR} = \frac{peak - mean}{\sigma}$$

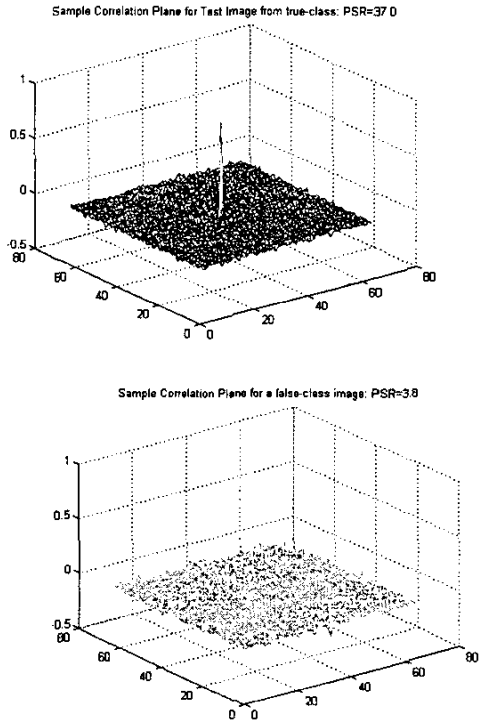

Figure 5. Correlation outputs when using a MACE filter designed for Person A. *(Top):* Input is from Person A. *(Bottom):* Input is not from Person A.

Figure 5 (top) shows a typical correlation output for an authentic face image. Note the sharp correlation peak resulting in a large PSR value of 37. The bottom correlation output in Fig. 5 shows a typical response to an impostor face image exhibiting low PSRs (<10).

We used only 3 training images for the synthesis of each person's MACE filter. These three images were at a uniform interval in order to capture some of the expression variations in the dataset (e.g., images # 1, 21 and 41). To evaluate the performance of each person's MACE filter, cross-correlations of all the images in the dataset were computed using a person's MACE filter resulting in 13*75=975 correlation outputs (corresponding to 75 true class images and the 900 false class images) and the corresponding PSRs were measured and recorded.

One very important observation from PSR sets for all 13 individuals is that all impostor face images (12*75=900) yielded PSR values consistently smaller than 10 for all 13 subjects. For each person, a PSR threshold was selected and if the test input resulted in a PSR larger than the threshold, it was declared as an authentic and if the PSR is lower than the threshold, the input was declared as an impostor. FAR refers to the percentage of impostors with PSRs above the threshold and FRR refers to the percentage of authentics with PSRs below the threshold. By changing the threshold, we can trade off FAR for FRR. Equal error rate (EER) refers to the value where FAR=FRR=EER.

Table 1 Error percentages for 13 MACE filters synthesized using only 3 training images

Person	1	2	3	4	5	6	7	8	9	10	11	12	13
FAR, FRR=0	0	1.3	0	0	1	0	0	0	0	0	0	0	0
EER	0	0.9	0	0	1	0	0	0	0	0	0	0	0
FRR, FAR=0	0	0.2	0	0	2.6	0	0	0	0	0	0	0	0

Table 2 Error percentages for 13 MACE filters synthesized using the first 5 training images

Person	1	2	3	4	5	6	7	8	9	10	11	12	13
FAR, FRR=0	0	2.4	0	0	0	0	0	0	0	0	0	0	0
EER	0	1.3	0	0	0	0	0	0	0	0	0	0	0
FRR, FAR=0	0	2.6	0	0	0	0	0	0	0	0	0	0	0

Table 1 shows the error rates achieved using MACE filters designed from only 3 training images. Table 1 shows that the overall EER (13 filters each tested on 975 images) is only 0.15% from MACE filters designed from only 3 training images per person.

We also performed a similar experiment using the first 5 training images from each person in the dataset to design that person's filter. These 5 images exhibit a different range of variability and have been placed there out of sequence. Table 2 summarizes the results of using 5 training images per person. There is some improvement in that Person 5 is now 100% correctly classified. However, class 2 gives 1.3% EER for an overall EER of 0.1%.

Although we have shown that the verification accuracy of the MACE filters increases as more training images are used for filter synthesis, it is attractive that this method can work well with as few as 3 training images per class for this database.

4. CONCLUSIONS

In this paper, we have briefly reviewed how correlation filters can be employed successfully for biometric image recognition. Correlation filters are particularly attractive because of advantages such as shift-invariance, closed-form expressions, and distortion-tolerance.

This research is supported in part by Sony Corporation.

5. REFERENCES

[1] B.V.K. Vijaya Kumar, "Tutorial survey of composite filter designs for optical correlators," *Appl. Opt.* 31, pp. 4773-4801 1992.

[2] C. F. Hester and D. Casasent, "Multivariant technique for multiclass pattern recognition," *Appl. Opt.* 19, pp.1758-1761 1980.

[3] A. Mahalanobis, B.V.K. Vijaya Kumar, and D. Casasent, "Minimum average correlation energy filters," *Appl. Opt.* 26, pp. 3633-3630, 1987.

[4] Ph. Réfrégier, "Optimal trade-off filters for noise robustness, sharpness of the correlation peak, and Horner efficiency," *Opt. Lett.* 16, pp. 829-831, 1991

[5] B.V.K. Vijaya Kumar and L. Hassebrook, "Performance Measures for Correlation Filters," *Applied Optics*, 29, pp. 2997-3006 1990.

[6] A. Mahalanobis, B.V.K. Vijaya Kumar and S. R. F. Sims, "Distance classifier correlation filters for multi-class target recognition," *Applied Optics*, 35, pp. 3127-3133, 1996.

[7] M. Savvides, B.V.K. Vijaya Kumar and P. Khosla, "Face verification using correlation filters," Proc. Of Third IEEE Automatic Identification Advanced Technologies, Tarytown, NY, pp. 56-61, March 2002

[8] <http://amp.ece.cmu.edu> - Advanced Multimedia processing Lab web page at Electrical and Computer Engineering Department at CMU.

[9] F. J. Huang and T. Chen, "Tracking of Multiple Faces for Human-Computer Interfaces and Virtual Environments", *IEEE Intl. Conf. on Multimedia and Expo.*, New York (2000).