NON-INTRUSIVE FACE VERIFICATION BY A VIRTUAL MIRROR INTERFACE USING FRACTAL CODES *

Ben A.M. Schouten, Johan W.H. Tangelder

Centre for Mathematics and Computer Science (CWI), Amsterdam, the Netherlands

{B.A.M.Schouten, J.W.H.Tangelder}@cwi.nl

ABSTRACT

Key factors in the public acceptance of biometric systems are non-intrusiveness, ease of use, and trust. In this paper we propose a biometric identity verification system consisting of a non-intrusive virtual mirror interface, and a face verifier using fractal coding to store the biometric template on a smart-card. The virtual mirror interface assists the user to obtain a frontal face image. The limited memory requirements of the fractal template and processing requirements of fractal decoding enable the implementation of the verification procedure on a smart-card. This set-up facilitates non-intrusive and easy to use biometric verification, and provides trust by adding a visualization to the biometric yes/no decision. Since the system does not require user assistance, it enables secure access over the Internet.

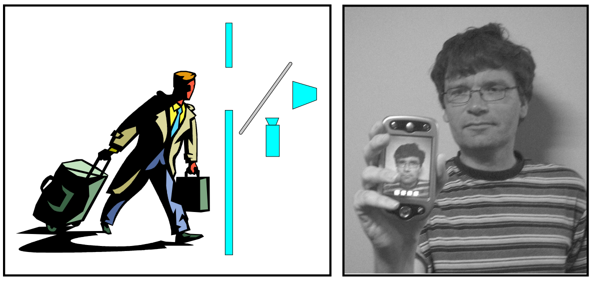

Figure 1: Supporting biometrics over the Internet with a virtual mirror interface: (a) from a public access point, and (b) from a mobile phone. The webcam and video display share the same optical axis through a half-silvered mirror.

1. INTRODUCTION

User convenience, non-intrusiveness, and trust are key factors for the public acceptance of biometric systems [14]. Therefore, authentication should be as easy as possible for the user, and the user should be able to monitor the authentication process. In this paper we present a smart mirror interface meeting these requirements. The system can be applied to provide secure access over the Internet from home, from mobile phones, or from public access points to personal data of the user, see figure 1. Moreover, the limited memory and processing requirements, facilitate the application of the system in advanced mobile phones.

The virtual mirror interface, which consists of a display visible through a half-silvered mirror, supports all user interaction in a natural way. The half-silvered mirror mirrors the user's image both back to the user, and to a webcam. To enroll the user has only to look into the mirror, enabling the detection of a frontal face image by the webcam. Fractal encoding is applied to compute a compact biometric template of the face image. This biometric template of the user can for instance be stored on a smart-card. To verify his/her identity the user presents the smart-card and looks again in the mirror and only has to align his face with a mask (with the same pose as the enrollment image) shown on the display behind the mirror, see figure 2. Again, a frontal face image is detected by the webcam. Next, the face verifier applies fractal decoding to morph on the display the new detected face to the enrolled face, see figure 3.

An advantage of using fractal coding of the enrolled face image is the small size of the template which fits on a smart-card. Moreover, morphing the actual presented image to the previous enrolled image of the user, enhances trust in the biometric verification process.

In the next section we describe the virtual mirror interface and a user scenario. In section 3 we discuss fractal coding and in section 4 we present experimental results on using fractal codes for face recognition. We conclude and indicate directions for further research in section 5.

2. INTERFACE AND USER SCENARIO

Darrell et al. [3] demonstrate the application of a virtual mirror interface in an interactive entertainment system displaying

*Part of this research has been funded by the Dutch BSIK/BRICKS project.

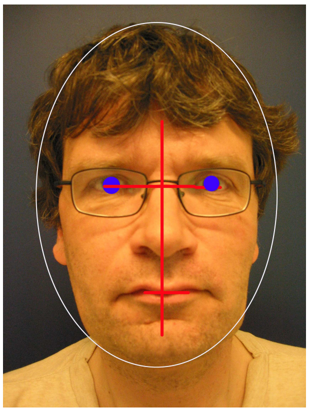

Figure 2: The user is invited to present his face to the system, guided by a mask denoting a frontal pose.

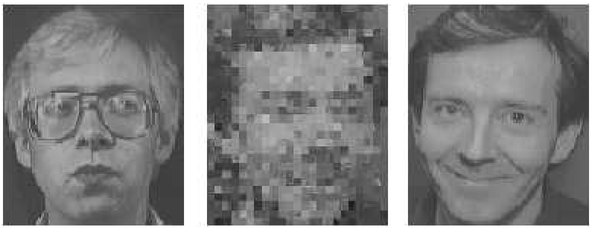

Figure 3: The face image of an impostor is morphed into the face of the authorized user of an application, showing three intermediate steps.

a user's face distorted by various graphical effects. We propose to use the virtual mirror interface to provide secure access over the Internet and guide the user in the authentication process. Figure 1 illustrates our set-up. The virtual mirror is created by placing a camera sharing the same optical axis as the video display, using a half-silvered mirror to merge the two optical paths. The camera views the user through a right-angle half-silvered mirror, so that the user can view a monitor while also looking straight into (but not seeing the camera).

At enrollment the user is invited to present his face in front of the mirror. A face extractor detects and scales the face of the user. To obtain the face in a frontal pose, the user has to align his face with a mask as illustrated by figure 2. On the display the mask is superimposed on the user's face. If the face and the mask align, a biometric template is extracted from the face, e.g. a fractal code of the presented face as explained in the next section. The template can be stored on a smart-card and in that case the system prints a smart-card containing the template.

For verification the client or the impostor presents her/his face and (stolen) smart-card to the smart mirror of the same or another intelligent kiosk or device. To visualize the verification process a morph from the presented face to the true face is shown as illustrated by figure 3.

3. FACE RECOGNITION USING FRACTAL CODES

Several face recognition techniques, such as principal components analysis, active appearance models, or elastic bunch graph matching, can be applied for biometric verification. Unfortunately, due to memory limitations these methods are sometimes difficult to implement on a smart-card. Therefore, to the problem of face recognition we would like to apply fractal coding, which is a relatively new technique which emerged from fractal geometry [7]. It is recognized that the search for similarities is best approached by a fractal mechanism and can be used to create fractal features, invariant under scaling, small rotations and translations [2, 4, 5, 6, 12]. An advantage of using fractal coding is the small size of the fractal code, which fits on a smart-card and the possibility of on-card processing.

Fractal coding [2, 4] is based on the self-similarity in a picture, which means that (small) regions of a picture can be transformed versions of some other (larger) regions of the same picture. *Partitioned iterated function systems* (PIFSs) encode this self-similarity by a limited set of affine transformations on the support and gray values of the image. The number of functions in the system is large, typically hundreds. In this paper we examine the properties of these fractal functions for the use of face recognition.

At encoding, an image f is encoded by finding a transformation W and an image $\hat{f} \approx f$ for which

$$W(\hat{f}) = \hat{f}. \tag{1}$$

In order to do so, a given image is partitioned into non-overlapping range blocks. The fractal encoder searches for parts called domain-blocks (which can be larger and overlapping) in the same image that looks similar under some fixed number of affine transformations. Such an affine transformation can be written as:

$$w_i(\vec{x}) = A_i\vec{x}+\vec{o}, \qquad A_i \equiv \begin{pmatrix} a_i & b_i & 0 \\ c_i & d_i & 0 \\ 0 & 0 & u_i \end{pmatrix}, \tag{2a}$$

$$\vec{x} \equiv \begin{pmatrix} x \\ y \\ f(x,y) \end{pmatrix}, \quad \vec{o} \equiv \begin{pmatrix} s_i \\ t_i \\ o_i \end{pmatrix}, \|u_i\| \leq 1. \tag{2b}$$

Index i indicates the range-blocks within the image, $f(x,y)$ denotes the gray-value at position (x,y). u_i is a contrast scaling on the gray-values and o_i is a luminance offset on the same values. The parameters $a_i, b_i, c_i, d_i, s_i, t_i$ constitute a geometric transform on the support of the image. The parameters u_i and o_i are used to match the gray-values of the domain with the gray-values of the range-block, within the limits of an imposed accuracy ε. Usually, a domain-block has twice the size of a range-block. The contractive nature of the transformations w_i makes the fractal encoder work. In the encoding all parameters describing the transformation $W = \bigcup_{i=1}^{N} w_i$ (where N is the total number of range blocks in the image) are stored.

According to the Contractive Mapping Fixed-Point Theorem [4], the fixed point $\hat{f}$ of W can be restored by iterating W in the decoding phase starting with an arbitrary given image f_x; with every iteration new detail is created.

$$\hat{f} \equiv \lim_{n\to\infty} W^{\circ n}(f_x);\; W^{\circ n}(f_x) = \underbrace{W \circ \cdots \circ W(f_x)}_{n\ times} \qquad (3)$$

Fractal theory has found many applications in image processing. Particularly, PIFSs have received a great deal of attention in image compression [2, 4, 5] and fractals have been applied to object and/or face recognition [6, 12]. Two basic approaches are found in the literature. In the first approach [1, 8, 9, 11, 13], features extracted from the fractal code of the input object are compared against features extracted from the fractal codes of the objects stored in the database. The second approach [6, 12], is based on comparing distances, using the Euclidean distance measure, between one object and another object modified by one iteration using a fractal code.

Both methods, may be applied for biometric identification. However, only the latter method allows to morph the face presented to the virtual mirror to the genuine face. Therefore, in the remainder of the paper we focus on a method modifying the input object using the fractal code derived from the face image of the user g, whose identity is to be verified.

3.1. Fractal Feature Extraction for Virtual Mirror Interfaces

At enrollment a picture f_g is taken from the client g. A fractal code W_g is generated from f_g for which

$$W(f_g) \approx f_g. \qquad (4)$$

In the first state of the authentication process, the user i, not necessarily being the genuine user, claims the identity g and presents a (stolen) smart-card to the reader. The system reads the fractal codes W_g from the smart-card and generates the previous enrolled image of the client, or in fact the fractal estimation of the enrolled image, $\hat{f}_g$.

However, this image is not presented to the user, as this would immediately unmask a possible impostor before the authentication process is completed. Instead a mask as shown in figure 2, is used to guide the user to the authentication process and to guarantee that a picture f_i can be taken in the same pose as the enrolled image, improving the robustness of the application.

During the authentication process we calculate:

$$d(W_g(f_i), \hat{f}_g) \qquad (5)$$

where

$$d(f,g) = \sqrt{\sum_{k=0}^{I_h} \sum_{l=0}^{I_w} (f^{k,l} - g^{k,l})^2}, \qquad (6)$$

and $f^{k,l}$ denotes the pixel value of image f at position (k,l). I_h and I_w are the height and width of the image. According to the threshold set in the system, the identity of the user is verified.

Now, in the next step, as a result of the authentication process, an image $W_g^{\circ 10}(f_i)$, which resembles the enrolled image sufficiently, is generated and presented to the user and/or supervisor of the system, showing the similarity between the enrolled image and the presented image and allowing the user to see for him self if the authentication process was successful.

All intermediate steps are shown resulting in a morph from the enrolled image to the presented image at the time of the authentication process, as illustrated by figure 3. In general ten iterations is enough to render a clear approximation of the previous enrolled image.

4. EXPERIMENTAL RESULTS

The aim of this section is to investigate the feasibility of the fractal coding for biometric authentication in a virtual mirror interface. For our experiments we used the fractal coding software, which is described in the book by Fisher [4]. The Olivetti Research Labs (ORL) face database [10] was used in our experiments. Although, the ORL database is considered as an easy database, it was used because the faces are centred on the image, so face detection was not required, and it contained faces of varying pose and expressions. The ORL face database contains ten different images of each of the 40 distinct subjects. To investigate the robustness of the fractal distance measure with regard to pose, we created two databases containing images with similar pose. For the first database we selected per subject 2 images with similar pose, and for the second database we selected per subject 3 images.

For all images in the complete database, we used the other 9 images of the subject in the database to evaluate client claims and the other 390 images not of the subject to evaluate impostor claims. For the complete database this evaluation procedure resulted in 3600 client claims and 156.000 impostor claim.

For all images in the two pose similar databases, we used the other image (two images) of the subject to evaluate client claims and the other 78 images (117 images) to evaluate impostor claims. For the first pose similar database this evaluation procedure resulted in 80 client claims and 6.240 impostor claims, and for the second pose similar database in 240 client claims and 14.040 impostor claims.

We plotted for the three databases the receiver operating characteristic (ROC) curves in figure 4. The ROC curves show that using pose similar images, improves performance: from an EER of 12.3 % for the ORL database, to an EER of 6.9 % for the subset containing three images per subject, and an EER of 6.0 % for the subset containing two images per subject.

However within our experiments we did not use the automatic pose correction. In future research we will test the results, generating a new database using the pose guidance system and expect the results to further improve. Also, instead of using the default parameter settings of the fractal coding software we would like to optimize its parameter setting to improve the results.

5. CONCLUSIONS AND FURTHER RESEARCH

In this paper a virtual mirror interface supporting secure access over the Internet, is proposed. The virtual mirror interface assists the user to obtain a frontal face image. Because the system does not require user assistance, it facilitates secure access over the Internet. Since fractal coding provides compact codes, we apply face recognition based on fractal coding to implement the proposed scenario using smart-cards. Fractal methods could be used for on card processing which improves both privacy and security within the biometric authentication process. To evaluate the recognition performance for frontal poses we used the ORL database [10], and we selected two subsets from the ORL database, consisting of face images in a frontal pose. Our results show that the recognition performance of fractal coding improves using automatic pose reconstruction.

Fractal codes achieve very compact coding, compressing each image from the ORL face database from 10.1 K to a range of 1-1.8 K fractal code. Hence, fractal compression of features obtained by filtering images, for instance using Gabor filters, is a promising research direction to obtain both compact biometric templates and high recognition rates.

Also, to improve recognition rates, fusion of speaker and face modalities using the relatively low quality images and low quality sound from a webcam, is an important research issue. For liveness detection video can be applied to detect the presence or absence of spontaneous facial expressions changing the face. For high security applications, the system can ask the user to show facial expressions, e.g. blinking, which are difficult to spoof.

6. REFERENCES

[1] Baldoni, M., Baroglio, C., Cavagnino, D., Egidi, L.: *Learning to Classify Images by Means of Iterated Function Systems.* In: Fractals and Beyond: Complexities in the Sciences, 173-182, World Scientific, 1998.

[2] Barnsley, M.F., Hurd, L.P.: *Fractal Image Compression.* AK Peters Ltd., 1993

[3] Darrell, T., Gordon, G., Woodfill J., Harville, M.: *A Virtual Mirror Interface using Real-time Robust Face Tracking.* In: Proc. of the Third International Conference on Face and Gesture Recognition, April 14-16, 1998, Nara, Japan.

[4] Fisher, Y. (ed.): *Fractal Image Compression, Theory and Application.* Springer Verlag, 1995.

[5] Jacquin, A.E.: *Fractal image coding: a review.* in: Proc. of the IEEE, 81 (10), 1451-1465, 1993.

[6] Kouzani, A.Z., He, F., Sammut, K.: *Towards Invariant Face Recognition.* In: Information Sciences 123, 75-101, 2000.

[7] Mandelbrot, B.B.: *The Fractal Geometry of Nature.* Freeman and Company, New York, 1983.

[8] Marie-Julie, J.M., and Essafi, H.: *Image Database Indexing and Retrieval Using the Fractal Transform.* In: Proc. of Multimedia Applications, Services and Techniques, 169-182, Springer Verlag 1997.

[9] Neil, G., Curtis, K.M.: *Scale and Rotationally Invariant Object Recognition using Fractal Transformations.* In: Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing, 3458-3461, 1996.

[10] Samaria, F.S., Harter, A.C.: *Parameterisation of a stochastic model for human face identification.* In: 2nd IEEE Workshop on Applications of Computer Vision, 1994

[11] Schouten, B.A.M., de Zeeuw, P.M.: *Fractal Transforms and Feature Invariance.* In: Proc. of the International Conference on Pattern Recognition (ICPR'00), 2000.

[12] Tan, T., Hong Y.: *The Fractal Neighbor Distance Measure.* In: Pattern Recognition 35, 1371-1387, 2002.

[13] Vissac, M., Dugelay, J., and Rose, K.: *A Fractals Inspired Approach to Content-Based Image Indexing.* In: Proc. IEEE International Conference on Image Processing, on CDROM, 1999.

[14] *Privacy best practices.* In: Biometric Technology Today, Vol. 11, Issue 11, 8-9, 2003.

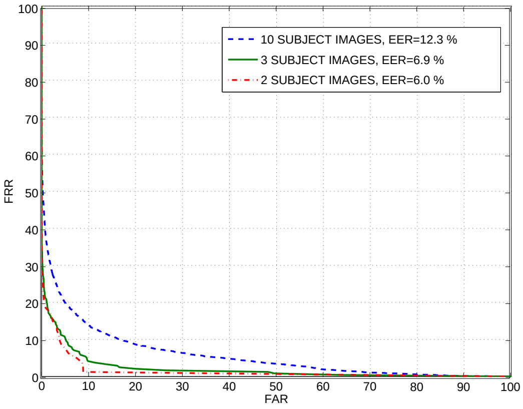

Figure 4: Plot comparing ROC curves using the full ORL database with 10 images per subject, a subset of 3 frontal pose images per subject, and a subset of 2 frontal pose images per subject.