A Face-Unlock Screen Saver by Using Face Verification Based on Identity-Specific Subspaces

Shiguang Shan[1], Wen Gao[1,2], Xilin Chen[2,3], Bo Cao[1], Wenbin Zeng[4]

[1] ICT-YCNC FRTJDL, Institute of Computing Technology, CAS, Beijing 100080,China
{sgshan, wgao, bcao}@ict.ac.cn
[2] Department of Computer Science, Harbin Institute of Technology, Harbin, 150001, China
{wgao,xlchen}@vilab.hit.edu.cn
[3] Interactive Systems Labs, School of Computer Science, CMU, Pittsburgh, PA15221, USA
xlchen@cs.cmu.edu
[4]YCNC Co. Chengdu, SiChuan Province, 610016, China
webzeng@163.net

Abstract: A face-unlock screen saver prototype system is presented by using face verification technique based on identity-specific subspace. Instead of using password to unlock the screen saver, the proposed system can only accept the current legal user by his face as easily as just looking at the USB camera for a second, meanwhile refusing any other faces. The core techniques of the system are the proposed novel face verification algorithm based on identity-specific subspace and the maximum likelihood (ML) rule. Choosing these techniques is based on the fact that, for a task as screen saver, sufficient training facial images can be easily acquired. To achieve real-time verification, robust real-time facial feature localization and face normalization is presented, based on which an automatic samples collection tool is implemented. Practical experiments have shown the effectiveness of our proposed approaches.

1. Introduction

Traditional screen savers are based on passwords to prevent illegal users from accessing the personal computer locked by the current user. It is inconvenient for the legal user to unlock the screen saver, and there exists the risks that illegal users crack or steal the password to access the computer illegally. Faces are exclusive character for specific subjects, which provide a convenient and reliable way to prevent illegal access. In this paper, we present such a prototype by designing a face-unlock screen saver based on face verification techniques. The core technique in the system is face recognition. Face recognition is an important task in Human Computer Interface (HCI) and has significant applications for building more intelligent and intuitive HCI. Furthermore, tremendous potential applications in commerce and law enforcement have attracted more and more attention in the area.

While automatic face identification remains a great challenge, it does have a long history going as far back as the work in the 1960s [1]. It is believed that the most promising techniques should be the perfect combination of all kinds of information including shape, local appearance features and holistic appearance feature etc. In recent years, Eigenface [2], Elastic Bunch Graph Matching (EBGM) technologies [3], flexible models [4], and Fisherface [5]/LDA [6] based approaches have attracted much attention. FERET evaluation provided extensive comparisons of these algorithms [7]. More recently, SVM have been successfully applied to face recognition [8]. For detailed survey of FRT, [1] should be referred to.

Among the current state-of-the-art techniques, "eigenface" methods originated by Turk and Pentland's [2] are the most distinguished. In this paper, we extend Eigenface in an essentially different way by representing each face by using one face subspace private to the corresponding subject. Based on the identity-specific subspaces and maximum likelihood rules, a face verification technique is derived and applied to a practical face-unlock screen saver system with corresponding facial feature localization and face normalization techniques.

2. Identity-Specific Subspaces

"Eigenface" method [2] is PCA or KLT essentially, belonging to a kind of linear projection transform. The face subspace captures the common information of human faces, while the "noise" subspace contains three kinds of information: between-person variance, interpersonal variance and stochastic noise, among which between-person difference is essential for distinguishing different individuals. Unfortunately, the between-person difference crucial for recognition is blended inseparably with the within-person difference and noise information in the "noise" subspace. So we argue that "eigenface" technique might be more appropriate for face detection rather than distinguishing different faces. Based on the notion, we proposed the concept of identity-specific subspace.

Facial images, with the same specific identity, have similar appearance, for which they can be regarded as a stochastic observed signal. So one private signal subspace can be used to model them, by which the invariant facial feature belonging to the same person is mostly remained as the expected signal, while most of the within-class variance useless for classification is thrown away in the "noise" subspace.

For any specific person with an identity *K* denoted by Ω_k as a class, it can be analyzed by using eigenvalue decomposition as: $R_k = \sum_{i=1}^{d_k} l_i^{(k)} v_i^{(k)} v_i^{(k)H} + s_k^2 \sum_{i=0}^{M_k} v_i^{(k)} v_i^{(k)H}$. Then the signal subspace and corresponding noise subspace for the specific identity are $S_{face}^{(k)} = Span\{U_{face}^{(k)}\} = span\{v_1^{(k)}, v_2^{(k)}, ..., v_{d_k}^{(k)}\}$, $S_{noise}^{(k)} = Span\{U_{noise}^{(k)}\} = span\{v_{d_k+1}^{(k)}, v_{d_k+2}^{(k)}, ..., v_{M_k}^{(k)}\}$. They are *K*-identity-specific subspace and *K*-identity specific noise subspace respectively. Then any face image Γ can be projected to the *K*-identity-specific subspace $S_{face}^{(k)}$ by a matrix transform $W^{(k)} = U_{face}^{(k)\,T} \Phi^{(k)}$, in which $\Phi^{(k)} = \Gamma - \Psi^{(k)}$ is the difference image and $\Psi^{(k)}$ is the mean image obtained from the training images of the *K*-identity. And the input image can be reconstructed by $\Phi_r^{(k)} = U_{face}^{(k)} W^{(k)}$.

Then the distance between any input face image and the *K*-identity-specific subspace can be calculated as follows: $e^{(k)} = \left\| \Phi^{(k)} - \Phi_r^{(k)} \right\|$. We denote the distance by DFISS to measure the similarity between the input image and the *K*-identity.

3. Face Verification Based on ISS and Maximum Likelihood Rules

As a two-class problem, face verification can be resolved by using the Bayesian method based on the maximum a posteriori (MAP) rule: $x \in \Omega_k$ if $P(\Omega_k \mid x) > P(\overline{\Omega}_k \mid x)$, where $P(\Omega_k \mid x) = \frac{P(x \mid \Omega_k) * P(\Omega_k)}{P(x \mid \Omega_k) * P(\Omega_k) + P(x \mid \overline{\Omega}_k) * P(\overline{\Omega}_k)}$ and $P(\overline{\Omega}_k \mid x) = \frac{P(x \mid \overline{\Omega}_k) * P(\overline{\Omega}_k)}{P(x \mid \Omega_k) * P(\Omega_k) + P(x \mid \overline{\Omega}_k) * P(\overline{\Omega}_k)}$, with $\overline{\Omega}_k$ the class containing the non-k-identity faces, which can be learned by using similar analysis as Ω_k.

For general face verification problem, equal probability $P(\Omega_k) = P(\overline{\Omega}_k) = 1/2$ is satisfied, so we only need to estimate class conditional probability density $P(x \mid \Omega_k)$, by which the rules converted to the maximum likelihood rule. While it is not an easy work to estimate $P(x \mid \Omega_k)$ since face images are hi-dimensional data with much variance due to the 2D appearance deformation caused by 3D facial pose and lighting changes. Fortunately, ISS we proposed provides a simple and convenient method to estimate the density. Since a Gaussian model can be used to approximately model a specific identity's distribution, the class conditional probability density corresponding to the *K*-identity is: $P(x \mid \Omega_k) = \frac{\exp[-\frac{1}{2}(x - \overline{x_k})^T \Sigma_k^{-1} (x - \overline{x_k})]}{(2p)^{N_k/2} \left|\Sigma_k\right|^{1/2}}$. And $P(x \mid \overline{\Omega}_k)$ can be estimated similarly. Then, base on the ISS we proposed in section 2, we adopt the algorithm in [3] to estimate $P(x \mid \Omega_k)$ as:

$$\hat{P}(x \mid \Omega_k) = \left[\frac{\exp[-\frac{1}{2} \sum_{i=1}^{M} \frac{(y_i^{(k)})^2}{l_i^{(k)}}]}{(2p)^{M/2} \prod_{i=1}^{M} l_i^{(k)}} \right] \cdot \left[\frac{\exp(-\frac{e_{(k)}^2(x)}{2r^{(k)}})}{(2pr^{(k)})^{(N_k - M)/2}} \right].$$

Where: $l_i^{(k)}, i = 1,2,\ldots,N_k$ are the eigenvalues calculated from training data of *k*-identity and ordered non-increasingly. M is the truncated dimension of eigenvalues. And $[y_1^{(k)}, y_2^{(k)}, \cdots, y_M^{(k)}]^T = Y^{(k)} = U_{face}^{(k)\,T} x$ is the transformed vector when *x* is projected to the *k*-ISS. $e_{(k)}^2(x)$ is the DFISS. $r^{(k)} = \frac{1}{N_k - M} \sum_{i=M+1}^{N_k} l_i$ is the optimal weight coefficient. Refer to [3] for details.

Using the similar algorithm $\hat{P}(x \mid \overline{\Omega}_k)$ can be estimated. So we get the following for k-identity face verification rule: $x \in \Omega_k$ if $\hat{P}(x \mid \Omega_k) > \hat{P}(x \mid \overline{\Omega}_k)$.

4. Face-Unlock Screen Saver Based on Face Verification

4.1 Localization of the Facial Features, Face Normalizations and Masking

In our system, based on the results of our face detection system [9] and the observations that the two irises are the most salient features, the two irises are localized first. Then other organs are localized by integral projection. Please refer to [10] for details.

To eliminate the effect of the hair and the background, normalization is necessary in order to achieve robust identification. In our system all faces are normalized as those in Fig.3, by face warping, affine transformation, luminance and scale normalization, and masking. After normalization, the eyes are positioned at fixed locations to achieve a certain extent of shape-free appearance. The normalized faces are 32x32 pixels in size. Some normalized faces are shown in Fig.2. In our system, no less than 25 samples for a specific user are needed.

Fig.2 Normalized Facial Images

4.2 Automatic Training Samples Collecting Tool

To learn a new face automatically and conveniently, an automatic training sample collecting tool is designed, which can automatically capture enough samples (normalized facial images) needed to train the ISS for the specific identity by just requiring the user to sit before the USB camera and move his head for about tens of seconds. “Bad” samples, derived from occasional errors of features localization, are automatically deleted based on the quality of the sample as a normalized face. And the administrator is allowed to further check all the samples by deleting visually bad samples.

4.3 ISS Training

After collecting enough samples of the specific user, ISS of the specific face is trained by the eigen-analysis algorithm. In our system, $P(x\,|\,\overline{\Omega}_k)$ is trained by an independent face set containing 1000 faces. Then the two class conditional probability density functions are estimated, where the dimension of the principal subspace is set to 25 as an experiential choice. And eigenfaces specific for the first author of the paper (so called eigen-SGSHAN-faces) are illustrated in Fig.3, from which the main characteristics of the first author’s face can be seen.

Fig.3 Top Eigen-SGSHAN-faces

4.4 System Setup and Experiments

The overall architecture of the face-unlock screen saver system is illustrated in Fig.4. Please note that, to reduce the occurrence of the occasional false acceptance, a strategy is designed to accept one user only when he passes the verification more than one time in a given time slot.

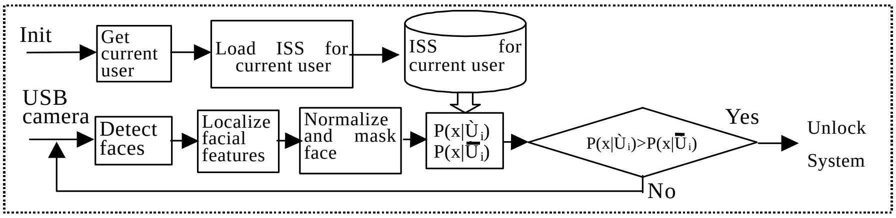

Fig 4. Architecture of the Face-Unlock Screen Saver

Using ordinary USB camera, under 320x240 image size, our system can verify a face (including the whole process from face detection, feature localization, normalization and verification finally) in less than 200 milliseconds, that it, about frames can be verified in one second. Practical experiments are conducted on legal user's unlocking and imposter's attempts to login. The legal user can always unlock the saver successfully during the experiments, with average time needed to unlock the saver less than two seconds under relatively uniform illumination and less than four seconds under poor lighting conditions. The system refused all the imposters among all the 50 attempts.

5. Conclusion and Future Works

Unlocking screen saver by the user's face is an interesting application of face recognition technology. Based on the fact that, for such kind of tasks, sufficient facial images can be easily obtained, the proposed algorithm can model the distribution of every person based on the identity-specific subspaces. And the verification is completed by the maximum likelihood rule based on the estimation of the distribution of the corresponding ISS private for the person. Related techniques to localize facial features and normalize facial images are proposed, which could work well in real-time. Practical experiments have shown effectiveness and excellent performance of our screen saver system.

Though we have failed to unlock the system by photos of the legal user, no techniques are adopted now to prevent this kind of cheats. Future work includes the discrimination between a live face and a photo of the legal user.

Acknowledgment

The research is sponsored partly by National Science Foundation of China (No.69789301), National Hi-Tech Program of China (No.863-306-ZD03-01-2), 100 Talents Foundation of Chinese Academy of Sciences, and all the researches are done under the sponsor of the YCNC Co. Chengdu, Sichuan, China.

References

1. R. Chellappa, C. L. Wilson, and S. Sirohey, Human and Machine Recognition of Faces: A Survey, Proceedings of the IEEE, Vol.83, No.5, pp. 705-740,1995
2. M. Turk, and A. Pentland, Eigen-faces for Recognition, Journal of Cognitive Neuroscience, Vol. 3, No. 1, pp. 71-86, 1991
3. L Wiskott, J.M.Fellous, N.Kruger and C.V.D.Malsburg, “Face Recogniton by Elastic Bunch Graph Matching”, IEEE Trans. On PAMI, 19(7), pp775-779, 1997.7
4. Lanitis A. Taylor CJ. Cootes TF. Automatic interpretation and coding of face images using flexible models. IEEE Trans. on Pattern Analysis & Machine Intelligence, vol.19, no.7, July 1997, pp.743-756
5. P.N.Belhumeur, J.P.Hespanha and D.J.Kriegman. “Eigenfaces vs Fisherfaces: recognition using class specific linear projection”. IEEE trans. on PAMI, vol.20, No.7, 1997.7
6. W.Zhao and R.Chellappa, “Robust Image-Based 3D Face Recognition”, CAR-TR-932, N00014-95-1-0521, CS-TR-4091, Center for Auto Research, UMD, 2000.1
7. P.J.Phillips, H.Moon, etc. “The FERET Evaluation Methodology for Face-Recognition Algorithms”, IEEE Transactions on PAMI, Vol.22, No.10, pp1090-1104, 2000
8. G.Guo, S.Z.Li and K.Chan, “Face Recognition by Support Vector Machines”, Proc. of the 4th Int. Conf. on Auto. Face and Gesture Recog., pp.196-201, Grenoble, 2000.3
9. Baback Moghaddam, Tony Jebara, Alex Pentland, Bayesian Face Recognition, Pattern Recognition Vol.33, pp1771-1782, 2000
10. Wen Gao, Mingbao Liu. A hierarchical approach to human face detection in a complex background. Proceedings of the First International Conference on Multimodal Interface, pp.289-292, 1996
11. S.G. Shan, W.Gao, J.Yan etc. Individual 3d face synthesis based on orthogonal photos and speech-driven facial animation. Proceedings of the International Conference on Image (ICIP'2000), Vol. III, pp238-242, 2000