WWJMRD 2018; 4(1): 348-351
www.wwjmrd.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal
UGC Approved Journal
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Anandhi Giri
VELS University, Chennai, India

S. K. Srivatsa
Retd, Senior Professor, Anna University, Chennai, India

Overview of Face Recognition and Security Using Mobile Phones

Anandhi Giri, S. K. Srivatsa

Abstract
A major driver behind building 3G networks is to increase revenue through new data services, and to counteract the gradual decrease in voice revenue. To achieve this, new data services need to be increased through mobile phone handsets and wireless devices. Increasing capabilities of mobile phone handsets implies that new computing data applications can be implemented. Face recognition is attracting much attention in network multimedia information access. Areas such as network security, content indexing and retrieval, and video compression will benefit from face recognition technology because 'people' are the center of attention in lot of video. Network access control via face recognition not only makes stealing of passwords by hacking virtually impossible, but also increases user-friendliness in human-computer interaction. We are studying the existing face recognition algorithms, their strengths and weaknesses including recognition rate. Mobile devices are becoming more similar to personal computers, hence they are also becoming repositories for sensitive information. In this context a more powerful authentication mechanism than simple passwords becomes essential. The paper describes an overview of face recognition approach for mobile devices, discusses important issues related to the practical implementation of the authentication scheme.

Keywords: face recognition, 2G networks, 3G networks, mobile phone handsets, Deep network Face recognition, Illumination change, Insufficient training data.

1. Introduction

With recent developments of mobile phones, security of personal information on mobile phones is becoming more important. Hence fingerprint recognition phones have been already manufactured. However, they are more expensive and bigger than conventional mobile phones because they require an additional fingerprint sensor as well as a DSP (Digital Signal Processor) chip for fingerprint recognition. In addition, because the fingerprint sensor should be small due to the size limitation of mobile phone, it may lead to unreliable authentication performance. So, fingerprint recognition phones have not become widely popular yet. With rapid developments of mobile phone, many companies have adopted a built-in mega-pixel camera in mobile phone which gives the possibility of face and iris recognition on mobile phone without additional sensor. Biometrics is one of the most important branches of pattern recognition [1-3]. Face recognition is one of the most attractive biometric techniques. However, face recognition in real applications is still a challenging task [4]. The main reason is that the face is a non-rigid object, and it often has different appearance owing to various facial expression, different ages, different angles and different illumination intensity. In recent years, deep learning has become more prevalent in computer vision. Face recognition could be considered as a special classification task and deep network is pretty suitable for face recognition.

2. Face Detection

Face detection is a process that determines whether there are any faces in an image. Face detection is not an easy process, as there are external and internal factors that affect the detection. A minor change in appearance, like wearing sunglasses or growing a mustache can make the task of face detection even more challenging. Also different illumination changes the color of faces extensively. There are several algorithms available in the literature that can

Correspondence:
Anandhi Giri
VELS University, Chennai, India

help us to identify whether it is a face in an image. In a survey for Image Understanding, the Face Detection techniques are organized in two main categories: Feature-based approach [5]. Image-based approach [6] Feature-based approach requires prior information of the face. It makes an explicit use of facial features, which includes use edge information, skin color, motion and symmetry measures, feature analysis, deformable templates and point distribution. Image-based approach does direct classification without any face knowledge derivation and analysis. It incorporates facial features implicitly into the system through training. Image based techniques include neural networks, linear subspace method like Eigenfaces [7], fisherfaces [8]

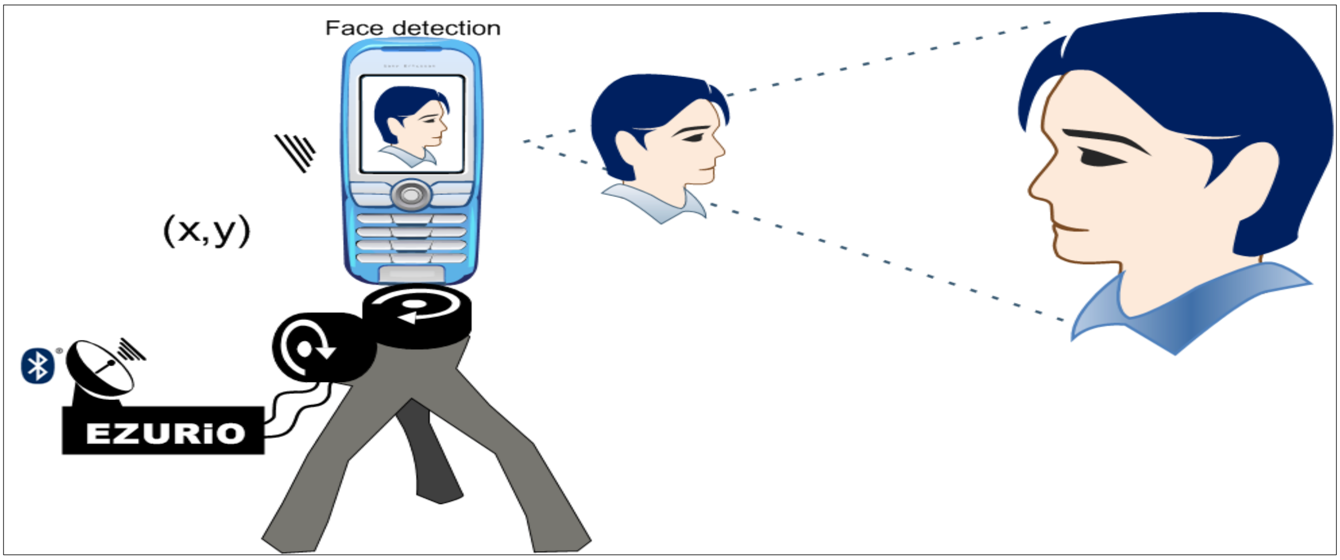

Fig.1: System for Face detection

Human skin is relatively easy to detect controlled environments, but detection in uncontrolled settings is still an open problem (5; 8). Many approaches to face detection are only applicable to static images assumed to contain a single face in a particular part of the image. Additional assumptions are placed on pose, lighting, and facial expression. When confronted with a scene containing unknown number of faces, at unknown locations, they are prone to false detection rates and computational inefficiency. Real-world images have many sources of corruption (noise, background activity and lighting variation) where objects of interest, such as people, may only appear at low resolution. The problem of reliably and efficiently detecting human faces is attracting considerable interest.

2.1 Motion approach

The problem of face detection in still images is more challenging and difficult when compared to the problem of face detection in image sequence, since motion information can lead to probable regions where a person could be located. On the other hand, the results can be mistaken with other regions in the image that move. For example in the case when the camera is mobile, we can come across moving background. The method of finding image is a feature-base approach. This finds features such as image edges, corners and other structures well localized in two dimensions. Firstly, the features are found in two or more consecutive images and after these features are matched between the frames. The algorithm eliminates unimportant parts and creates an area of interest on the motion vectors. Alternatively, the features in one frame can be used as seed points at which to use other methods (for example, skin color detection on motion parts). Motion is easy to Implement. But alone can be hard to identify where the face of the human is.

3. Authentication

Today's world security issues are the most important segment among all. Therefore, segmen of authentication plays a major role. When a person or a system checks the person's identity against another person then we are in process of authentication. That means one who is authenticated can confirm that he/she is the person compares to. There are two essential type o authentication:

Verification

This is a process of confirming identity of any person by comparing the input data with ones existing in database. This is 1:1 authentication method

Identification

In this case we are matching the input data with all samples in the database with a view to retrieving the data related for the person. This system represents the 1:N authentication model

3.1 Cutting Edge Mobile Authentication

Since mobile phones are becoming a computer in medium, security issues have arisen due to many applications which run on the phones [9]. Therefore, the focus will be on resolving the security issue with previously – proposed models which can be integrated to upgrade new approaches. With the introduction of 3G, mobile phones changed significantly. Increase of application and data has increased the user need to protect the data which exist in mobile devices. The current approach is to protect with PIN. Such an approach could be used both on Subscriber Identity Module, PDA and smart-phone devices; are password based. Both PIN and password have been established many years ago. Even though they have been applied by different coding and encryptions of digital PINs and password, they remain weak. The most frequent weakness of breaking the password or PIN by third party is based on assumption.

4. Development Environment

System consists of two different parts, the server part and the face recognition part as follows:

- *Mobile Platform* – System is embedded into Samsung Galaxy S model of mobile phone and supports Java technology and is integrated with Java.
- *Android Mobile Technology* – Java SDK and Android technology, with DROID emulator
- *Hosting Web Server* – A server is required to host the application. This application will transmit and receive data over the Internet. Tomcat Apache HTTP Server is used as the web server.
- *Database* – Small database is developed for testing and evaluation. Database consists of face images.
- *Face Recognition Method* – Face Recognition part is developed using Matlab. It is integrated with the server.

4.1 2D biometrics

Various types of 2D biometrical scanners on mobile devices target various parts of the body, from fingerprints and eyes (iris or retina) to an entire face. A few years ago, this type of technology sounded like something straight out of science fiction - for both manufacturers and mobile app developers - and was believed to guarantee top-notch security. Yet, as other technology sectors have been evolving too, without any ill intention they've paved the way to a hack for these sophisticated biometrical locks.
Today's photography provides high enough quality to capture all the details necessary for scanners to analyze a sample and match it with the one stored on the mobile device. So be it an iris or a finger, the pattern can be captured clearly: any face-capturing faults are all the more so out of the question. A pattern can then be printed out and, with the help of some easy-accessible materials (a transparent contact lens for an iris and glue/plaster for fingerprint printouts), turns into a biometrical 'lock-pick'.

4.2 3D biometrics

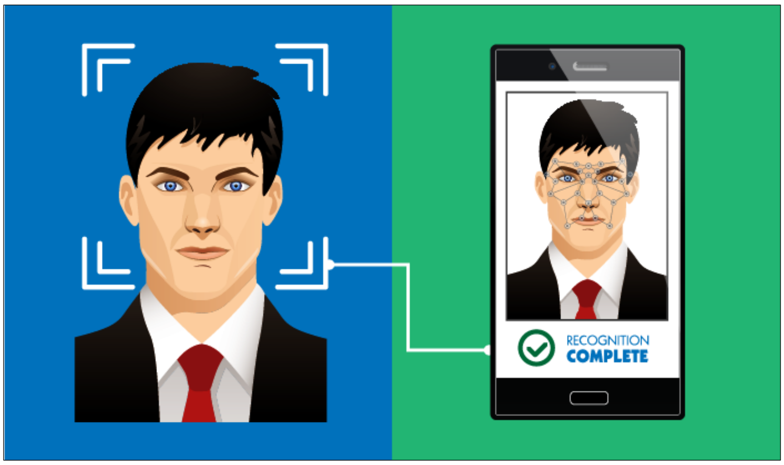

Fig.2: Basic 3d sample picture capture

Using an attachable camera with 3 lenses, Microsoft's Windows Hello creates a 3D projection of the user's face and can recognize them from about 0.5-4 feet distance. The camera is compact, but still *is* attachable, because it did not fit in the company's Surface laptop a few years ago. Needless to say, Microsoft did not see any point in trying to implement 3D recognition on their mobile phones (although their mobile app development team did try to create a 3D Capture scanning app). Perhaps now that Apple and Android device manufacturers are taking a step forward, Windows Phone will see more action as well. It is not that 3D biometrics is absolutely secure. A three-dimensional printout is technically possible too, and it has already helped Michigan police to create a fingerprint sample and unlock a murder victim's phone. Still, 3D printing is definitely not so easy to access, so as long as 2D printing remains more ubiquitous and advanced, 3D biometrics authentication will remain more secure

Conclusion

This system is aimed to increase mobile phone usage by providing a new source of data traffic that is carried by a data network. Because the system will be deployed in many locations the data traffic generated will be high and the system will then have the potential to generate revenue for an operator. Mobile phones are becoming the primary personal gateway to access information Face recognition on portable mobile phones may help to protect sensitive data in future.

References

1. K. He, X. Zhang, S. Ren, et al., Deep Residual Learning for Image Recognition, IEEE Conference on Computer Vision and Pattern Recognition. IEEE Computer Society, 2016, pp. 770-778

2. J. Liu, Y. Deng, T. Bai, Z. Wei, C. Huang, Targeting Ultimate Accuracy: Face Recognition via Deep Embedding, 2015

3. F. Schroff, D. Kalenichenko, J. Philbin, Facenet: a Unified Embedding for Face Recognition and Clustering, 2015, pp. 815-823.

4. O.M. Parkhi, A. Vedaldi, A. Zisserman, Deep face recognition, in: British Machine Vision Conference, 2015.

5. Y. Taigman, M. Yang, M. Ranzato, L. Wolf, Deepface: closing the gap to human level performance in face verification, in: Conference on Computer Vision and Pattern Recognition, 2014, pp. 1701-1708.
6. Y. Sun, X. Wang, X. Tang, Deep Learning Face Representation from Predict 10,000 Classes, 2014, pp. 1891-1898.
7. Z. Liu, P. Luo, X. Wang, X. Tang, Deep Learning Face Attributes in the Wild, 2015, pp. 3730-3738.
8. Y. Xu, Y. Lu, Adaptive weighted fusion A novel fusion approach for image classification, Neuro computing 168 (2015) 566-574
9. O.M. Parkhi, K. Simonyan, A. Vedaldi, A. Zisserman, A Compact and Discriminative Face Track Descriptor, Computer Vision and Pattern Recognition, 2014, pp. 1693-1700
10. K. Simonyan, O. Parkhi, A. Vedaldi, A. Zisserman, Fisher vector faces in the wild, in: British Machine Vision Conference, 2013, pp. 8.1-8.11