

Multi-resolution approach to facial recognition and *Biometrics-based Authentication*

Sabah Jassim

University of Buckingham, U.K.

Email address: sabah.jassim@buckingham.ac.uk

Introduction. The lack of trust and public confidence in the security and privacy of electronic transaction seems to be among the most serious concerns, and is one of the main factors that could explain the slow down in e-commerce growth. It is a serious obstacle to the utilisation of information technology in various areas of e-commerce, e-government, as well as e-services. Credit card fraud is becoming a major cause of concern for online trading, its volume is growing annually and costing billions. By far, the most serious concern about online credit card transactions is that of repudiation. If a small, but significant, percentage of a business's online credit card transactions are challenged, then its operation costs mount and may even have its card acquisition service withdrawn. Secure and strong Identification/Authentication schemes are essential for tackling the problem of repudiation. The task of detecting and preventing fraudulent repudiation of web transactions is particularly challenging for mobile/wireless and smartcard platforms for a number of reasons. These platforms have constrained memory, limited computational powers, and slow transmission rate. Conventional identification/authentication methods such as passwords and PINs are inadequate for privacy and security requirements of mobile/smartcard technology. The security of these methods is often compromised through human error/ignorance. Knowledge of a secret and/or the possession of some token such as a card, do not protect against impersonation. Tools are available to those who have the knowledge to forge identities (in the physical as well as digital world) to access unauthorised information and to avoid being detected by law enforcement authorities. In itself, the possession of a mobile phone or a card does not prevent theft or fraud. The tragic events of September 11th have highlighted the inadequacy of traditional identification to control access to sensitive locations. Rigidly applied passport control checks did not seem to stop the hijackers, the identity of many of whom may remain a mystery for a long time. Hence the urgent need for reliable, efficient, and non-intrusive automatic identification systems. Secure identification/authentication must bind the card (or the mobile phone) to the cardholder's physical appearance in a way that is less dependent on human intervention. It is not only desirable, but also essential for technologically advanced and networked society in which the use of, as well as the range of services on, mobile/wireless communication are expanding very rapidly. Long term solution to the trust and confidence problem requires building ***Biometrics-based Authentication Infrastructures*** to complement Public Key Infrastructures. Moreover, as larger-memory multi-application smartcards become widespread and multiple business entities start to provide downloadable applications, managing access control to different applications becomes a serious challenge. Biometrics-based authentication is an ideal alternative. But there is an urgent need to support research into developing efficient facial biometrics-based authentication systems that are specifically designed for the mobile/wireless communication.

Biometrics for Smartcards/mobile platforms

Biometrics are unique human characteristics that can be used to identify individuals. These include fingerprints, hand geometry, face, iris patterns, retinal pattern, DNA, ear features, facial thermography, and voice recognition. The rapid growth in Internet and mobile telephony usage in e-commerce led to a surge of interest in using biometric signal processing for identification and authentication. Biometrics systems work in two stages: the enrolment stage and the identification stage. In the first stage biometrics characteristic are extracted from a digital image of the person, from which a compact template is created and stored for future reference either on a database or a token (e.g. a smartcard). In the identification stage the biometrics scanner creates a digital representation together with the corresponding template to be compared with the stored version.

Despite the fact that biometrics and mobile/smartcard technologies have been around for sometime and even before the emergence of e-commerce, there has been very little effort in

integrating the two technologies. It is now recognised that biometrics can play an important role in making smartcards more secure, and smartcards can make biometrics pervasive and useful. There have been attempts to implement a number of biometric-based identification on a smartcard platform. Smartcards with fingerprint-based identification are available on the market. Such a system is seen as too intrusive to be accepted by many users. Recently, there have been reports of medical concerns associated with the use of some biometrics. Hence the recently growing interest in facial biometrics as the most obvious and non-intrusive tool for secure authentication. Biologists believe that a significant part of human cognitive function evolved to provide efficient ways of recognising other people's facial features and expressions. But the ability to recognising friends' faces doesn't extend well to identifying strangers by photo identity. Hence the need to automate the process of face recognition.

A number of facial recognition/identification systems have been developed with a various degree of success. The most common such system is based on the concept of *Eigenface* that is based on principle component analysis. However such systems and most existing biometrics based identification systems are designed for specific purposes, and may not be particularly suitable for mass use in mobile/smartcard platforms. Smartcard and mobile system applications, pose serious challenges due to cards constrained memory, limited computational powers, and slow transmission rate (only 9600 bits/sec). Hence, the need for efficient to compute invariant facial feature-dependent parameters.

At Buckingham University, a multiresolution facial profiling system is being researched for identification/authentication in smartcard applications. Elements of the intended facial profiling system arose from an ongoing medical related research project on measuring facial muscle movement during speech. Although computational efficiency is not a serious concern in that research, working with raw image/video data (i.e. in the spatial domain) is made much more cumbersome as a result of data size. Instead, a multiresolution image-decomposition provides the potential to represent patterns as well as anomalies in the decomposed images. Our research revealed a very interesting property that is satisfied by facial features at all resolutions, which provides the necessary elements for fast and efficient *facial profiling systems*. Associated with each facial feature (eyes, nose, mouth, chin, etc.) in a face image, and at each resolution, there are a small numbers of parameters that can be computed efficiently. These parameters can be used to automatically detect the boundaries and location of the main facial features, and thereby providing a powerful and efficient tool to validate the profile data for each feature. Preliminary results also indicate that these parameters are sufficient, on their own, for face recognition/identification. This result may also be used to support any other known biometric-based facial identification system. The efficiency of computing the profiling data, together with its small size makes it suitable for smartcard/mobile applications and in particular for identification/authentication purposes. Our research also reveal great potentials for new efficient face recognition systems that are based on modified principle component analysis of multi-resolution decomposition of facial images. Indeed we have identified a number of plausible ways to develop multiresolution versions of Eigenface concept for authentication. Future research would focus on developing systems that provide many authentication functionality including:

- Authenticating the holder,
- Authenticating the smartcard and its holder to the issuer and application providers, and
- Biometrics based signatures.

Summary

Recent events have shown that biometrics-based authentication provide a reliable solution for the widespread problem of credit card fraud and repudiation of online transactions. In this short note, we argue that the constrained platforms of smartcards and mobile systems require specially designed efficient facial biometrics, and the multiresolution approach is the answer. This is even more essential in the near future when multi-applications and services are to be provided on these platforms. *In our view this area should be among the priorities for future research on mobile privacy and security.*