Image Quality Assessment for Fake Biometric Detection

G.H.Chandana Priyanka[1]
[1]Department of Computer Science & Engineering
[1]Saveetha School of Engineering, Saveetha University, Chennai, India

Abstract--- To ensure the actual presence of a real rightful trait in difference to a fake self-manufactured synthetic or reconstructed sample is a significant trouble in biometric verification, which requires the development of new and efficient protection measures. Background to fingerprint recognition describes the biometric use of fingerprints scanning is also done by biometric technologies. The objective of proposed system is to enhance the security of biometric recognition frameworks, by adding liveness assessment in a fast, user friendly and non-intrusive manner, through the use of image quality assessment. The experimental results, obtained on publically available data sets of fingerprints, iris, and 2D face. Collection Variables: Physical variations during biometric collection that may change the capacity. Translation or scaling or rotation usually compensated in software. Can the device detect that the subject is live? Fake face recognition with a photograph? Or a rubber print image (fingerprint)? Or a glass eye (iris encoding)?

I. INTRODUCTION

In recent years the rising interest in the estimation of biometric systems security has led to the creation of plentiful and very diverse initiatives focused on this major field of research. All these initiatives clearly highlight the importance given by all parties involved in the development of the systems security to bring this rapidly emerging technology into practical use.

Currently used for identity, confirmation and forensic purposes, biometric technologies can be broadly grouped into four areas with several techniques in each:

- Hands;
- Heads and face;
- Other physical characteristics; and
- Behavioral characteristics.

The first three categories are physiological and are based on measurement of physical characteristics. Except in the case of a serious disaster or operation, this biometrics is generally unaffected over time. Behavioral characteristics are more susceptible to change and can be affected by age, illness, disease, tiredness and can also be deliberately altered. These are therefore, less consistent as authenticators or identifiers.

Among the different threats analyzed, the so-called direct or spoofing attacks have forced the biometric community to study the vulnerabilities against this type of synthetically produced artifact or try to minic the behavior of the genuine to unfairly access the biometric system. As this type of attack performed in the analog domain and the interaction with the device is done following the regular protocol, the usual digital protection mechanisms are not useful.

The two types of methods present certain advantages and drawbacks over the other and, in general, a mixture of both would be the most popular protection approach to increase the safety of biometric systems. As a coarse comparison, hardware-based schemes usually present a higher fake detection rate, while software-based techniques are in general less costly and less intrusive since their implementation is obvious to the user.

The vast majority of present protection methods are based on the properties of a given trait which gives them a much reduced interoperability, as they may not be implemented in recognition systems based on other biometric modalities, or even on the same system with a dissimilar sensor.

II. IMAGE QUALITY ASSESSMENT FOR LIVENESS DETECTION

The use of image quality assessment for liveness detection is motivated by the statement that: “It is expected that a false image captured in an attack attempt will have different quality than a real sample acquired in the normal operation scenario for which the sensor was designed.”

Expected quality differences between real and false samples may include: degree of sharpness, color and luminance levels, local artifacts, amount of information found in both types of images. For example, iris image captured from a printed paper or out of focus due to trembling; it is common that fingerprint images captured from a sticky finger present local acquisition artifacts such as spots and patches.

III. COMPARISION RATE MEASURES

There are two methods of measuring the relationship rate. They are: Penetration Rate and Bin Error Rate. Penetration Rate: percentage of templates that must be individually compared to a candidate, given some binning. Search problem is done usually by complete search, with some comparison algorithm, no reliable tree or hash classification. Low penetration rate implies faster searching. For example, fingerprints.

Bin Error Rate: Probability that a search for a matching template will fail owing to awrong bin placement. Related to confidence in the binning strategy.AFIS (automated Fingerprint Identification Systems) Bin error usually< 1%.

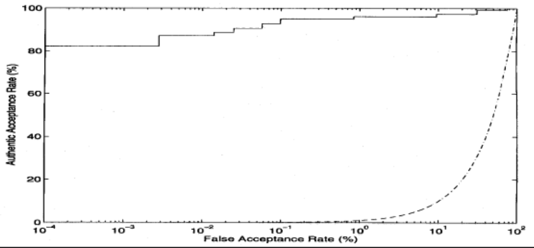

Fig. 1:

IV. Fingerprints

Fingerprint analysis, also known in the US as dactylography, is the science of using fingerprints to recognize anindividual. Fingerprint recognition is well recognized and a mature science. Palms and the soles of feet also have distinguishing epidermal patterns. Even identical twins will have contradictory fingerprints patterns. No two persons have been found to have the same prints.

There are three basic categories of fingerprint: Visible prints, such as those made in oil, ink or blood. Latent prints which are unseen under normal viewing conditions. And plastic prints which are left in soft surfaces such as new paint.

There are now over forty methods available for collecting prints including powders, use of chemicals such as iodine, digital imaging, dye strains, and fumes. Lasers are also used.

Fig. 2:

V. Automated Identificaton Systems

AFIS were formerly based on the Henry Classification System and designed to speed the manual search process. The Henry Classification Systems is not, however, easily automated and works well only when all ten fingerprints are recorded. Partial print and incomplete fingerprint records could not be correctly classified.

Most recently automated classification of finger prints is based on ridge flow analysis or ridgeline counting which generates a unique map of each fingerprint. These maps are stored as mathematical representations, occupy less storage space than the original image and are more suitable for computerized search and similar. This process is known as feature extraction. The use for fingerprints for verification and recognition in non-law enforcement application, for instance welfare payment management or border control, has lead to the improvement of plain impression AFIS applications.

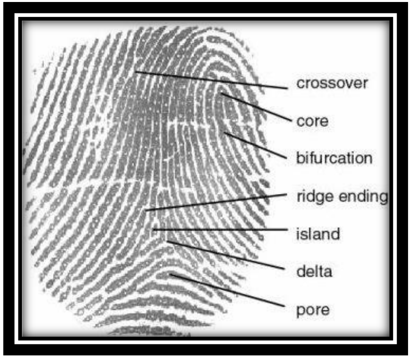

Fig. 3:

VI. Fingerprint Readers

Fingerprint readers an employee several techniques. The principle methods are: Capacitive and Optical.

Capacitive readers measure the differences in electrical signals generated by the valleys and ridges of fingerprints when presented to the reader. Capacitive readers use a sensor that measures conductivity of a large amount of points over the surface of the sensor. Limited by the size of the individual finger, sensors measure roughly 15x20mm. Grid embedded in the sensors createsdistinct points of measurement, sometimes described as pixels. Active capacitive sensing is considered to have a high tolerance for parasitic effects compared to passive capacitive sensing, thus improving accuracy.

A key advantage of a capacitive reader is the requirement for a fingerprint-type shape, rather than an image. This can be a defense to spoofing.

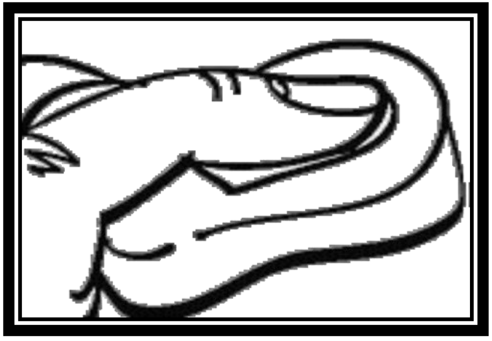

Fig. 4:

Optical: Optical readers use either a complementary metal oxide semiconductor (CMOS) device or more usually, a charge coupled device (CCD). A fingerprint scanner typically has its own light source, usually a LED array. CMOS image sensor offer lower power consumption and more on-chip functionality. They are also frequently found in high volume, portable applications.

A. CMOS (Source: Omni Vision):

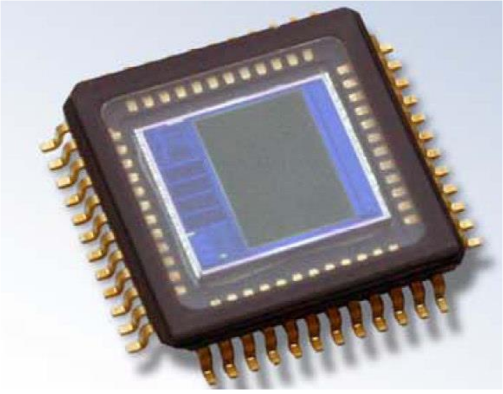

Fig. 5:

B. CCD (Source: Fairchild Imaging):

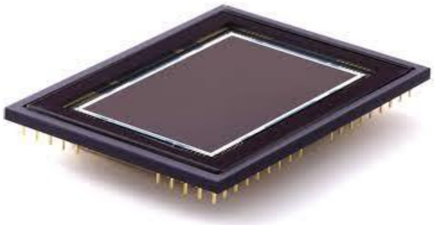

Fig. 6:

VII. The Security Protection Method

The difficulty of fake biometric detection can be seen as a two-class categorization problem where an input biometric model has to be assigned to one of two classes: real or fake. The key point of the process is to find a set of discriminate features which permits to build an appropriate classifier which gives the probability of the image “realism” given the extracted set of features.

The four selection criteria are:

- Performance. Only widely used image quality approaches which have been consistently tested showing good performance for different applications have been considered.
- Complementarity. In order to generate a system as general as possible in terms of attacks detected and biometric modalities supported, we have given priority to IQMs based on complementary properties of the image
- Complexity. In order to keep the simplicity of the method, low complexity features have been preferred over those which require a high computational load.
- Speed. This is, in general, closely related to the previous complexity. To assure a user-friendly non-intrusive application, users should not be kept waitingfor a response from the recognition system. For this reason, big importance has been given to the feature extraction time, which has a very big impact in the overall speed of the fake detection algorithm.

VIII. Conclusion

Need for independent evaluation of biometric devices is clear. Adequate testing usually requires a special version of the software. Fingerprints have been widely used as a form of identification for many years and are well-established in many places.

The evaluation experimental protocol has been designed with two-fold objective:

- First, evaluate the “multi-biometric” dimension of the protection method.
- Second, evaluate the “multi-attack” dimension of the protection method.

Reference

[1] The Henry Classification System, International Biometric Group, 2003 http://www.biometricgroup.com/ Henry%20Fingerprint%20Classification.pdf, accessed02 December 2005

[2] All About Fingerprints, Chapter 4 - The Techniques,http://www.crimelibrary.com/criminal_mind/forensics/fingerprints/4.htm, accessed 02 December2005

[3] Capturing an Image, Eastman Kodak Company, http://wwwdk.kodak.com/global/en/corp//capturingAnIkmage.jhtml, accessed 12 February 2006

[4] Omni Vision Camera Chips ,http://www.ovt.com/p_cameraChips.html#5m, accessed 12 February 2006

[5] CCD143A Specification Sheet, Fairchild Imaging, http://www.fairchildimaging.com/main/ccd_linear_143a.htm, accessed 12 February 2006

[6] http://www.engr.sjsu.edu/wbarrett/

[7] http://www.engr.sjsu.edu/biometrics/