BIOMETRICS IN ABC: COUNTER-SPOOFING RESEARCH

Hong Wei, Lulu Chen, James M Ferryman
Computational Vision Group,
School of Systems Engineering, University of Reading, Reading RG6 6AY, UK
(h.wei,|l.chen,|j.m.ferryman@reading.ac.uk)

Abstract: Automated border control (ABC) is concerned with fast and secure processing for intelligence-led identification. The FastPass project aims to build a harmonised, modular reference system for future European ABC. When biometrics is taken on board as identity, spoofing attacks become a concern. This paper presents current research in algorithm development for counter-spoofing attacks in biometrics. Focussing on three biometric traits, face, fingerprint, and iris, it examines possible types of spoofing attacks, and reviews existing algorithms reported in relevant academic papers in the area of countering measures to biometric spoofing attacks. It indicates that the new developing trend is fusion of multiple biometrics against spoofing attacks.

Keywords: biometrics, ABC, counter-spoofing mechanisms

INTRODUCTION

The FastPass project[1] aims to build a harmonised modular reference system for all European automatic border crossing points. With growth in travellers and complexity of travel documents, it is desired to have fast and secure processing for intelligence-led border control. Biometrics, the identification of humans by their traits, is a key means used in automated border control (ABC). By automating identity checks, biometrics can confirm quickly and accurately that travellers are whom they claim to be. As early as in 2002, the US Congress had asked the General Accounting Office (GAO) to assess biometric technologies that can be used for US border control applications (News-1 2002). In Biometrics Review: 2008/09 (News-2 2009), it stated that biometrics at the border received a boost when the European Commission unveiled plans to strengthen Schengen zone border security, while facilitating travel for citizens, tourists and legal migrants. The recent survey conducted by Frost & Sullivan forecasted that the biometrics market in the global border control will expand steadily due to increasing international co-operation on travel security issues (News-3 2013).

The commonly used biometric traits in ABC are face, fingerprint, and iris. A typical biometric ABC may work in such a way that a passport is read by a document reader followed by machine checking the face, fingerprint, or/and iris. Then, a positive checking result opens the gate; otherwise the gate remains closed. For example, the UK Border Agency uses face matching for all its operational e-gate systems, which are currently only open to EU citizens holding electronic machine readable travel document (e-MRTD). The UK Border Agency also collects fingerprint scans (10 flat fingerprints) from persons applying for UK visas and these can be matched on arrival[2]. It becomes crucial to increase the reliability of biometric systems. In some cases, a multimodal biometric system is in place to enforce the security of a machine identification system.

However, machine intelligence is challenged by spoofing attacks. At the biometric sensor level, these attacks could be, for example of face, a printed face on a piece of paper, a face on an iPad screen, or a face mask (could be 3D) worn by an attacker. The vulnerabilities of algorithms used for biometric based identification need further exploration to mitigate potential attacks. Software based solutions are under research to find counter-spoofing mechanisms to optimise performance of biometric recognitions (Gomez-Barrero, Galbally, and Fierrez 2013). This paper overviews the current research in the area of anti-spoofing attacks in biometrics. It particularly focuses on recent algorithm developments based on literature review. The review is categorised by three different biometric traits (i.e. face, fingerprint, and iris). In the next section, the detailed reviews are presented with the three categories, followed by a conclusion in the final section.

RESEARCH ON COUNTER-SPOOFING MECHANISMS IN BIOMETRICS: AN OVERVIEW

Depending on sensors and recognition algorithms used in biometric systems, counter-spoofing algorithms can be attempted. Software solutions may take place to improve performance of biometric systems against spoofing attacks. Mechanisms have been sought by research, and relevant counter-spoofing algorithms are developed. In this section, seminal algorithms used for countering spoofing attacks for face, fingerprint, and iris are reviewed.

---

[1] FastPass is a collaborative project funded by the European Commission under the 7th Framework Programme, with grant agreement no. 312583 (https://www.fastpass-project.eu/).

[2] Acknowledgement: The information is provided by Chris Hurrey from IntrePID Minds Ltd, UK, a FastPass project partner, closely working with the UK Border Agency.

Counter-spoofing algorithms in face recognition

A falsified face could be a printed photograph, a photograph displayed on a screen, and videos replayed on a screen. Techniques used in countering spoofing attacks for 2D face recognition can be broadly classified into three categories, i.e. motion, texture and liveness (Kahm and Damer 2012).

- Motion analysis: the analysis is based on the fact that there is significant difference between motions of planar objects and real human faces (3D). Algorithms of spoofing detection based on motion analysis are usually associated with optical flow. The assumption is that different patterns of optical flow fields reveal the difference between movements of 3D face (real face) and 2D face (spoofing face).
- Texture analysis: it is assumed that printed/LED faces contain outstanding texture patterns that do not exist in real faces. The other common observation is that images/videos with spoofing faces (printed or replayed) are usually noisier than those of real faces. In this case, noise variance may be used as a distinction feature for the detection.
- Liveness detection: Life signs may include eye blinking, lips movements, etc. This requires analysis of local movement against global movement. Developed algorithms under this approach focus on the movement of a certain identified part of a face.

Among the three categories, texture analysis dominants approaches to distinction of live and spoofing faces. In the recent competition on counter measures to 2D face spoofing attacks (Chingovska 2013), eight teams took part in the competition, and seven of them made use of image textures in their algorithms. These texture features include local binary code (LBP), gray-level co-occurrence matrix (GLCM), and Gabor features. LBP has shown its effectiveness as image features in face spoofing detection(Chingovska, Anjos, and Marcel 2012). Statistical features, such as first and second moments are also used as descriptors in the feature space. For motion analysis, optical flows are popularly adapted in algorithm development (Bao et al. 2009); and live signs are connected to both eye blinking and lip moving (Pan et al. 2007; Wang, Ding, and Fang 2009). With regards to classifiers, a variety of Support Vector Machines (SVMs) have seen their applications in face spoofing detection (Chingovska 2013).

Texture analysis has advantages of simple implementation, possible decision from a single frame, and no user collaboration needed. However it requires data covering all possible attacks, and may fail with low textural attacks. Algorithms based on motion and life sign detection are independent to textures and very hard to spoof by 2D images, but it needs a video sequence, and may also need user-cooperation. The new developing trend of 2D face anti-spoofing algorithms is fusion of different categories of cues, either in the feature level (a single classifier) or in the score level (multiple classifiers). Such an approach is effective in tackling a diverse set of face spoofing attacks (Chingovska 2013).

Counter-spoofing algorithms for fingerprint recognition

The fingerprint is another biometric trait widely used in biometric border crossing systems. Two types scanning technology dominate commercial products: optical sensors and capacitive sensors. After capturing fingerprints, a scanner performs one-against-one or one-against-all matching with enrolled data. Fingerprint scanners are robust and achieve high accuracy for identification tasks, however, they are potentially vulnerable to spoofing attacks, which reproduce fake fingerprints from original copies (Galbally et al. 2011; Espinoza, Champod, and Margot 2011). Common spoofing attacks use scanned finger images, artificial fingers, or cadaver fingers. The materials for making artificial fingers include silicone, latex, gelatin, play-doh, waxes, and wood glue (van der Putte and Keuning 2001; Matsumoto 2002).

Counter-spoofing algorithms incorporate liveness detection, which can be implemented in two ways: hardware and software. The hardware solution detects liveness based on natural features such as odour, pulse, blood pressure, temperature and electrical resistance. The obvious limitation of these methods is the requirement for additional hardware, hence extra security measures for the hardware. Software-based solutions analyse the image data directly and do not require extra hardware. A common method for liveness detection is based on fingerprint perspiration patterns (Derakhshani et al. 2003; Parthasaradhi et al. 2005; Abhyankar and Schuchers 2009). When touching the scanner's surface, a real fingertip becomes wetter over time due to the perspiration process. Especially, the pattern of the ridges on a fingerprint becomes darker on a capacitive fingerprint sensor. This will not appear on an artificial finger or a photocopy of the fingerprint image. Thus, by measuring the variation of the perspiration patterns over time, for instance 2–5 seconds, liveness can be detected. This method may cause false alarms when people have a skin condition which is not suitable for the detection, or may require a different period of touching.

It is reported that fake fingers will lose some details, such as pores, when they are fabricated from the materials listed above (Marcialis, Roli, and Tidu 2010). The size of the pores is less than 1 mm, so that they are very difficult to replicate on an artificial finger, i.e. real fingers have many more pores than artificial fingers. Therefore,

counting the number of pores may be an approach to identify fake fingers. Skin distortion occurs during movement such as rotating the finger on the scanner surface, whereas fake fingers give less or different deformation. Signal analysis of fingerprint ridges and valleys has shown the difference between real and fake fingerprints (Tan and Schuckers 2010). Coli et al. (Coli, Marcialis, and Roli 2007) found that the frequency between ridges and valleys is altered during the fabrication process. They use power spectrum analysis based on the Fourier transform to detect fake fingers. Various image features have been attempted to distinguish live and fake fingerprint images. Again, LBP has shown promising results among all the features (Nikam and Agarwal 2008a; Ojala, Pietikainen, and Maenpaa 2002). More recently, Ghiani et al. (Ghiani, Marcialis, and Roli 2012) proposed the Local Phase Quantization (LPQ) feature, which shows competitive performance. Fusion of multiple image features is popularly used in practice (Pereira et al. 2012; Nikam and Agarwal 2008b). It has been demonstrated to improve the performance of fingerprint spoofing detection.

Counter-spoofing algorithms for iris recognition

Iris patterns are epigenetic and possess a high degree of randomness (Daugman 2003). Like face identification, Iris identification is non-intrusive. This makes iris and face more suitable to be integrated in a future FastPass system. However, to capture high quality iris images from a long-distance moving target is currently still a challenging task. On the other hand, compared with face, iris provides a higher degree of uniqueness, and unlike face, iris is believed to be stable over a person's lifetime.

Similar to face and fingerprint, iris systems can be deceived using cheap spoofing methods, such as printed iris images, cosmetic contact lenses with a printed iris pattern, artificial eyes and handheld displays. Previous research has evaluated the vulnerability to such spoofing attacks and the importance of applying counter-spoofing mechanisms (Ruiz-Albacete et al. 2008; Galbally et al. 2012).

Daugman (Daugman 2003) proposed theories that using optical properties from different parts of an eye (blood, melanin pigment, tissue and fat), retina reflection (the red eye effect) and purkinje reflection. High quality cameras are required for capturing these features. Chen et al. (Chen, Lin, and Ding 2012) proposed an approach based on texture changes of the conjunctival blood vessel and iris patterns from multispectral images. They claimed that with a real iris texture varies with light frequency, whereas with a fake one it stays constant. Image texture analysis has also been popular in academic research. A simple method is to analyse high-frequency spectral magnitude based on Fourier transform (Daugman 2003). The method recognizes spurious coherence from printed iris patterns. However, this method would fail for partially blurred printed iris patterns or high-resolution printed patterns (He, Lu, and Shi 2009). Rather than using optical or texture features alone, Lee and Son (Lee and Son 2012) recently combined both optical and texture features in iris anti-spoofing detection. Galbally et al. (Galbally et al. 2012) proposed a liveness detection system based on a set of image quality related features. More recently, Connel et al. (Connel et al. 2013) proposed an approach to detect cosmetic contact lenses by projecting additional structured light patterns onto the eye. They found that without a contact lens, the reflected patterns have straight lines, whereas with a contact lens, the patterns had curved lines. Eye movement has also been used as a basis for spoofing countermeasures. Movement includes eye hippus, constriction and dilation of the pupil and iris, and eyelid blinks, which can all be captured by a normal camera. Bodade et al. (Bodade, Talbar, and Batnagar 2009; Bodade and Talbar 2011) calculated variations of pupil dilation from multiple iris images and recent research uses pupil constriction in iris liveness detection (Huang et al. 2013).

CONCLUSIONS

Biometrics have shown its practice in ABC, and will be continously used in the future ABC. Counter-spoofing attacks in biometrics have to be considered. An ideal ABC may have a nature of non-intrusive, efficiency, and effectiveness. These require advanced algorithms to identify/verify submitted biometric traits in such a way that both accuracy and computational cost are taken into account. In this paper, as one of the objectives in the FastPass project, we present an overview of current research of counter-spoofing mechanisms in biometrics. Algorithms and features used in these algorithms are broadly discussed. Their pros and cons are briefly summarised for reference. It has been noted that the new developing trend of counter-spoofing algorithms is data fusion at different levels, such as, feature level fusion, decision level fusion, and fusion of multiple traits.

REFERENCES

Abhyankar, A., and S. Schuchers. 2009. Integrating a wavelet based perspiration liveness check with fingerprint recognition. *Pattern Recognition* 42 (3):452 – 464.

Bao, Wei, Hong Li, Nan Li, and Wei Jiang. 2009. A liveness detection method for face recognition based on optical flow field. In *International Conference on Image Analysis and Signal Processing*, 233-236, 11-12 April 2009.

Bodade, R. , and S. Talbar. 2011. Fake iris detection: A holistic approach. *International Journal of Computer Applications* 19 (2):1-7.

Bodade, R. , S. Talbar, and A. Batnagar. 2009. Dynamic iris localisation: a novel approach suitable for fake iris detection. In *IET International Conference on Ultra Modern Telecommunications & Workshops*.
Chen, R. , X. Lin, and T. Ding. 2012. Liveness detection for iris recognition using multispectral images. *Pattern Recognition Letters* 33 (12):1513 – 1519.
Chingovska, I. 2013. The 2nd competition on counter measures to 2D face spoofing attacks. In *The 6th International Conference of Biometrics (ICB 2013)*, 4-7 June 2013, at Madrid, Spain.
Chingovska, I., A. Anjos, and S. Marcel. 2012. On the effectiveness of local binary patterns in face anti-spoofing. In *International Conference of the Biometrics Special Interest Group (BIOSIG 2012)* 1-7, 6-7 Sept. 2012.
Coli, P., G Marcialis, and F Roli. 2007. Power spectrum-based fingerprint vitality detection. In *2007 IEEE Workshop on Automatic Identification Advanced Technologies*, 169–173.
Connel, J. , N. Ratha, J. Gentile, and R. Bolle. 2013. Fake Iris detection using structured light. In *IEEE ICASSP 2013*.
Daugman, J. . 2003. Demodulation by complex-valued wavelets for stochastic pattern recognition. *International Journal of Wavelets, Multiresolution and Information Processing* 1 (1):1-17.
Derakhshani, R., S. A. Schuchers, L. A. Hornak, and L. O'Gornam. 2003. Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners. *Pattern Recognition* 36 (2):383 – 396.
Espinoza, M., C Champod, and P Margot. 2011. Vulnerabilities of fingerprint reader to fake fingerprints attacks. Forensic Science International. *Forensic Science International* 204 (1-3):41-49.
Galbally, J. , A. Ross, M. Gomez-Barrero, J. Fierrez, and J. Ortega-Garcia. 2012. A new vulnerability of iris recognition systems. *From the iriscode to the iris - White Paper for Black Hat USA*.
Galbally, J., J. Fierrez, F. Alonso-Fernandez, and M. Martinez-diaz. 2011. Evaluation of direct attacks to fingerprint verification systems. *Telecommunication Systems* 47 (3-4):243–254.
Ghiani, L. , G. Marcialis, and F. Roli. 2012. Fingerprint liveness detection by local phase quantization. In *ICPR2012 - 21st International Conference on Pattern recognition*, 537–540, at Tsukuba Science City, Japan.
Gomez-Barrero, Marta, Javier Galbally, and Julian Fierrez. 2013. Efficient software attack to multimodal biometric systems and its application to face and iris fusion *Pattern Recognition Letters* (in press) available on-line 10 May 2013.
He, X. , Y. Lu, and P. Shi. 2009. A new fake iris detection method. In *Proceedings of the Third International Conference on Advances in Biometrics - ICB09*, 1132–1139.
Huang, X. , C. Ti, Q. Z. Hou, A. Tokuta, and R. Yang. 2013. An experimental study of pupil constriction for liveness detection. In *IEEE Workshop on Applications of Computer Vision (WACV 2013),*.
Kahm, O., and N. Damer. 2012. 2D face liveness detection: An overview. In *2012 BIOSIG - Proceedings of the International Conference of the Biometrics Special Interest Group*, 1-12, 6-7 Sept. 2012.
Lee, E. C. , and S. H. Son. 2012. Anti-spoofing method for iris recognition by combining the optical and textural features of human eye. *TIIS* 6 (9):2424–2441.
Marcialis, G., F. Roli, and A. Tidu. 2010. Analysis of fingerprint pores for vitality detection. In *ICPR2010 - 20th International Conference on Pattern Recognition*, 1289–1292, 23-26 Aug. 2010, at Istanbul, Turkey.
Matsumoto, T. 2002. Gummy and conductive silicone rubber fingers. In *Proc. of ASIACRYPT 02*, 574–576, at London, UK.
News-1. 2002. GAO to study biometrics for border control applications. *Biometric Technology Today* 10 (5):2.
News-2. 2009. Biometrics review: 2008/2009. *Biometric Technology Today* 17 (1):9-11.
News-3. 2013. Frost & Sullivan forecasts expansion of border control biometrics. *Biometric Technology Today* 2013 (4):3-12.
Nikam, S. , and S. Agarwal. 2008a. Fingerprint liveness detection using curvelet energy and co-occurence signatures. In *Fifth International Conference on Computer Graphics, Imaging and Visualisation*, at Penang, Malaysia.
Nikam, S. , and S. Agarwal. 2008b. Texture and wavelet-based spoof fingerprint detection for fingerprint biometric systems. In *IEEE ICETET'08*, 675-680.
Ojala, T. , M. Pietikainen, and T. Maenpaa. 2002. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 24 (7):971–987.
Pan, Gang, Lin Sun, Zhaohui Wu, and Shihong Lao. 2007. Eyeblink-based Anti-Spoofing in Face Recognition from a Generic Webcamera. In *IEEE 11th International Conference on Computer Vision (ICCV 2007).* , 1-8, 14-21 Oct. 2007.
Parthasaradhi, S., R. Derakhshani, L. Hornak, and S. A. C. Schuckers. 2005. Time-series detection of perspira- tion as a liveness test in fingerprint devices. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews,* 35 (3):335–343.
Pereira, L. , H. Pinheiro, J. Silva, A. Silva, T. Pina, G. D. C. Cavalcanti, T. I. Ren, and J. de Oliveira. 2012. A fingerprint spoof detection based on mlp and svm. In *The 2012 International Joint Conference on Neural Networks* at Brisbane, Australia.
Ruiz-Albacete, V., P. Tome-Gonzalez, F. Alonso-Fernandez, J. Galbally, J. Fierrez, and J. Ortega-Garcia. 2008. Direct Attacks Using Fake Images in Iris Verification. In *Biometrics and identity management*. Berlin: Springer-Verlag.
Tan, B., and S. Schuckers. 2010. Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise. *Pattern Recognition* 43 (8):2845 – 2857.
van der Putte, T., and J. Keuning. 2001. Biometrical fingerprint recognition: don't get your fingers burned. In *Proc. of the 4th Working Conference on Smart Card Research and Advanced Applications*, 289-303, at Norwell, MA, USA.
Wang, Liting, Xiaoqing Ding, and Chi Fang. 2009. Face Live Detection Method Based on Physiological Motion Analysis. *Tsinghua Science & Technology* 14 (6):685-690.