FAKE IRIS DETECTION USING STRUCTURED LIGHT

Jonathan Connell, Nalini Ratha, James Gentile & Ruud Bolle

IBM T. J. Watson Research Center
Yorktown Heights, NY 10598
{jconnell, ratha}@us.ibm.com

ABSTRACT

Iris recognition has gained popularity due to factors such as its perceived high accuracy, significant usability advantages attributed to its non-contact acquisition method, and the availability of low cost sensors due to improvements in technology. However, non-contact biometrics authentication systems are vulnerable to different types of attacks than contact-type biometrics, such as fingerprints, for which there are a number of simple techniques to guard against attacks. In particular, the fashion industry has developed designer contact lenses with patterns that range from a simple change in eye color to the imposition of stars or other festive decorations. As these lenses are readily available and can be personalized at a very affordable price, their use in thwarting or spoofing iris-based authentication systems becomes plausible. Given the high security nature of many of these systems, there is a urgent need for a some countermeasure to this type of attack. In this paper, we describe a novel method to detect the presence of fake iris patterns, such as designer contact lenses, during the image acquisition stage to further enhance the basic security value of iris biometrics. Exploiting the anatomy and geometry of the human eye, we present a structured light projection method to detect the presence of artificial items obscuring the real iris. The detection principle has been verified using an inexpensive experimental setup consisting of a miniature projector and an offset camera. We also describe a novel algorithm to process the acquired images to find patterned contact lenses, and measure its performance using data collected with our apparatus. We argue that the addition of the proposed system and algorithm to existing iris biometrics based authentication systems will significantly improve their security.

Index Terms— structured light projection, designer contact lenses, iris recognition, spoofing iris acquisition

1. INTRODUCTION

Automated biometric authentication systems help to alleviate the problems associated with existing methods of user authentication based on possessions and/or knowledge. Often introduction of biometrics is considered to improve security. However, a thorough security analysis needs to be carried out to identify weak points that may exist or will be introduced in any biometric-based authentication system. These weak points will be exploited during operation of a system by hackers. There have been several instances where artificial fingerprints [1] have been used to circumvent biometric security systems. Similar attacks are possible in other biometrics modalities: e.g., face masks to hide identity, designer iris lenses to fool iris recognition systems. Often the popular press is very much concerned with spoofing of biometrics systems which creates a very negative impression about biometrics for the common users. The advantages of biometrics based human recognition and its role in a secure authentication system is very clear and undisputed, particularly when it comes to non-repudiable technologies. The biometrics system designers need to be aware of the threats and security holes created by biometrics in the overall system and address them at the outset to avoid being hacked later. In order to analyze the possible weak points, we use a pattern recognition model for biometrics authentication systems [2]. Any biometric system can be described as a four-stage system as in Figure 1. Using this model (Figure 1) we identify several basic attacks that plague biometric authentication systems.

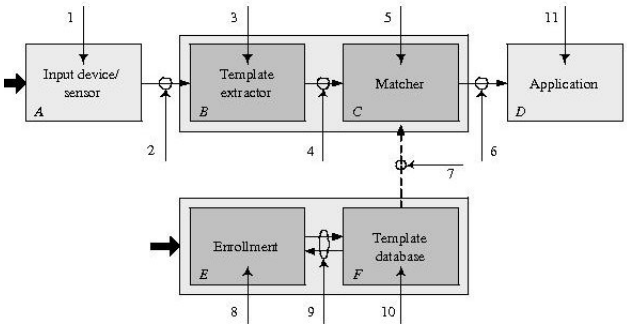

Fig. 1. Stages of biometrics-based authentication system and enrollment system, with identified points of attack (adapted from [2]).

These attacks can be thwarted by several methods applicable to each weakness:

- Livenesss detection can alleviate issues with fake biometrics to fool the sensors.
- Channel attacks can be solved by using information security methods such as encrypting the message.
- Replay attacks can be addressed using challenge-response techniques.
- Policy based remedies to prevent dictionary attacks.
- Using smartcard based secure storage methods for templates to address attacks on template databases.
- Trojan horse attacks can be prevented by using secure crypto hardware such as IBM 4764.

Note that these methods require additional resources in terms of hardware or extra time to protect and defend against various attacks. For more details, please refer to [2, 3, 4].

The attacks take on a different dimension when it comes to non-contact biometrics like iris. For example, very nicely designed contact lenses on the top of the real eye cannot be detected by liveness

Fig. 2. Examples of designer contact lenses currently available. The top two are clearly artificial patterns, but the bottom two look nearly normal.

detection alone. Nearly 20 years ago the first automated iris recognition system was proposed. While the basic recognition algorithms continue to move forward, the image acquisition systems have also made very significant progress due to many advances in the sensors area. Research efforts continue to focus on boosting performance to a higher level through more robust segmentation methods, better matching algorithms, or mechanisms to deal with loosely constrained environments and user presentations.

In a very different but related area, the eye care industry around contact lenses have been making lenses cheaper and more varied for users. One of the trends seems to be personalizing contact lenses for different occasions by making contact lenses with various patterns printed on them. Fig. 2 shows several examples of the lenses available. The top two would obviously not be mistaken as a real iris by a human observer, yet the bottom two are much more subtle. Such patterns can pose significant challenges to the iris recognition methods. First, they may contain random texture that could be construed as iris texture thereby obscuring the user's true identity. More importantly, the contact lens could conceivably have the iris image of another person printed on it to create false positives in the system thereby allowing unauthorized access.

The paper is organized as follows. In section 2, we review the prior work in this space and characterize it using the taxonomy outlined above. The projector and camera set up, along with the algorithm, is explained in Section 3. The data collected by our setup and results obtained are presented in Section 4 along with our conclusions.

2. RELATION TO PRIOR WORK

While there are several general biometrics spoofing methods reported in literature ([1, 5]), we will focus on iris spoof methods. Based on the survey of iris recognition as described in [6], we can expect the iris images attacks to come primarily at the sensor or template level. At the sensor level, often liveliness is checked by the dilation of the pupil. While this is very useful, the real iris can be obscured by another artifact with a hole in it. Early work on contact lens detection is described in [7]. The solution proposed there requires registration of the contact lenses, which can then be verified at the imaging time using texture analysis. Other ideas presented in the literature deal with printing a high resolution iris on paper and presenting it to the camera [8]. The countermeasure for such attacks is to look for the presence of dither patterns [**?**], or analyze the temporal frequency spectrum if the image is displayed on a screen instead of paper [9]. Chui et al [10] use multi spectral imaging in both infrared and blue light wavelengths to estimate the relative number of conjunctival vessels. Similarly, Lee and Park [11] use additional infrared sensors along with the iris sensor to construct the full 3-D shape of the iris. The method proposed by He et al. [12] operates by examining the change of iris texture and light spot using different wavebands and positions of infrared illumination. This can then be used to calculate the reflection properties in different parts of the iris. A countermeasure using the Purkinje image was proposed by Lee et al. in [13]. Punhan et al. [14] propose a method of detecting semi-transparent contact lenses using the texture dissimilarity between localized iris regions. A novel fake iris detection algorithm based on improved LBP and statistical features has been reported in [15]. A recent paper by Galbally et al. [16] analyzes the potential of quality assessment metrics to identify real and fake iris samples using high quality printed images.

There has also been past research focused on creating synthetic iris textures, which could be used to spoof the overall iris recognition system. The latest comprehensive results are presented in [17] where they show how to recreate the iris texture from the iriscode of the original. Other references ([18, 19]) also discuss ideas for generating the necessary iris texture using Markov models [18] and geometric/anatomical models [19]. However, the aim of generating such synthetic irises is for testing iris system accuracies.

Our proposed method differs from all these techniques in many ways. Primarily we are using a structured light projection method to produce contour changes in a stripe pattern to detect a contact lens, as shown in Figure 3. This takes advantage of the anatomy of the eye. The iris is a largely flat sheet of muscle unlike the cornea, where (semi-)opaque contact lenses reside, which is a curved dome shape. On a more general note, our anti-spoofing approach operates by adding hardware to the acquisition system rather than using software to perform additional analysis of an already acquired image.

3. PROPOSED SYSTEM AND ALGORITHM

In this paper, we propose to address detecting fake iris patterns on contact lenses. The geometry of the eye can help us if we can exploit it as shown in Figure 3. A normal eye without a contact lens will have a straight line over it when a ray of light is projected on it, as shown on the left. However, in the presence of an opaque contact lens, the ray of light will hug the lens and hence take the shape of contact lens, which is different from flat iris. The right side shows examples from our system using actual eyes and real contact lenses (bottom). Our solution is motivated by this observation. We design a set up that can project light rays on the subject's eye and measure the curvature of the light ray as observed through the camera. The curvature will help us decide if there is a patterned contact lens.

The experimental apparatus consists of an LED-based microprojector and an offset VGA resolution color camera, as shown in Fig. 4. The projector generates a pattern of thin vertical black and white stripes that impinges on the user's eye about 6 inches away. Two examples were shown in Fig. 3. Since the pattern is fixed, a video projector is not really necessary, it is simply easier to adjust this than use a fixed slide. Note that in a real installation the fake iris detection system could easily co-exist with the iris reader. This is because the projector operates in the visible range, while most

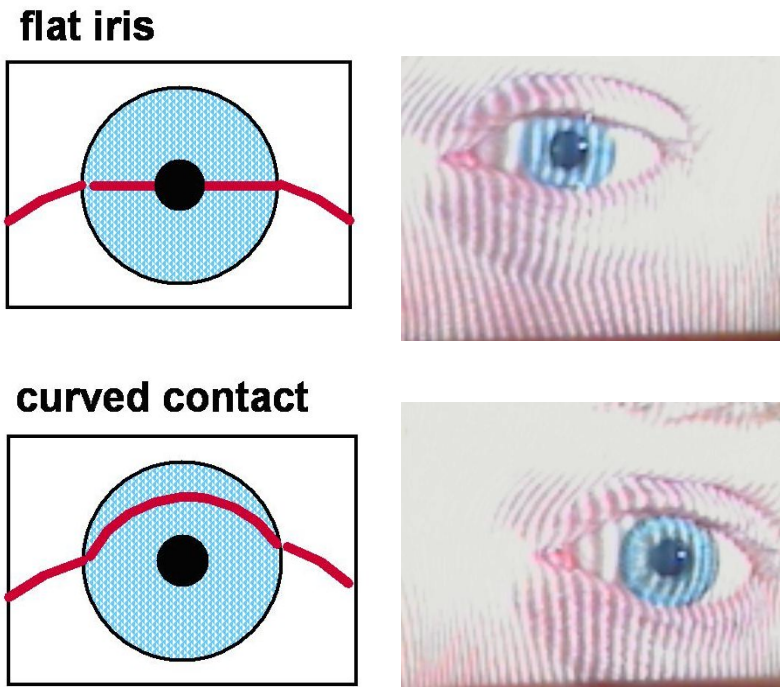

Fig. 3. Motivation: a normal eye and one with a patterned contact lens generate different deformations of a projected stripe pattern.

Fig. 4. Our experimental set up is composed of a micro-LED projector and an offset visible light camera.

iris capture systems operate in the near infrared for better contrast. Alternatively, if the bright light is objectionably to users, the pattern could be projected in infrared. Here two images would be acquired: one with the pattern on to check for contacts, and the other with it off to analyze the iris.

The goal of the detection system is to determine whether the stripes appear straight (genuine flat iris) or curved (non-transparent contact lens on cornea). As Fig. 5 shows, there are a number of steps needed to implement this. First, the system locates the pupil of the eye. It starts by looking for a dark area near the center of the image by setting a threshold based on the lowest 4% of the pixels in the search box. It then refines the position by histogramming the intensity of the red color channel in a box around the coarse position, and setting a threshold above the lowest peak in a presumed bimodal distribution. Finally, it uses connected components analysis to choose the biggest spot, then applies morphological operators to smooth and grow the blob. The result is shown in the upper left (cross hairs).

The next phase locates the approximate position of the iris. Starting with the pupil position it uses the statistics of nearby pixels to perform a contrast stretch on the image to enhance color. It then converts the RGB values into a saturation image and creates separate horizontal and vertical projections around the pupil. The falling edges of the color peaks flanking the colorless iris are taken as potential iris edges. Finally, some sanity checking is performed to ensure the iris estimation is reasonable in terms of size and position relative to the pupil. The resulting bounding box is shown in the upper right of Fig. 5.

We can now identify the stripes that actually lie on the iris itself. To do this a monochrome version of the image is generated and contrast enhanced around the iris. After this, a horizontally elongated center-surround operator is applied to the grayscale image and significant extrema (bright and dark stripes) are thresholded. A mild thinning operator is applied to both sets of stripes to yield the combined version shown in the lower left of the figure.

To determine if the resulting stripes are straight or curved, they are artificially split along a horizontal line passing through the center of the pupil. Next a connected component analysis is run to discard small blobs, or blobs with low elongation. The remaining stripe fragments are shown in the lower right of Fig. 5. Finally, we extract the orientation and area of each such blob and compute an area-weighted standard deviation of all the orientations. This spread value is taken as a proxy for curvature. Note that since we broke long flanking

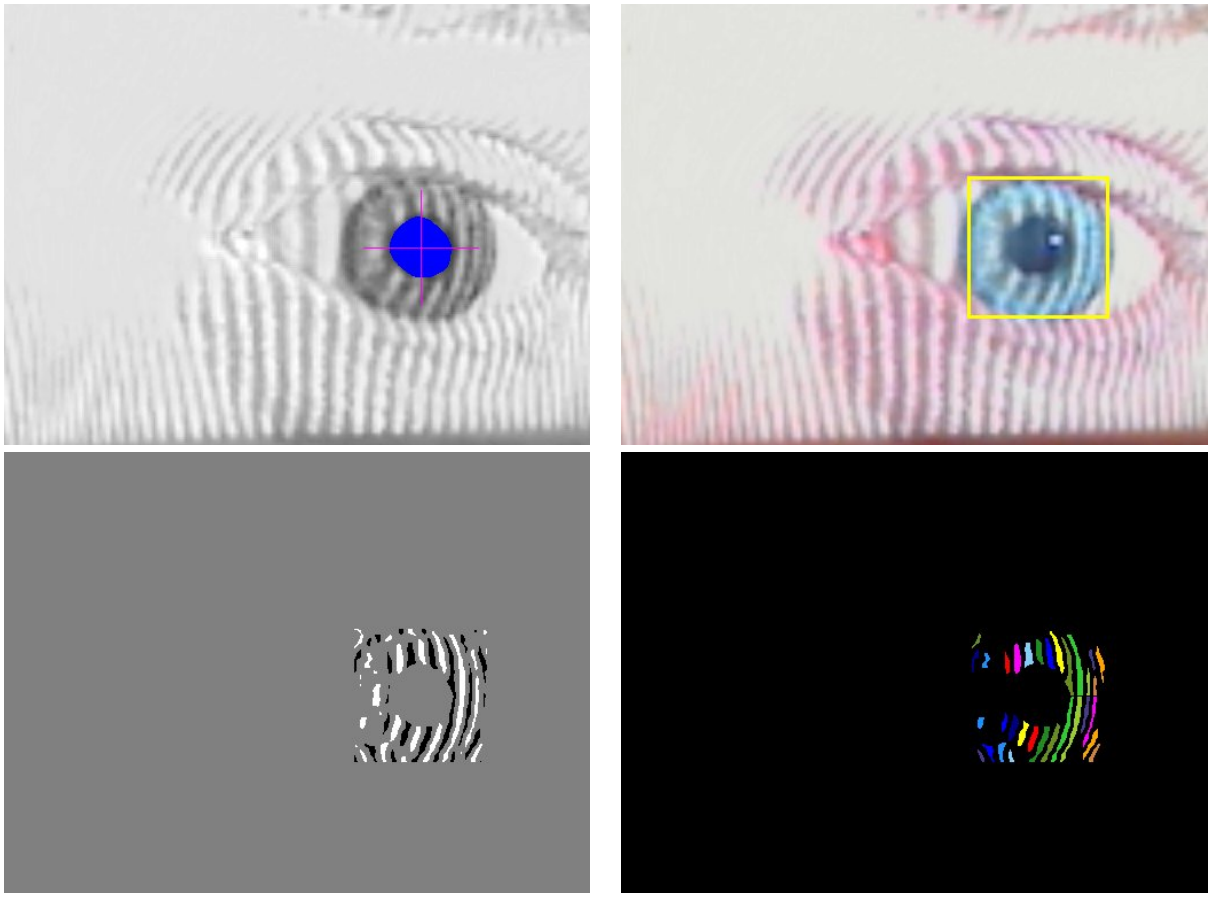

Fig. 5. To determine stripe curvature the system first finds the pupil and iris area (top row). It then detects the projected stripes and breaks them into fragments (bottom row).

stripes into a top half and a bottom half, the resulting linear approximations will point in different directions if the stripe is curved.

4. RESULTS AND CONCLUSIONS

We have tested the system on only one (blue-eyed) individual due to the limited supply of fake contact lenses and hygiene requirements of single use contact lenses. We collected 6 images of the subject's naked eyes (both left and right). We also collected 6 images with normal (lightly tinted) prescription contact lenses in place. Finally, we collected 24 images across 6 different kinds of designer contact lenses installed on the user's eyes. We then measured the standard deviation of blob angles, as described above, for all 36 images. The results are shown in Table 1. Note that the maximum deviation observed in both the naked (6.9 degrees) and normal contact (6.4 degrees) cases is less than the minimum deviation observed in the patterned contact case (9.1 degrees). This means, at least for our small sample, that the patterned contacts can be reliably detected (i.e. using a fixed threshold around 8 degrees). While the approach has no inherent dependency on user, in the absence of any public image set this single user data is all we could readily obtain to evaluate our system's performance.

Recognizing the need for a robust fake iris detection to alleviate the security challenges in iris recognition systems, we have presented a novel, inexpensive technique based on structured light. The method uses a projector and camera to image the subject's eye. Our system can be integrated with existing iris scanners since the projected pattern is in visible light. Our experimental results suggest that the proposed method has the potential to improve the detection of printed contact lenses. Future work would include looking at far more individuals. We could also search for the optimal pattern (beyond stripes) to detect contact lenses efficiently. The usability aspect of the system needs a thorough evaluation, which has not been addressed in this study. Finally, our system should be integrated with an iris scanner to evaluate end-to-end performance and crosstalk.

Eye condition	images	min std	max std
Naked eye	6	4.0	6.9
Normal contact	6	2.8	6.4
Patterned contact	24	9.1	22.2

Table 1. Results on our test data show that patterned contacts generate a larger variation of angles for the stripe fragments.

5. REFERENCES

[1] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial gummy fingers on fingerprint systems," in *Proceedings of SPIE*, 2002, vol. 4677, pp. 275–289.

[2] R.M. Bolle, J.H. Connell, S. Pankanti, N.K. Ratha, and A.W. Senior, *Guide to biometrics*, Springer, 2003.

[3] N.K. Ratha, J.H. Connell, and R.M. Bolle, "Biometrics break-ins and band-aids," *Pattern Recognition Letters*, vol. 24, no. 13, pp. 2105–2113, 2003.

[4] R.M. Bolle, J.H. Connell, and N.K. Ratha, "Biometric perils and patches," *Pattern Recognition*, vol. 35, no. 12, pp. 2727–2738, 2002.

[5] K. Nixon, V. Aimale, and R. Rowe, "Spoof detection schemes," *Handbook of biometrics*, pp. 403–423, 2008.

[6] R.P. Wildes, "Iris recognition: an emerging biometric technology," *Proceedings of the IEEE*, vol. 85, no. 9, pp. 1348–1363, 1997.

[7] U.C. von Seelen, "Countermeasures against iris spoofing with contact lenses," in *Biometric Consortium Conference BC2005*, 2005.

[8] T. Matsumoto, "Gummy finger and paper iris: An update," in *Proceedings of the 2004 Workshop on Information Security Research*, 2004.

[9] X. He, Y. Lu, and P. Shi, "A fake iris detection method based on fft and quality assessment," in *Pattern Recognition, 2008. CCPR'08. Chinese Conference on*. IEEE, 2008, pp. 1–4.

[10] R. Chen, X. Lin, and T. Ding, "Liveness detection for iris recognition using multispectral images," *Pattern Recognition Letters*, 2012.

[11] E.C. Lee and K.R. Park, "Fake iris detection based on 3d structure of iris pattern," *International Journal of Imaging Systems and Technology*, vol. 20, no. 2, pp. 162–166, 2010.

[12] Y. He, Y. Hou, Y. Li, and Y. Wang, "Liveness iris detection method based on the eye's optical features," in *Security+ Defence*. International Society for Optics and Photonics, 2010, pp. 78380R–78380R.

[13] E.C. Lee, Y.J. Ko, and K.R. Park, "Fake iris detection method using purkinje images based on gaze position," *Optical Engineering*, vol. 47, no. 6, pp. 067204–067204, 2008.

[14] NB Puhan, N. Sudha, and A. Suhas Hegde, "A new iris liveness detection method against contact lens spoofing," in *Consumer Electronics (ISCE), 2011 IEEE 15th International Symposium on*. IEEE, 2011, pp. 71–74.

[15] Hui Zhang, Zhenan Sun, and Tieniu Tan, "Contact lens detection based on weighted lbp," in *Pattern Recognition (ICPR), 2010 20th International Conference on*, aug. 2010, pp. 4279 –4282.

[16] J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris liveness detection based on quality related features," in *Biometrics (ICB), 2012 5th IAPR International Conference on*, 29 2012-april 1 2012, pp. 271 –276.

[17] S. Venugopalan and M. Savvides, "How to generate spoofed irises from an iris code template," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 2, pp. 385 –395, june 2011.

[18] S. Shah and A. Ross, "Generating synthetic irises by feature agglomeration," in *Image Processing, 2006 IEEE International Conference on*, oct. 2006, pp. 317 –320.

[19] Jinyu Zuo, Natalia A. Schmid, and Xiaohan Chen, "On generation and analysis of synthetic iris images," *Information Forensics and Security, IEEE Transactions on*, vol. 2, no. 1, pp. 77 –90, march 2007.

[20] John Daugman, "Demodulation by complex-valued wavelets for stochastic pattern recognition," *International Journal of Wavelets, Multiresolution and Information Processing*, vol. 1, no. 01, pp. 1–17, 2003.