Analysis of Vulnerabilities of Iris Scanning Personal Authentication

Michael J.S. Kang, Oscar T. Plag, *UBC Engineering Physics*

April 7, 2007

***Abstract*—This report provides an analysis of fundamental vulnerabilities in iris scanning authentication technology. Iris scanning is a growingly popular form of biometric identification, and vulnerabilities that exists is it can be exploited if the appropriate techniques are applied. The proposed method of spoofing is the Microlithographic Iris Spoofing Attack Approach, or MISAA.**

***Index Terms*— Biometrics, iris scanning, vulnerability, spoofing, photoablation**

I. Introduction

Biometric identification is a growing field of personal authentication. Instead of using things that you know or that you posses (e.g. passwords, keycards) for identification, biometrics uses physiological or behavioural characteristics. There are many different types of biometric identifiers that are or have been used in the past. These range from very well known traits such as fingerprints or voice patters to some more obscure or newly developed ideas like a persons keystroke pattern (the way a person types). Iris recognition is a strong form of biometric identification. Iris scanning technology consists of comparing the texture of a subject's iris. An Iris is a particularly strong identifier for several reasons. Firstly there is a very large amount of data within a persons Iris, and this data differs substantially from user to user, in fact, it even differs significantly from left eye to right. Secondly, a person's iris is very stable from birth until death, meaning that once a person is scanned their iris, barring any unforeseen eye trauma, will not change[3]. Iris scanning is becoming more commonplace, even finding its way into the house office legislative counsel[9]. The proposed method of attack on an iris scanner found in this report focuses on unsupervised iris scanning. This may at first appear to be somewhat useless, with the lack of commonplace iris scanners. However with the ironing out of some bugs, iris scanners are likely to become much more common in banks, airports, and other businesses, and especially in personal workstations[15].

II. Existing Iris Recognition Technology

A. Anatomical Background of Iris

An iris is a part of the human eye that regulates the amount of light that enters the organ and makes contact with the retina. It is formed out of fibrovascular tissue known as stroma, and is connected on the anterior surface to two sets of muscles: the dilator muscles and the sphincter muscles. Photosensitive cells inside the eye sense the levels of light that enter it, and the iris then contracts or expands due to the pupillary reflex. In very dim light, the pupillary reflex causes the dilator muscles to open the pupil, which is the whole in the centre of the iris, allowing more light to enter. In bright light, the pupillary reflex causes the sphincter muscles to contract, making the pupil smaller and allowing less light to enter.

Other relevant features of the eye include the cornea, the aqueous humor, and the lens. The cornea is a thin layer if tissue that covers the front of the eye, underneath which is the aqueous humor, a liquid pocket that covers the posterior surface of the iris. On the anterior surface of the iris are the aforementioned sphincter and dilator muscles, behind which is the lens, which focuses light onto the retina, the organ that is sensitive to the light and allows one to see[14]. The anatomy of the human eye can be seen in figure 1.1.

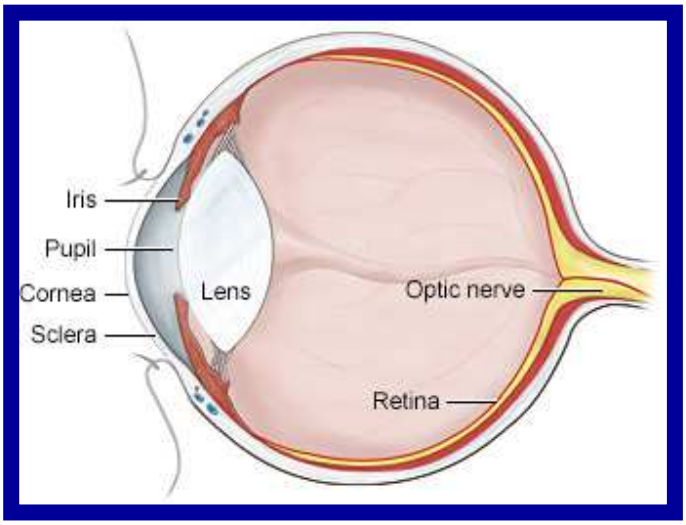

Figure 1.1: The Anatomy of the Human Eye

B. Iris Identification with Existing Technology

Under the existing technology, the first step in the identification of a human iris is the acquisition of a high resolution (640 by 480), 8-bit grayscale image of the iris using a CCD camera[4]. The iris is illuminated using an infrared imager in order to effectively highlight the texture. Depending upon the application, image acquisition generally takes 1 to 2 seconds and can required to user to stand anywhere from 3 inches to 3 feet from the acquisition camera[3].

Generally, only a portion of the iris image is actually used for identification. Portions of the top and bottom of the iris image are ignored to account for eyelid occlusion of the iris image[3].

One the iris image has been acquired, the image undergoes 2-Dimensional Gabor Filtration, a data processing algorithm used to turn biometric information into template code. This large set of binary data is termed "iris code", and is typically 512 kb in size. Iris code is generated by taking the image data at each coordinate of the grayscale image and convolving it with the following double dimensionless function[5]:

$G(x, y; \theta, \omega) = exp\{-1/2 [x'2 / A 2 + y'2 /B2]* exp (i\omega(x+y))$
in which $x' = x \cos \theta + y \sin \theta$,
$y' = y \cos \theta - x \sin \theta$,

and *A, B,* co-vary inversely proportional to ω, all of which can be chosen. The variable θ is the chosen orientation of the filter, which can vary between 0 and 360 degrees.
This is a complex valued convolution, so it outputs real and imaginary parts. The iris code is generated by evaluating the real and imaginary parts *G* at each coordinate *(x,y)* of the image. The iris code bit pairs (h_{Re} ,h_{Im}) are generated depending on the sign of *Re(G)* and *Im(G)*[5]*:*

(if $G >= 0$, $h = 1$; if $G < 0$, $h = 0$)

The iris image is generally divided into 8 radial zones with 8 angular columns in each[3]. An example of an iris image, the 8 radial zones, and an iris code can be seen in figure 1.2.

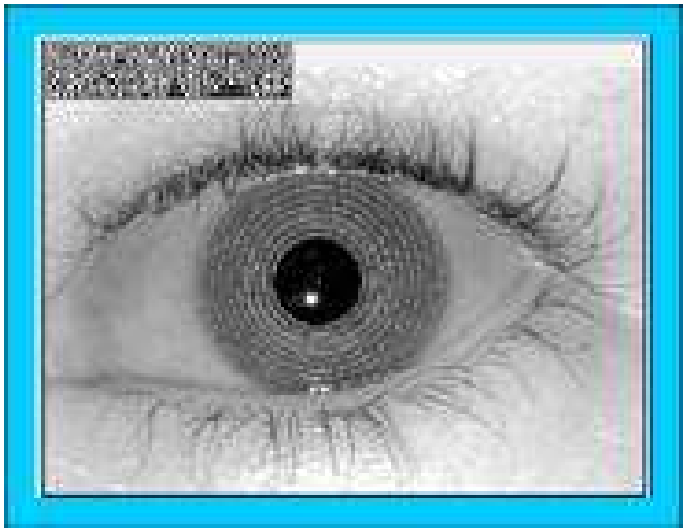

Figure 1.2: An Iris Image and Iris Code

After the code has been generated, comparison between the data and the control data (the already-verified iris code against which the image must be authenticated) is done using the Hamming Distance as follows. Unverified code X is compared to unverified code Y with an XOR of each bit of the iris code. The results of this operation are summed across the entire length of the code and divided by this length, giving a ratio that represents how "far away" a set of data is from a control.

$$HD = 1/N \Sigma X_i \text{ (XOR) } Y_i \quad (i=1..i=N)$$

It has been shown experimentally that the odds of false positive or false negative are 1 in 1.2 million if HD threshold is 0.342. So, if the result is less than 0.342, the system determines it to be a match. Otherwise, the image is rejected as a non-match[5]. The Hamming Distance is used in this way because it is virtually impossible to record the same result more than once when scanning even an identical iris.

C. Approaches to Spoofing

At first glance, there appears to be two fairly simple ways of faking an iris for use in an iris scanner. The simplest and most obvious approach would be to print a fake iris, based on a high resolution image and to show this image to the image acquisition software. The second and significantly more robust approach would be to use a high-resolution display (allowing for movement of the eye) of the iris to be spoofed.

D. Existing Countermeasures to Obvious Spoofing Approaches

inspection it is very clear that neither of the two aforementioned spoofing methods is capable of fooling even the most basic iris scanner. To ensure that the thing being scanned is not simply an image, most scanners vary the light level present and check to make sure that the iris dilates or contracts as would be expected. Some scanners also look for the presence of dither patterns, which are patterns left by printers while mixing pixels to try to approximate colours not available in the palette. A fairly simple countermeasure that some scanners have against the use of a high resolution digital display is an analysis of the temporal frequency spectrum, in other words looking for the presence refresh rate. Many scanners also have some simple countermeasure that would prevent either of the two simple spoofing methods from being used. They can check for movement of the entire eye (i.e. ask you to look left, right, up, down, etc.), or for the presence of the red-eye effect. Some scanners even look for the reflections from other components of the eye, namely the cornea and the lens. As light waves change interfaces, the reflected portion of the wave energy comes back a total of 4 times: twice from each surface of the cornea and twice from each surface of the lens. These reflections can be measured to verify the presence of these parts of the eye.

E. Vulnerabilities to Currently Implemented Countermeasures

All of the aforementioned existing countermeasures against fake irides only check if the iris is from any real eye, not a specific eye. This means that, once the system has acquired the iris code, all other tests it performs do not depend on the identity of the subject; they only depend on whether or not the subject is a human being with normal eye features. In addition, the image that is acquired of the iris is monochromatic, so all information about iris colour is lost through the image acquisition process. This immediately reduces the degrees of freedom for the iris image, greatly

reducing the necessity for complexity in a spoofing attack.
There is only one unique characteristic about the iris that is used for authentication or verification, the iris texture. This clearly violates one of the principals of designing secure systems, Principal 9: Defense in Depth. As such, all that would be necessary for the attacker to do is spoof the iris texture and convince the system that the iris comes from any real eye.
This is a fundamental weakness of the technology: no iris colour or any other identifiable biometric data are used in iris scanning.

III. The Microlithographic Spoofing Approach

In light of the inherent vulnerabilities that are evident in the existing countermeasures to spoofing approaches, it is proposed that an advanced approach to spoofing is possible.
This approach proposed in this report, termed "The Mircolithographic Iris Spoofing Attack Approach (MISAA)", begins with the acquisition of a high resolution image of a person's iris to be spoofed. For the purposes of this report, no specific methodology for the acquisition of such as image is suggested as this is not the focus of the attack approach. It is assumed that, whether through subterfuge, spying, or some other method, a high-resolution image of someone's iris could be fairly easily obtained.
Upon the acquisition of an iris image, step two of MISAA would involve recreating the texture of the victim's iris on some type of flexible membrane. This would lead into step three, the mounting of the spoofed iris onto an adjustable aperture so that the pupillary reflex of the pupil could be recreated. Finally, additional eye features, which would be cosmetic and non-functional, would be added to the system to circumvent other countermeasures to spoofing attacks in iris scanning technology.

A. Recreating Iris Texture

An attack approach such as this poses a significant technical challenge to a would-be attacked: how one can recreate an iris texture. There exist many methods of machining of materials in high resolution and recreating very fine textures. For example, gelatinous or plaster moulds, electron beam lithography, and milling can all remove material from some kind of sample or substrate with a high degree of accuracy. However, in order to be able to provide extremely high precision, predictability of results, and very high texture resolution, excimer laser microlithography is an intriguing approach. Excimer laser microlithography, which uses high density UV radiation with wavelengths of 351 nm to 157 nm, has comparable resolution to that of electron beam lithography, except that it has the ability to remove much more material from the substrate in a given amount of time[16].
Excimer pulse laser lithography works as a micromachining method through the process of photoablation, the process of subliming, or vaporizing, solid material with limited thermal effects through exposure to near ultraviolet radiation from a laser[16]. This is the exact technology that is used to reshape the lens of the human eye during laser eye surgery.
This approach has a very high resolution (on the order of 1 μm), which is necessary in order to dodge the aforementioned countermeasure of the 2-D spectral analysis searching for dither patterns[14].
The process of texture recreation through excimer laser photablation follows the photoablation equation:

(desired depth at each point) ÷ (material ablated per pulse) = number of pulses at each point

It is a known parameter of any excimer laser what depth of material will be ablated by one pulse at a known fluence (special energy density) for any given material. The grayscale image of the iris will have shadows and lighter spots that indicate the presence of freckles, dimples, ridges, etc. for an iris. In the proposed MISAA process, the image could be translated into numbers at from 0 to 255 corresponding to the level of saturation at each image coordinate (which is already the case for an 8-bit monochromatic image), and this number could then be mapped to the laser instruction code: one extreme corresponding to a very deep ablation, and the other extreme corresponding to no ablation at all. This would recreate the iris texture.
With this concept in place, the next challenge is to find a material that has two main characteristics: it that can be machined using laser photoablation, and it has an appropriate elastic modulus to be able to simulate pupillary reflex.
It is common knowledge among photoablation researches that many organic polymers respond to photoablation. Materials like PTFE, PMMA, and other plastics can often be photoablated, but most of them are quite stiff and would not be able to undergo enough stretching to be able to recreate the pupillary reflex[11].
However, a material was found that did have the correct properties. The human iris has an elastic modulus of 9-10 kPa radially[12], and there exists an organic polymer known as light permelastic Polysulfide that has an elastic modulus of 11.3 kPa[11]. These numbers are of a similar magnitude, and this material can be photoablated using excimer laser UV radiation[13]. As such, polysulfide would be suitable material for this attack approach.
The elastic modulus of this material does not have to match exactly that of the human iris, but merely be comparable. If the material is too stiff, it will not be able to easily undergo the contraction and expansion necessary for recreation of the pupillary reflex. The aforementioned elastic modulus of the human iris is given for the radial direction; the modulus on the angular direction is much greater. Polysulfide is an axially homogeneous polymer, so the elastic modulus is the same in all directions. As such, the radial modulus of polysulfide is, as mentioned, 11.3 kPa[11].

B. Recreating Pupillary Reflex

In order to recreate the pupillary reflex, the fake polysulfide iris would be mounted on a device with an electronically controllable pupil dilation device. It is proposed that an adjustable aperture be used for this. An aperture is a whole of an adjustable radius, just like the device used to regulate the amount of light entering a camera. The normal range of human pupil dilation is 1.5mm to 8.0mm, and an adjustable aperture device, the Melles Griot 04 IDM 001 Actuated Iris, has a range of 1.0 to 8.5 mm. Any part with similar specifications would work for this application, but the point is that there exist apertures within the appropriate range.

The proposed process would have the fake iris attached to the aperture with two rings of adhesive: one on the anterior surface of the limbus (the outer edge of the iris), and one on the anterior surface of the pupil. The limbus ring of adhesive would be used to hold the iris in place, and the pupil adhesive ring would be used to dilate and contract the iris as the aperture dilates and contracts. This concept is shown in figure 1.3 below.

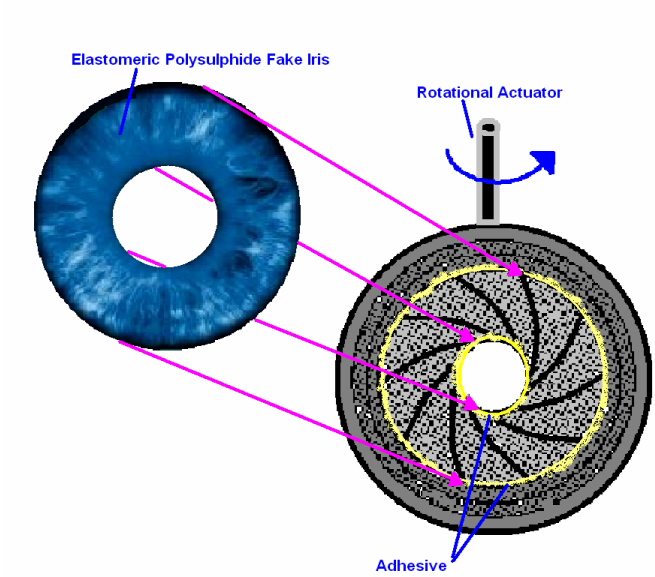

Figure 1.3: Mounting of the Fake Iris

The pupillary reflex of the pupil involves three observable actions: the dilation of the pupil in dim light, the contraction of it is bright light, and the random fluctuation of it due to the biological control process that governs its movement.

In order to spoof this process, a system would be set up using a photodiode or phototransistor to measure the incoming light level, a microcontroller with a programmed algorithm to adjust the iris accordingly and incorporate randomness, and a servo to mechanically control the iris actuator that dilates and contracts the polysulfide annulus. The actual algorithm has not been determined; however, due to the fact that existing scanning technologies only check that the reflex is occurring but do not quantify the algorithm by which it is taking place.

C. Additional Necessary Features to Spoofing Approach

As mentioned before some scanners check for the physical movement of the eye and for the presence of other components to the eye (such as: the cornea, lens, etc.). This however, poses no great problem for the design. The movements could be quite easily replicated by the presence of two rotational actuators that would be controlled by the microcontroller. Since the scanners that check for other components to the eye only check for their presence and not actually for their functionality, simple plastic replicas could be created that should have no trouble in fooling these scanners.

An illustration of the overall design concept is shown in figure 1.4, and representation of the overall software concept is shown in figure 1.5.

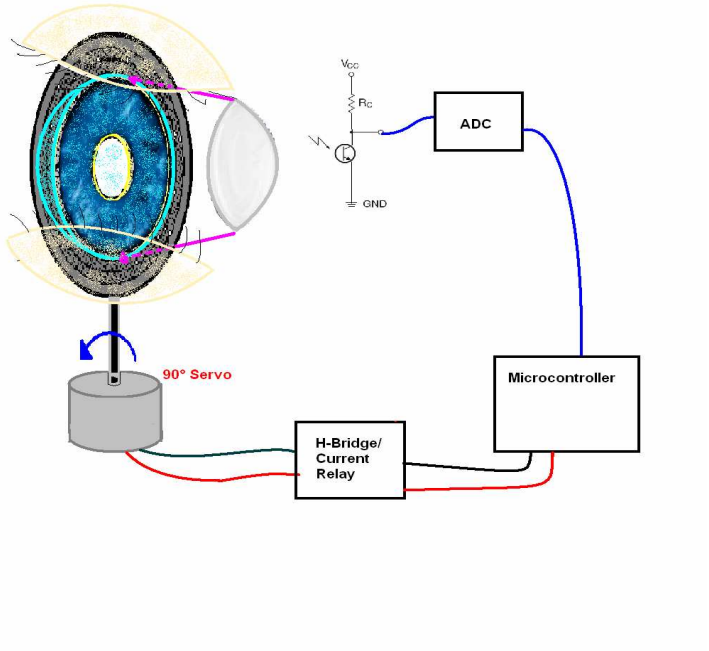

Figure 1.4: The MISAA Overall Design Concept

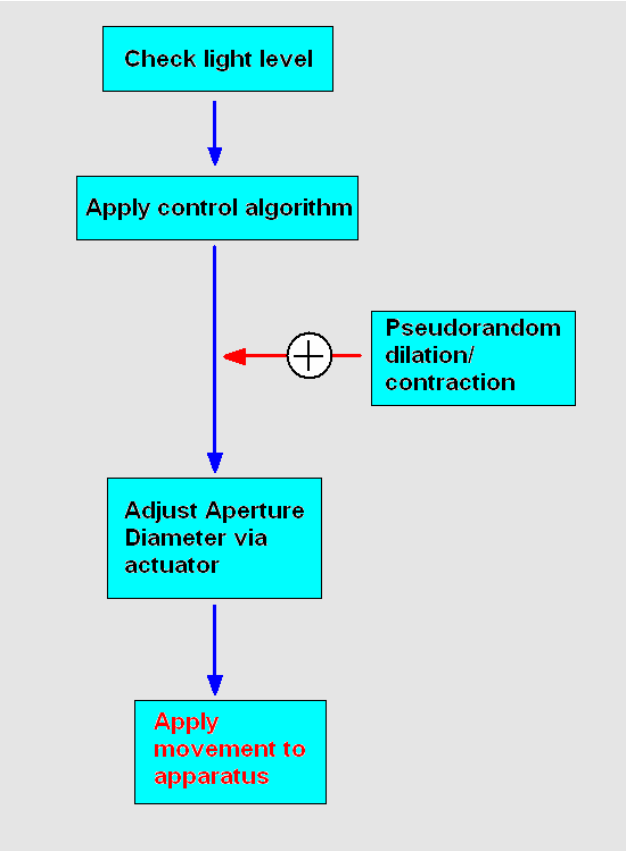

Figure 1.5: The MISAA Software Concept

IV. Conclusion

Iris scanning is a very strong form of biometric identification and authentication, but it is not infallible. Iris scanning technology acquires an image of the subject's iris and quantifies it into iris code, but only uses one unique identifier to accomplish this: the iris texture. With the proposed MISAA approach, the texture can be recreated, and the countermeasures that are currently in place to guard against fake irides can be circumvented.

References

[1] John Chirillo; Scott Blaul, Implementing Biometric Security, pp-pp, Wiley Publishing Inc., 2003
[2] Julian Ashbourn, Biometrics: Advanced Identity Verification, pp-pp, Springer-Verlag London Limited, 2000
[3] Samir Nanavati; Michael Thieme; Raj Nanavati, Biometrics: Identity Verification in a Networked World, pp-pp, John Wiley & Sons, Inc., 2002
[4] Ruud M. Bolle; Jonathan H. Connell; Sharath Pankatnti; Nalini K. Ratha; Andrew W. Senior, Guide to Biometrics, pp-pp, Springer-Verlag New York, Inc., 2004
[5] David D. Zhang, Automated Biometrics: Technologies and Systems, pp-pp, Kulwer Academic Publishers, 2000
[6] Dr. Qussay A. Salih; Vinod Dhandapani, "Iris Recognition Based on Multi-Channel Feature Extraction Using Gabor Filters", Proceedings of the IASTED International Conference, pp 168-173, January 23-25, 2006
[7] Javier R. Mollevan, "Tutorial on Gabor Filters", http://mplab.ucsd.edu/tutorials/pdfs/gabor.pdf, 2005
[8] John Daugman, " How Iris Recognition Works", University of Cambridge, The Computer Laboratory, January 2004
[9] Dipka Bhambhani, "The Eyes Have It: House Office Signs on Iris Scanning", http://www.washingtontechnology.com/print/17_8/18571-1.html , Washington Technology, Vol. 17 No. 8, 07/15/02
[10] Combined Research and Curriculum Nontraditional Manufacturing (NTM), Laser Machining Processes: Level 1 Section 5.2: Introduction to Laser Machining of Polymers, http://www.mrl.columbia.edu/ntm/level1/ch05/html/l1c05s02.html, Manufacturing Research Laboratory, 10/27/06
[11] Dr William J. O'Brien, "Elastic Modulus E", http://www.lib.umich.edu/dentlib/Dental_tables/Elasmod.html, Biomaterials Properties Database, University Michigan, Quintessence Publishing, 1996
[12] Eric C. Huang; Victor H. Barocas, "Accommodative Microfluctuations and Iris Contour", Journal of Vision (2006) 6, pp 653-660
[13] Jean-marc Bureau; Gerard Coussot, "Mechanical Sensor Produced from a polymer film", http://www.patentstorm.us/patents/5437195-description.html, United States Patent 5437195, Issued on August 1, 1995
[14] Iris Anatomy, http://en.wikipedia.org/wiki/Iris_%28anatomy%29, Wikipedia ,The Free Encyclopedia, 4 April 2007
[15] Joe Kissell, "Iris Scans: A new angle on photo identification", http://itotd.com/articles/212/iris-scans/, Interesting Thing of The Day, June 11, 2004
[16] Erol C Harvey, Phil T Rumsby, Malcolm C Gower, Jason L Remnant; "Microstructuring by Excimer Laser", date unknown, http://www.exitech.co.uk/pdfFiles/Microstructuring%20by%20Excimer.pdf