International Journal of Electrical Electronics Computers & Mechanical Engineering (IJEECM)
ISSN: 2278-2808
www.ijeecm.org Volume 6 Issue1 ǁ Jan. 2018

IJEECM journal of Computer Science Engineering (ijeecm-jec)

Pattern Matching based Iris Recognition System

Panchadarla jayalakshmi[1], Bhaghyasree manepalli [2] , G.Phani Kumar[3]

[1,2] *Electronics and Communication Engineering Department,*

[1,2,3] Sai Ganapathi Engineering College, Visakhapatnam, Andhra Pradesh., India.

Abstract: **Iris biometrics is widely recognized as being one of the most practical biometrics in use today. The iris of the human eye is the angular region between the pupil and sclera. The iris pattern consists of complex and distinctive ligaments, furrows, ridges, rings, corona, freckles and collarette. Also, the iris is relatively stable over the lifetime of a person starting from the eighth month of gestation and demonstrates high pattern variability, even for identical twins and between the left and right eye of the same person. These characteristics make the iris a very suitable candidate for biometric user authentication in smart phones. a novel liveness detection method that exploits the acquisition workflow for iris biometrics on smart phones using a hybrid visible (RGB)/near infra-red (NIR) sensor. This is able to capture both RGB and NIR images of the eye and iris region in synchronization.**

Keywords: Smartphone, consumer biometrics, iris recognition, liveness.

I.INTRODUCTION

Traditionally biometrics has been used for many years by law enforcement to establish the identity of criminals and by government and industry to secure and restrict access to resources and facilities. In such applications biometric technology is employed in a supervised use-case – another person oversees the authentication procedure in order to ensure correctness. More recently, biometric technology has been employed in non-consensual use-cases such as airports, train-stations and similar public areas. In these example use cases there is limited scope for 'spoofing' a user biometric. However when biometric technology is adapted for use on a consumer device, the acquisition process differs significantly as it represents an "unsupervised" use-case. As fingerprint authentication was the first technology to be widely adopted in mobile devices there are many examples of 'spoofing' techniques and countermeasures in the literature.

A. Smartphones**:** Since the introduction of first smartphone in 1994, there has been a rapid evolution of smartphone technology to a point where it plays a central role in our day to day life. Approximately 2 billion people will be using a personal smartphone in 2016, which is expected to grow to a third of the world's population in 2018. These devices have become much more than a computer, providing the functions of a phone, a personal database, an infinite jukebox, a camera, a hub for location based services and a gateway to all the information in the world. It is speculated that the smartphone's role as a constant companion, helper, coach and guardian has only just begun. The majority of these devices are connected to the Internet all the time. As many as 57% of U.S. smartphone users are reported to carry out online banking through these device As today's smartphones are increasingly used to transmit sensitive financial and personal information, a reliable assessment of smartphone user's identity is emerging as an important new service. PIN or passwords may not be sufficient for this purpose, but personal biometrics could be effectively used .

B. Iris Biometrics on Smartphones.

Iris biometrics is widely recognized as being one of the most practical biometrics in use today The iris of the human eye is the annular region between the pupil and sclera. The iris pattern consists of complex and distinctive ligaments, furrows, ridges, rings, corona, freckles and collarette Also, the iris is relatively stable over the lifetime of a person starting from the eighth month of gestation and demonstrates high pattern variability, even for identical twins and between the left and right eye of the same person These characteristics make the iris a very suitable candidate for biometric user authentication in smartphones. The implementation of iris biometrics on smartphone devices has recently become an emerging research topic As the use of iris biometrics on smartphone devices becomes more widely adopted, it is to be expected that there will be similar efforts in the research community to beat the biometric by exploring new spoofing methods and this will drive a corresponding requirement for new liveness detection methods.

Smartphone user authentication using iris biometrics is a remote and unsupervised form of authentication. In other words, only the person performing the authentication needs to be present during the process workflow. As a

consequence, it is more susceptible to spoofing of the biometric input than traditional authentication techniques such as PIN entry at a point-of-sale terminal where the sales clerk is present. Spoofing attack on biometric system is an artificial mimic of a real biometric to gain access to the device and its services. This become worrisome as the iris biometric sample can be recorded without user co-operation. Hence it is essential to build in protection against attacks into such a system. Various types of spoofing include presenting a picture, a recorded video or a high quality iris image kept in front of original eye while trying to use iris authentication. These attacks are collectively called 'presentation attacks'. Liveness detection is an anti-spoofing technique to determine if the biometric being acquired is an actual measurement from a live person who is present at the time of capture. Arguably, human supervision can be the most effective way for detecting such presentation attacks and widely used in many applications including UAE border control program. But, it is impractical in the case of smartphones and other consumer electronic devices. Hence, effective automatic liveness detection is necessary. Czajka categorizes the automatic liveness detection techniques into three categories: (a) extraction of intrinsic properties of a living body, (b) analysis of involuntary signals and (c) challenge-response method. The extraction of intrinsic properties includes analyzing spectrographic properties of the human eye, analyzing red-eye effect or analyzing 3-D curvature of iris surface. Examples for analyzing involuntary body signals include eyelid movements and hippus. The third category mainly considers user's response when prompted to carry out some tasks like blinking, or looking at a different direction. A detailed literature review of iris liveness detection can be found. Even though liveness detection is an essential part of iris recognition system as a countermeasure against spoofing, it comes with the cost of an increase in processing time, increase in hardware or software and negative effect on recognition performance.

Background:

Ophthalmologists Alphonse Bertillon and Frank Burch were one among the first to propose that iris patterns can be used for identification systems. In 1992, John Daugman was the first to develop the iris identification software. Other important contribution was by R.Wildes et al. Their method differed in the process of iris code generation and also in the pattern matching technique. The Daugman system has been tested for a billion images and the failure rate has been found to be very low. His systems are patented by the *Iriscan Inc*. and are also being commercially used in Iridian technologies, UK National Physical Lab, British Telecom etc.

This paper consists of six main parts, which are image acquisition, preprocessing, iris localization, normalization, encoding and the iriscode comparison. Each section describes the theoretical approach and is followed by how it is implemented. The paper concludes with the experimental results in the appendix. the standard deviation, σ and it is taken to be 2 in this case.

II. PROJECT DESCRIPTION

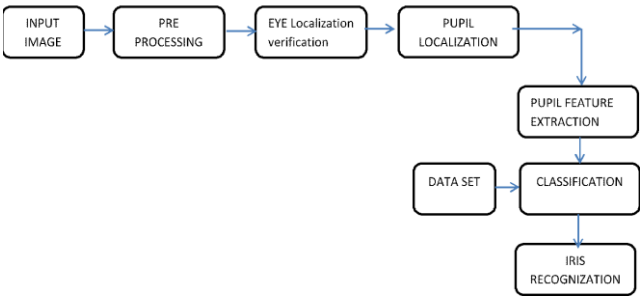

FIG 1. Algorithm For Implementing The Iris Detection

filtering and decimation are done simultaneously in the convolution stage. this algorithm implements edge enhancement and edge detection. edge enhancement is done using laplacian filter mask the edge image obtained using laplacian filter mask is scaled and added to the original image to enhance the edges. the images obtained after convolution of the original image with each of these masks are added to give the edge detected image. mean is calculated for the edge detected image and then thresholding is done to find the person identification.

III.IMPLEMENTATION:

1 IMAGE ACQUISITION

This step is one of the most important and deciding factors for obtaining a good result. A good and clear image eliminates the process of noise removal and also helps in avoiding errors in calculation. In this case, computational errors are avoided due to absence of reflections, and because the images have been taken from close proximity. This project uses the image provided by CASIA (Institute of Automation, Chinese Academy of Sciences, http://www.sinobiometrics.com/) These images were taken solely for the purpose of iris recognition software research and implementation. Infra-red light was used for illuminating the eye, and hence they do not involve any specular reflections. Some part of the computation which involves removal of errors due to reflections in the image were hence not implemented.

THE HUMAN EYE:

The human vision system (HVS) behaves like a band pass filter for spatial frequencies with bad sensitivity to small colors variation (eg. image compression) but it operates over 10 orders of magnitude of illumination. The retina is

composed of two kind of photoreceptors:_ About 100 millions of rods provide scotopic vision (low illumination, high resolution, black & white)._ About 6.5 millions of cones in the center of the retina (fovea) provide photopic vision (high illumination, low resolution, colors).
The combination of the rods and cones (intermediate illumination)provide colors vision with high resolution and high sensitivity tointermediate spatial frequencies (eg. edges).

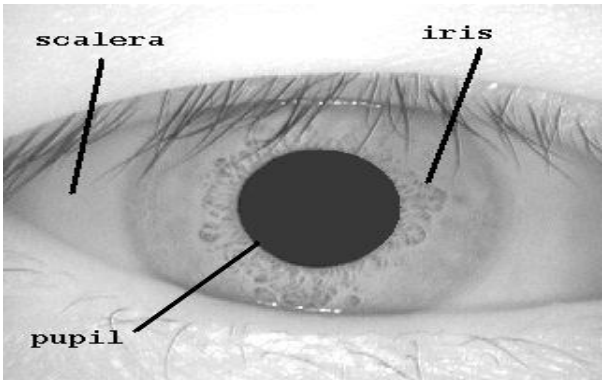

Fig 2. Human Eye

IMAGE PREPROCESSING

Due to computational ease, the image was scaled down by 60%. The image was filtered using Gaussian filter, which blurs the image and reduces effects due to noise. The degree of smoothening is decided by

Figure 3: Canny edge image

Edge detection is followed by finding the boundaries of the iris and the pupil. Daugman proposed the use of the Integro-differential operator to detect the boundaries and the radii. It is given by

$$\max_{(r,x_0,y_0)} \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} ds \right|$$

This behaves as a circular edge detector by searching the gradient image along the boundary of circles of increasing radii. From the likelihood of all circles, the maximum sum is calculated and is used to find the circle centers and radii.

The Hough transform is another way of detecting the parameters of geometric objects, and in this case, has been used to find the circles in the edge image. For every edge pixel, the points on the circles surrounding it at different radii are taken, and their weights are increased if they are edge points too, and these weights are added to the accumulator array. Thus, after all radii and edge pixels have been searched, the maximum from the accumulator array is used to find the center of the circle and its radius. The Hough transform is performed for the iris outer boundary using the whole image, and then is performed for the pupil only, instead of the whole eye, because the pupil is always inside the iris.

There are a few problems with the

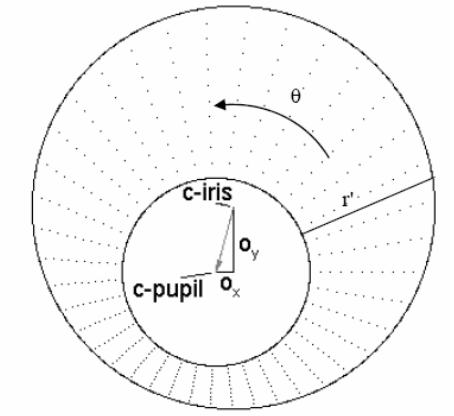

Figure 4 : Normalization process

$$r' = \sqrt{\alpha}\beta \pm \sqrt{\alpha\beta^2 - \alpha - r_I^{\,2}}$$

where r1 = iris radius

$$\alpha = o_x^2 + o_y^2$$

$$\beta = \cos\left(\pi - \arctan\left(\frac{o_y}{o_x}\right) - \theta\right)$$

The radial resolution was set to 100 and the angular resolution to 2400 pixels. For every pixel in the iris, an equivalent position is found out on polar axes. The normalized image was then interpolated into the size of the original image, by using the interp2 function. The parts in the normalized image which yield a NaN, are divided by the sum to get a normalized value.

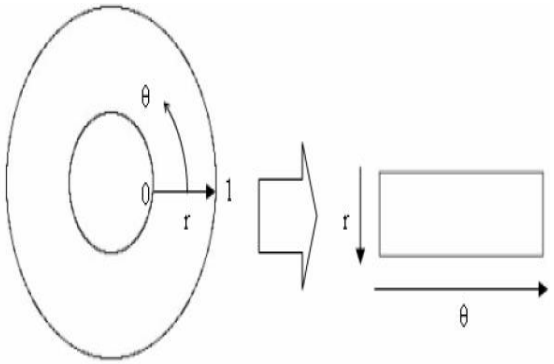

Figure 5: Unwrapping the iris

ENCODING

The final process is the generation of the iriscode. For this, the most become a better choice. LogGabor filters are constructed using

$$G(f) = \exp\left(\frac{-(\log(f/f_0))^2}{2(\log(\sigma/f_0))^2}\right)$$

Since the attempt at implementing this function was unsuccessful, the gabor- convolve function written by Peter Kovesi was used. It outputs a cell containing the complex valued convolution results, of the same size as the input image. The parameters used for the function were:

nscale = 1
norient = 1
minwavelength = 3
mult = 2
sigmaOnf = 0.5
dThetaOnSigma = 1.5

Using the output of gaborcovolve, the iriscode is formed by assigning 2 elements for each pixel of the image. Each element contains a value 1 or 0 depending on the sign + or – of the real and imaginary part respectively. Noise bits are assigned to those elements whose magnitude is very small and combined with the noisy part obtained from normalization. The generated IrisCode is shown in the appendix.

CODE MATCHING

Comparison of the bit patterns generated is done to check if the two irises belong to the same person. Calculation of Hamming Distance (HD) is done for this comparison. HD is a fractional measure of the number of bits disagreeing between two binary patterns. Since this code comparison uses the iriscode data and the noisy mask bits, the modified form of the HD is given by:

visible patterns are unique to all individuals and it has been found that the probability of finding two individuals with identical iris patterns is almost zero. Though there lies a problem in capturing the image, the great pattern variability and the stability over time, makes this a reliable security recognition system.

IRIS LOCALIZATION

The part of the eye carrying information is only the iris part. It lies between the scalera and the pupil. Hence the next step is separating the iris part from the eye image. The iris inner and outer boundaries are located by finding the edge image using the Canny edge detector.

The Canny detector mainly involves three steps, viz. finding the gradient, non-maximum suppression and the hysterisis thresholding. As proposed by Wildes, the thresholding for the eye image is performed in a vertical direction only, so that the influence due to the eyelids can be reduced. This reduces the pixels on the circle boundary, but with the use of Hough transform, successful localization of the boundary can be obtained even with the absence of few pixels. It is also computationally faster since the boundary pixels are lesser for calculation.

Using the gradient image, the peaks are localized using non-maximum suppression. It works in the following manner. For a pixel imgrad(x,y), in the gradient image, and given the orientation theta(x,y), the edge intersects two of its 8 connected neighbors. The point at (x,y) is a maximum if its value is not smaller than the values at the two intersection points.

The next step, hysterisis thresholding, eliminates the weak edges below a low threshold, but not if they are connected to a edge above a high threshold through a chain of pixels all above the low threshold. In other words, the pixels above a threshold T1 are separated. Then, these points are marked as edge points only if all its surrounding pixels are greater than another threshold T2. The threshold values were found by trail and error, and were obtained as 0.2 and 0.19.

Hough transform. Firstly, the threshold values are to be found by trial. Secondly, it is computationally intensive. This is improved by just having eight-way symmetric points on the circle for every search point and radius. The eyelashes were separated by thresholding, and those pixels were marked as noisy pixels, since they do not include in the iriscode.

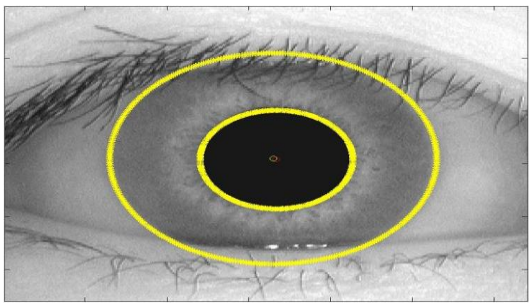

Figure 6: Image with boundaries

IMAGE NORMALIZATION

Once the iris region is segmented, the next stage is to normalize this part, to enable generation of the iriscode and their comparisons. Since variations in the eye, like optical size of the iris, position of pupil in the iris, and the iris orientation change person to person, it is required to normalize the iris image, so that the representation is common to all, with similar dimensions.

Normalization process involves unwrapping the iris and converting it into its polar equivalent. It is done using Daugman's Rubber sheet model. The center of the pupil is considered as the reference point and are mapping formula is used to convert the points on the Cartesian scale to the polar scale.

The modified form of the model is shown on the next page.

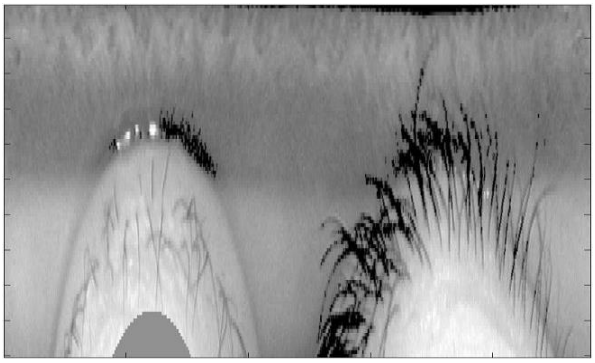

Figure 6: Normalized iris image

discriminating feature in the iris pattern is extracted. The phase information in the pattern only is used because the phase angles are assigned regardless of the image contrast. Amplitude information is not used since it depends on extraneous factors. Extraction of the phase information, according to Daugman, is done using 2D Gabor wavelets. It determines which quadrant the resulting phasor lies using the wavelet:

$$h_{\{Re,Im\}} = \mathrm{sgn}_{\{Re,Im\}} \int_{\rho}\int_{\phi} I(\rho,\phi) e^{-i\omega(\theta_0-\phi)} \cdot e^{-(r_0-\rho)^2/\alpha^2} e^{-(\theta_0-\phi)^2/\beta^2} \rho d\rho d\phi$$

where, $h_{\{Re,Im\}}$ has the real and imaginary part, each having the value 1 or 0, depending on which quadrant it lies in.

An easier way of using the Gabor filter is by breaking up the 2D normalized pattern into a number of 1D wavelets, and then these signals are convolved with 1D Gabor wavelets.

Gabor filters are used to extract localized frequency information. But, due to a few of its limitations, log-Gabor filters are more widely used for coding natural images. It was suggested by Field, that the log filters (which use gaussian transfer functions viewed on a logarithmic scale) can code natural images better than Gabor filters (viewed on a linear scale). Statistics of natural images indicate the presence of high-frequency components. Since the ordinary Gabor fitlers under-represent high frequency components, the log filters

Where, Xj and Yj are the two iriscodes, Xnj and Ynj are the corresponding noisy mask bits and N is the number of bits in each template.

IV.EXPERIMENTAL RESULTS

The images in the database had been specifically taken for research related to iris recognition and hence the boundaries between the iris, the pupil and the sclera were quite distinctive .

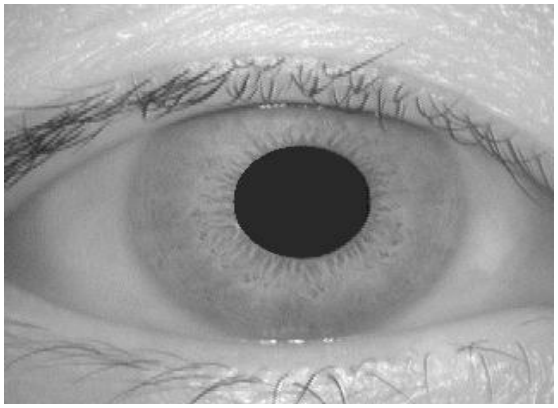

Figure 7. Input Image

The first step is taking input image from data base . The figure7 is input image taken from the dataset which is an RGB/ NIR image and this image is going to tested . This image is applied to a Gaussian noise filter for pre processing .

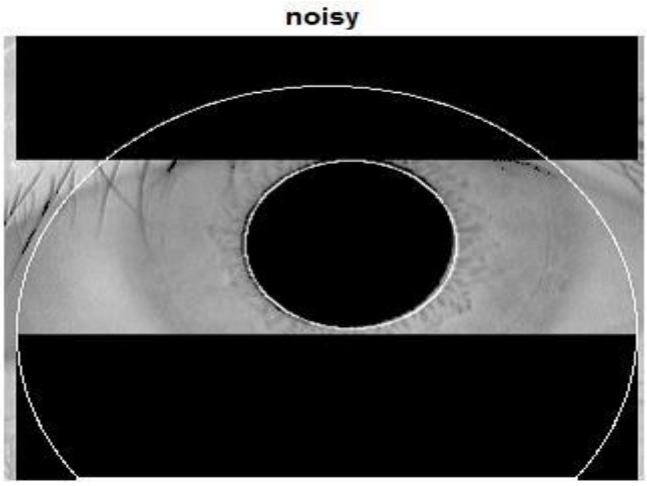

Figure 8 Noisy Image

In order to avoid the noise in the image we have convolve the image data with Gaussian noise function. The input image is given to Gaussian filter as the filter removes the noise present in the image. The figure 8 is noise removed figure of input image . The noise removal success rate is 80% .

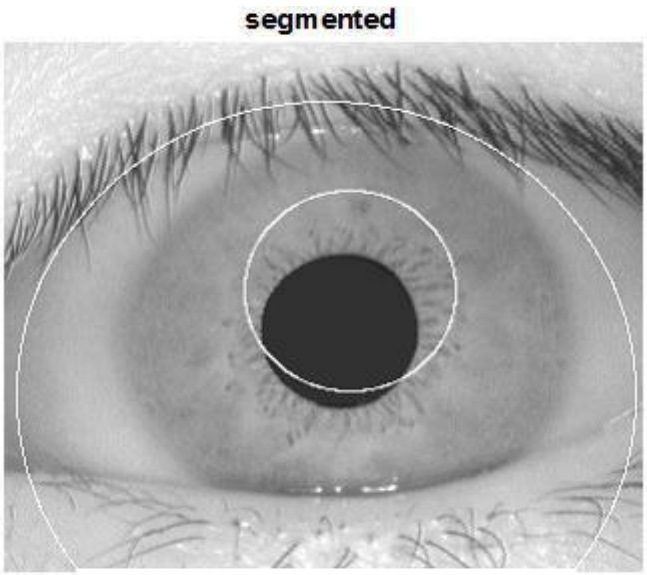

Figure9 .Segmented Image

The next stage of processing is edge detection of noise removed image .Here the used edge detector is Canny detection segmentation method for getting the Sharp edges. Edge Enhancement is done using Laplace filter mask the edge image obtained from Laplacian filter mask is scaled and added to the original image to enhance the edges. The figure 9 is segmented image using canny detection method.

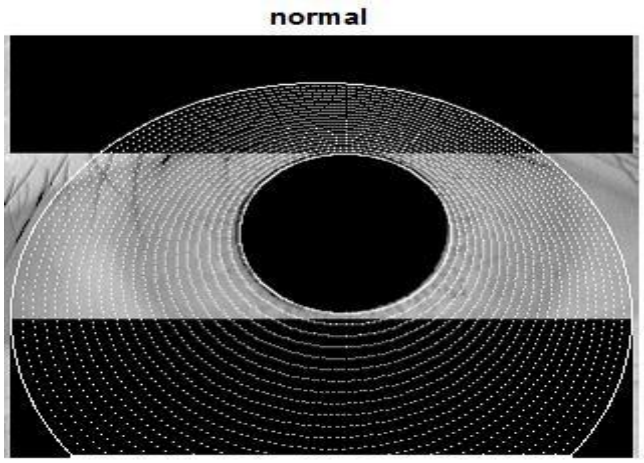

Figure 10 normalized iris

After edge detection and edge enhancement the iris is detected. this iris is compared with the already trained iris if is this iris is allowed to get access

Figure 11. polar image

Figure 12.noise

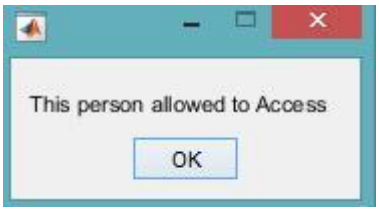

Figure 13. authentication message

V. CONCLUSION:

This paper presented pattern matching based iris recognition on smartphones. This technique relies on the capability of iris biometrics enabled smartphones to acquiring RGB and NIR image pairs simultaneously. This work can provide robust liveness detection without requiring additional hardware or significant change in the acquisition workflow. This paper explained the detailed workflow. the experimental results also shown that the proposed technique is effective for detecting a range of presentation attacks. The conclusions are that iris biometrics

can be made more robust than other well-known biometrics developing an improved database to verify this technique over a large range of people iris. This work can be further enhanced for the voice based authentication along with the iris recognition.

REFERENCES

[1] S. Curtis, "Smartphone at 20: IBM Simon to iPhone 6," The Telegraph, Aug. 2014.

[2] S. Curtis, "Quarter of the world will be using smartphones in 2016," The Telegraph, Dec. 2014.

[3] H. Orman, "Did you want privacy with that?: personal data protection in mobile devices," IEEE Internet Comput., vol. 17, no. 3, pp. 83–86, May. 2013.

[4] D. Siewiorek, "Generation smartphone," IEEE Spectr., vol. 49, no. 9, pp. 54–58, Aug. 2012.

[5] A. Smith, "U.S. Smartphone Use in 2015," Pew Research Centre, Apr. 2015. [6] N. L. Clarke and S. M. Furnell, "Authentication of users on mobile telephones - A survey of attitudes and practices," Comput. Secur., vol. 24, no. 7, pp. 519–527, Oct. 2005.

[7] P. Corcoran, "Biometrics and consumer electronics: a brave new world or the road to dystopia?" IEEE Consum. Electron. Mag., vol. 2, no. 2, pp. 22–33, Apr. 2013.

[8] C. Sousedik and C. Busch, "Presentation attack detection methods for fingerprint recognition systems: a survey," IET Biometrics, vol. 3, no. 4, pp. 219–233, Dec. 2014.

[9] D. Menotti, G. Chiachia, A. Pinto, W. R. Schwartz, H. Pedrini, A. X. Falcão, and A. Rocha, "Deep representations for iris, face, and fingerprint spoofing detection," IEEE Trans. Inf. Forensics Secur., vol. 10, no. 4, pp. 864–879, Apr. 2015.

[10] T. Ring, "Spoofing: are the hackers beating biometrics?," Biometric Technol. Today, vol. 2015, no. 7, pp. 5–9, Aug. 2015.

[11] E. Marasco and A. Ross, "A survey on antispoofing schemes for fingerprint recognition systems," ACM Comput. Surv., vol. 47, no. 2, pp. 1–36, Jan. 2015. [12] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1, pp. 4-20, Jan. 2004.

[13] J. Daugman, "How iris recognition works," IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1, pp. 21–30, Jan. 2004.

[14] A. Martin, "NTT Docomo takes another step into a future without passwords," Wall Street Journal, Japan, May. 2015.

[15] S. Thavalengal, P. Bigioi, and P. Corcoran, "Iris authentication in handheld devices – considerations for constraint-free acquisition," IEEE Trans. Consumer Electron., vol. 61, no. 2, pp. 245-253, May 2015.

[16] S. Thavalengal, I. Andorko, A. Drimbarean, P. Bigioi, and P. Corcoran, "Proof-of-concept and evaluation of a dual function visible/NIR camera for iris authentication in smartphones," IEEE Trans. Consumer Electron., vol. 61, no. 2, pp. 137-143, May 2015.