Advances and Applications in Mathematical Sciences
Volume 20, Issue 11, September 2021, Pages 2707-2714

AN APPROACH FOR INTELLIGENT MACHINE WITH HUMAN FACE COMPUTER VISION

R. KRISHNA ROHITH, Y. YESWANTH and B. NANDAKISHORE

Department of Computer
Science and Engineering
Pragati Engineering College
Surampalem, East Godavari
Kakinada, India
E-mail: rohith5453@gmail.com
yashwanthyash7ms@gmail.com
nandakishore14v@gmail.com

Abstract

A biometric device is a security identification and authentication device. These characteristics include fingerprints, facial images, and iris and voice recognition. In these we will bring face recognition tools which have better security. In this tool, the technique is to recognize eye veins in sclera the white portion of eye to build a strong security to our mobile; In addition to it we can implement an app for scanning Eye for Eye checkup using retina recognition to keep us healthy.

I. Introduction

Biometrics are body measurements and calculations related to human characteristics. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. A biometric device is a security identification and authentication device. Such devices use automated methods of verifying or recognizing the identity of a living person based on a physiological or behavioral characteristic. These characteristics include fingerprints, facial images, and iris and retina recognition. Face

2010 Mathematics Subject Classification: 68T10.

Keywords: recognise retina, eye veins detecting, face unlock, security, eye checkup, detecting eye problems.

Received October 9, 2020; Accepted November 11, 2020

unlocking tech was first introduced in Android 4 way back in 2011. Shocked right? Many of you, who used android 4 when it was introduced, may not even know about this. It was looked like a revolutionary feature at that time.

Unfortunately, it was very poor in security because it used to take our picture and store it when we used to unlock then it will match our face with that picture so it is easy to fool that technique. Now the latest technique is Iris Recognition to improve the face unlock technology iris recognition is used in order to counter the fools. But it is still developing. If we create a deep eye recognition feature in this face unlock system which is detecting eye veins and blood vessels which are unique for each person, then it will be very accurate to increase the security. In any situations, we can unlock and security level can't be breakable because individual has their own blood vessels in Eye veins so no one can match our patterns hence it is very tough to fool this technique.

II. Problems Encountered and Solutions to be Referred

Actually we used to scan retina to detect eye problems but the problem is to use Infrared ray of wavelength (~900nm-~1400nm) which cause damage to retina when we overexposed to that light.

Infrared radiations divided into the following three bands:

- IR-A (near-infrared): 760 and 1,400 nm.
- IR-B (mid-infrared): 1,400 and 3,000 nm.
- IR-C (far-infrared): 3,000 nm and 1 mm.
- The threshold limit values (TLVs) refer to values for incoherent (non-laser) visible and infrared radiation in the wavelength region of 305-3,000 nm that nearly all workers may be exposed to without adverse health effects.

Limits:

- retinal thermal injury from exposure to 385-1,400 nm radiation.
- retinal photochemical injury from chronic blue light (400-500 nm) exposure.

- possible delayed effects leading to cataract formation from exposure to 770-1,400 nm radiation.
- Thermal damage of the cornea, approximately 1,400 nm-1 mm.
- Thermal damage of the iris, approximately 380-1,400 nm.
- Near-infrared thermal damage of the crystalline lens, approximately 800–3,000 nm.
- Thermal damage of the retina 380-1,400 nm.
- "Blue-light" photochemical damage of the retina, principally 380-550 nm (300-550 nm for the aphakic eye).
- Photochemical damage of the eye from chronic exposure to bright light.

In such cases we can't scan retina in our mobiles for unlocking system so we just use eye vein scanners, implemented through IR emitters and camera which was already used to recognize iris. But as we mentioned previously iris recognition is not at all secure. Even while we setting a face unlock it will display a message that "face unlock is not better secure than pin, password, pattern."But there is no chance to copy eye veins patterns so it will be more secured.

III. Related Work

A. ZTE Eyeprint ID:

Eye print ID used the phone's high-resolution front camera to scan the user's eye, identifying blood vessel patterns that are unique to each individual. While that's a great way save costs, it's more prone to being fooled than modern infrared implementations. ZTE Hawkeye's technology would also have allowed users to control Android using eye motions

B. How an eyeprint id works? How to implement it further based on previous things we mentioned?

Eye print works by creating a map of the veins in your eyes, creating a secure ID. Then, when your device is locked, you press the power button and swipe down from the top of the display. You then look at the screen, from a

distance of around 15cm, and after around half a second, the Eye print function identifies you, allowing access to the inner workings of your Smartphone. Depending on your perspective, the fact that Eye print can only be set-up to identify one person at a time could be a good or a bad thing. We can also use this Eye print ID for payments app because it is most secured. In future we can also implement full eye blood vessels scan using this technology to check eye problems from normal Eye Infection to Age-Related Macular Degeneration (AMD).

C. How To Recognize Eye Blood Vessels In Eye Veins (White Portion Of Eye Ball)?

The veins in the sclera-the white part of the eyes can be imaged when a person glances to either side, providing four regions of patterns: one on each side of each eye.

Verification employs digital templates from these patterns, and the templates are then encoded with mathematical and statistical algorithms. These allow confirmation of the identity of the proper user and the rejection of anyone else. It detects and excludes eyelashes, eyelids, and specular reflections that typically block parts of the veins. The final result is a set of pixels containing only the patterns of blood vessels and veins iris. Advocates of eye vein verification note that one of the technology's strengths is the stability of the pattern of eye blood vessels; the patterns do not change with age, alcohol consumption, allergies, or redness. Eye veins are clear enough that they can be reliably imaged by the cameras on most smartphones. The technology works through contacts and glasses, though not through sunglasses. At least one version of eye vein detection uses infrared illumination as part of the imaging, allowing imaging even in low-light condition. Using that samples creating a map of the veins in your eyes, creating a secure ID. Then, when your device is locked, you press the power button and swipe down from the top of the display. You then look at the screen, from a distance of around 15cm, and after around half a second, the Eye print function identifies you, allowing access to the inner workings of your Smartphone simply unlocking your mobile after matching your eye veins and face patterns.

Figure 1. Model for Detecting Eye blood vessels along with iris and Eye veins for Biometric security for mobile.

Future Implementation: Deep Learning with Eyeprintscanner (Hawkeye) along infrared emitter and infrared camera can be used to detect those eye related problems. Researchers at New York Eye and Ear Infirmary of Mount Sinai (NYEE) have developed deep learning tools and algorithms to identify Eye problems. Using those algorithms that technique can be attached to our mobiles in front facing camera with Hawkeye's that the technology can be used for both unlocking the mobile (securing mobiles from unauthorized users) as well as detecting Eye problems. An App is developed for information regarding that scan; we can also add some features to share that result of scan to nearest Eye-Cares which have online consultancy, when it is complicated or emergency. Convolution neural networks are deep-learning algorithms adept at processing images, but researchers typically need to train them on more than a million medical images before they can test how well the algorithms work. Convolution neural network capable of learning with many fewer images. The algorithm identified critical cases of these conditions as accurately as six experts in ophthalmology. The algorithm also identified pediatric pneumonia from chest X-rays, suggesting that the technique could be broadly applied across medicine. OCT images obtained between 2010 and 2015 at Nagoya City University Hospital were obtained retrospectively. Patient information was synonymized and unconnected to OCT images before transfer to the study investigators.

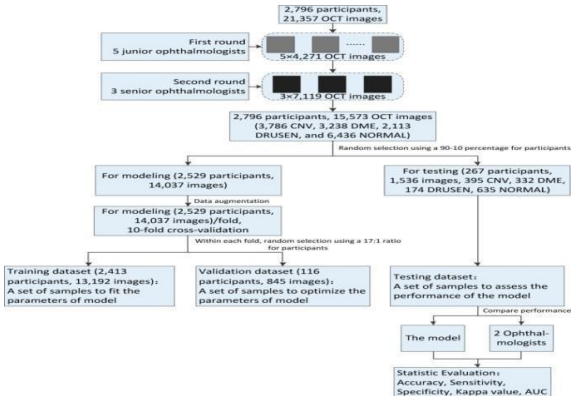

Figure 2. Training CNN with OCT to evaluate the reports and results.

In the current study, a pair of horizontal and sagittal fovea-centered sectional images obtained by Cirrus HD-OCT, Model 4000 (Carl Zeiss Meditec AG, Jena, Germany), was used. Images that were unclear because of hazy media such as dense cataracts, fixation failures during the image capture, and other reasons were excluded. Six hundred eyes of 300 patients were chosen randomly. A total of 1,200 OCT images of 600 eyes were collected. An experienced ophthalmologist (T. Y.) provided one diagnosis to a pair of OCT images in a masked fashion. When there were multiple diagnostic suggestions, the most pathological diagnosis was recorded. he model's precision and recall were calculated to evaluate the automated detection of macular diseases with five or more test images according to the following formulas: precision = (true_positive)/([truepositive] + [falsepositive]); recall = (sensitivity),(truepositive)/([truepositive] + [falsenegative])

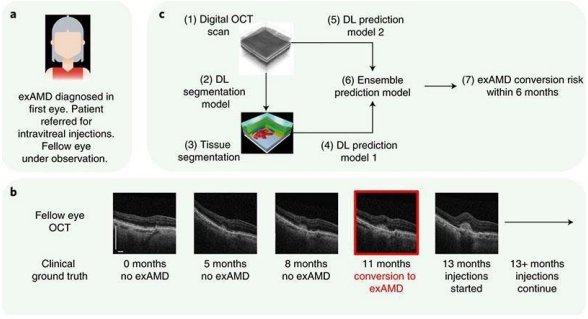

Figure 3. Model for detecting AMD (Age-related Macular Degeneration) disease with Deep Learning.

Advantages

1. Eye vein patterns are unique to each person
2. Patterns do not change over time and are still readable with redness[Works with contacts and glasses
3. Resistant to false matches

Disadvantages

1. Phone must be held close to face
2. Not supported on devices without cameras or on older smart phones

IV. Conclusion

In this article we are concluding that we can enhance our latest technology into future technology by implementing a Hawkeye as Eye print Scanner which is used to scan our eye blood vessels in eye vein –white portion of eyeball, which are unique to each. Using that sample we can build a Face unlock ID which is most secured than ever in which we can add that security to payments and other important things, and by implementing deep learning algorithms with Infrared emitter and camera to scan Eye Retina we can also detect Eye problems. We can share the results of that Eye scan to nearest Eye-cares /Hospitals which have online consultancy through an app.

References

[1] A. Jain, B. Ruud and P. Sharath, et al., Biometrics personal Identification in Network Society, Kluwer Academic Publishers, Dorrecht Google Scholar (1999), 123-141.

[2] M. B. Ruud, H. C. Jonathan, P. Sharath, K. R. Nalini and W. S. Andrew, Guide to Biometrics, Springer, Heidelberg (2004), 53-54.

[3] K. R. Nanili and G. Venu, Advances in Biometrics Sensor, Algorithms and Systems, Springer, Heidelberg (2008), 133-155.

[4] S. Baker, K. W. Bowyer and P. J. Flynn, Empirical evidence for correct iris match score degradation with increased time-lapse between gallery and probe matches, Proc. Int. Conf. on Biometrics (2009), 1170-1179.

[5] J. Daugman, How iris recognition works, IEEE Trans. Circuits and Sys, For Video Tech. 14 (2004), 21-30.

[6] J. Thornton, M. Savvides and V. Kumar, A Bayesian Approach to Deformed Pattern

Matching of Iris Images, IEEE Trans. PAMI 29 (2007), 596-606.

[7] N. Kalka, J. Zui, N. Schmid and B. Cukic, Image Quality Assessment for Iris Biometric, SPIE 6202: Biometric Technology for Human Identification III, Orlando, FL, (2006).

[8] K. P. Hollingsworth, K. W. Bowyer and P. J. Flynn, Pupil dilation degrades iris biometric performance, Computer Vision and Image Understanding 113(1) (2009), 150-157.

[9] D. Monro, S. Rakshit and D. Zhang, DCT-Based Iris Recognition, IEEE Trans. PAMI 29 (2007), 586-595.

[10] K. Miyazawa, K. Ito, T. Aoki, K. Kobayashi and H. Nakajima, An Effective Approach for Iris Recognition Using Phase-Based Image Matching, IEEE Trans. PAMI. 30 (2008), 1741-1756.