HCI-HPR

Sponsored by Sheffield Hallam Alumni,
DOI: 10.5281/zenodo.11209919

Advancement in Human Computer Interaction and Human Physiological Modelling

ISSN/ISBN-10: 1-100-22302-9

An Eye Authentication APP through Image Sensing Modelling

Fatima Isiaka
Department of Computer Science, Nasarawa State University, Keffi, Nigeria

Zainab Adamu
Department of Computer , Ahmadu Bello University, Zaria, Nigeria.

Abstract

An eye authentication software or tool is a form of the embedded module that includes an image data extraction front-end unit for determining the main concentric circle of the image of the eye as an integrating circle; a pupil radius detection unit which is used for detecting the integrated value of the integrating circle in stepwise order. This paper dealt with this approach by using system control dynamics for physical systems to determine the predictive focus of the eye by detecting constant changes in pupil dilation and constriction. Most current research has found that there are a lot of stories behind the concept of emotional response related to pupillary metrics on both constriction and dilation. We approach the current concept by using a contour integrating unit for integrating the captured image data extracted by the image data extraction unit with the eye circumference. The N4SID is a physical dynamic system for predicting complex behaviour patterns and this is used here to address the problem of outlier inclusion as part of the image data acquisition. The system is used here as a front-end engine integrated for detecting and controlling pupil response from a mobile camera lens in real-time. Initial results show that N4SID with the first order perfectly predicts the centric coordinate of the pupil in both constriction and dilation of all five epochs used on the differential equation.

Keywords: Eye authentication, Integrating circle, Pupil dilation, N4SID, Complex behaviour patterns, Pupil constriction.

Accepted: 10th February, 2024
Revised: 16th March, 2024
Published:10th April, 2024

Corresponding Author: Fatima Isiaka
Correspondent Email: fatima.isiaka@outlook.com

1 Introduction

In recent research, pupil detection and authentication are mostly devices that include initial data imaging and extraction, which are units for determining the multiplicity of concentric circles on an eye image as both an integrated circle and a contouring integration of units for implementing image data extraction by the image data extraction unit with the circumference circle.

On the other hand, an authentication process is a technology that enables people to have online access to services, through physical settings and other basic resources through images captured by an advanced lens. The lens can be in the form of an eye scan, eye authentication mostly relies on mobile and other hardware devices and native sensing forms of technology such as third-party biometrical algorithms. These algorithms are deployed as embedded software that leverages both device cameras and their focal lens for this purpose.

Most eye authentication solutions are architected using a decentralised model like Fast Identity Online (FIDO) that ensures that a person or an employee's eye is saved to the archive on the device. In this paper, a user's eye can be scanned for verification locally, and static imaging of the eye captured is then used for detection of the centric point of the eye (the iris) this is then sent as a token to the server centre and access is granted by sending a print out of the information obtained about the person, provided all information is archived online. The software is not usually stored at the server centre only when authorised as consent from the person. Most eye authentication solutions are architected in the form of a legacy centre scheme where the user's eye image templates are sometimes stored at the service provider. Most eye authentication services are common in criminal justice parastatals, national security and border protection services. Some of these systems rely on specialised hardware at border agencies as a point of care or access. Sometimes these systems are abused Ma et al. [10], Mlakar et al. [12], De Luca et al. [5], and this leads to false-positive cases. Here we adopted the implementation of a dynamic state-space model for the prediction and reduction of false-positive cases.

2 Literature Review

Most research Sakatou et al. [17], Badawi et al. [2], Brindha et al. [3], Gupta and Gupta [7] uses the eye vein verification method of biometric eye authentication which applies pattern recognition techniques like KLM's. And Jone Violes filter method Khan et al. [9], Kaburu et al. [8], Patel [14], Maity et al. [11]. This is mostly applied to video images of the veins in a user's eyes. There are unique random and complex patterns which are unique and can be differentiated using modern software and hardware to detect the patterns at some point distance from the eyes. The centric veins in the sclera of the eye are the white part of the eye which can be imagined only when a person looks to both sides thereby providing the four regions of patterns such as the one on each side of each eye. The verification employs some digital templates included in the patterns and these templates are encoded with a model and a statistical algorithmic process for feature detection Peli [15], Courtney et al. [4], Wu and Zhang [20]. This process allows for initial confirmation of the identity of the person or rejection of the eye authentication.

Research on eye vein authentication has noted that one of the strengths of this method is the stability of the patterns in the blood vessels of the eye; these patterns do not change with age or drowsiness. The eye veins are vivid enough that are reliable and can be imaged by the camera lens in most advanced smartphones. The detection process used infrared illumination a part of the imaging that allows imaging in low light intensity conditions. Other methods Delna et al. [6], Narasimha-Iyer et al. [13], Suganya and Sivitha [18] use the veins in the white part of the eyes for identification for the concept of application of blood vessels in the white part of the eye as a form of unique identifier. There is also research by Thomas et al. [19], Radha et al. [16], Alkassar et al. [1] that usess vein patterns in the iris and sclera for recognition and authentication. This process is used in a range of mobile banking, healthcare, government security and security situations. Based on this, there are bound to be advantages and disadvantages of authentication. Part of the advantages include the uniqueness of eye vein patterns for each person, the basic patterns do not change over a certain period and can be readable with redness. They are also adept and resistant to false matches in most cases. But one of its advantages is that mobile phones are mostly held close to the face and might not be supported on devices without advanced digital cameras or older smartphones. The paper addresses this by implementing the process on recently modernised Android with high memory speed and controls that are capable of embedding the control dynamics used as the inference engine. The proceeding section discusses the method employed for the project.

3 Method

The initial stage involves a singular real-time capture of the static image of the eye with the head at an upright head position Figure 1 at a point of accuracy derived by the model (Equation 1), this is then used as input data matrix for the model, the eye authentication process uses the N4SID system for physical attributes to detect the patterns of eye movement based on pupil changes (constriction and dilation) a most accurate way of detecting the emotional response of a person. The singular participant was first asked some simple questions about their familiarity with the application to induce some expectant reaction that would help detect an accurate and genuine authentication of the pupil response; this is done in real-time, and the state image is then captured and served as the input matrix. The N4SID relies most on input parameters which are automatically subject to features extracted based on unsupervised learning. The model is based on an identity space state (IDSS) as an input matric and used for representing the system:

$$\begin{aligned} \widehat{X}_i(t) &= Au(t) + Bu(t) + Ce(t) \\ \widehat{Y}_i(t) &= Du(t) + Eu(t) + Fe(t) \end{aligned} \tag{1}$$

Where *A, B, D*, and *E* are state-space matrices. *C* is the disturbance matrix. *(t)* is the input, is the output, is the vector of *nx* states and *e(t)* is the disturbance.

All the entries of the *A, B, D* and *C* matrices are free estimation parameters by default. *D* is fixed to zero by default, meaning that there is no feedthrough, except for static systems *(nx=0)*.

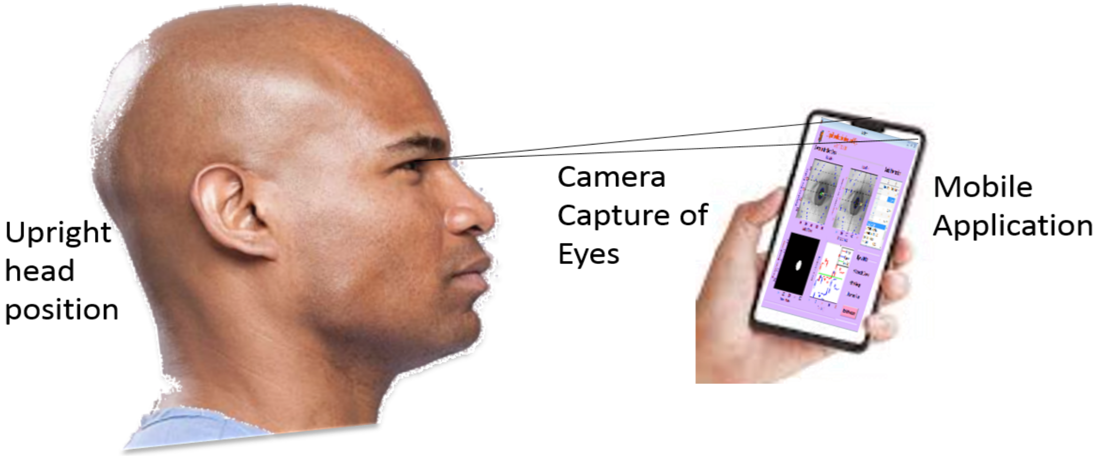

Figure 1: The pilot study started with eye movement capture on a mobile lens.

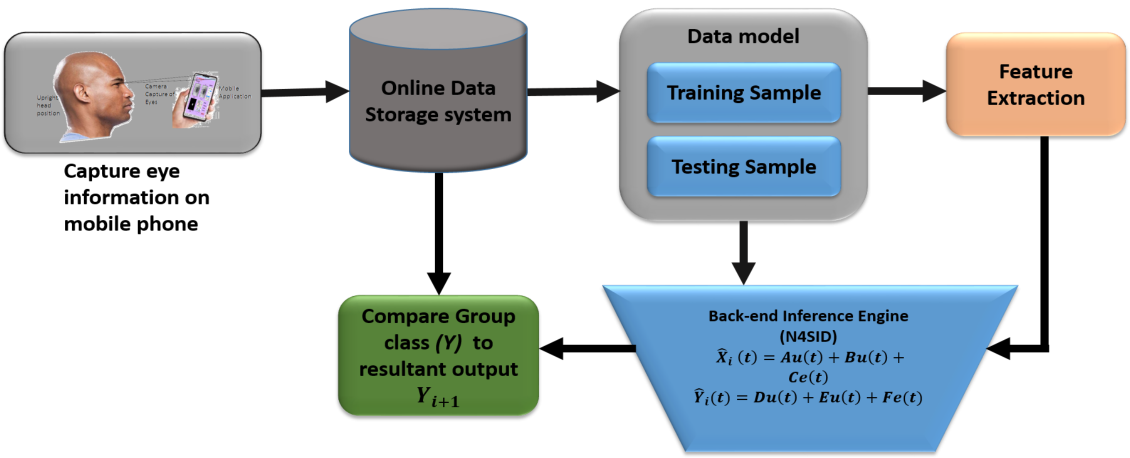

Figure 2: Framework for eye authentication using the N4SID model.

The initial stage is to capture an eye image by looking straight into the camera lens, the set of the matrix generated for a single pupil reading is transferred online to a station with the app as a form of a data model to be divided into training and test sample and feature extraction stage (Figure 2); the model (N4SID) is used as back-end model for classification and feature extraction this produces a result vector matrix as the centroid of the eye and the pupil dilation or constriction depending on the area reduction or increment in the pupil area region. Both eyes are set and captured for the same analysis. Matlab was used to design the window interface for a comfortable and a user friend analytical procedure and result generation. The final output and result alteration for the input matrix can be visualised with a single-window frame. The next section discusses the output and user information from a recorded pupil authentication.

4 Result

Figure 3 shows the result window with pupil authentication and authorisation dialogue; this can print the user pass for every authentication. The detected coordinates for both eyes can also relay information about the emotional response of a person at a point in time e.g. the pupil could be constriction or dilated to represent an intense focus or a distracted expression at the time of stagnant capture. This also indicates one of the novelties of this method and an exemplary method for advanced based biometric pupil detection. The mood is set based on the baseline of the pupil measure for both eyes. Other attributes such as the eye color detection module are also included and make it a multimodal eye authentication scheme of unconventional purposes. Pupil authentication is done for both eyes in background and foreground structure.

In Figure 4, one of the initial parameters *u1* is represented by the pupil baseline for the right eye and the performance and error check for that set is shown to be less than 0.001% and less than the expected error with

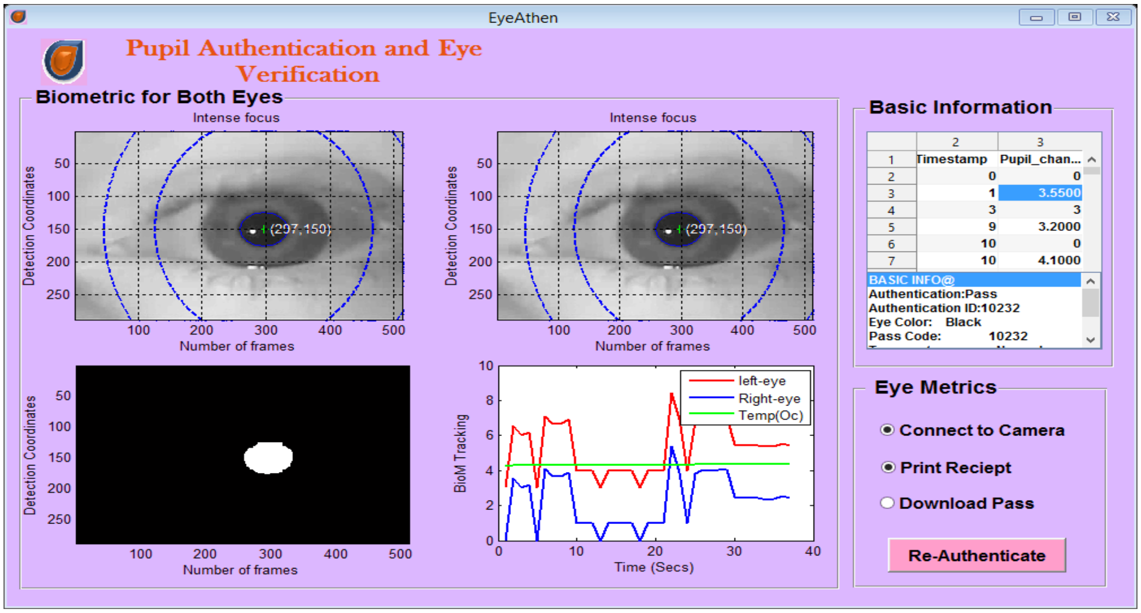

Figure 3: Result from the window with pupil authentication and authorisation dialogue; this can print user pass for every authentication.

an 86.5% simulation focus. The simulation in this case is the detection rate with a speed as high as 75% *ms*. The main aim is to obtain a high confidence level that best fills the adopted procedure in terms of the complexity of pupil constriction and dilation. Mood swing is one of the attributes that can also affect detection accuracy since this is sometimes highly unpredictable. The N4SID is set to tackle this issue of false detection and intrusion.

The figure also shows $y1$ as the response output for the input matrix, the mean square error (MSE) was calculated based on the residuals for every given authentication. This residual was used for outlier estimation and residual verification. The model also follows outlier inclusion, since, for a given behaviour generated, every outlier is important given the continuous nature of the biometric readings recorded. Eye color detection is set to four different colors which include *'brown'*, *'green'*, *'black'*, and *'hazel'*, depending on the nature of the light intensity and the system memory. A pass containing information for the pupil verification is also available for security authorisation and authentication to the intended serves online. The rationale for the embedded system information about the N4SID is for impervious confidence for lack of error detected and proof for authentication accuracy which a user can use as reliable information about their pass.

The result in Figure 5 was computed for the accuracy in performance for all five epochs used for the N4SID model. The epochs are based on the order of the differential equation which exceeds five counts for a pupillary response. The noise in image capture can also include voice and background parameters and also lens and camera set accuracy. Using an epoch up to five orders in each response variable can include noise and help to exclude irrelevant anomalies detected by the model.

5 Conclusion

This paper set out to investigate an app with N4SIDmode a control system for eye authentication through image sensing for real-time mobile application validation procedures. The process adopts the N4SID method prediction of the physical phenomenon as a time-variant state-space model for complex concepts. Such a concept is adopted in eye authentication verification to avoid false detection. The accuracy is based on simulation focus which was quite high for this purpose. The main contribution to the paper is the embedding of eye color and the cognitive state of a person whose pupil is set as input. They can easily be adapted for a multimodal eye authentication system that requires information about a person and passes for security purposes. The future perspective is to modify the module to predict the cognitive responses of users based on pupil dilation and constriction to external stimuli.

References

[1] Alkassar, S., Woo, W. L., Dlay, S. S., and Chambers, J. A. (2015). Robust sclera recognition system with novel sclera segmentation and validation techniques. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 47(3):474–486.

[2] Badawi, A. M. et al. (2006). Hand vein biometric

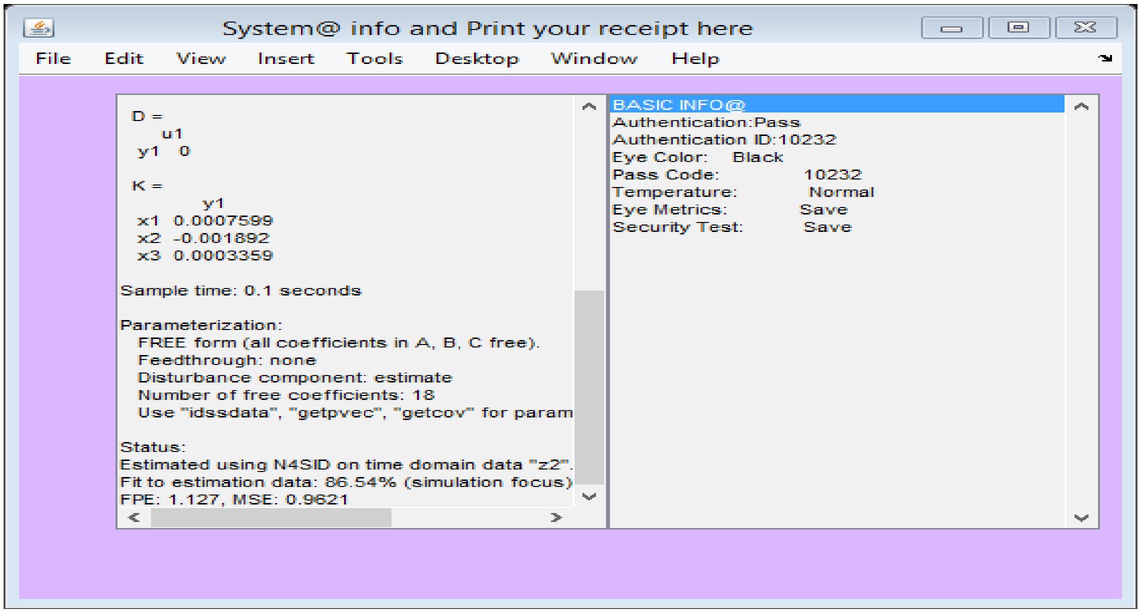

Figure 4: System information and a formal printout of authentication receipt for every eye authenticatio.

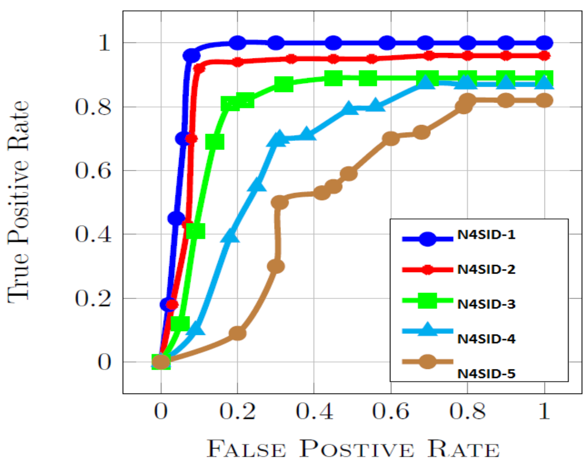

Figure 5: Performance of N4SID in a different order for the trained data mode.

verification prototype: A testing performance and patterns similarity. *IPCV*, 14(3):9.

[3] Brindha, M. S., Vennila, I., and Nivedetha, M. B. (2014). Performance analysis of fused eye vein and finger vein multimodal biometric system. *International Journal of Engineering Research and Development*, 10:69–75.

[4] Courtney, P., Thacker, N., and Clark, A. F. (1997). Algorithmic modelling for performance evaluation. *Machine Vision and Applications*, 9(5):219–228.

[5] De Luca, A., Weiss, R., Hussmann, H., and An, X. (2008). Eyepass-eye-stroke authentication for public terminals. In *CHI'08 Extended Abstracts on Human Factors in Computing Systems*, pages 3003–3008.

[6] Delna, K., Sneha, K., and Aneesh, R. (2016). Sclera vein identification in real time using single board computer. In *2016 International Conference on Next Generation Intelligent Systems (ICNGIS)*, pages 1–5. IEEE.

[7] Gupta, P. and Gupta, P. (2015). An accurate finger vein based verification system. *Digital Signal Processing*, 38:43–52.

[8] Kaburu, D. M., Sansa-Otim, J., Mayanja, K., Mirembe, D. P., and Bulega, T. (2018). A usability based approach to designing continuous user biometric authentication system. *Quality and User Experience*, 3:1–14.

[9] Khan, S., Devlen, C., Manno, M., and Hou, D. (2024). Mouse dynamics behavioral biometrics: A survey. *ACM Computing Surveys*, 56(6):1–33.

[10] Ma, Z., Yang, Y., Liu, X., Liu, Y., Ma, S., Ren, K., and Yao, C. (2019). Emir-auth: Eye movement and iris-based portable remote authentication for smart grid. *IEEE Transactions on Industrial Informatics*, 16(10):6597–6606.

[11] Maity, P., Sur, K., and Muhopadhyay, I. (2023). The future of the internet of things (iot) and iot authentication. In *2023 11th International Conference on Internet of Everything, Microwave Engineering, Communication and Networks (IEMECON)*, pages 1–6. IEEE.

[12] Mlakar, T., Zaletelj, J., and Tasic, J. F. (2007). Viewer authentication for personalized itv services. In *Eighth International Workshop on Image Analysis for Multimedia Interactive Services (WIAMIS'07)*, pages 63–63. IEEE.

[13] Narasimha-Iyer, H., Beach, J. M., Khoobehi, B., and Roysam, B. (2007). Automatic identification of retinal arteries and veins from dual-wavelength images using structural and functional features. *IEEE Transactions on Biomedical Engineering*, 54(8):1427–1435.

[14] Patel, V. (2018). Airport passenger processing technology: a biometric airport journey.

[15] Peli, E. (2002). Feature detection algorithm based on a visual system model. *Proceedings of the IEEE*, 90(1):78–93.

[16] Radha, G., Saranya, C., and Suganyadevi, B. (2019). A new multimodel approach for human authentication: Sclera vein and finger vein recognition. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 37(3):47–56.

[17] Sakatou, H., Toyoshima, K., Yoshida, S., and Utsugi, T. (2016). Authentication support solution for realizing safe and secure society: Trust eye. *FUJITSU SCIENTIFIC and TECHNICAL JOURNAL*, 52(3):15–22.

[18] Suganya, A. and Sivitha, M. (2014). A new biometric using sclera vein recognition for human identification. In *2014 IEEE International Conference on Computational Intelligence and Computing Research*, pages 1–4. IEEE.

[19] Thomas, N. L., Du, Y., and Zhou, Z. (2010). A new approach for sclera vein recognition. In *Mobile Multimedia/Image Processing, Security, and Applications 2010*, volume 7708, pages 38–47. SPIE.

[20] Wu, J. and Zhang, X.-L. (2011). An efficient voice activity detection algorithm by combining statistical model and energy detection. *EURASIP Journal on Advances in Signal Processing*, 2011:1–10.