ORIGINAL ARTICLE **Open Access**

ISSN 2278-1404

International Journal of Fundamental & Applied Sciences (IJFAS)

ADVANCEMENT IN CONTINUOUS MONITERING OF MULTIMODAL BIOMETRIC USING MODULAR POINT SENSITIVITY TRACKING

SuhasBharadwaj GR *[1], Sujanashraya S[1], Dhanya K.N[1] , Harshitha M[1] , Sushma S[1]

[1] MRIT Engineering College, Mysuru. VTU, India

*** Corresponding author email address**: suhas.gr.bharadwaj@gmail.com

DOI: https://doi.org/10.59415/ijfas.377

Abstract

In the Evolving landscape of Digital Examinations and remote interviews, ensuring continuous and reliable identity verification has become increasingly critical. After the covid pandemic, Online examination and interviews have made a remarkable impact on Global Education and Recruitment process for which in this modern examination and interview environment, ensuring authenticity and continuous monitoring of candidate is very much essential, Hence continuous user authentication is critical to maintaining academic integrity and security. Ensuring the Authenticated user at the login time is one time Security, monitoring the candidate is very much essential as they can use AI for searching the answers or any other person sitting next to them for helping to solve the given question. using multimodal Biometric by giving a sensitivity in the Border value along with recognizing new voice, moving of foreign items behind the candidate will be the key during continues Monitoring. Where this paper proposes a multimodal biometric framework using facial point tracking and sensitivity-based co-ordinate analysis. A System is designed to capture and compare real time co-ordinate points which will be compared with pre-recorded values in Data Base. Where, the deviation beyond sensitivity threshold triggers a monitoring mechanism which logs inconsistencies and flags potential anomalies. Unlike conventional one-time authentication systems, the proposed solution continuously captures and compares real-time biometric data against pre-recorded reference Senstivity increased Border points, Coordinates of Foreign Objects behind the Candidate stored in a database. Facial coordinates are tracked within a predefined sensitivity threshold for physical movement and recognizes if any extra Noise is heard during the session.

.

Keywords: Multimodular Biometric monitoring, Authentication, Boundary Value, Co-ordinate Sensitivity, Modular Score Analysis, Threshold Value

1. Introduction

Biometrics were used in authentication which started by unimodal fingerprint, Iris, voice. Due to age context, physical damage matching the uniqueness of fingerprint among individuals one in 500. Even though Iris was found little more accurate, using Facial Biometric became secured which covers multiple areas by points & recognized by the distance from one key point to another make a facial signature which acts as a digital map of face and it will be stored in database.

Multimodal biometrics covering Face, IRIS, voice covered the limitations of unimodal [1] by enhancing reliability and minimizing errors like FAR & FRR. But while you want to monitor continuously the entire session of examination or interview process needs a predefined data to get matched with current data continuously [2] by real time monitoring. As online exams are prone to academic dishonesty, impersonation and cheating, despondingly, collecting the data at the login phase and storing in database [2] matching the raw data regularly and testing its boundary value along with sensitivity continuously will help in tracking malpractice. Unlike one time login and authentication [5] the System verifies identity throughout the session by giving certain marginal fluctuations in Boundary Value with respect to real world activities and identifying any new foreign objects and noise in the middle of session as a red mark.

2. LITERATURE SURVEY

Multimodal biometrics with 3-tier architecture and 3 tier modality by recognizing Face, IRIS and Voice enhancing reliability & mitigate error types [1] which used fusion technique at different levels pre and post mapping function and feature level fusion which was considered most effective due to the richness of raw biometric data. Proposing to the message/SMS alert system during E-exam for either admin or invigilator [2] if any one of modality in the multimodal authentication fails, either username or password, Iris, or Facial Recognition, the current points will be matched with pre-stored data points that were captured during enrollment process before exam [2]. As the online exams authorities gives for certain duration, adding checkpoints at equal intervals of time and again matching [3] with pre-stored data [3] to check anomaly.
At the score level fusion to merge the biometric data [4] in which the individual scores of individual biometrics will be merged into one at equal interval of time. [4] Face recognition uses PCA for feature extraction and Manhattan distance for matching it.

Unlike one time login, System also verifies identity throughout the session by Eigen Face method with PCA for Face recognition and timing analysis [5] using a hybrid distance metric for which each keystroke data & ORL Face Dataset will be Input and ERR will be calculated [5].

During the continuous biometric Authentication while attending the exam/interview, the keystroke Behavior Authenticator [6] is used where the key dynamic is a behavioral biometrics that aims to identify original candidate based on the analysis of their typing rhythms on a keyboard [6], where the keystrokes can be collected unobtrusively using standard keyboard throughout the session without any knowledge of the user [6].
By referring all the Authors, the study of all below mentioned Authors, this paper just shows how continuous monitoring can be done parallel with different modularity by giving a buffer sensitivity during boundary value and above that value will be counted as fraud action.

3. METHEDOLOGY:

Continues monitoring of candidate taking up the examination or interview through online is very much needed for a fruitful operation for entire session. As per Author [6] keystroke behavior authenticator is also a technique where continues minter can be done.

Login methods and authentication by covering multimodal biometrics [2] will be done at the initial stage.Once the session starts, as shown in figure 1 the entire screen area will be captured with centre of screen pointing (x,y)=(0,0). The constant objects on screen behind the candidate will be recorded and the Coordinate points of those will be stored in Data Base.

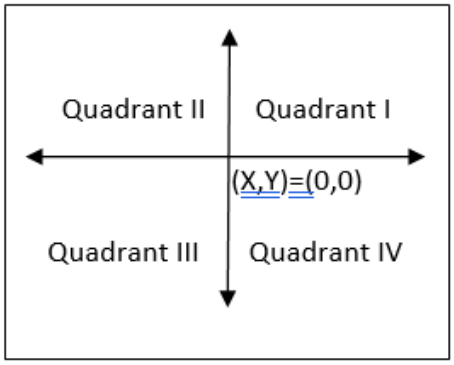


Figure 1 : Centre of Screen Area pointing (x,y)=(0,0)

Centre (x,y)=(0,0)----------Equation 1

From the Quadrant I, Co-ordinate points of (x,y) (+,+) will be recorded and stored in Database

From the Quadrant II, Co-ordinate points of (x,y) (-,+) will be recorded and stored in Database

From the Quadrant III, Co-ordinate points of (x,y) (-,-) will be recorded and stored in Database

From the Quadrant IV, Co-ordinate points of (x,y) (+,-) will be recorded and stored in Database

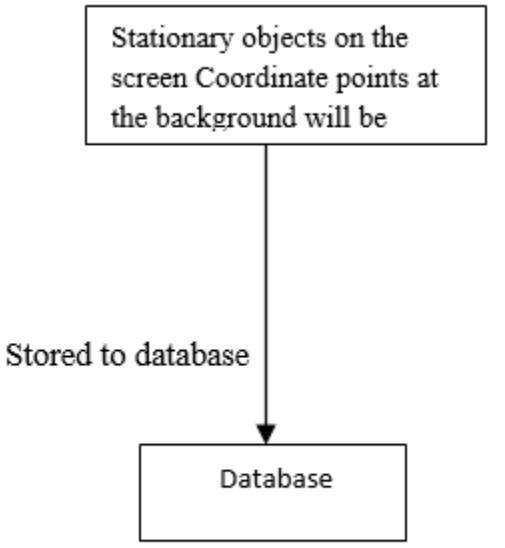


Figure 2 : Stationary Objects coordinate points will be recorder and stored in Database

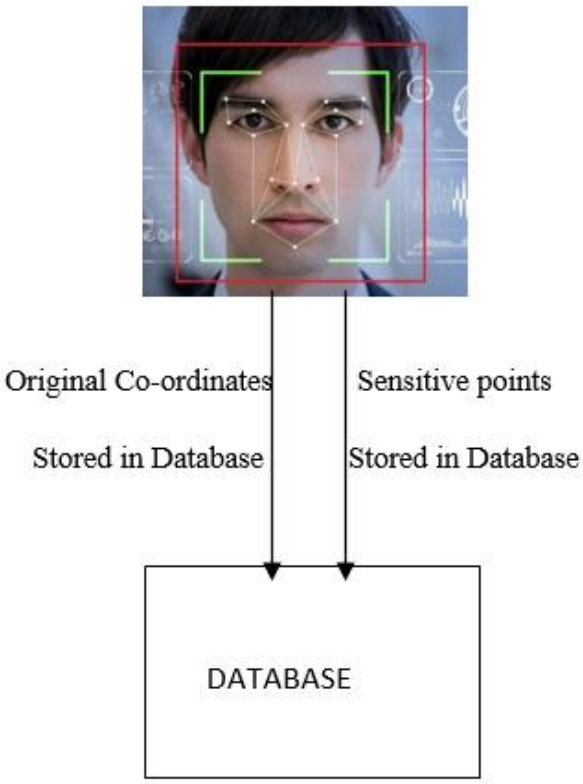


Figure 3: Border Values of face and incremented Border Values will be stored in Database separately.

Once the candidate login, The Facial Multimodal Bio metrics will be Recorded and stored in the database.[1].

The entire Biometric Facial Border Region or Boundary of Authentication coordinate points (x, y) will be incremented by a sensitivity of +1 or +2 in both (x, y) in all coordinates and stored in Database as shown in Figure 3. and every time the score increases the border values it will be counted.

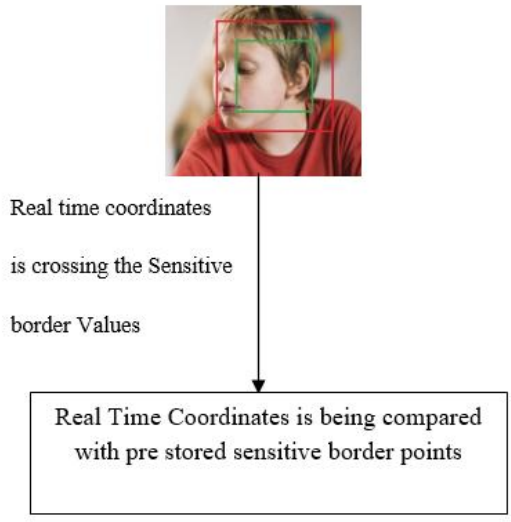


Figure 4 : Real Time Coordinate points is crossing the Border Values shown in Red Color and it will be Taken Count.

Admin or the host will decide to keep the COUNT_MAX Value.

For Every deflection in the (x,y) coordinates within the original Pre stored Score to Sensitive +1 points will be accepted. Crossing the sensitive points (shown in Figure) every time will be noted and marked to COUNT. For every COUNT, Marks will be decremented by 1.

If COUNT > COUNT_MAX

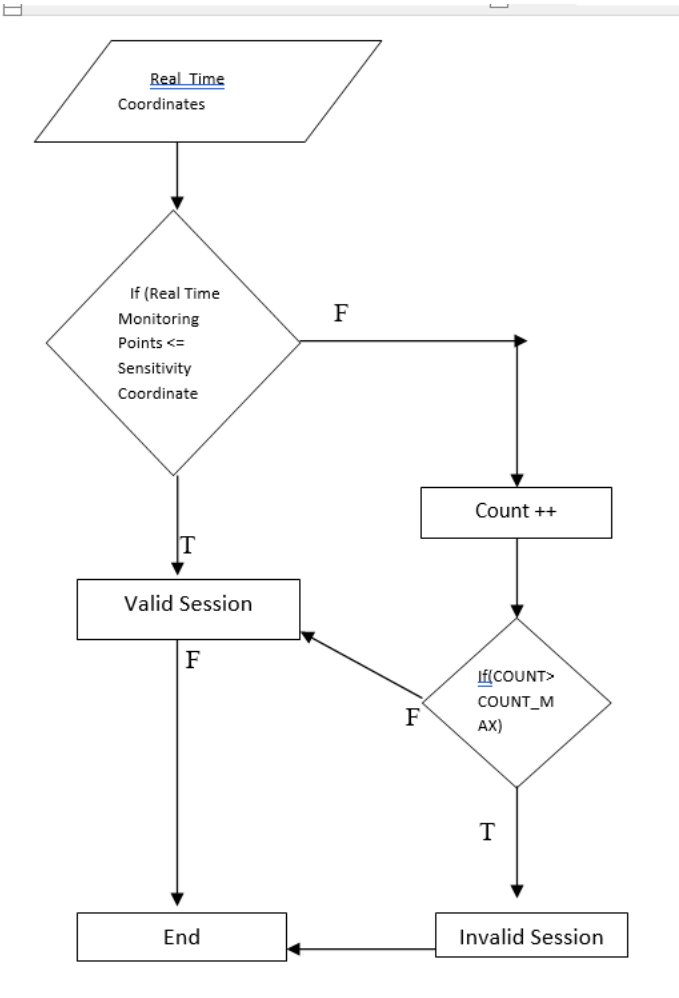
then session will be reflected as invalid.

If(COUNT>0&&COUNT<=COUNT_MAX)

Decrement the marks by 1

If(COUNT>COUNT_MAX)

Invalid session



4. RESULT AND METHEDOLOGY:

The proposed System successfully implements a robust monitoring approach during critical sessions such as exams/interviews. Using facial biometric point tracking and modular score analysis, the authenticated candidate based on pre mapping function. The co-ordinate points are stored in database. The tracking of facial co-ordinate (x, y) was continuously compared with sensitivity-adjusted boundary limits using:

If((Realtime(x,y)coordinates)<=(Sensitivity(x,y)co-ordinates)

Sensitivity-Based Threshold Logic:

The integration of sensitivity co-ordinate window we marked using Boundary Value helped to filter out minor head movements and allowed focus on significant behavioral anomalies.

The Real-time monitoring logic Controlled the session using the following rule :

For every COUNT incremented, deductions were made until it exceeds the COUNT_MAX. When it exceeded a configurable threshold session was flagged and marked as invalid session.

Candidate_ID	Deviation Count	Max Threshold (COUNT_MAX)	Marks Deducted	Status
C001	2	5	2	Valid Session
C002	6	5	5	Invalid Session
C003	0	5	0	Valid Session
C004	8	5	5	Invalid Session

5. CONCLUSION:

This system as cited in [2], enhances reliability by cross-verifying face location, foreign items behind the screen captured after session started, movements, behaviors in real time. The fusion of techniques improves resistance to spoofing attacks and unauthorized access and authorized access being using external sources during the session will be captured and relevant result will be proportional to the Deviations Counter.

6. LIMITATIONS AND FUTURE ENHANCEMENT

While the prototype SLM works well in controlled environments, performance may vary with lighting conditions, camera resolution, head pose variation beyond ±15°.

Future Work will include

Incorporating 3D Head Tracking,

Integrating with voice biometrics and Adaptive thresholding

7. STATEMENTS & DECLARATIONS

AI Statement: The authors declare that they have not used generative artificial intelligence, specifically ChatGPT, in the writing of this manuscript and/or in the creation of images, graphics, tables, or their corresponding captions.

Authorship Contribution: SuhasBharadwaj GR , Sujanashraya S, Dhanya K.N , Harshitha M: Carrying out the data collection, data curation, and writing the original manuscript.

Ethical Standards: All the ethical research standards were followed while writing this conceptual paper.

Conflict of Interest: The authors state that they do not have any conflict of interest.

Informed Consent / Ethical Compliance: As this is a conceptual paper, no consent is required.

Human or animal involvement in the article: None

Data Availability: All data included in this research article will be provided on request

8. REFERENCES

1. Aman Kathed, Sami Azam, Bharanidharan Shanmugam, Asif Karim, Kheng Cher Yeo, Friso De Boer, Mirjam Jonkman "An Enhanced 3-Tier Multimodal Biometric Authentication" 2019 International Conference on Computer Communication and Informatics (*ICCCI* -2019)

2. Diligence R. Mdaka, Tonderai Muchenje, Tshimangadzo M. Tshilongamulenzhe, Topside E. Mathonsi "A Multimodal Authentication Method for Electronic Exams"

3. Roopesh Kevin Sungkur, Irma Beekoo, Dicshita Luveena Bhookhun "An Enhanced Mechanism for the Authentication of Students taking Online Exams"

4. Achour Achroufene, Nassima Slimani, Mustapha Sadi "Multimodal biometric authentication using face and Signature based on Dempster-Shafer Theory", 2024 2nd International Conference on Electrical Engineering and Automatic Control (ICEEAC)

5. Stuti Srivastava , Prem Sewak Sudhish "Continuous Multi-biometric User Authentication Fusion of Face Recognition and Keystoke Dynamics"

6. Chao Shen, He Zhang, Zhenyu Yang, Xiaohong Guan "Modeling Multimodal Biometric Modalities for Continuous User Authentication" 2016 IEEE International Conference on Systems, Man, and Cybernetics' SMC 20161

7. sudip vhaduri, christian poellabauer "multi-modal biometric-based implicit Authentication of wearable Device users "ieee transactions on information forensics and security, vol. 14, no. 12, december 2019

8. rami al-hmouz, khaled daqrouq, ali morfeq, witold pedrycz " multimodal biometrics using multiple feature representations to speaker identification system", 2015 international conference on information and communication technology research (ictrc2015)

9. D. Crouse, H. Han, D. Chandra, B. Barbello, and A. K. Jain, ''Continuous authentication of mobile user: Fusion of face image and inertial measurement unit data,'' in *Proc. Int. Conf. Biometrics (ICB)*, May 2015, pp. 135–142.
10. G. Martín, I. Martín de Diego, A. Fernández-Isabel, M. Beltrán, andR. R. Fernández, ''Combining user behavioural information at the feature level to enhance continuous authentication systems,'' Knowl.-Based Syst., vol. 244, May 2022, Art. no. 108544.