International Journal of Computer Science Engineering Techniques (IJCSE) Volume 10 Issue 1 ,January 2026

ISSN : 2455-135X

Human Blink Sequence as a Morse Code Authentication System

Bhumika K L[1], E. Vennela Chowdary[2], Harshitha T[3], Asha Rani M[4]
[1]Department of Computer Science & Engineering,
GSSS Institute of Engineering & Technology for Women, Mysuru, Affiliated to VTU, Belagavi, Karnataka, India
Email: {bhumikalokesh2004@gmail.com, Chowdaryvennela27@gmail.com, tharshitha57@gmail.com}
[4]Assistant Professor, Department of Computer Science & Engineering,
GSSS Institute of Engineering & Technology for Women, Mysuru, Affiliated to VTU, Belagavi, Karnataka, India
Email: {asharanim@gsss.edu.in}

Abstract- This study introduces a secure and accessible authentication approach that enables users to log in simply by blinking their eyes in a pattern similar to Morse code. This approach is designed especially for people with limited motor control or reduced hand mobility or traditional input devices. Instead of entering PINs or passwords, users can authenticate themselves through intentional eye blinks, making the system completely hands-free. The model uses OpenCV to track facial landmarks and dlib to calculate the Eye Aspect Ratio (EAR), which helps detect purposeful blinks accurately. These blinks are then converted into Morse code signals and compared with stored authentication patterns. Our experiments show that the system works reliably in normal lighting and responds with minimal delay, providing smooth interaction. Because it uses basic hardware and open-source tools, the solution is economical and can be deployed with minimal resources. The findings of this research indicate that eye-blink-based Morse code can be a practical, inclusive, and user-friendly alternative to conventional login mechanisms, especially for individuals who need assistive technology.

Index Terms- eye blink detection, Morse code, authentication system, OpenCV, assistive technology

I. INTRODUCTION

As digital systems continue to grow in the personal, business, and governmental spheres, ensuring safe and trustworthy user authentication has become increasingly vital in modern digital environments. Traditional login approaches such as passwords, PINs, or pattern-based locks, and physical tokens are no longer adequate to secure sensitive data due to the explosive expansion of online services and connected devices. These conventional techniques are vulnerable to shoulder surfing, brute-force attacks, phishing attempts, password reuse, and human memory constraints, among other flaws. However, these methods are often insufficient in meeting accessibility requirements, particularly for individuals who face motor or physical disabilities who might have trouble using keyboards, touchscreens, or other physical input devices.

Because biometric authentication can provide improved security and usability, it has received a lot of attention lately. Many platforms including smartphones, financial services, and ID verification systems heavily rely of fingerprint, facial recognition, iris scan, and voice verification systems. These modalities offer greater security than passwords alone, but they also come with drawbacks, including the possibility of compromised biometric templates, hardware dependence, spoofing threats, environmental sensitivity, and privacy issues. In order to achieve greater resilience and user adaptability, there is an increasing interest in creating multimodal and behavioural biometric approaches.

In this area, eye-blink-based authentication is a promising approach. Eye blinks are suitable to be used as a behavioral biometric since they are natural, involuntary physiological actions that are difficult to replicate. With advancements in computer vision, blinks can now be detected and analyzed in real time using only a regular webcam, removing the necessity for specialized sensors. When integrated with Morse code, where short blinks denote dots and long blinks denote dashes, blinking becomes a flexible and expressive modality for secure authentication.

This method provides hands-free interaction,which is advantageous in situations requiring contactless authentication and accessible for users with restricted mobility.

This study suggests a Human Blink Sequence as a Morse Code Authentication System, a multimodal authentication model that combines three separate security layers: blink-based Morse code decoding, facial recognition, and password verification, in order to overcome present shortcomings in conventional and biometric authentication systems. Deep learning-based face recognition techniques are employed in this system to capture and encode the user's facial features, and the Haar Cascade classifier detects the eye region and tracks blink duration to differentiate short and long blinks. To ensure that authentication requires both biometric identity and behavioral input, these blinks are subsequently translated into Morse code and compared with the user's registered blink pattern.

The suggested system has a number of benefits. By requiring two distinct user-specific factors, a facial biometric and a blink-based behavioral pattern, it first improves security. By allowing users with motor impairments to authenticate without the need for physical touch or movement, it also promotes inclusivity. Third, the system operates in real time using widely accessible hardware, proving its viability and practicality for real-world implementation. Unlike spoken or typed passwords, the incorporation of Morse code guarantees that blink sequences are private and impervious to observation attacks.

Overall, this study demonstrates how computer vision, behavioral biometrics, and traditional communication standards can be combined to create a novel, safe, and accessible authentication system. The suggested system supports continuous efforts to develop authentication solutions that are inclusive and flexible for a range of user demographics in addition to being safe and dependable.

II. LITERATURE REVIEW

An overview of current studies on eye-blink detection, biometric authentication, and Morse code-based communication systems is given in a literature review. A variety of methods and strategies that support the creation of gaze-based and blink-based authentication mechanisms are highlighted in the reviewed studies.

Eye-tracking technologies have been explored for secure authentication in several studies. One such study suggests a real-time gaze-based PIN entry system that uses a smart camera to track and identify eye movements. Because this method eliminates physical traces like keystrokes and touchscreen gestures, it reduces the likelihood of password theft.

Research has also focused on eye movement analysis in the context of performance evaluation. Eye-tracking systems have the potential to capture precise ocular behavior, as evidenced by comparative studies between expert and beginner athletes that revealed significant differences in eye movement patterns. Such findings provide foundational insights for designing blink-based authentication modules.

A smart eye-tracking system designed for individuals with disabilities is presented in another pertinent work. This system employs a webcam and image-processing techniques to track eye movements for controlling appliances, wheelchairs, and communication devices. Blink-based commands are utilized in place of keyboard inputs, confirming the feasibility of using intentional blinks as control signals in real-time applications.

Additional research highlights the use of eye blinks for hands-free control. Systems integrating support vector machines (SVMs) and blink detection have been shown to enable robot navigation and interaction, providing an accessible interface option for users with severe motor impairments. These works underline the reliability of blink-based input as a practical substitute for hand-operated devices.

Eye movement-induced EEG signals for communication interfaces are the subject of further research. These studies show the stability and repeatability of event-related potentials produced during particular eye movements. Although primarily focused on medical or brain-computer interface applications, they highlight the strong correlation between eye movements and reliable system control

To increase focus and engagement, mixed-reality-based systems for kids with ADHD also make use of eye contact and eye movement analyses. These studies demonstrate the wider role of eye-tracking technologies in interaction and behavioral assessment, confirming their applicability beyond accessibility.

Overall, the literature reveals that eye tracking and blink recognition are well-established areas with diverse applications in authentication, accessibility, brain-computer interfaces, and assistive technologies. These findings support the development of a multimodal authentication system that incorporates blink-based Morse code and facial recognition for improved security, accessibility, and user convenience.

III. PROPOSED SYSTEM

The suggested system presents a safe, multimodal authentication framework that combines blink-based Morse code decoding with facial recognition to offer a dependable and user-friendly login process. This system allows hands-free authentication and provides improved defense against spoofing, observation attacks, and unauthorized access, in contrast to conventional authentication techniques that only rely on passwords or in-person interactions.

The system monitors the user's face and eye area in real time through vision-based techniques. A standard webcam captures video frames, and OpenCV's Haar Cascade classifier is employed to detect the user's facial features and determine the eye state (open or closed). Blink duration is measured continuously, allowing the system to differentiate between:

Short blinks → Dot (.)

Long blinks → Dash (-)

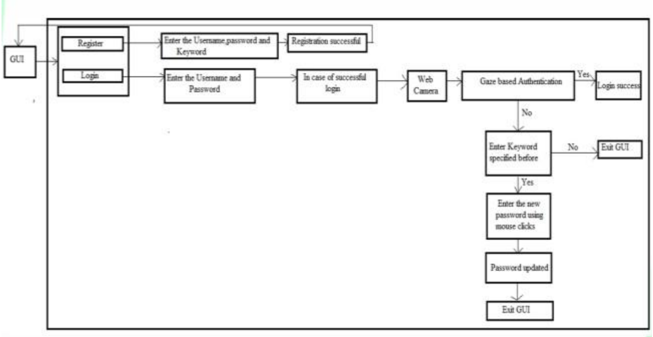

GUI
Register
Login
Enter the Username,password and Keyword
Registration successful
Enter the Username and Password
In case of successful login
Web Camera
Gaze based Authentication
Yes
Login success
No
Enter Keyword specified before
No
Exit GUI
Yes
Enter the new password using mouse clicks
Password updated
Exit GUI

Figure 1. System architecture of the proposed model

A Morse code sequence is created by adding up these blink patterns. During registration, the user intentionally creates a personalized Morse code phrase using controlled eye blinks. This phrase is decoded using a predefined Morse dictionary and stored securely as a behavioural authentication factor.

The system incorporates facial recognition to confirm the user's identity in addition to blink-based input. During registration, the user's facial features are captured and converted into facial encodings using the face recognition library. During login, live facial encodings obtained from the webcam are compared with the stored encodings to validate the user.

Only when all of the following factors match will the authentication process be finished:

- Verification of passwords
- Recognition of faces
- Blink-based validation of Morse code

System security is greatly strengthened by this structured multi-factor model. Additionally, it guarantees accessibility by allowing individuals with limited hand mobility or motor impairments to authenticate themselves without using tangible devices like touchscreens or keyboards.

The entire system is implemented using Python, OpenCV, Haar Cascade classifiers, and face recognition libraries, making it lightweight and easy to deploy with just a standard webcam and basic computing hardware. The design focuses on security, efficiency, and inclusivity, ensuring that users can authenticate themselves in a convenient and highly secure manner.

IV. METHODOLOGY

In order to integrate password verification, facial recognition, and blink-based Morse code decoding into a single multi-factor authentication framework, an organized and methodical approach was used in the development of the Human Blink Sequence as a Morse Code Authentication System. An extensive review of previous studies on eye-blink detection, biometric authentication, and Morse code interpretation is the first step of the development process. This review of the literature aids in determining the appropriate algorithms and resources needed to create a safe and effective authentication system.

Examining different eye-detection and blink-recognition methods is the first step.

ISSN : 2455-135X © 2025 International Scientific and Academic Research (ISAR) Publisher

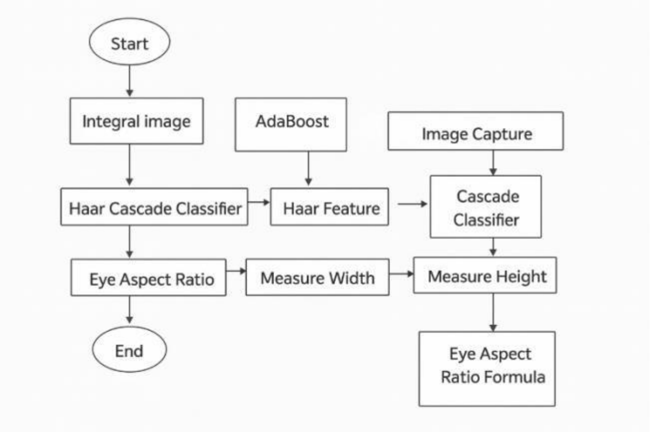


Figure 2. System processing workflow

The Haar Cascade classifier from OpenCV is chosen among the available methods because it strikes a balance between speed, accuracy, and suitability for real-time video processing. The classifier tracks changes between the open and closed eye states by identifying the eye region from webcam frames. Blink duration helps differentiate between intentional and involuntary blinks; in Morse code, shorter blinks are represented by dots (.) and longer ones by dashes (–). The captured blink sequence is then translated using a predefined Morse dictionary. This method is based on well-established research demonstrating that Morse symbols can be reliably generated using blink duration.

In order to strengthen system security, facial recognition is integrated alongside blink-based detection. During registration, the user's facial image is converted into a numerical encoding using the face recognition library. During authentication, live webcam frames are processed to extract facial encodings, which are subsequently matched against stored encodings for identity verification. This step ensures that blink patterns cannot be used in isolation, preventing unauthorized access.

The three-factor authentication model is completed with a conventional password input step. The system's security and dependability are improved by the combination of (i) password, (ii) facial recognition, and (iii) Morse-based blink authentication.

CustomTkinter was used to create a GUI that allows users to register, record their face, and enter Morse code blinks during authentication. While the backend processes real-time frames taken by the webcam, the GUI manages user interactions.

The integrated system is rigorously evaluated across different lighting conditions, camera positions, and blink speeds in the final step of the methodology. These tests guarantee dependable facial recognition, precise blink differentiation, and steady, real-time performance.

All things considered, the approach combines behavioral biometrics, computer vision, and conventional authentication methods into a unified, effective, and user-friendly security system.

V. IMPLEMENTATION

Face detection, facial recognition, blink monitoring, and Morse code decoding are all integrated into a single multi-factor authentication model in order to implement the Human Blink Sequence as a Morse Code Authentication System. Python, OpenCV, Haar Cascade classifiers, the face recognition library, and a typical webcam for real-time input processing are used in the system's development.

The implementation starts with the registration stage, in which the user uses the GUI to input a username and set a password. The face recognition library is used to transform a webcam-captured facial image into numerical encodings. The blink-detection module is activated by the system following face registration. To create a unique Morse code sequence, the user purposefully blinks. To differentiate between short blinks (dot) and long blinks (dash), blink durations are measured. The password, facial encodings, and the decoded Morse sequence are then saved.

The user first inputs their login information during the authentication stage. The webcam records live facial frames if the password matches, and identity is confirmed by comparing the generated and stored facial encodings. The blink-based input module is started after the face has been successfully authenticated. The user uses eye blinks to replicate the previously registered Morse code. Access is only allowed if all authentication factors match after the blink pattern has been decoded and compared to the stored Morse sequence.

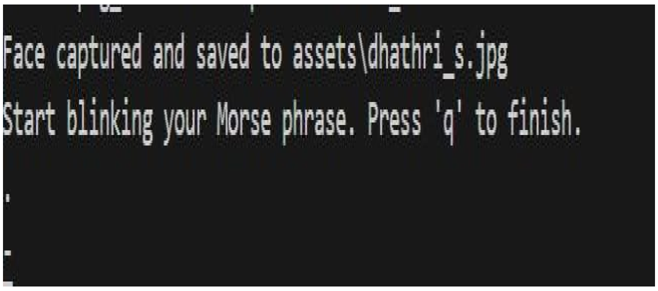
Two primary algorithms are utilized in the implementation. In real-time video frames, the face and eye regions are detected using the Haar Cascade classifier. The system detects whether a blink has occurred and calculates its duration by analyzing changes in eye openness over successive frames. By identifying 68 important facial points, the facial landmark detection technique improves accuracy even further and makes it possible to precisely track eyelid movement using Euclidean distance calculations.

Python, OpenCV, CustomTkinter for the GUI, Haar Cascade XML files, and the face recognition library are among the software elements utilized in the system. Real-time image processing, blink detection, facial encoding, Morse code interpretation, and interface handling are all supported by these tools. The overall implementation produces a multi-layered authentication framework that incorporates blink-based Morse code input, facial recognition, and password verification. This guarantees an accessible, safe, and hands-free authentication procedure that is appropriate for both ordinary users and people with motor impairments.

VI. RESULTS AND DISCUSSION

The efficacy, accuracy, and real-time performance of the implemented Human Blink Sequence as a Morse Code Authentication System were assessed through implementation. The findings show that a dependable and secure multi-factor authentication method can be achieved by combining password verification, facial recognition, and blink-based Morse code input.

The system successfully recorded user credentials, blink-generated Morse sequences, and facial encodings during the registration process.

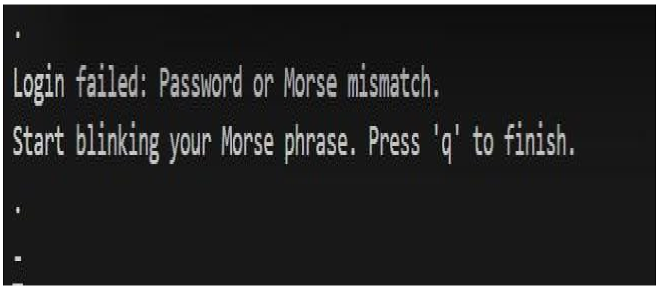


```
Face captured and saved to assets\dhathri_s.jpg

Start blinking your Morse phrase. Press 'q' to finish.


.


-
```

Figure 3. Eye-blink password entry during registration

Users were able to accurately register their identities thanks to the stable and consistent facial encoding generation. The blink-detection module accurately identified short blinks as dots and long blinks as dashes, enabling the formation of unique Morse-based passwords. The classification remained reliable under normal lighting and during moderate head movements.

ISSN : 2455-135X © 2025 International Scientific and Academic Research (ISAR) Publisher



```
.
Login failed: Password or Morse mismatch.
Start blinking your Morse phrase. Press 'q' to finish.
.
-
```

Figure 4. Eye-blink mismatch and Morse code entry during login

Before moving on to biometric checks, the system verified the username and password during the authentication phase. Facial recognition performed accurately by matching live webcam frames with the stored encodings, demonstrating strong resistance to pose and expression variations. Blink-based Morse decoding translated intentional blinks into their corresponding Morse characters, and the system granted access only when the decoded sequence matched the registered pattern. This ensures that all three layers password, facial recognition, and blink-based behavioural input must be satisfied for successful authentication.

The hands-free interaction model improved accessibility from a usability standpoint, particularly for users with motor impairments who might have trouble using conventional input devices. Despite the fact that blink-based input is slower than password typing, users claimed that with practice, the procedure became intuitive. Additionally, the system's lack of physical touch surfaces makes it appropriate for settings requiring contact-free, hygienic authentication.

The multimodal approach's strength is highlighted by the security evaluation. While blink-based Morse code reduces vulnerability to observation attacks like shoulder surfing, facial recognition stops unwanted access through password theft. The system is resistant to spoofing and replay attacks because blink patterns are hard to replicate and difficult for outside observers to record. Behavioral biometrics are used to guarantee that each user's authentication is distinct.

Notwithstanding the favorable outcomes, some restrictions were noted. The accuracy of facial recognition was impacted by extremely low lighting, and very quick or involuntary blinks occasionally resulted in incorrect classification. For best results, the user must also stay in the webcam's field of view. Nonetheless, the system continued to be reliable, effective, and efficient under normal operating circumstances.

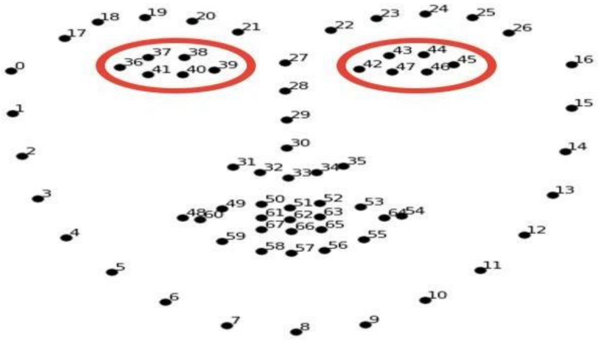


Figure 5. Real-time blink detection output

Overall, the findings support the practicality, security, and accessibility of the suggested authentication model. By combining behavioral and biometric elements into a single verification process, it offers a potent substitute for traditional password-based systems.

VII. CONCLUSION

The Human Blink Sequence as a Morse Code Authentication System combines blink-based Morse code decoding, facial recognition, and password verification into a safe, user-friendly, and efficient multi-factor authentication framework. Hands-free and contactless authentication is made possible by the system's successful demonstration of eye-blink patterns as a dependable behavioral biometric. Under typical operating conditions, the system achieves robust face recognition and accurate blink detection by utilizing real-time image processing, Haar Cascade classifiers, and facial encoding techniques.

The findings show that the suggested method offers notable benefits over conventional password-based authentication, especially in terms of lowering vulnerabilities like impersonation, shoulder surfing, and password guessing. The combination of behavioral and biometric factors adds an additional layer of security, which significantly increases the difficulty of unauthorized access. Furthermore, the hands-free design improves accessibility for individuals with motor impairments and supports hygienic, touch-free login environments.

Even though the system works well, some environmental elements, like dim lighting and fast involuntary blinks, may have an impact. However, the system's overall viability is not compromised by these drawbacks. The study confirms that blink-based Morse code, when combined with facial recognition, can serve as a practical and innovative authentication method suitable for real-world applications.

In conclusion, the work demonstrates a promising direction for future authentication technologies, offering enhanced security, improved usability, and inclusive design through the integration of computer vision and behavioural biometrics.

VIII. FUTURE WORK

Even though the suggested eye-blink-based Morse code authentication system works well in typical circumstances, there are still a number of opportunities for improvement. One potential direction involves incorporating deep-learning–based eye-state detection models, such as CNN-based or transformer-based classifiers, to improve blink recognition accuracy under challenging scenarios such as low illumination, partial occlusions (glasses, hair), or non-frontal head positions. Adaptive calibration methods could also be introduced to automatically adjust blink-duration thresholds according to the individual user’s natural blinking behaviour, improving both usability and system responsiveness.

The incorporation of liveness detection methods for facial recognition is another significant extension. Attempts to spoof existing systems with high-quality photos or videos might still be possible. Techniques such as depth sensing, thermal imaging, challenge–response gestures, micro-expression analysis, or remote photoplethysmography (rPPG) can significantly strengthen the facial verification process. Additionally, incorporating anti-spoofing for blink detection for example, detecting micro eye muscle movements would further secure the behavioural component of the system.

Future research may also investigate multi-modal biometric fusion, which goes beyond facial encodings and blinks to include gaze patterns, pupil dilation behavior, voice recognition, or keystroke dynamics for users who would rather use optional backup techniques. Such multimodal fusion may lead to more customized and flexible authentication processes that are appropriate for a variety of user groups.

Enabling cloud-based authentication pipelines can help with scalability by enabling safe management of Morse patterns and facial encodings for large-scale implementations in public systems or organizations. Optimized image-processing models could also be used to create a lightweight mobile version of the system, which would make it appropriate for wearable technology like smart glasses and smartphones.

Future iterations could support customizable Morse sequences, offer real-time feedback during blink entry, and include training modules to help novice users get used to blink-based input. The system's inclusivity could be increased by adding accessibility-focused updates, like support for users with limited blinking ability.

In general, future research should focus on improving user adaptability, scalability, and robustness. These enhancements will contribute to the system's evolution into a more complete, intelligent, and globally deployable authentication solution.

ACKNOWLEDGMENT

The Department of Computer Science and Engineering at the GSSS Institute of Engineering and Technology for Women, Mysuru, is greatly appreciated by the authors for providing the facilities, materials, and learning environment needed to complete this research project.

The authors also want to express their sincere gratitude to Mrs. Asha Rani M, their project guide, for her invaluable advice, perceptive recommendations, and unwavering support during this project. Her knowledge and helpful criticism were very helpful in determining the approach, execution, and general course of the project. The authors also thank the department's technical staff and faculty for their timely assistance and cooperation. We greatly value their readiness to assist and offer suggestions as needed.

Additionally, the authors wish to thank their peers and classmates for their encouragement, suggestions, and cooperative discussions throughout the project's development. Their assistance was crucial in improving some aspects of the system.

Lastly, the authors express their appreciation to family members for their unwavering moral support, understanding, and encouragement, all of which were crucial to the successful completion of this study.

REFERENCES

[1] P. Viola and M. Jones, “Rapid object detection using a boosted cascade of simple features,” *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2001.

[2] G. Bradski, “The OpenCV Library,” *Dr. Dobb's Journal of Software Tools*, 2000.

[3] A. Krizhevsky, I. Sutskever, and G. Hinton, “ImageNet classification with deep convolutional neural networks,” *Advances in Neural Information Processing Systems*, vol. 25, 2012.

[4] S. Liao, A. K. Jain, and S. Z. Li, “Partial face recognition: Alignment-free approach,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 35, no. 5, pp. 1193–1205, 2013.

[5] A. Jain, A. Ross, and S. Prabhakar, “An introduction to biometric recognition,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, 2004.

[6] C. Rathgeb and A. Uhl, “A survey on biometric cryptosystems and cancelable biometrics,” *EURASIP Journal on Information Security*, vol. 2011, pp. 1–25, 2011.

[7] International Telecommunication Union (ITU), “Morse Code Standard,” Recommendation ITU-R M.1677-1, 2009.

[8] F. Ahmed, R. Bari, and M. R. Islam, “Eye-blink based communication system for physically impaired people,” *International Journal of Computer Applications*, vol. 180, no. 44, 2018.

[9] D. Setu and M. Paul, “Human–computer interaction through blink detection using computer vision,” *International Journal of Advanced Research in Computer Science*, vol. 9, no. 3, 2018.

[10] G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, “Labeled Faces in the Wild: A database for studying face recognition in unconstrained environments,” University of Massachusetts Amherst, Technical Report 07-49, 2007.