

Morse Code Based Secured Authentication System Using Eye Blink

¹Sonali Verma P, ²Supreethi R, ³Vinutha Palaksha, ⁴Yogashree N, ⁵Dr. Hemanth Kumar N P

¹²³⁴Don Bosco Institute of Technology Visvesvaraya Technological University, Bengaluru, India.

⁵Associate Professor, Computer Science and Engineering, Don Bosco Institute of Technology, Bengaluru, India.

Abstract : Authentication is a part of keeping systems and personal data safe from people who are not supposed to access them. Most of the time people use passwords or PINs to get into their accounts. These methods usually need typing on a keyboard or touchscreen.. This kind of entry can be risky. Someone nearby might. Copy the password.. A hacker might guess it. The system could be broken into without permission. This paper introduces a way to authenticate users using Morse Code.. Instead of typing the user blinks in a pattern. The system uses a camera to watch the user's eyes. It detects the blinking. Turns the pattern into Morse Code. Each blink is a dot or a dash. The sequence of dots and dashes is compared to a stored pattern. If they match the user is verified. Since the user does not touch anything the system works without hands. This makes it easier and safer. The user's input is not visible, to others. The system uses computer vision and eye tracking to make this possible. It is simple and works in time. This method shows that using eye movements to enter Morse Code can be an option. It is especially useful when people need to stay secure and keep their authentication private. In places where someone cannot use their hands or where the input must stay hidden this system can be very helpful.

Keywords: Morse Code Authentication, Eye Tracking, Gaze-Based Authentication, Computer Vision, Password Security, Biometric Authentication, Hands-Free Authentication

I. INTRODUCTION

Technology has continuously changed the way people live, communicate, work and access information. As digital systems have become a part of everyday life the amount of information being generated and stored has also increased. This has created a growing need for systems that can process information efficiently while protecting it from access. Data science has emerged as a field in this development combining data analysis, computational methods and technology to obtain useful information from large amounts of data. By identifying patterns and relationships in unstructured data data science can support better decision-making and improve the efficiency of different systems. Its applications can be found in areas such, as healthcare, finance, business, image processing and user identification.

Machine learning is another area that has grown along with data science. In my view Machine learning lets computers study patterns in existing data. Then use those patterns to make predictions or decide on actions without having every single situation written out. I notice that Machine learning methods are now being used more and more in jobs like image recognition, pattern spotting and biometric identification. These moves also open doors to security and authentication systems. As online services keep expanding authentication becomes a need to make sure only the right people can reach protected resources. Old tricks, like passwords and Personal Identification Numbers (PINs) are common because they are easy and familiar. They can be seen, guessed or stolen in other ways.

Usability is as important as security when designing an authentication system. I believe a security system should not make the authentication process unnecessarily difficult for the user. I think if a security mechanism requires much effort or complex interactions users will find it hard to use and may stop following secure practices. I believe researchers have looked into authentication techniques that give security while cutting down the effort the user has to give. I think gaze-based authentication is one technique using eye movements or gaze direction, as input instead of usual physical actions. I think a camera can track the eye position across frames letting the system figure out the users intended input.

In this work Morse Code is combined with real-time eye tracking to create an authentication method. Morse Code represents information using combinations of dots and dashes and these dots and dashes can be used to build an authentication sequence. In the proposed system a camera captures the users eye movements and the detected gaze-based interactions are interpreted as Morse Code symbols. The generated sequence is then compared with the registered authentication sequence to verify the users identity. This approach provides a hands- method of entering authentication credentials and reduces the need for direct interaction with a keyboard, keypad or touchscreen. By combining computer vision, eye tracking and Morse Code the proposed system explores an interactive approach to authentication that aims to provide both usability and an additional level of privacy, during password entry.

II. LITERATURE SURVEY

Wei Hoong Chuah, Siew-Chin Chong and Lee-Ying Chong proposed a two-factor authentication approach that uses eye blinks. Their system relies on video processing and a Haar Cascade Classifier to spot intentional eye blinks. These intentional eye blinks are then used as an authentication factor. The study showed that eye blinks can act as a feature for authentication without needing a physical input device. However the accuracy of eye-blink detection can suffer when lighting conditions change and the system might also be vulnerable to spoofing attacks, such as replaying a recorded video. The study focused on eye-blink-based authentication. Did not explore the use of eye movements for entering Morse Code-based authentication sequences [1].

Buddesab, Nanda Ashwin, Shruthi M, Rekha P and Pavan Mulgund developed a password authentication system that relies on eye blinking. In their study a webcam was used to watch the user's eyes and pick out blink patterns in time. These blink patterns were then turned into password characters to form the required password sequence. The method gives a hands-free way of entering a password without needing a keyboard or touchscreen. However the system has limitations, especially the slower speed of entering passwords and the challenge of distinguishing intentional eye blinks from normal involuntary blinking. The study therefore points to the need, for accurate eye-blink detection and faster input methods to make eye-based authentication more reliable and convenient [2].

Rekha Jayaram, Ramya M Sandhya A Sinchana M K and Tejashree proposed an eye blink-based PIN authentication system that relies on the Histogram of Oriented Gradients (HOG) algorithm. In their study HOG was used to pull out characteristics from the eye area and to spot patterns by looking at how the gradient directions change. This approach helped the eye blink-based PIN authentication system spot eye blinks with precision and to use those blinks for entering a PIN. Yet the eye blink-based PIN authentication system can suffer when the user moves the head because changes in the user's position can alter how the system detects blinks. The eye blink-based PIN authentication system also needs the camera to stay in one place and to be very steady.

Thus while the eye blink-based PIN authentication system enhances blink detection it faces limits when the user or the camera is not stable [3].

A. Balaji, Doppalapudi Balanjali, Guntu Subbaiah, Avula Anil Reddy and Daggubati Karthik introduced a biometric authentication system that blends facial recognition with eye-blink data using federated deep learning. Their method combines features with blink patterns to confirm a person's identity, which makes the multi-modal biometric authentication system more dependable and harder to trick. By using two biometric signals the multi-modal biometric authentication system can deliver stronger security than a single cue alone. However the multi-modal biometric authentication system demands a lot of computing power because of the deep learning models involved. It also requires storage and careful handling of facial and eye data, which are sensitive. The research shows the advantage of mixing signals but the heavy resource needs may make it tough to run on devices with limited power [4].

Krishnakanth Medichalam, V. Vijayarajan, V. Vinoth Kumar, I. Manimozhi Iyer, Yaswanth Kumar Vanukuri and V. B. Surya designed an eye tracking with Morse Code recognition system that merges eye tracking and Morse Code for communication. Their focus is on helping people those with disabilities to talk using eye movements instead of normal input tools. Artificial intelligence helps to detect and read eye movement patterns and to turn them into Morse Code symbols. The study is especially useful for the work because it proves that eye tracking and Morse Code can be combined effectively for input recognition. Yet the accuracy of the eye tracking with Morse Code recognition system may drop when the user's eyes move involuntarily and the system depends on good hardware for reliable eye tracking. While the study talks about communication of authentication it offers a solid basis for using eye-tracking-based Morse Code recognition in authentication systems [5].

A. Srivastava introduced an intelligence-based authentication system that uses Morse Code as the main way to verify users. The system applies pattern classification and supervised learning to recognize and interpret Morse Code signals during authentication. The study shows that artificial intelligence can identify Morse patterns and process them reliably indicating that Morse Code could be an alternative input for secure authentication. Nevertheless the Morse Code authentication system needs users to know Morse Code before they can use it which might make it less convenient for people who're new to Morse signals. The authentication process can also be slower than some methods. Despite these drawbacks the research confirms that Morse Code authentication is doable and provides a path, for secure authentication and communication [6].

I think learning Morse Code is challenging. The system could still be useful. Renuka N. And Devaraju B. M. Proposed a secured authentication system that combines eye blinks with Morse Code to provide an alternative to password and PIN-based authentication. Their system uses the Haar Cascade algorithm to detect the users face and eyes while the Facial Landmark algorithm is used to track eye movements and identify blinks. The detected blink patterns are then converted into Morse Code in the form of dots and dashes which are used to generate a PIN for authentication. This approach reduces the need for password entry and provides a biometric-based method of authentication. The study shows that combining eye-blink detection with Morse Code can be useful for developing a secure and hands-free authentication system. However the effectiveness of the system depends on eye detection and reliable blink recognition during the authentication process [7].

Pushya D., Shreyas N., Shreya P. And Sandeep Varma N. Proposed a two-step authentication technique called FDMCA, which combines face detection with gaze-based Morse Code password entry. In the stage the system verifies the users identity through real-time face recognition. After face verification the user enters the password using eye blinks, where different blink patterns represent the dots and dashes of Morse Code. A keyboard and camera-based eye tracking are used to detect and interpret the users gaze and blink patterns. The two-step authentication process provides a layer of security and helps reduce the risk of attacks such as

shoulder surfing, thermal tracking and keylogging. The study demonstrates that combining recognition with gaze-based Morse Code input can provide a secure and contactless authentication method. However the effectiveness of the system depends on face detection and reliable tracking of eye movements during password entry [8].

S. Sushmitha, H. B. Prasad and V. M. Sapna proposed a -layer authentication system that combines facial recognition, login credentials and Morse Code-based eye-blink detection. Their approach uses facial landmark detection and Convolutional Neural Network (CNN) techniques to identify eye blinks and distinguish the users intended blink patterns. The detected blinks are interpreted as Morse Code signals allowing users to enter authentication information through combinations of dots and dashes. By using authentication layers the system provides stronger protection against unauthorized access compared with traditional PINbased methods. The approach also offers an accessible form of authentication for users who may have difficulty using conventional input devices. However the overall performance depends on facial and blink detection particularly when there are changes in lighting, head position or other environmental conditions [9].

Ranjani G., Swapna H. A., Chandrashekar Gurammanavar, S. Balaji, Darshan B. Surname and Aishwarya D. M. Proposed a multimodal authentication system that combines recognition Morse Code-based input and OTP verification. The system uses a webcam along with Python modules to detect and verify the users face before proceeding with the authentication process. For password entry the user can provide eye blinks of different durations, which are interpreted as Morse Code symbols. The system also supports input methods, such as mouse gestures and uses encrypted storage to protect authentication information. An additional fallback verification mechanism is included to provide another way of confirming the users identity when required. The study demonstrates that combining authentication methods can provide stronger protection, than relying on a single authentication technique. However the use of verification stages may increase the complexity and time required to complete the authentication process [10].

Paparao Nalajala, Bhavana Godavarthi, M. Lakshmi Raviteja and Deepthi Simhadri developed a Morse Code generation. Decoding system using a microcontroller and an alphanumeric keypad. In their system users can enter letters and numbers through the keypad. The input is converted into the Morse Code signals. The generated Morse Code can be transmitted to another device. It is also displayed on an LCD screen. This makes it easier for the user to view and understand the encoded information. The study shows how a simple microcontroller-based system can be used to generate and decode Morse Code for communication purposes. However the system mainly depends on keypad input. It does not include a hands- biometric authentication mechanism such as eye tracking or eye-blink detection [11].

Cheng-Hong Yang, Li-Yeh Chuang, Cheng-Huei Yang and Ching-Hsing Luo proposed an environmental control system that uses

Morse Code to help severely disabled individuals interact with electronic devices. The system allows users with disabilities to send Morse Code signals. These signals are. Converted into commands for controlling different devices. The proposed system consists of modules for user input Morse Code recognition, wireless communication and device control. This allows the commands to be transmitted and executed remotely. The study demonstrates that Morse Code can be used as an alternative means of communication and device control for individuals who have difficulty using conventional input methods. However the system is mainly designed for control and communication rather than user authentication. Its performance depends on the reliability of the input and Morse Code recognition process [12].

Mrs. Pavitra S. R. Proposed a gaze-based PIN authentication system as an alternative to password entry methods. In this approach users do not need to type their PIN using a keyboard or keypad. Instead a smart camera is used to detect the users eye position and track the direction of their gaze. The detected gaze movements are then used to identify the numbers selected by the user and generate the PIN. This approach provides a contactless method of entering authentication credentials. It can help reduce the risk of exposing the PIN through physical input. However the system relies on eye tracking and a suitable camera setup. This may affect its performance when the users gaze or camera position changes [13].

Bhumika K. L., E. Vennela Chowdary, Harshitha T. And Asha Rani M. Proposed a hands- authentication system called HumanBlinkSequence. This system uses eye blinks as Morse Code signals for user authentication. Their system uses OpenCV and facial landmark detection through the dlib library to monitor the users eyes. It calculates the Eye Aspect Ratio (EAR) for identifying blinks. The detected intentional blinks are converted into dots and dashes. These are then compared with the stored authentication pattern to verify the user. This approach eliminates the need for a keyboard or other physical input device. It can be particularly useful for users with motor abilities. However the system depends on blink detection. Distinguishing blinks from natural or involuntary eye movements can affect the reliability of authentication [14].

Sunil Gowda S. And Smitha N. Proposed a Morse Code-based authentication system that uses intelligence and a webcam to provide an alternative method of password entry. In their approach the webcam is used to monitor the users eyes. It detects intentional eye blinks and movements. These blink patterns are then interpreted as Morse Code symbols in the form of dots and dashes. They are compared with the stored password to verify the users identity. Image processing techniques are used to support eye tracking. These techniques help identify the users intended input during the authentication process. The system provides a hands- approach to password entry. It reduces the need for physical input devices. However the reliability of the system depends on eye and blink detection. Variations, in eye movement or environmental conditions may affect the authentication process [15].

Table 1: Competitive analysis of Morse code authentication

Ref.	Technique	Input	Morse Biometric	Main Limitation
[1]	Blink + Haar Cascad Blink	X	✓	Lighting, spoofing
[2]	Blink Password Blink	X	✓	Slow, involuntary blinks
[3]	HOG Blink PIN Blink	X	✓	Head movement
[4]	Deep Learning Face + Blink	X	✓	High computation
[5]	AI Morse Recognition Eye tracking	✓	✓	Hardware dependency
[6]	AI Morse Authentication Morse	✓	X	Slow, needs Morse knowledge
[7]	Blink + Morse Blink	✓	✓	Blink detection
[8]	FDMCA Face + Gaze	✓	✓	Multiple stages
[9]	Multi-layer System Face + Blink	✓	✓	System complexity
[10]	Morse + OTP Face + Blink	✓	✓	More authentication time
[11]	Microcontroller Morse Keypad	✓	X	Physical keypad

[12]	Wireless Morse Control Morse	✓	✗	Device-control focused
[13]	Gaze PIN Eye gaze	✗	✓	Camera dependency
[14]	Human Blink Sequence Blink	✓	✓	Blink accuracy
[15]	AI Morse System Eye + Blink	✓	✓	Tracking/environment
	Proposed Morse + Eye Tracking Eye gaze	✓	✓	Eye detection accuracy

III.FINDINGS

The review of the selected research papers shows that different methods have been explored to make authentication more secure and easier to use. A number of studies have used eye blinks as an alternative to entering passwords through a keyboard or keypad. Other studies have used eye gaze, facial recognition and Morse Code for authentication or communication. These methods show that eye-based interaction can be useful for hands- authentication. At the time the reviewed studies also show that detecting eye blinks or gaze accurately can be difficult when there are changes in lighting, head position, camera placement or natural eye movements.

Morse Code is also found to be a method for representing authentication information. By using dots and dashes a user can create a sequence without directly entering a conventional password. Some of the reviewed works have already combined Morse Code with eye blinks or facial features, which shows that this type of interaction is possible in real-time systems. However some approaches require verification methods such as facial recognition and OTPs which can make the authentication process more complicated and time-consuming. Other Morse Code systems depend on devices such as keypads, which means they cannot provide a completely hands-free experience.

When the different approaches are compared each method has its advantages and limitations. Blink-based systems are simple and hands-free. They can sometimes mistake natural blinking for an intentional input. Gaze-based systems avoid this problem to some extent by using the direction or position of the users eyes. They require accurate tracking of eye movement. Systems that combine authentication methods can provide additional security but they also require more processing and more steps from the user. These differences show that there is still scope for developing an authentication method that's simple hands-free and does not depend heavily on additional hardware or multiple verification stages.

The proposed system combines the ideas found in these previous studies by using real-time eye tracking along with Morse Code for authentication. In this approach the user does not need to type a password using a keyboard, keypad or touchscreen. Instead eye movements are detected through a camera. Used to generate Morse Code symbols in the form of dots and dashes. The generated sequence is then checked against the registered authentication sequence. This makes the authentication process contactless and hands-free while keeping the basic interaction simple.

From the comparison the proposed system provides a combination of features that are useful for an alternative authentication method, including real-time operation, eye-based interaction Morse Code input and reduced dependence on physical input devices. The system still has challenges in accurately detecting eye movements under different conditions. However the findings from the reviewed papers support the use of eye-based

Morse Code as a direction, for authentication and provide a foundation for further improving the proposed system.

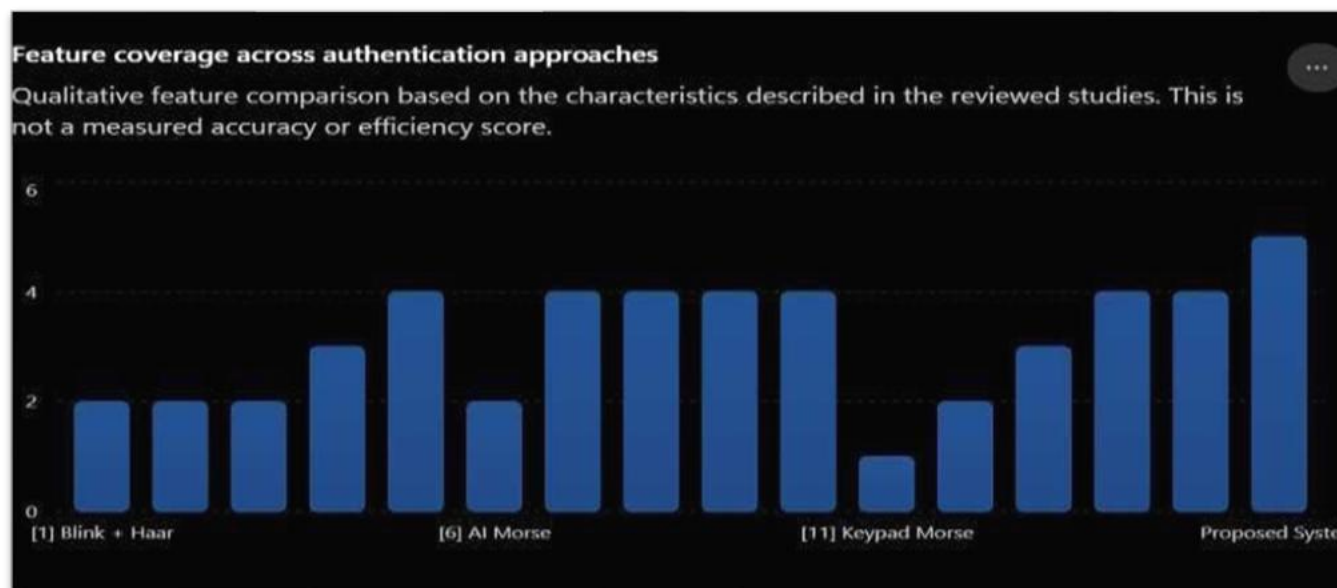


Figure 1 : Efficiency comparison table of Morse code Authentication

IV. IMPLEMENTATION

The proposed system was built as a real-time authentication application. It uses eye movement and Morse Code of relying only on regular password entry. The whole system was developed using Python. It includes a graphical user interface or GUI to make the app simple and easy for users to work with. First the user must register in the system. During registration they enter a username, a password and a keyword for recovery. These details are stored securely in the system. They are used later when the user tries to log in. When the login process starts the system checks the entered username and password. If the login is successful the system turns on the webcam. Then it moves to the eye-based authentication stage. The main idea here is to let the user authenticate themselves using their eye movements of typing a password with a keyboard or keypad. Since a webcam is used the system works with computer hardware. This makes it accessible and practical, for use.

For detecting the users face and eyes OpenCV is used for image processing and webcam handling. The system uses the Haar Cascade Classifier to locate the face and eye regions in the captured video frames. The webcam continuously provides frames. Each frame is processed to find the required facial region. After the face is identified the eye region is. Tracked while the user is interacting with the system. Haar Cascade was selected because it is relatively simple to implement and can perform face and eye detection in time. OpenCV also handles the reading of the webcam feed and the processing of the captured images. By checking the eye region the system can observe the users interaction and use the detected movement as an input. This makes it possible to perform the authentication process without asking the user to press keys or buttons.

The detected eye interaction is then used to enter the authentication password in Morse Code. Morse Code represents information using two symbols, a dot and a dash and these symbols are used by the system to create the authentication sequence. Based on the eye interaction defined in the application the users input is recorded as dots and dashes in the order. For example a particular eye action can be treated as a dot and another defined action can be treated as a dash. As the user continues providing input the system stores the symbols. Forms the complete Morse Code sequence. Once the required sequence has been entered it is. Matched with the corresponding stored authentication value. The system then compares the entered sequence with the registered sequence. When the two sequences are the same the authentication is considered

successful. The user is allowed to proceed. If the sequences do not match the system treats the attempt, as unsuccessful. Provides the appropriate next step.

To make the system easier to use I added a recovery option. When the gaze-based authentication does not succeed the user is asked to type the keyword that was given when the user signed up. The keyword is a way to check that the person who wants the account is the real user. If the keyword is typed correctly the system lets the user create or change the password. The new password can be entered again with the Morse Code method. Is then saved for later use. If the keyword is wrong the password stays the same. The user is asked to exit the application. This part of the system is handy because eye tracking can fail when lighting changes, the camera moves the user moves or other things happen. Having a recovery option gives the user another way to get in without turning off the main eye-based authentication.

The interface links all these functions. Shows the user what to do next. There are options for registration and login and the system shows clear messages when the user logs in fails updates the password or exits. The webcam and eye-detection only run when needed, not all the time. This keeps the process simple for the user. All parts of the system—Python code, OpenCV, Haar Cascade face and eye detection, webcam input, eye tracking, Morse Code conversion, password comparison and keyword recovery—work together as one authentication process. The implementation gives a way to use eye-based input for authentication without special biometric gear.

During implementation I also looked at the problems that can happen when using a webcam for eye tracking. Detection quality can vary with lighting how the face is positioned how far the user is, from the camera and natural eye movements. Because of this the eye detection and tracking must be checked all the time so that accidental movements are not taken as authentication. These limits do not stop the system from proving the idea but they matter for real use. Overall the implementation shows how Haar Cascade, OpenCV, eye tracking and Morse Code can come together in one app to make a hands-free authentication system..

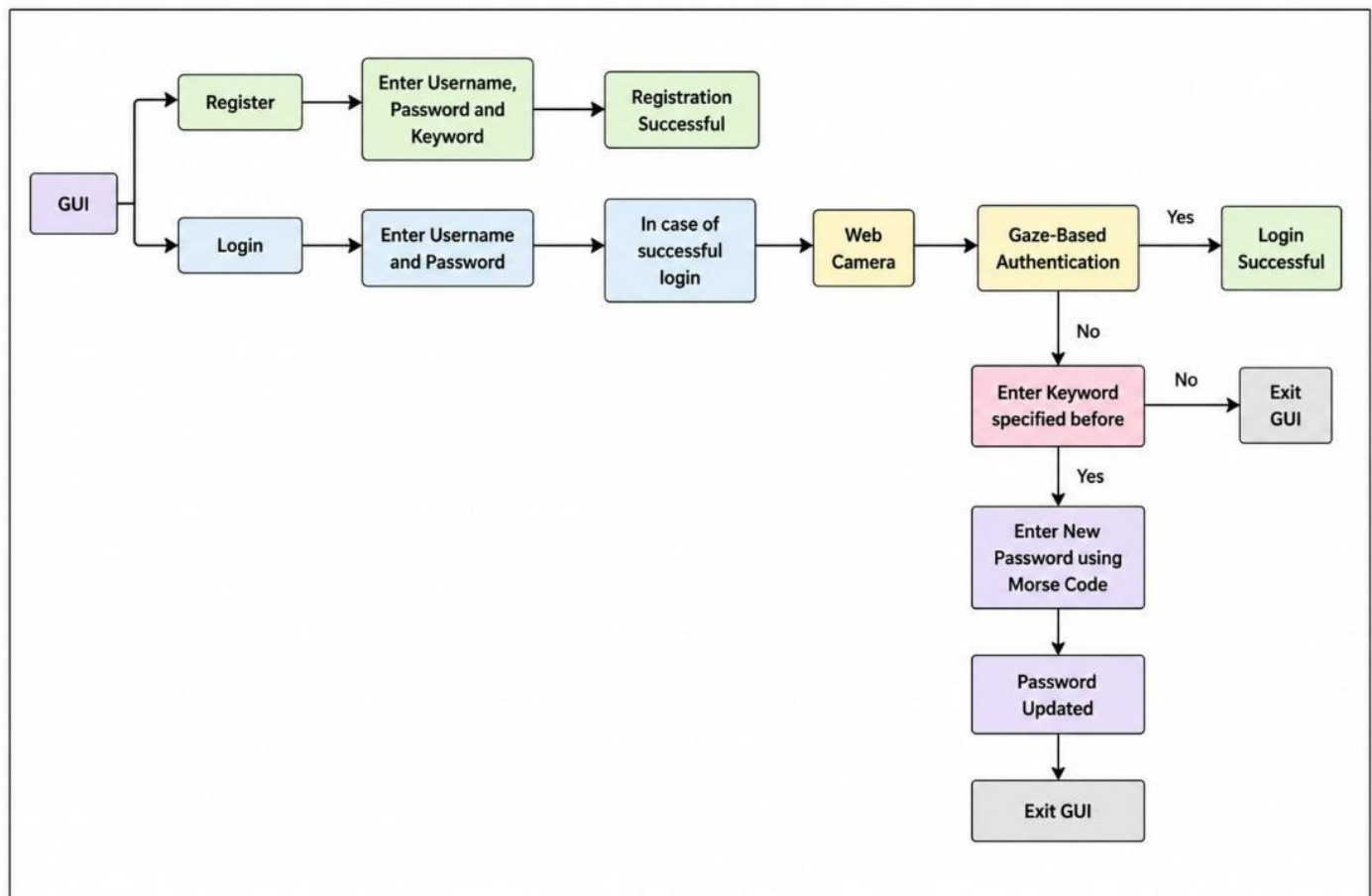


Figure 2: Implementation architecture

V. METHODOLOGY

The proposed system was built by combining three authentication methods: an username and password face verification and Morse Code that is entered with eye blinks. The first step was to read research about eye-blink detection, Morse Code, facial recognition and biometric authentication. That research guided the choice of methods that would fit a webcam and would react while the user is looking at the camera. From that research the designers made a plan in stages so that registration, face capture, blink detection, Morse Code translation and authentication all work together. The main aim was to make the process easy for the user without needing any eye-tracking gadget.

The first part of the process is detecting the users face and eyes from the webcam video. Python is used to develop the application while OpenCV reads the webcam feed and processes the captured frames. The Haar Cascade Classifier locates the face and eye regions in the video. Once the eye area is found the system continuously checks the eye position. Whether the eyes are open or closed. This continuous checking is necessary because authentication input is provided while the camera is running. The Haar Cascade method was chosen because it is simple and works well for real-time image processing, which's essential, for this type of application.

After eye detection the system uses the length of every blink to create Morse Code. A brief eye closure becomes a dot (.) whereas a longer eye closure becomes a dash (-). As the user keeps blinking the system records each dot and dash in order. Builds a Morse Code sequence. Once the entire sequence is entered it is decoded using a predefined Morse Code mapping. The decoded result is then used as part of the users authentication data. This method gives the user a way to enter a sequence without physically typing on a

keyboard. The durationbased method also helps deliberate input from normal blinking although natural eye movements can still affect detection.

Table 2: Morse Code Table (A–Z, 0–9)

Character	Morse Code	Character	Morse Code
A	• —	N	— •
B	— • • •	O	— — —
C	— • — •	P	• — — •
D	— • •	Q	— — • —
E	•	R	• — •
F	• • — •	S	• • •
G	— — •	T	—
H	• • • •	U	• • —
I	• •	V	• • • —
J	• — — —	W	• — —
K	— • —	X	— • • —
L	• — • •	Y	— • — —
M	— —	Z	— — • •
0	— — — — —	5	• • • • •
1	• — — — —	6	— • • • •
2	• • — — —	7	— — • • •
3	• • • — —	8	— — — • •
4	• • • • —	9	— — — — •

• (dot) = short blink
— (dash) = long blink

The system also uses face recognition to make the authentication process more reliable. During registration the webcam captures the users face. The image is converted into a facial encoding using the face-recognition library. This encoding is stored with the users account details. When the user tries to log in another image is captured and a new encoding is generated. The two encodings are compared to check whether the person in front of the camera is the person who registered earlier. In addition to face recognition the project uses landmark detection to identify important points around the face and eyes. The landmark points help in following eyelid movement closely and distance calculations can be used to understand changes, in the eye region.

The application interface was created using **CustomTkinter**, which provides the screens needed for registration and login. During registration, the user enters the required account information, provides a face sample, and creates the Morse Code sequence using eye blinks. These details are then saved for future verification. During login, the user first enters the normal credentials. After that, the webcam is used for face checking and eye-based Morse Code entry. The different parts of the application communicate with the main authentication logic so that the result from each stage can be checked before the final decision is made.

The complete authentication process follows a simple sequence. The user first registers the required information, including the password, facial information, and Morse Code pattern. During a later login, the entered credentials are checked first. The webcam then captures the user's face, the face is compared with the saved facial information, and the eye region is monitored for the Morse Code input. The blink pattern is converted into dots and dashes and then compared with the stored sequence. In the three-factor version described in the project, access is given only when the required password, face, and Morse Code information are successfully matched. This makes the system depend on more than one type of user information rather than relying only on a password.

VI. RESULT ANALYSIS

I tested the system to see whether the different parts could work together during use. The testing mainly focused on face detection eye-blink detection, Morse Code conversion and the overall authentication process. The system was also observed under changes in lighting, speed and camera position since these factors can affect what the webcam captures. The results described in the project show that the individual modules could be connected into one working authentication process and that the system could perform its tasks using a standard computer and webcam.

I noticed that the webcam is essential. The webcam gives live frames for face recognition and eye-blink detection. When the image is clear and the user stands correctly the system can spot the face and eyes. Move on. The Morse Code part then uses the length of each blink to decide if it is a dot or a dash. This lets the user give a sequence without touching a keyboard or keypad. At the time the test shows why camera position and lighting matter; changes in these conditions can make eye detection less reliable.

The face-recognition stage adds another check before access is granted. Than accepting the Morse Code sequence alone the system can first compare the live face with the stored face data. This means the authentication process uses both what the user knows and data about the user's face and eye behavior. The combination is meant to make the system harder to bypass than a password method. The project also calls the system hands-free, which can help people who struggle with keyboards or touchscreens.

The test also points to limits. Eye-based input depends on the camera image quality, surrounding light face position and normal eye movements. A person may blink naturally while using the system and these natural blinks can be hard to separate from blinks. For this reason reliable eye detection is essential for authentication results. The project also lists lighting, head position and camera quality as factors that can affect blink detection

Overall the implementation shows that Python, OpenCV, Haar Cascade, facial landmark detection face recognition, Morse Code processing and CustomTkinter can be combined to build a hands-free authentication application. The approach is practical because the main hardware needed is a webcam and a computer, not a special eye-tracking device. Still the system should be tested with users and, under a wider range of conditions before claiming high accuracy or reliability.

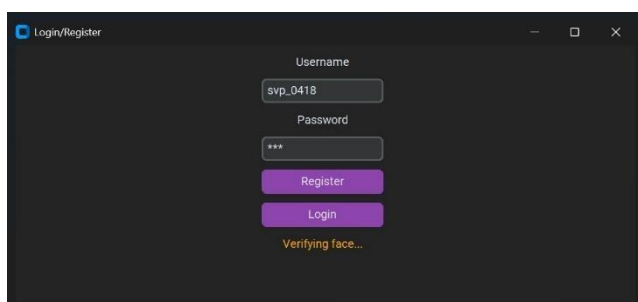


Figure 3: Login by Morse Code

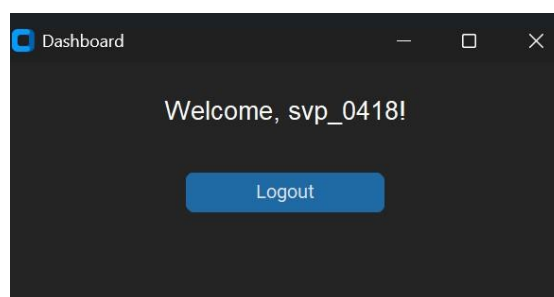


Figure 4: Final Output

V. CONCLUSION

Authentication is important for keeping systems and personal information safe. From the papers we reviewed it is clear that researchers have tried methods such as eye blinking, eye movement, face recognition, Morse Code and artificial intelligence to improve the traditional password and PIN systems. These methods can make authentication easier. Reduce the need for typing on a keyboard or keypad. However they also have some common problems, such as difficulty in detecting eye blinks correctly changes in lighting, head movement and camera position. To address some of these issues our proposed system combines real-time eye tracking with Morse Code. The camera detects the users eye movements. Converts them into dots and dashes which are then used to create an authentication sequence. The sequence is compared with the stored password to check whether the user is authorized.

The proposed system provides an hands-free way of entering a password without directly using a keyboard or keypad. It brings together eye tracking and Morse Code in one authentication process. Can be useful where normal password entry is not convenient. At the time the system still needs to handle problems such as accurate eye detection and changes, in the surrounding environment. In future the system can be improved by making eye tracking more accurate reducing errors caused by eye movements and testing it with different users and lighting conditions. These improvements can help make the proposed authentication method reliable and easier to use in real-world situations.

REFERENCES

- [1] W. H. Chuah, S. C. Chong, and L. Y. Chong, "The Assistance of Eye Blink Detection for Two-Factor Authentication," *Journal of Computer Science Research*.
- [2] Buddesab, N. Ashwin, S. M., Rekha P., and P. Mulgund, "Real-Time Eye-Based Password Authentication by Eye Blinking System," *International Journal of Innovative Research in Technology*.
- [3] R. Jayaram, R. M., S. A., S. M. K., and T. R., "User Authentication Through Eye Blink-Based PINs Using Histogram of Oriented Gradients Algorithm," *International Journal of Advanced Computer Science*.
- [4] A. Balaji, D. Balanjali, G. Subbaiah, A. A. Reddy, and D. Karthik, "Federated Deep Learning for Robust Multi-Modal Biometric Authentication Based on Facial and Eye-Blink Cues," *Journal of Biometric Systems*.
- [5] K. Medichalam, V. Vijayarajan, V. Vinoth Kumar, I. M. Iyer, Y. K. Vanukuri, and V. B. Surya Prasath, "Trustworthy Artificial Intelligence and Automatic Morse Code Based Communication Recognition with Eye Tracking," *River Publishers Journal of Artificial Intelligence*.
- [6] A. Srivastava, "Morse Code Authentication System Using Artificial Intelligence," *International Journal for Research in Applied Science and Engineering Technology (IJRASET)*, vol. 10, 2022.
- [7] R. N. and B. M. Devaraju, "Morse Code Based Secured Authentication System Using Eye Blink Through Haar Cascade and Facial Landmark Algorithm," *International Journal of Engineering Research*.
- [8] P. D., S. N., S. P., and S. V. N., "FDMCA: A Novel Authentication Technique Using Face Detection and Gaze-Based Morse Code Entry," *IEEE Conference on Computer Vision and Security Systems*, 2021.
- [9] S. Sushmitha, H. B. Prasad, and V. M. Sapna, "Multi-Layer Secure Authentication Using Morse Code and Eye Blink Detection," *IEEE Conference Proceedings*.
- [10] R. G., S. H. A., C. Gurammanavar, S. Balaji, D. B., and A. D. M., "PIN Authentication Using Morse Code," *IEEE Conference Proceedings*.
- [11] P. Nalajala, B. Godavarthi, M. L. Raviteja, and D. Simhadri, "Morse Code Generator Using Microcontroller with Alphanumeric Keypad," *IEEE Conference Proceedings*.
- [12] C. H. Yang, L. Y. Chuang, C. H. Yang, and C. H. Luo, "Morse Code Application for Wireless Environmental Control Systems for Severely Disabled Individuals," *IEEE Conference Proceedings*.
- [13] P. S. R., "Eye Tracking Using Gaze PIN Entry for Password Authentication," *International Journal of Engineering Research*.
- [14] B. K. L., E. V. Chowdary, H. T., and A. R. M., "Human Blink Sequence as a Morse Code Authentication System," *International Journal of Computer Science and Engineering*.
- [15] S. Gowda and N. Smitha, "Morse Code Based Secured Authentication System Through Artificial Intelligence," *IEEE Conference Proceedings*.

Copyright & License:

© Authors retain the copyright of this article. This work is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.