Login Page using Face Recognition

Prof. Aruna Kamble[1], Nilesh Thote[2], Harsrita Mishra[3], Vrushali Meher[4]

[1]Prof., Dept of Computer Engineering, Bharati Vidyapeeth College of Engineering Navi-Mumbai, Maharashtra, India.

---***---

Abstract - *Facial recognition is very useful and has various application in various sector some of the example are Snapchat filter, Photo tagging. But in login services using face recognition has been used only with complex and costly technologies for example iPhone X. The aim of This project is to use machine learning techniques so as to differentiate user with normal web camera and for more security we are using gesture recognition to make face recognition logins more accessible for website and software developer. To point the practicality of the thought, we created a web application that recognize a user's face to log them in to their account.*

1. INTRODUCTION

Computer security is a important concept to prevent the loss or theft of data for almost any software or hardware that is designed. It is important for a number of reasons; it is a means of keeping information safe. The term computer security refers to the security of the data and information, that most users store on their hard drives. Mostly people want computer security in corporate or business sector. Companies store a lot of very sensitive information electronically, including, trade secrets, extensive corporate documents and customer lists, both those in progress and finished. The importance of computer security is must. It is also must for home computer users. Computers are not open to risks such as data breach or hacking. In order for outsiders to get into a computer, the computer must open itself up to intrusion. Internet activity is the primary highway. Many users do not realize that accessing the web could make computers more vulnerable. So, user authentication is a process that allows a device to verify the identity of the user who is using the system. User authentication is mandatory for the security of the Network system and Computer.

Current methods like token-based security or password are very popular but have numbers of flaws like passwords can be stolen, hacked or forgotten, it is very common to notice that people are using very simple passwords like birthdates, 1234567, names etc. or use same password for different applications as a solution to forgetting passwords. As complex passwords are more secure, though they are difficult to remember.

Similarly, in token-based method the tokens can be duplicated for misuse or stolen. Over traditional password and token-based authentication methods the biometric based authentication system offers several advantages. The biometric systems also raise several privacy concerns. A biometric authentication system cannot be changed or modified and is permanently associated with the user.

2. LITERATURE REVIEW

Face recognition is an successful and interesting application of Image analysis and Pattern recognition. Face Recognition is one of the most popular biometrics authentication technique from the past few years. Face recognition system does two main tasks: identification and verification. According to Research advance in integration of big data and soft computing "Face identification means a 1: N problem which compares a query face image against all image templates in a database"and"Face verification means a 1:1 match which compares a face images against a template face images whose identity being claimed". Recognition of faces is becoming very important due to its wide range of law enforcement and commercial applications, which includes border surveillance, access control, forensic identification and availability of low-cost recording devices and human interactions. For the purpose of human recognition various biometric features can be used like hand geometry, fingerprint, speech, palm print, face, gaits, signature, iris etc. Face recognition is a process which does not require active co- operation of a person so without instructing the person can recognize the person while the problem with finger print, iris palm print, speech, gaits are they require active co-operation of person. Hence, face recognition is much more advantageous as compared to the other biometrics.

Yogish Naik said that"Face recognition features a recognition rate or high identification of greater than 90% for huge face databases with illumination conditions and well-controlled pose".

Che-Wei Lee described that new blind image authentication method with a input repair capability for binary-like grayscale document images depending on secret sharing has been proposed. The generated content and the authentication signal of a block have been transformed into partial shares.

Yan Zhao said that Image hashing is the technique that is used for authentication. Hashing is the process of extracting some features from image & authenticating by comparing these features, he has also described different methods of authentication. Both local and global features are used and have tried to provide good efficiency with short image hash. A practical method for real-time and non- contacting feature extraction for personal authentication is proposed using palm and finger feature extraction method. This is the traditional method for authentication.

Konstantinos Moustakas presents a novel framework for gait recognition which is augmented with soft biometric information. Geometric gait analysis is based on gait energy images and on radon transforms "User stride length and height information's are extracted and then utilized in a probabilistic framework for detection of soft biometric features of considerable discrimination power".

Judith Liu-Jimenez has shown a case of high security environment, where low error rates are vital, the microprocessor solution is suggested, especially when the number of individuals in the system are high; however, if the number of users is of lower size and execution times are significant constraints, the dedicated hardware solution should be chosen.

Konstantinos Moustakas presents a novel framework for gait recognition which is augmented with soft biometric information. Geometric gait analysis is based on gait energy images and on radon transforms "User stride length and height information's are extracted and then utilized in a probabilistic framework for detection of soft biometric features of considerable discrimination power".

Hard biometric and soft biometric are the different methods used for authentication hard biometric has the advantage that it requires less memory while the possibility of error is more in hard biometric and efficiency is less, while soft biometric has good efficiency. Research on biometric methods has gained attention in recent years because of an increase in security concerns. Many biometric techniques are developed and are being improved with the foremost successful being applied in everyday enforcement and security applications. Biometric methods include many state-of-the-art techniques. Fingerprint recognition is considered one of best technique for security authentication.

3. METHODOLOGY

Human facial expressions are often easily classified into 7 basic emotions: happy, sad, surprise, fear, anger, disgust, and neutral. With the help of specific set of muscle Emotion are expressed. These sometimes subtle, yet complex, signals in an expression often contain an abundant amount of knowledge about our state of mind. For instance, retailers may use these metrics to determine customer interest. Healthcare providers can provide better service by using additional information about patients' spirit during treatment. Human are trained in reading emotions. But can computers do a much better job than us in accessing emotional states? To answer the question, we designed a deep learning neural network that provides machines the power to create inferences about our emotional states. Inother words, we give them eyes to visualize what we are able to see.

Facial expression recognition is performed by humans or computers, which consist of:

A. Facial expression recognition is performed by humans or computer.
B. Extracting facial features
C. Analyzing the motion of the features of the face and/or the changes in the appearance of the features of the face and classifying this information into some facial- expression like happy, sad, angry etc.

4. PROBLEM STATEMENT

In many system passwords or tokens are used which can be easily stolen or forgotten. So, system is less secure and hence facial recognition is used in order to overcome these issues. However, there is an obvious issue with using facial recognition ie. Anyone can use your picture in order to login to your account or system. Hence apple has provided a solution to this photo trick by relying on dual camera and an array of projected infrared dots. But such a solution is limited to expensive hardware and can't be applied to lower cost applications. Hence, we require a system to address these issues, that will use a video stream, rather than a still image, to check whether the correct user is logging into the system. However, this system can be spoofed by simply holding a video Infront of the camera, so the system will also ask the user to perform some random gestures to ensure whether it's a real person in front of the camera. Therefore, it can be used for wide range of application as its purely software based.

5. CONCLUSION

User authentication is very important for security of network systems and computers. It is the process that allows the device to verify the identity of someone who is using the system. The proposed method can be used to prevent the confidential data of the system to be access by the unauthenticated user. Since the face recognition algorithm we use is over 99% accurate, the positioning only must compare the user's face to at least one stored image, instead of against a 1,000,000 different faces like Face- book, and this implementation checks the user's identity over several frames, therefore its believe that face recognition is a secure, reliable, and straightforward method of authentication.

In the future, there might not even be need for passwords or captcha checks to prevent bots.

REFERENCES

[1] http://ijcttjournal.org/Volume5/number- 4/IJCTT-V5N4P136.pdf

[2] https://pdfs.semanticscholar.org/7be7/26b5f7659a3418517056afbebafb981854ee.pdf

[3] http://www.mecs-press.org/ijem/ijem-v8-n1/IJEM-V8-N1-6.pdf

[4] http://ijcttjournal.org/Volume5/number-4/IJCTT-V5N4P136.pdf