Continuous Authentication using Biometrics Techniques to prevent Session Hijacking

Jignesh Patel, Abhijeet Sonaje, Kaustubh Vaidya, Prof. Kailas Devadkar
Sardar Patel Institute of Technology, Mumbai, India.
patel.jignesh705@gmail.com, sonaje.abhijeet@gmail.com, kaustubh.213@gmail.com, kailas_devadkar@spit.ac.in

Abstract: Session hijacking attacks are one of the commonly experienced cyber threats in today's Internet. The primary reason behind session hijacking is the authentication process that only takes place during the initial login process. The session is initiated once both the users are authenticated. But the main issue regarding this is, the attacker could obtain the session key and hijack the ongoing session, thus getting access to messages he is not authenticated to see. To avoid session hijacking, continuous authentication is required. This project presents a method for providing continuous user authentication using biometric techniques such as face recognition and pattern matching. To avoid inconvenience caused to users due to continuous authentication, the process must be kept transparent to the user. Along with the traditional user id and password requirement, blink detection is done as well to provide additional authentication. The attacker is thus restricted from hijacking the session due to continuous authentication method like pattern matching. If the continuous authentication fails, the session is suspended and the face recognition method is invoked. Also, encryption algorithm is implemented on both sides to prevent message sniffing.

Key Words: Continuous Authentication; Blink Recognition; Eigen Faces.

1. INTRODUCTION
In this advanced world of cyber technology, the hackers try to stay one step ahead of the security measures taken to secure any system. Industry experts have over the years came up with various measures to curb the cyber attacks, introducing new softwares, algorithms, tools one after the other. Out of many such security techniques, biometric security check has proved to be one of the most effective ones.

Face recognition is applied worldwide today, the applications ranging from mere mobile application to top-security database. The advanced algorithms for face recognition available today have managed to obtain an optimal level of accuracy. Merging this technology with the authentication process will provide an enhanced sense of security which is user friendly at the same time.

2. LITERATURE SURVEY
Various modules of the project required referring to different papers and understanding the working of those modules. A brief overview of tracking strategies like region based, active contour based, etc. with their positive and negative aspects. A continuous authentication scheme that continuously monitors and authenticates the logged in user. An eye detection algorithm for employing blink detection, which is capable to detect eye blinks along with the relative eyelid movement. The face detection approach which combines Haar-like features and the convolutional neural network for the final verification. There have been various studies related to continuous authentication. Many of such studies include the use of soft biometric traits, but none of them uses the most accurate method of face recognition with the traditional authentication process.

Niinuma and Jain proposed a system for session management through continuous authentication, but using the soft biometric traits like color of user's clothing and facial-skin. Though this system works well in ideal situation, it has proved to be vulnerable when considering real-life applications.

Popovici and Stancu proposed a continuous authentication system using the keystroke matching. Instead of the facial recognition, this system mostly deals with the pattern matching algorithm which takes a lot of keystroke data as input, making the system complex.

3. TECHNOLOGIES USED
3.1 OpenCV
Developed by Intel, OpenCV is an open source computer library for real-time image processing, available under a BSD license. OpenCV's application areas include 2D and 3D feature toolkits, facial recognition system, gesture recognition, object identification, motion tracking and many more. To support
these areas, OpenCV also includes a machine learning library containing decision tree learning, k-nearest neighbor algorithm, Naive Bayes classifier and artificial neural networks among others.

3.2 Haar-like features

Haar-like features derive its name from the Haar wavelets owing to their similarity. They are the digital image features used for object identification. A Haar-like features sums up the pixels of various adjacent rectangular regions located at different locations. The calculated sum is then used to categorize the subsections of an image. The locations of these rectangles are relative to a detection window which acts similar to a bounding box to the target object, which in this case is a face. The most vital advantage of Haar-like feature is its calculation speed, which, thanks to the use of integral images, can calculate any size in constant time.

3.3 Eigenface

Eigenface, based on eigenvectors, is used in computer vision for the face recognition technique. Eigenface is basically a set of all images used for constructing a co-variance matrix. This produces dimension reduction by allowing the smaller set of basis images to represent the original training images. The basis images, also known as Eigenpictures, are linearly combined to reconstruct images in original training set. The error in reconstruction can be reduced by increasing the eigenpictures. The eigenpictures that are created appears as a dark and light areas arranged in a particular pattern. The difference in these patterns are singled out to be evaluated and scored.

4. SYSTEM IMPLEMENTATION

Figure 1 shows the architecture diagram of the system.

The system is broadly divided into 2 main phases: 1. Initial Login and 2. Continuous Authentication.

4.1 Initial login

To log into the system, dual security measures have been taken. This includes the traditional login process involving an UID and a password. On successful login attempt, a face recognition portal will be opened which will prompt the user's machine to take a sample image of the user using the web-cam. The system will match this sample with the one already stored in the Eigenface dataset. If this second level of login process is valid, the session will be created.

4.2 Continuous Authentication

Once the session is created, the system continuously keeps on tracking the user's face in the background. As long as the facial data matches the corresponding Eigenface dataset faces, the session will run smoothly. In case the sample face recorded during the continuous authentication period fails to come up with any matches, implies that an unauthorized attempt is being made to hijack the session. In such case, the session will be temporarily suspended, so that there could be no misuse of the session or the confidential information.
shared on the session. The system will take the user back to the face recognition login portal. The user will be logged in to the system again only when an authorized face is recognized. On successful recognition, the session will be resumed again. This process will continue till the user manually terminates the session.

4.3 Additional Authentication to avoid video/photo attack
A 2D face recognition technique can be easily fooled by using the photograph of a user. Blink detection technique could be applied to counter it. But the issue remains if the attacker is using a pre-recorded or an edited clip of a person to bypass the login procedure. To overcome this problem, a technique could be used where the system prompts the user to answer a security questions at a random interval of time. These questions can be selected as security questions by the user during the sign-up process. The interval of time for popping the security question is based on a random generator function. In case if the user fails to answer the security question correctly, the session will be temporarily suspended. To resume the session, the user needs to answer the same question after which the system will redirect the user back to the face recognition portal. The only drawback of this technique will be the increase in total authentication process time by the system.

5. WORKING OF THE SYSTEM\[^6\][^7]


The system needs as many facial images of an user as possible for enhancing the recognition accuracy. For this purpose, the user's facial image will be saved in a training set everytime he/she logs into the system. This training set is subject to further processing by normalizing them so that the different lighting conditions do not affect the accuracy level for recognizing the face. Figure 2 depicts the initial training set while figure 3 shows the training set after it is normalized. Suppose E is the set of Eigenface training images with N face images. Each image is converted into a vector of size n before placing it into the set.

\[
E = \{ I_1, I_2, I_3 \ldots \ldots I_N \}
\]  

(1)
Figure 3. Normalized Training set

Step–2. After getting the set, obtaining the mean image $\mu$. Figure 4 represents a sample mean image.

$$\mu = \frac{1}{N} \sum_{i=1}^{N} I_i$$  \hspace{1cm} (2)

where $\mu$ is mean

Figure 4. Mean Image

Step–3. Finding the difference $d$ between input image and mean image.

$$d_n = I_n - \mu$$  \hspace{1cm} (3)

Step–4. Finding a set of $N$ orthogonal vectors $v$. The $i$th vector is chosen such that

$$\lambda_i = \frac{1}{N} \sum_{n=1}^{N} (v_i^T d_n)^2$$  \hspace{1cm} (4)

is maximum, subject to

$$v_j^T v_i = \begin{cases} 1 & \text{if } j = i \\ 0 & \text{otherwise} \end{cases}$$  \hspace{1cm} (5)

Note: $v$ and $\lambda$ are the eigenvectors and eigenvalues of the covariance matrix $C$

Step–5. Obtaining the co-variance matrix $C$

$$C = \frac{1}{N} \sum_{n=1}^{N} d_n d_n^T$$  \hspace{1cm} (6)

Step–6. Finding the Eigenfaces through eigenvectors,$w$,$u$.

$$V_j = \sum_{i=1}^{N} w_{ij} d_i \hspace{1cm} j = 1,2,\ldots,N$$  \hspace{1cm} (7)
Recognition Procedure\cite{6}

**Step 1.** Converting a facial image into eigenface components.

The new input image is compared with mean image and the difference $d$ is multiplied with each eigenvector of the $L$ matrix. Each value is saved on vector $O$.

$$ w_i = v_i^T(l - \mu) \quad (8) $$

$$ O^T = [w_1, w_2, ..., w_m] \quad (9) $$

**Step 2.** Determining the face class which provides the best resemblance with the input image. Euclidean distance ($D$) minimization is done for this purpose.

$$ D = \| O - O_i \| \quad (10) $$

If the Euclidean distance is less than the threshold, the input image is said to be a known face. If it is above the given threshold but below the second threshold, the image can be termed as unknown face. Difference beyond both the threshold level states that the image is NOT the face.

6. RESULT

Figure 6 shows the GUI for the Login page. It includes a traditional login process along with the face recognition window.

If the login attempt is successful, session will be initialized. This is represented in Figure 7.
Figure 7. Session Initialized

Figure 8 depicts a case where an unknown face is detected by the system. The system will check for this face in its dataset, and on not getting any match, will suspend the session.

Figure 8. Unknown Face Detected

The suspended session is depicted in Figure 9. On suspension, the system will go back to login phase for verifying the credentials of the valid user.

Figure 9. Session Suspended

Table 1 represents the assumptions we have made and the constraints that are attached with the system.

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Procedure</th>
<th>Description</th>
<th>Outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ample light conditions</td>
<td>An ample bright light condition is necessary for the webcam to detect the</td>
<td>If the proper light condition is not available, face detection process will fail.</td>
</tr>
</tbody>
</table>
face effectively.

2 Training set

The Eigenface training set must be large enough for the algorithm to perform efficient training on the data. A smaller training set size will result in the output being less accurate.

3 Recognition of user wearing spectacles

It often happens that a person’s eyes are obscured by the reflection of a light on the glasses he/she is wearing. This reflection on glasses will restrain the detection of the eyes by the system and hence will hamper the system’s performance. Also, if the spectacles have huge glasses, it is difficult for the Haar-cascades to work on it.

7. CONCLUSION

Combining continuous authentication with biometric techniques can be an effective approach to improve the security performance. As the use of e-learning applications, FTP and Telnet network protocols is on the rise, the need for such an application is of utmost important. Using the latest technology available, the system ensures that the accuracy is provided up to optimal level. Security, along with the accuracy and stability, is the priority of the system.

ACKNOWLEDGEMENT

We would like to express our gratitude to Mr. Umesh Tare, project manager of Hinduja Global Solutions Ltd., for his invaluable contribution regarding the feasibility of continuous authentication.

We would also like to thank Prof. Jignesh Sisodia, Information Technology Department for reviewing our project and providing us the required technical insight.

REFERENCES


