Use of Computer Vision to Authenticate Retail Invoices with the Convolution-Neural Networks

Aditya Abeysinghe[1], Arundathie Abeysinghe[2], and Sena Seneviratne[3](✉)

[1] Virtusa Pvt. Ltd., 752 Dr Danister De Silva Mawatha, Colombo 9, Sri Lanka
arabeysinghe@virtusa.com
[2] SriLankan Airlines, Colombo, Sri Lanka
[3] Sydney University, Sydney, Australia
ssen2304@uni.sydney.edu.au

Abstract. Digital signatures are a new trend when signing electronic documents in shopping cart platforms. The mundane process involves a login application where a user is authenticated using login credentials and then proceeding to a cart application to produce invoices. In this process, a user is required to authenticate invoices created using a digital signature by using a text input. However, intruders could easily impersonate the user by login to the application and creating a digital signature whereby the authorized user is responsible for invoices created. This impersonation process has caused several breaches in the confidentiality of data. Therefore, this research proposes a system that uses the webcam image of a user in the invoice producing process. The image gathered is validated as a human using a convolutional neural network and then a watermark is created using the system's date and added to the invoice instead of the current digital signature mechanism. Results demonstrated that the performance of invoice creation was high and less CPU and time was required under high brightness.

Keywords: Human-Computer Interaction · Digital authentication · Computer Vision · Face recognition · Convolutional Neural Networks

1 Introduction

E-Commerce has been the new trend in consumer purchases worldwide. Early E-Commerce platforms were maintained with web apps and over the last decade. These applications have diversified into web apps, mobile apps and desktop apps. Most E-Commerce companies expose data providers including API endpoints with which these app types interact. As the same backend is used using these APIs, a user can simply login to the website application, select items to buy and use a mobile app to make purchases. Desktop applications are a new arena in the technology domain. The advantage of desktop apps is that these do not specify a URL (Uniform Resource Locator) and is more secure compared with that of web applications.

Security of these E-Commerce applications are ensured by encrypted communication with the central server and using hashing mechanisms for authentication. A user

W. Hong and G. Kanaparan (Eds.): ICCSE 2023, CCIS 2023, pp. 185–193, 2024.
https://doi.org/10.1007/978-981-97-0730-0_17

authenticated is granted privileges based on their authorization level and can make purchases given their valid transaction details. However, intruders could impersonate users and hack into systems commonly using techniques such as SQL (Structured Query Language) injection or brute force attacks. Desktop applications are somewhat secure as they are difficult to be accessed remotely. However, they are prone to risks of intrusion given current malware methods, which include backdoors or Trojan horses, can place scripts or files that provide access to a remote machine once connected to the internet.

In any E-Commerce application, sessions are maintained to specify which user integrates with the system. Once intrusion is made to the system, the impersonator could use this caveat to create an invoice as if the legitimate user created it. The legitimate user is charged and scams could be made to recover information submitted by this third-party. Therefore, there exists a need for proper authentication not only during the initial login stage but also during the invoice preparation stage to properly specify which user interacts with the system. Traditional approach to sign a document electronically is using a digital signature of the user. However, if the digital signature were hacked by the intruder, authentication could be easily made to create a valid request to generate an invoice. Therefore, an alternative, such as with biometric characteristics, is required to validate the request [1]. Therefore, this research proposes a system that requires a webcam image along with a watermark as a digital authentication mechanism in invoice creation to properly authenticate the user submitting the request for purchase.

2 Literature Review

Several researches in the domain of biometric authentication have been performed to enhance security of different platforms. For example, Trusted Platform Module (TPM) has been popular as an external device used for authentication. However, [2–4] reported a security breach of a TPM module that resulted in expose of encryption keys. Another research [4] proposed the use of TPM for strong authentication. The main issue with this technique is the requirement of use of additional hardware for the authentication system.

Moreover, [5] demonstrated the use of iris-based authentication to validate login to an E-commerce application. This research suggested use of encrypted iris image that will be validated by an existing value at a credit card agency system where the E-Commerce application is used as the middleware. Issues with this system proposed include its high complexity in computation due to its use of Principal Components Analysis (PCA), use of encryption and decryption, unresponsive client side if the credit card system is shut down by intrusion, and scalability issues in distribution of public keys.

Multi-modal techniques are currently used as a performance enhancer in biometric authentication systems [6]. For example, [7] used a genetic algorithm and an artificial neural network combination to combine recognition of human interaction with a system. The system developed was able to achieve a very high true positive rate. Main drawbacks in this research include the use of an external device to capture user images far from a computer screen, large time taken to classify humans due to use of multiple algorithms and the use of a database.

[2, 8] Demonstrated several key biometric authentication mechanisms for a cloud-based solution. Encryption mechanisms were also researched in [9] where a "user-centric" model was developed. However, this method typically inclines away from the system under development as a server-based environment needs to be used to process user templates.

It can be seen from the above review that several techniques have been used for biometric authentication. Main problems with existing techniques are high time and computational power used, use of remote servers that increases processing latencies, and use of complex encryption techniques. This motivates us to find solutions to these issues in existing methods to ensure that biometric authentication can be performed with less time and computation. Our aim is to reduce time and computation that is required to authenticate a user while ensuring confidentiality.

3 Methodology

The proposed architecture for the system is illustrated in Fig. 1. As shown, the proposed system[1] will connect to a MSSQL database to store and retrieve data for products and users. A user needs to load the application and sign in to view products they can purchase. When a user navigates to a product listing, the user can set the quantity and add products to a cart where these entries will be saved in the database with product and user data.

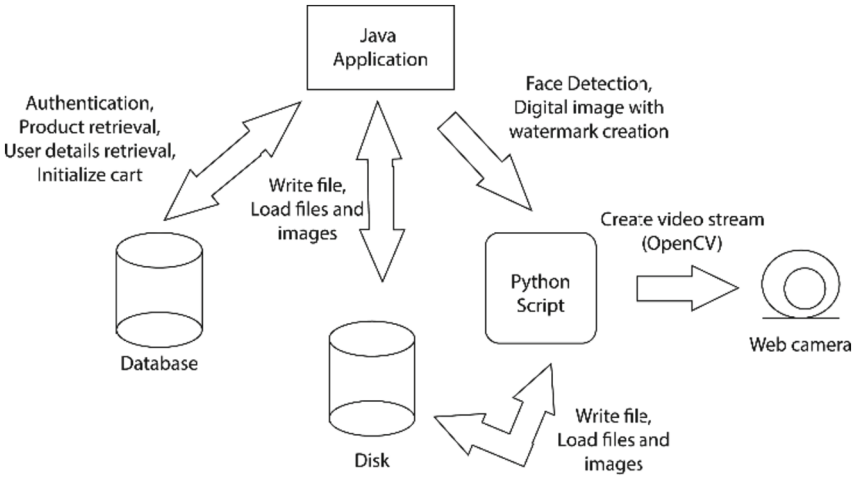


Fig. 1. The system's architecture

[1] https://github.com/aditya1962/BuyGrand.

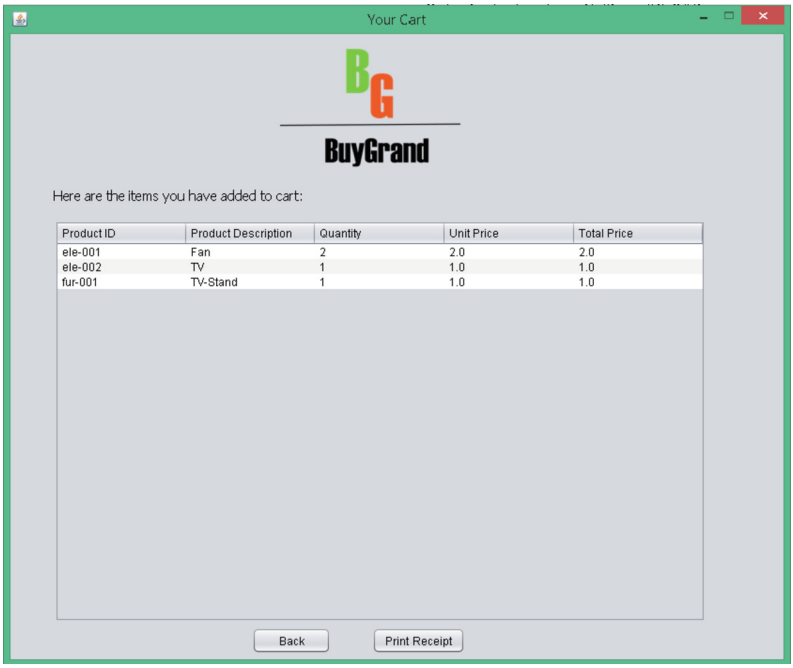


Fig. 2. Cart application

The user can view their cart generated once all transactions are completed. Data from the database will be loaded to the cart as shown in Fig. 2 and the user can go back and change their preferences in product frame and reload the cart. Once the user is satisfied with product purchases, the user can opt to print an invoice generated by the system based on cart data.

The system proposed uses a face detection mechanism as shown in Fig. 1 to authenticate the user. Algorithm 1 shows the steps used to create a video stream using the OpenCV package for python using user's webcam. This will open a video stream and the user can press the space key to capture video frames and press the escape key to quit the stream. Captured video frames will be stored in the project for processing.

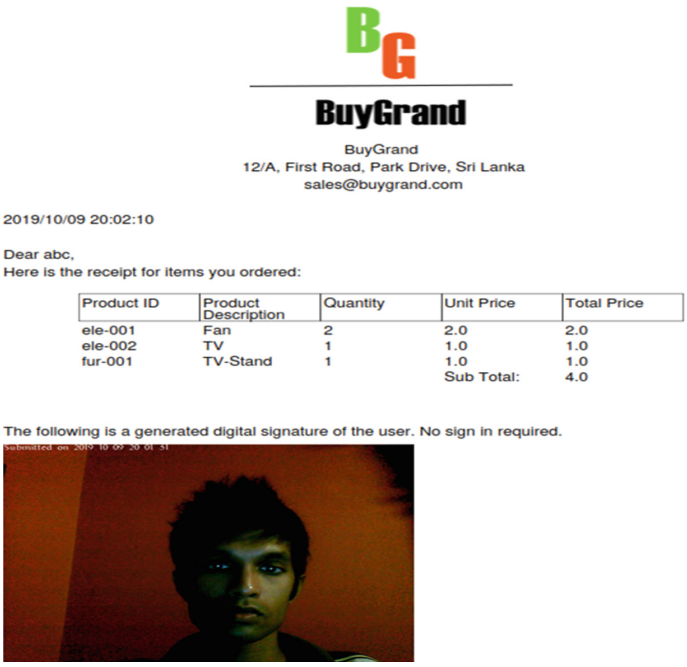
Algorithm 1 Face detection and digital signature creation

```
Get video input from webcamera
counter = 0
while True:
    initialize frames from the camera's read
    show the current frame to the user
    if the returning value is false break the loop
    if escape (esc) key is pressed end capturing frames and end video
    else if space button is pressed:
            create image file
            write to disk
            counter += 1
Release resources
img_value = counter-1
Get image name of the last image from image_value
Read last image
Check the number of detected faces
if 1 face is detected:
    write the digital signature to the image
    open the image to write data
    write current date and time to the image
    save image as a new image to disk
```

Once the user quits the stream, the script will obtain the last image captured and pass to a CNN (Convolution Neural Network). The CNN is based on the dlib package and uses a pre-trained model to train the model in the form of a data file. Then rectangular objects are drawn around faces detected in the image. The model created in this system will follow only if a face is detected, i.e. if no face or more than one face is detected an exception will be displayed to the user.

The final process involves the watermark composed of the system date at the time of compilation. For this process, the PIL package was used to read the image and draw text on it. A type face was used with a font size, colour and location to display. Finally, the image was resized and saved to disk to be used for generating the invoice.

The invoice generation process is done within the JFrame application with the use of the iText PDF library. The invoice created will use the logo of the brand, a sample letter head and the user to be addressed as illustrated in Fig. 3.



BuyGrand

BuyGrand
12/A, First Road, Park Drive, Sri Lanka
sales@buygrand.com

2019/10/09 20:02:10

Dear abc,
Here is the receipt for items you ordered:

Product ID	Product Description	Quantity	Unit Price	Total Price
ele-001	Fan	2	2.0	2.0
ele-002	TV	1	1.0	1.0
fur-001	TV-Stand	1	1.0	1.0
			Sub Total:	4.0

The following is a generated digital signature of the user. No sign in required.

Fig. 3. A sample invoice created using the application

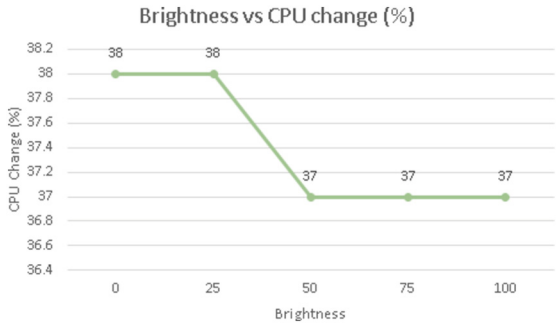


Fig. 4. Brightness vs CPU change

A table will be displayed containing cart information along with the sub total for products. Finally, the digital signature composed of the user image and the watermark is written to the file and the file is opened digital signature composed of the user image and the watermark is written to the file and file is open.

The confidence score was measured for different brightness levels of the background. This was achieved by either changing the brightness of the background of the room or changing the brightness level of the computer the user was using the application.

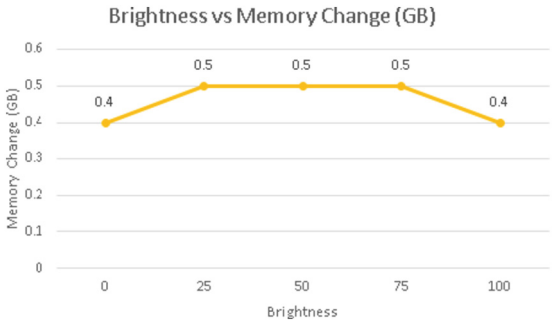


Fig. 5. Brightness vs memory change

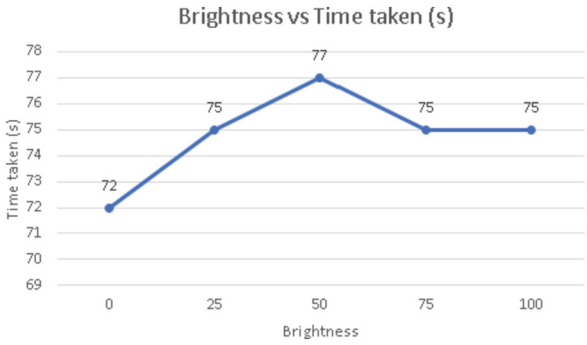


Fig. 6. Brightness vs detection time

4 Results and Discussion

As discussed above, the brightness of the screen of the computer used by the user was changed and the confidence level, time of execution, CPU usage change and memory change was tabulated to identify relationships. Figures 4, 5 and 6 illustrate these variations measured at 0 brightness, moderately low brightness (25%), mid brightness (50%), moderately high brightness (75%) and highest brightness (100%). The brightness was changed from the control panel of the computer and a balanced power plan. The machine under testing used an Intel ® Core ™ 2 Duo CPU at a maximum speed of 2.00 GHz and 2.0 GB DDR2 RAM for execution.

As seen in Fig. 7, higher confidence was seen in video streams filmed under high brightness. The execution time, CPU usage and the RAM usage were comparably low for high brightness streams. Total execution time was around 2.5 min including creating the watermarked image and the PDF file.

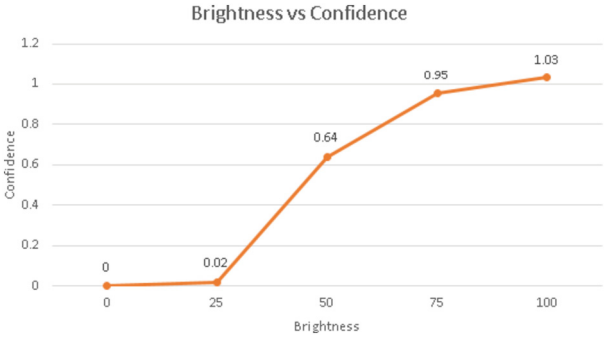


Fig. 7. Brightness vs confidence

5 The Conclusion and Future Works

In this research, a platform was created with.Net, Java, MSSQL and python. The objective was to create a watermark image of the user using a video stream captured from the webcam of the user and then embed the image as a digital signature in invoices created using the application while reducing time and computation required. The system was successfully tested under different brightness levels and a positive relationship was observed between hardware resources, time taken and confidence level with brightness. Therefore, the system could achieve its optimal predictions for higher brightness executions.

The main limitation of this system is that it is not immune to spoofing techniques. Therefore, an impersonator could provide an image of a user or display a video of a user in front of the webcam to create a digital watermarked image. However, though theoretically possible, the authentication level of such an attempt is limited given its artificial approach.

The system under research used digital authentication only during the creation of invoices. The system could be extended as a medium for authentication during the logging process as an alternative to username-password based authentication.

References

1. Phillips, P.J., Martin, A., Wilson, C.L., Przybocki, M.: An introduction evaluating biometric systems. Computer **33**, 56–63 (2000)
2. Al-Assam, H., Hassan, W., Zeadally, S.: Automated biometric authentication with cloud computing. Biometric-Based Phys. Cybersecurity Syst., 455–475 (2019)
3. Hacker extracts crypto key from TPM chip - The H Security: News and Features (2010, 2019-10-08). http://www.h-online.com/security/news/item/Hacker-extracts-crypto-key-from-TPM-chip-927077.html
4. Latze, C., Ultes-Nitsche, U.: Stronger Authentication in E-Commerce - How to protect even na¨ıve Users against Phishing, Pharming, and MITM attacks. In: Presented at the IASTED International Conference on Communication Systems, Networks, and Applications (CSNA 2007) (2007)

5. Vangala, R., Sasi, S.: Biometric authentication for e-commerce transaction. In: Presented at the IEEE International Workshop on Imaging Systems and Techniques (IST) (2004)
6. Conti, V., Militello, C., Sorbello, F., Vitabile, S.: A frequency-based approach for features fusion in fingerprint and iris multimodal biometric identification systems. IEEE Trans. Syst. Man, Cybern. Part C (Appl. Rev.) **40**, 384–395 (2010)
7. Priya, S., Mukesh, R.: Multimodal biometric authentication using back propagation artificial neural network. Int. J. Simul.: Syst. Sci. Technol. (IJSSST) **19**, 1–8 (2019)
8. O'Gorman, L.: Comparing passwords, tokens, and biometrics for user authentication. Proc. IEEE **91**, 2021–2040 (2003)
9. Zhou, K., Ren, J.: PassBio: privacy-preserving user-centric biometric authentication. IEEE Trans. Inf. Forensics Secur. **13**, 3050–3063 (2018)