*Human Interaction and Emerging Technologies (IHIET 2022),* Vol. 68, 2022, 612–618
https://doi.org/10.54941/ahfe1002784

# Controlar-Freeze: A New FinTech Approach in Visual Screen Security

**Noura AlTamimi[1], Abdallah Tubaishat[1], Fatima AlJneibi[2], and Marwa AlMenhali[2]**

[1]Zayed University, Abu Dhabi, UAE
[2]Higher Colleges of Technology, Abu Dhabi, UAE

## ABSTRACT

Shoulder surfing continues to be a serious privacy threat. Despite this, practical and efficient countermeasures against such attacks are still scarce. We are proposing a Controlar-Freeze as an original yet effective precaution against various types of shoulder surfing attacks in ATMs in Financial Technology (FinTech). Our proposal consists of a face detection algorithm, which (a) detects if two or more people are in the scope of the camera; (b) shows an alert; (c) freezes the controls of the screen until the threat source is gone; and (d) captures the threat to be referred to as evidence. We implemented this approach on MatLab and Simulink Software. We then conducted preliminary evaluations to validate its performance and effectiveness. Controlar-Freeze is proven success for the proposed theory that included the studied cases of the common features. We reported few concerns about this approach as well as suggestions for improvements. This paper is a revised version of what was published in IBIMA 2021 (Noura Altamimi, 2021).

**Keywords:** FinTech, Shoulder surfing, Privacy, Onlooker, Face detection, ATM.

## INTRODUCTION

Physical security is a significant part of any security plan and is primary to all security efforts. The objective of physical security is to safeguard personnel, information, equipment, IT infrastructure, facilities, and all other company assets as it is harder for an attacker to succeed in their conquest. The aggravation of shoulder-surfing phenomena makes it a tremendous privacy concern. According to (Lashkari et al., 2009) shoulder surfing is a type of physical attacks by using direct observation techniques, such as looking over someone's shoulder and is an effective way to obtain personal or sensitive information without any technical support. Most of the time, this simple practice is done without the intention of taking data. However, it is crucial to understand the nature of everyday shoulder surfing scenarios in order to inform the design of solutions and to understand if shoulder surfing is restricted to specific data types (e.g., passwords) or if it is a general problem. Nevertheless, it is essential to prevent unwanted parties from viewing confidential data or exchange privileged insights where it can be used maliciously. Somewhat, it does not have serious consequences, but evokes negative feelings for both parties, resulting in a variety of managing situations.

We are proposing a new software approach that contribute to notify for shoulder surfing in the real world and to inform implications for the design of privacy protection mechanism occurring in ATMs. Being said, the software shall be considered in financial technologies. Financial technology, often shortened to FinTech, is the technology and innovation that aims to compete with traditional financial methods in the delivery of financial services. It is an emerging industry that uses technology to improve activities in finance. Hence, the software that has been developed shall alert the user of a shoulder-surf attack that is taking place virtually. The aim is to assess the necessity of securing screens of vulnerable devices and establishing an integrative method of the developed software into these devices.

An incident occurred a couple of years ago where an individual was spotted lingering around an ATM of Bank of America, San Francisco, in an attempt of stealing money. Thedideus Donell Guidry was being observed by an off-duty policeman, who then took another turn around the area found the same convict in the same area. A woman then came to the ATM to withdraw money, and the policeman observed that Guidry was peeking over the victim's shoulder in order to figure the pin code. Later, moments after the woman left, the suspect proceeded to the ATM and inserted some numbers in the keypad; this was when the off-duty policeman paged the on-duty policemen and they reported to the area. After that, he was caught deducted from her bank account. The 29-year-old suspect was then taken to NAPA Police Department in San Francisco, as he was charged with a felony of identity theft and misbehavior of using an access card (Colby, 2016).

Shoulder-surfing, in particular, and physical attack, in general, is a huge deal as it is related to security and privacy of individuals. This issue is one of the drawbacks of technology and computerized systems. Therefore, an approach eliminating attackers who abuse technology to achieve malicious intentions should be established. Furthermore, this problem is significant due to the fact that it is easy to be conducted, familiar, and jeopardizing. Every person who uses ATMs, for instance, should feel 100% safe and they must be aware that in case any of these attacks occur, they will still be protected and so will their confidential details.

As a contribution to finding a reliable explanation to this problem, we are proposing a solution that could be categorized as a technology in FinTech and financial sectors. It contributes significantly towards privacy protection by reducing risks that are associated with unauthorized access to personal information. Assumptions can be triggered upon our proposed solution based on the movement toward e-wallets and online payments.

## DEVELOPMENT OF TECHNOLOGY CONTRIBUTING TO PROTECTION OF PRIVACY AT ATMS

Our research attempts to establish an integrative method of the developed software into vulnerable devices such as ATMs. A review of the current solutions was initially conducted, followed by the description of the proposed reliable approach associated with suggested precautious measures. Finally, a proof of concept was demonstrated to test its feasibility.

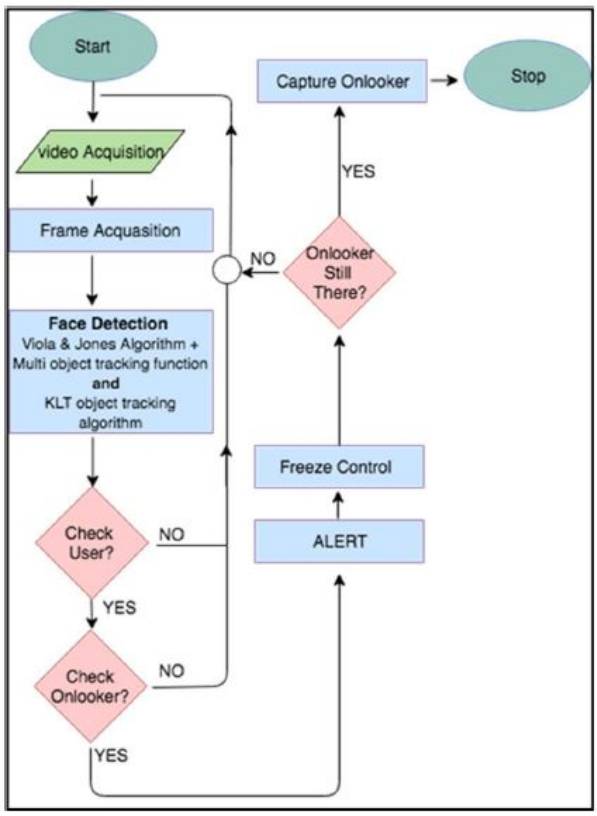


**Figure 1:** The controlar-freeze system overview and workflow.

## Controlar-Freeze System Overview

The flowchart above depicts the new proposed approach of Controlar-Freeze System of Visual Screen Security (see Figure 1).

The system Starts with input from MATLAB webcam support where it collects all the pixels together to create a video that integrates a preview and acquisition area with acquisition parameters so that settings can be changed and have the ability to see the changes dynamically applied to your image or video data. Once the pixels have created a video stream, the Frame Acquisition starts by defining and detecting faces within the scope of the built-in camera. Frame acquisition is considered essential in the use of preventing Shoulder Surfing attack.

After the acquisition of frame using MATLAB webcam support, it is intended to detect a face, using MATLAB system object toolbox '*vision.CascadeObjectDetector*' to identify the location of a face in a video frame. The cascade object detector uses the Viola-Jones detection algorithm. This algorithm uses HAAR basis feature filters, while the efficiency of the Viola-Jones algorithm can be significantly increased by first generating the integral image.

To track the face over time, the system uses the Kanade-Lucas-Tomasi (KLT) algorithm Kanade & Tomasi (Kanade and Tomasi, 1991). While it

is possible to use the cascade object detector on every frame, it is computationally expensive. It may also fail to detect the face when the subject turns or tilts their head. This limitation comes from the type of trained classification model used for detection. The system detects the face only once, and then the KLT algorithm tracks the face across the video frames. KLT algorithm tracks a set of feature points across the video frames. Once the detection locates the face, it identifies feature points that can be consistently tracked, with the feature points identified. the system uses the *'vision.PointTracker'* system object to track them. In addition to Viola-Jones and KLT algorithms, the Motion-Based Multiple Object Tracking Function is used to perform automatic detection and motion-based tracking of additional moving objects in the video from the stationary, moving the camera using *'vision.CascadeObjectDetector'* System object function.

Once the faces are detected using KLT and Viola-Jones detection algorithms, Check User is a condition that indicates the presence of a face. If yes, the software's algorithm identifies the number of faces in the scope of the camera. If one face is detected, it proceeds to the second condition. If there are not any, the process will turn back to its workflow.

Check Onlooker is the second condition where the camera will detect the presence of other faces within the scope of the camera in which the total of faces in the range is two or more. Additionally, the process designed is to notify the users of a presence of onlookers that suspiciously look at the screen. When the algorithm detects that, there are two faces in the scope, it will show an Alert with several options. The interrupt will be set showing three options to the users:

**Shoulder Surfing Alert: Do You Want to Continue the Transaction?**

a) **Yes, I know the person:** This will continue the transaction without any changes. This will also stop the algorithm from working and the user proceeds at their own risk.

b) **No, return to the Home Screen:** This will take back the user to the main screen and will freeze the controls of the screen to stop the onlooker form obtaining any of the password or pin.

c) **No, I don't understand:** This will freeze the controls of the screen and terminates the session.

Freezing the Screen Controls is an immediate action after the alert is on, the Control Freeze will get back into the normal screen when the onlooker is gone. As the last condition, the system checks whether the Onlooker is Still There. An eight second period is given before the action to occur if the onlooker is still standing; however, if the onlooker has left, the process will turn back to its usual workflow. Eight second period was chosen upon the average of human attention span. Furthermore, the Capture Onlooker process will occur if the onlooker has completed the five-second period after freezing controls and notifying the user of the presence of an onlooker. The Onlooker photo will be saved in a folder, through proper order and naming. Lastly, the workflow of Controlar-Freeze System of Visual Screen Security ends.

**Figure 2:** Setup used in our experimental evaluation.

## Controlar-Freeze System Evaluation

We performed some preliminary evaluation of our proof-of-concept implementation with the help of data collected from human participants. We specified our experimental setup, tasks performed by the participants, and the empirical parameters used in the evaluation.

### Experimental Setup

Figure 2 above depicts the setup used in our experimental evaluation. We requested eight participants; all of which were familiar with using ATMs.

The participants were informed about the shoulder-surfing attack and its implication on users. Participants were angled in front of a PC. We chose to use the HP PC because of its Windows Operating system. The built-in camera of the PC was configured using MatLab scientific language, and the display screen simulates the ATM screen. The PC camera requires an external support package from MatLab software to enable the detection. Our implementation of Controlar-Freeze can be accessed and altered from MATLAB software using the inbuilt Toolboxes and Functions. The software is a standalone application and can run on any system in spite of the configuration. As a result, the ATM simulation was usable, even as a regular Automated Teller Machine.

To evaluate the prototype, we measured the detection accuracy, in addition to usage-related parameters; we also measured the Alert System, Control Freeze, and the onlooker's capture feature perceived by using the webcam support package. There are four cases to study. Those were based on common features, such as people with eyewear, eye injuries, people with headwear, and Women with Niqab and people with face mask. Detection accuracy is the ability of the system to recognize facial features without obstruction of any kind. Below is example of one case was studied for detecting accuracy.

**Women with Niqab/Face Mask:** This case examined facial features that were covered such as women with niqab/face mask. The image acquisition and facial features detection process concluded the lack of accuracy regarding

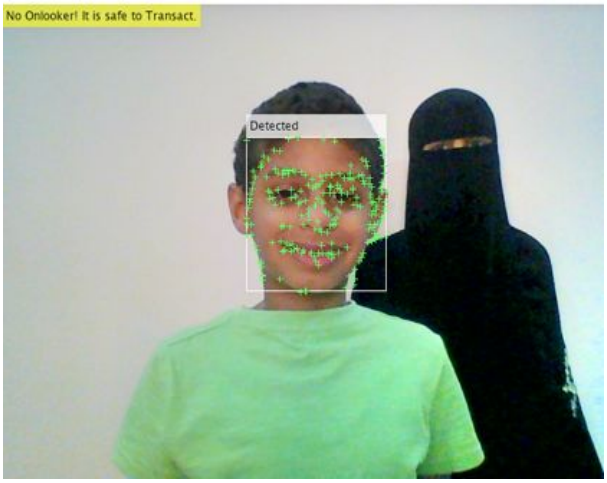


**Figure 3:** Recognition of Women in Niqab/Face mask.

niqab. Nevertheless, the eyes of the participant were not detected as shown in figure 3, which can be a window for improvement of this system.

## CONCLUSION

We proposed a novel technique to overcome various forms of shoulder surfing attacks against users typing pin or password in ATM, which can be considered to be a new solution in FinTech. Our proposal augments a face detection algorithm, detects if two or more people in the scope of the camera, shows an alert, freezes the controls of the screen until the threat source is gone, captures the threat in two situations in which can be referred to as a source of evidence. Our experimentation involved four different cases that showed the system is efficient with people with headwear, eyewear, and eye injuries. In certain instances, as with women in niqab, the detection process concluded the lack of accuracy regarding a niqab. Despite its objective, this case can be a window for improvement of this system in which to add an eye detection algorithm to detect various scenarios of the eyes along with faces.

## REFERENCES

AlTamimi, Noura, et al. "37th Ibima Conference: 30-31 May 2021, Cordoba, Spain." *International Business Information Management Association (IBIMA)*, 2021, https://ibima.org/accepted-paper/controlar-freeze-new-approach-in-visual-screen-security/.

Kanade, T.,& Tomasi, C.(1991). Detection and Tracking of Point Features. *International Journal of Computer Vision* [online]. Available from: https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.45.5770 [accessed 27 March 2022].

Lashkari, A., Farmand,S., Zakaria,O.,& Saleh,R.(2009). Shoulder Surfing attack in graphical password authentication. *International Journal of Computer Science and Information Security (IJCSIS)*.

Patch. (2016). *"Shoulder-Surfer" Arrested at Napa ATM*. [Online]. Available from: https://patch.com/california/napavalley/shoulder-surfer-arrested-napa-atm [accessed 27 March 2022].

Viola, P., Jones, M. (2001). Robust Real-time Object Detection. *Second international workshop on statistical and computational theories of vision – modeling, learning, computing, and sampling*.