IoT Based Modular and Offline Security System Designed for Offender Detainment

Amaan Shaikh*, Aman Pal, Mallika Ambhore, Amar Chavan, Amay Chivate, Prajyot Ambekar
Department of Electronics & Telecommunication Engineering, Vishwakarma Institute of Technology, Pune, India.
*Corresponding author email: amaan101179@gmail.com

Abstract

Since the beginning of time, people have been concerned about security, both for their own personal safety and the preservation of everything they hold. A variety of approaches have been used to achieve this goal. Modern security systems rely on a variety of sophisticated electrical technologies. Both the people who design security systems and those who attempt to breach them evolve over time. The security system concept proposed and described in this paper makes use of a number of already-available technologies, including face recognition, fingerprint authentication, personal identification number verification, and automated turrets. It seeks to make a target safer by combining the aspects of these that are more realistic and accurate in order to exponentially reduce the chances of a breach occurring, and if a breach does occur, it seeks to detain the perpetrator in the security room in lockdown mode using the autonomous turret in any of the available ways until the situation is taken under control. Here the modularity of the autonomous turret comes into play. It can be configured in multiple ways, from spewing fire suppressant to combat a fire in the security room to being equipped with tasers to temporarily disable perpetrators. The finest options for each circumstance have been suggested for the security system after several versions of these security measures were taken into account. Three different face recognition methods and three different retinal scan techniques were compared. Furthermore, a few variations of the personal identification number system and three variations of fingerprint scanning were also contrasted. The aim of these comparisons is to create the mathematically lowest probability of someone bypassing the entire security system.

Keywords: *Internet of Things (IoT), Personal Identification Number (PIN), Face Recognition, Fingerprint Recognition, Automated Turrets, Detention*

DOI Number: 10.48047/NQ.2022.20.20.NQ109136 **NeuroQuantology2022;20(20): 1315-1323**

Introduction

In an age where information is the most valuable resource, security measures are always increasing; nevertheless, more physical security methods are also adapting. We have progressed from Personal Identification Numbers (Milligan, 2017) (PIN) launched in 1967 to Fingerprint Scanners (Ghali, Ali and Yousif, 2020) prototyped in 1975 with FBI financing to Automated Turrets created by South Korean firm DoDAAM in 2010 (Blain, 2010). Originally, these technologies were used to secure ATMs, develop a database of known offenders, and provide high-priority security, respectively. However, with the ever-improving area of electronics, it is quite conceivable for the common person to manufacture all of these solutions at a reasonably low price. PIN-based IoT systems are extremely easy to make, so much so that they are made by undergraduate students as their academic projects (Ali, 2021). Even an automated turret, which sounds complex to make, is amazingly simple since complete code exists for live tracking made by enthusiasts (Eveland, Konolige and Bolles, 1998). The cost of such a system employing a Raspberry Pi and utilizing a pellet gun would be quite low (Alam *et al.*, 2017).

eISSN 1303-5150

In this paper, we propose a combination of these technologies to create an extremely secure system. It would employ two layers of security attached to a security room. The first layer would be an entry door that would utilize fingerprint and PIN verification. Passing this door would lead the person(s) into the security room. Here they would be presented with the second layer of security, namely face recognition and a retinal scan. The second layer would not function until the first door was closed. Failure to pass the face recognition and retinal verification would put the room on lockdown, rendering the exit door inoperable and the perpetrator in detainment. At this stage, the sentry turrets would activate. The turret's purpose can be changed by the user and would be unique to the situation where this system is being employed. For this paper, we have considered two purposes, namely 'Discouragement' and 'Fatal'. Discouragement would entail using disabling effects like tasers or water jets to discourage the perpetrator from attempting to damage or approach the exit door or the turrets themselves. Fatal is an optional step where the turrets would be loaded with live ammunition. The parameters for activating these would be set by the user, but if activated, it would shoot to kill or seriously harm the perpetrator (David *et al.*, 2020).

Methodology

2.1 PIN system

We started with the simplest part of our security system, a PIN verification system. A classic PIN is four digits long, so there are 10,000 possible four-digit combinations that the numbers 0 to 9 can be arranged into. In September 2012, interesting research on compromised numeric passwords was conducted, combining information from all the different PINs and correlating it to human behavior, as shown in Table 1. For example, 1234 is the most popular PIN in this data with a frequency of 10.713%.

Sr. No.	PIN	Frequency
1.	1234	10.713%
2.	1111	6.016%
3.	0000	1.881%
4.	1212	1.197%
5.	7777	0.745%
6.	1004	0.616%
7.	2000	0.613%
8.	4444	0.526%
9.	2222	0.516%
10.	6969	0.512%

Table 1: The most popular PINs and their usage frequency

With such a small number of combinations, in addition to the easily guessed pattern-based PINs used by people, it is logical to discard the four-digit PIN in favour of more digits. Even then, the human tendency for patterns is still a problem. Dates are written in the format DDMM, DDYY, MMYY, and so on in four digits, but they can easily be written similarly in six digits, such as DDMMYY, which is the most popular format. Ten digits would result in people using phone numbers as their PINs, at least in some countries. An odd-numbered PIN, either seven or nine digits, was considered the best option. Nine has 990000000 more combinations compared to

eISSN 1303-5150

seven, so it is the obvious choice (Berry, 2012).

Arduino-based password systems are common, which, when combined with solenoid locks, result in a real-world level of security. Solenoid locks with 1000 N to 4000 N lateral load bearing capacity are available for consumers, and multiple can be engaged by a single Arduino (*Locking Solenoids | Kendrion*).

2.2 Fingerprint authentication

Fingerprint authentication is one of the most reliable methods of verification (Borah, 2013). Every smartphone has an in-built fingerprint scanner. There exist three main methods of fingerprint recognition; however, not all of them are dependable. Optical fingerprint scanners are the most common and easily available variation. These rely on taking an optical image of the fingerprint and then running algorithms to detect patterns. They often employ their own source of light and contain many diodes. Unfortunately, they are incredibly easy to fool. Any prosthetic or a high-quality image is enough to deceive the sensor into giving a false positive. Therefore, these are not ideal for our purpose. Capacitive fingerprint scanners are another extremely popular variation (Triggs, 2022). They are commonly found on rear and side fingerprint scanners on smartphones and as hybrid scanners when combined with optical scanners. They contain arrays of open and charged capacitors. When a person places their finger on them, the ridges in the fingerprint short specific capacitors, while an absence of ridges creates an air gap. An op-amp integrator circuit tracks these, and they are recorded for comparison. These scanners are extremely secure compared to optical scanners, as they are not fooled by images, and any conductive prosthetics will record different charge changes in the capacitors. Ultrasonic fingerprint scanners are a recent technology. They emit ultrasonic waves at the fingerprint, and a sensor detects mechanical stress from the returning pulses that have not been absorbed. Their 3-D nature makes them as secure as capacitive scanners, but these are quite slow to process fingerprints. A point in their favour is their capability to detect a human pulse (Ronald A. Kropp, Richard Irving, 2013). Since time is not a constraint for the security system, the ultrasonic fingerprint scanner presents itself as the best option (Ghali, Ali and Yousif, 2020).

2.3 Face recognition

Face recognition is a developing method of identification. It is still in its initial stages, with simple things like different lighting, face masks, and varied positioning of the face drastically affecting its capability to precisely detect a person. There are two main approaches to face detection: the feature-based approach, which segments features like the mouth, the eyes, and such into inputs. The other is the holistic approach, which takes the entire face as an input for recognition. However, the hybrid technique, which combines both techniques, also exists (Gupta, 2019).

The Eigenface method is the most common algorithm for face detection. Eigenfaces divide the face into feature vectors. A linear combination of these creates a face. It is a simple and easily applied algorithm for face recognition. It is sensitive to lighting conditions and requires consistency or preprocessing to get the best results.

Neural networks are commonly used for object and pattern recognition. They can be more precise than Eigenface, but conversely, they require a lot of training and time to achieve precise results. However, that is not a disadvantage for us, as only the recognition is under scrutiny. Neural networks are the best solution as they are not affected by the positioning of the face or lighting conditions while providing the best results. They also happen to be easier to use compared to other methods like Eigenface, which have increased complexity.

2.4 Retinal Scanning

eISSN 1303-5150

Retinal scanning is a biometric identification method that uses the unique patterns on a person's retina to identify them. The retina is the layer of tissue at the back of the eye that contains the photoreceptor cells, which are responsible for converting light into electrical signals that the brain can interpret as visual information. In a retinal scan, a low-intensity light is shone into the eye, and a camera is used to capture an image of the pattern of blood vessels on the retina. This pattern is then used to create a unique digital signature for the individual, which can be used to identify them. The patterns on each person's retina are unique and don't change over time, so retinal scanning is a very accurate and reliable method of biometric identification (Qamber, Waheed and Akram, 2012; Borah, 2013; Sadikoglu and Uzelaltinbulat, 2016).

There are several techniques that are used in retinal scanning, that include:

1. *Fundus photography*: In this technique, a specialized camera is used to take a photograph of the back of the eye, including the retina and the optic disc (the area where the optic nerve connects to the retina).
2. *Scanning laser ophthalmoscopy*: This technique uses a low-intensity laser to scan the retina and create a detailed map of the blood vessel patterns.
3. *Optical coherence tomography*: This technique uses light waves to create a detailed cross-sectional image of the retina.
4. *Dual-wavelength imaging*: This technique uses two different wavelengths of light to create a more detailed image of the retina.

Overall, the specific technique used in a retinal scan will depend on the specific application and the technology that is available. The equipment involved in a retinal scan typically includes a specialized camera or imaging device, a low-intensity light source, and a computer or other processing unit to analyze the captured images. The specific equipment used in a retinal scan will depend on the specific technique being used as well as the technology that is available. For example, in a fundus photography retinal scan, a specialized fundus camera would be used to take a photograph of the back of the eye. This camera would typically be mounted on a tripod and positioned in front of the eye, and it would be controlled by a computer or other electronic device. In a scanning laser ophthalmoscopy retinal scan, a low-intensity laser would be used to scan the retina and create a detailed map of the blood vessel patterns. This laser would be mounted on a device that is held in front of the eye, and it would be controlled by a computer or other electronic device. In addition to these core components, you may also need additional sensors and equipment, depending on the specific requirements of your project. For example, if your system is being used to grant access to a secure area, you may need additional sensors and components to control access, such as a door lock or gate.

Image processing is a crucial step in the retinal scanning process, as it involves analyzing the images captured by the retinal scanning system and creating a digital signature of the individual's retina. This signature is then used to identify the individual and grant access to a secure area or system (Abrishami-Moghaddam, Farzin and Moin, 2008).

There are several AI algorithms that can be used in retinal image processing, depending on the specific requirements and goals of the system. Some common examples of AI algorithms that may be used in retinal image processing include:

1. *Convolutional neural networks (CNNs):* CNNs are a type of deep learning algorithm that are commonly used in image processing applications. They are particularly well-suited to retinal image processing, as they can be trained to recognize and interpret

eISSN 1303-5150

the complex patterns of blood vessels on the retina.

2. *Support vector machines (SVMs):* SVMs are a type of machine learning algorithm that can be used to classify data points based on their characteristics. In the context of retinal image processing, SVMs could be used to classify the different patterns of blood vessels on the retina and to create a digital signature for everyone.
3. *Decision trees:* Decision trees are a type of AI algorithm that can be used to make decisions based on a set of rules or conditions. In the context of retinal image processing, decision trees could be used to analyse the images of the retina and determine whether they match a registered signature to identify the individual.

2.5 Automated Turrets

Automated turrets, or sentry guns, are a pre-existing technology employed for the defense of multiple countries. Manual sentry guns are more common and can be seen on Navy battleships. However, we are concerned with autonomous turrets. These are less popular, with only semi-autonomous versions being used by countries like Qatar, which utilize the Super aEgis II, which can run automatically but has been configured to require human confirmation, as giving complete control of a weapon to software is still under ethical debate (Qamber, Waheed and Akram, 2012; Parodi, 2021).

It is a simple task to create the mechanical components of the sentry turret. It requires to rotate in two axes and a trigger mechanism for the module. Servos in two planes, attached to a "lazy Susan" or a similarly high load-bearing rotation mechanism, will provide more than ample freedom for the module to follow the target.

A working model of a gun turret has been developed (Yathavi *et al.*, 2020). Multiple sources also exist for creating similar or different sentries; therefore, this process is quite simple and inexpensive. Although, depending on the application—say, a bank—the quality and durability of the sentry will have to be dramatically increased to make it immune to all varieties of physical violence.

2.6 Live Tracking

The recommended method for live tracking of person/s inside the security room is the same as it was for the face recognition and retinal scanning, an implementation of neural networks. Neural networks have proven to be quite versatile during our research. In this scenario, it would involve taking a live video feed of the room from the camera module mounted on the sentry turret. This feed would be converted to images and processed by the neural network. Unfortunately, some tuning is required at this step, as this method would produce at least thirty frames per minute, or one frame every two seconds, and a very powerful computer would be required to do real-time identification of a person and what activity they are performing. It is recommended to have extremely bright lights in the room and to take the video in a 1280x720 resolution with progressive scanning, as this would reduce the image size and maintain high clarity for the camera at the same time. Upon detection, the system would move the turret to center on the individual. It is recommended to add a media system of some variety that reminds the person/s to stay within the yellow zone and away from the exit door (A. Cretual, 1998; Ben-Arie *et al.*, 2002).

eISSN 1303-5150

3. Proposed Modular and Offline Security System

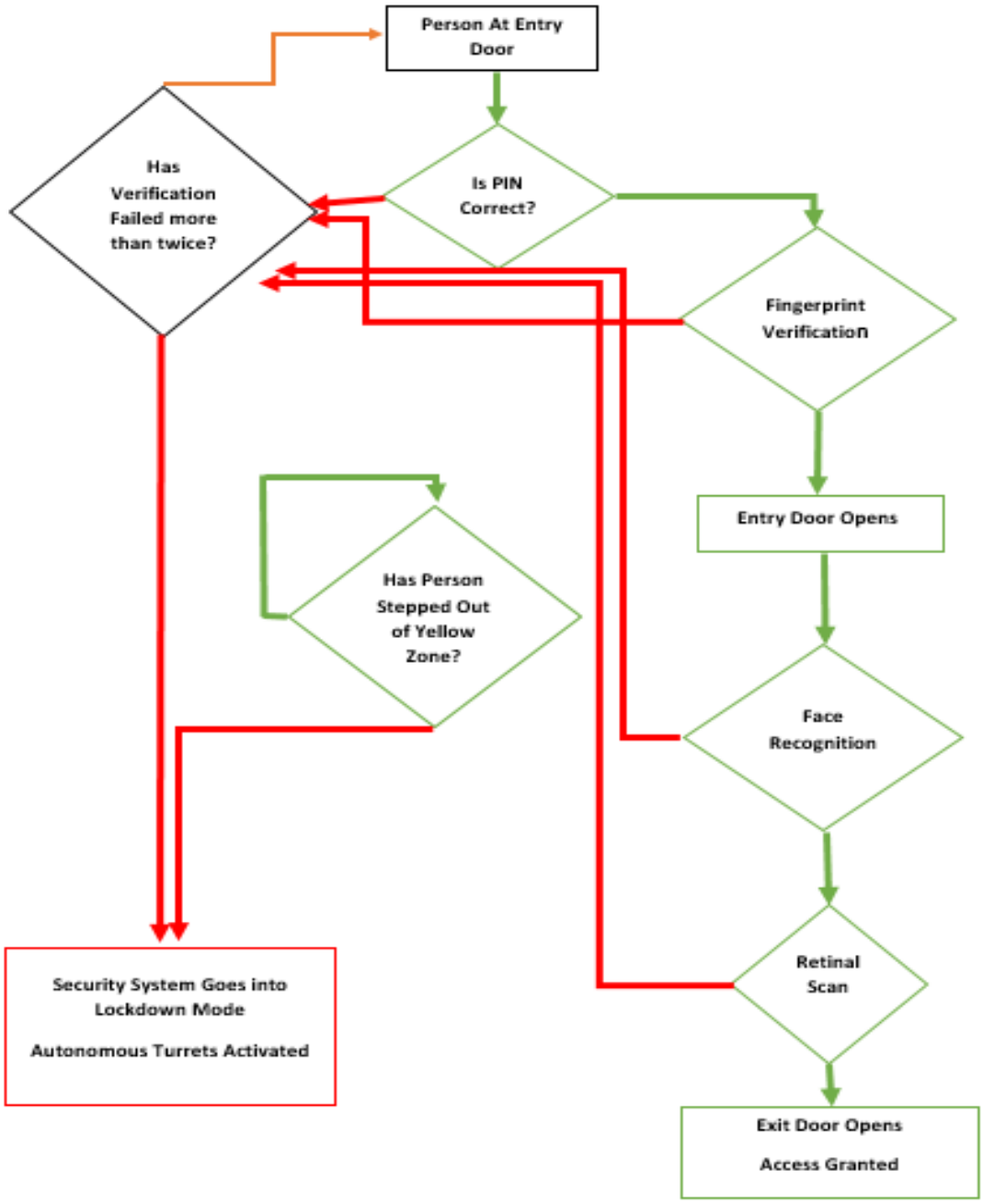

Figure 1. Schematic representation of a modular and offline security system

Specifically, in our application, we propose that two sentry turrets must be installed inside opposite walls, behind sliding doors that open when the sentries are activated. Entry to the room is dependent upon passing the first layer of verification, i.e., the password entry and fingerprint authentication. On entry, the system is in waiting mode, with the exit verification locked until the entry doorway is closed. The room is divided into three zones, with the central yellow zone leading from the entry door to the exit door. The exit door has the remaining security measures, i.e., face recognition and retinal scanning. Condition for activation for the turrets are such: 1) When verification fails three times consecutively on the exit door 2) When any person or persons step off the yellow zone into a white zone. 3) When it detects conclusively that the person or persons are attempting to damage something inside the room. In all three cases, the entry

eISSN 1303-5150

door will remain closed, along with the exit door. The exit door will become unable to be opened until the entry door is first opened from outside through the password and fingerprint verification. Then the system will reset back to waiting mode.

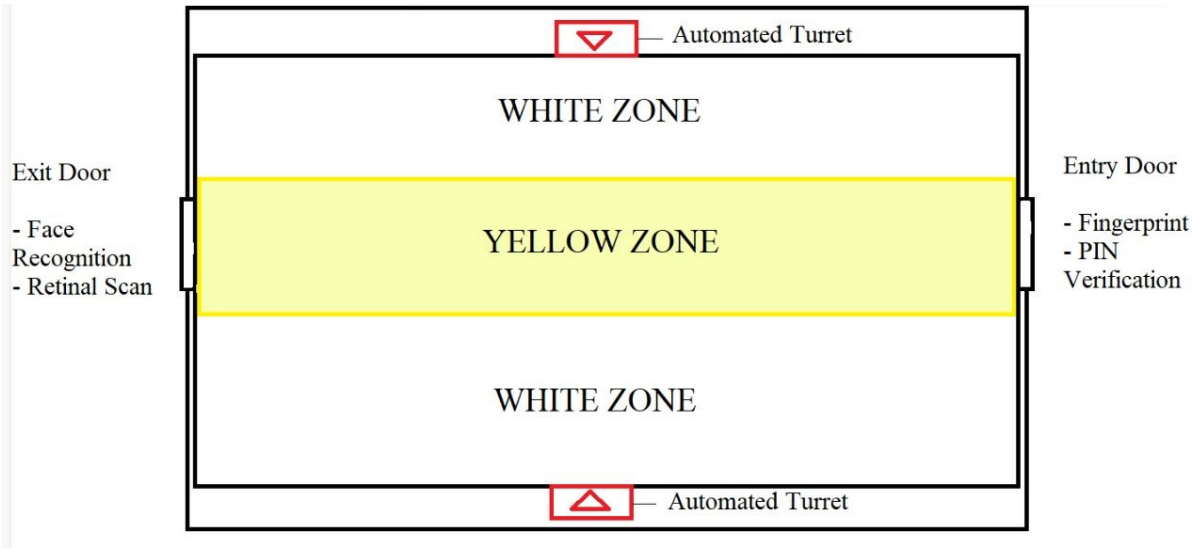

Figure 2. Detainment mechanism/zones

3.2 Database Protection

It might be worthwhile to mention now that all these security systems that we propose are in no way connected to the internet. They are all wired locally and use an onsite computer inside the security system as a database. This is to eliminate any possibility of database corruption or modification by perpetrators to gain access to the protected target. Any exposure would introduce risk and thus the need for risk prevention, which introduces unnecessary cost that is detrimental to the feasibility of such a solution. Therefore, for our purposes, we consider an offline database that would require access through the two layers of security in the first place to update in any way.

3.3 Modularity of the System

We established two versions of the security system earlier on, "Fatal" and "Discouragement." "Fatal" refers to the utilization of actual live ammunition in the sentry turret. This is not the recommended setup and is only presented as an actual option for places that require extremely high security, such as bank vaults or places where national security is at stake. Discouragement replaces live ammunition with something less severe. This is the recommended implementation of the security system when something less permanent but painful enough to discourage unwanted behavior is used. High-pressure water jets, pepper spray, or rubber bullets are the prime examples. However, the system can be rigged up in any manner, thus making it extremely modular. For example, it might be implemented in a mental institution with a taser installed to temporarily disable a patient to prevent self-harm. There are other use cases, like using the turrets' ammunition as a targetable fire suppressant filled with foam or water (Simpson, Roesner and Kohno, 2017).

Conclusion

The security system concept suggested in the present work utilizes a variety of current technologies, such as face recognition, fingerprint authentication, PIN verification, and automated turrets. It combines the most practical features of these technologies to drastically lower the likelihood of a breach. The current system's modularity can be set up in several ways. In order to completely rule out the possibility of database corruption or alteration by attackers to access the protected target, these security systems are not

connected to the internet. The project's goal is to generate the scenario with the lowest mathematical chance of someone disabling the entire security system.

References:

A. Cretual, F. C. and P. B. (1998) 'Complex object tracking by visual servoing based on 2D image motion', in *Complex object tracking by visual servoing based on 2D image motion (Cat 09/ICPR.1998.711927)*, pp. 1251–1254. doi: 10.1109/icpr.1998.711927.

Abrishami-Moghaddam, H., Farzin, H. and Moin, M. S. (2008) 'A novel retinal identification system', *Eurasip Journal on Advances in Signal Processing*, 2008. doi: 10.1155/2008/280635.

Alam, M. F. *et al.* (2017) 'Augmented and virtual reality based monitoring and safety system: A prototype IoT platform', *Journal of Network and Computer Applications*, 89, pp. 109–119. doi: 10.1016/j.jnca.2017.03.022.

Ali, M. (2021) *A low- cost portable electronic firing system*. Bangladesh University of Engineering & Technology (BUET).

Ben-Arie, J. *et al.* (2002) 'Human activity recognition using multidimensional indexing', *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24(8), pp. 1091–1104. doi: 10.1109/TPAMI.2002.1023805.

Berry, N. (2012) *The most common pin numbers: is your bank account vulnerable? | Debit cards | The Guardian*, *www.theguardian.com*. Available at: https://www.theguardian.com/money/blog/2012/sep/28/debit-cards-currentaccounts (Accessed: 15 December 2022).

Blain, L. (2010) *South Korea's autonomous robot gun turrets: deadly from kilometers away*, *News Atlas*. Available at: https://newatlas.com/korea-dodamm-super-aegis-autonomos-robot-gun-turret/17198/ (Accessed: 15 December 2022).

Borah, T. R. (2013) 'Retina and Fingerprint based Biometric Identification System', *Proceedings published in International Journal of Computer Applications® (IJCA) (0975 – 8887)*, pp. 74–77.

David, W. *et al.* (2020) 'AI-Powered Lethal Autonomous Weapon Systems in Defence Transformation. Impact and Challenges', *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 11995 LNCS, pp. 337–350. doi: 10.1007/978-3-030-43890-6_27.

Eveland, C., Konolige, K. and Bolles, R. C. (1998) 'Background modeling for segmentation of video-rate stereo sequences', *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, pp. 266–271. doi: 10.1109/CVPR.1998.698619.

Ghali, F., Ali, N. and Yousif, A. (2020) 'Fingerprint Recognition', *IOP Conference Series: Materials Science and Engineering*, 928(3), pp. 100–109. doi: 10.1088/1757-899X/928/3/032078.

Gupta, B. (2019) 'Face Recognition Techniques-A Review', *AKGEC INTERNATIONAL JOURNAL OF TECHNOLOGY*, 9(1). Available at: https://www.akgec.ac.in/wp-content/uploads/2019/06/2-Face-Recognition-Techniques-Bhaskar-Gupta.pdf (Accessed: 14 December 2022).

Locking Solenoids | Kendrion. Available at: https://www.kendrion.com/en/products/solenoids-actuators/locking-solenoids-door-lock-systems/locking-solenoids (Accessed: 15 December 2022).

Milligan, B. (2017) *BBC NEWS | Business | The man who invented the cash machine*, *Business reporter, BBC News*. Available at: http://news.bbc.co.uk/2/hi/business/6230194.stm (Accessed: 15 December 2022).

Parodi, I. (2021) *Autonomous Weapon Systems and Ethical Issues . A Focus on Targeted Killings*. Irene Parodi.

Qamber, S., Waheed, Z. and Akram, M. U. (2012) 'Personal Identification System Based on Vascular Pattern of Human Retina', in *2012 Cairo International Biomedical Engineering*

Conference (CIBEC) Cairo, Egypt, December 20-21, 2012, pp. 64–67.

Ronald A. Kropp, Richard Irving, R. M. S. (2013) 'Pulse-rate detection using a finger print sensor, United States Patent US 8.433,110 B2'.

Sadikoglu, F. and Uzelaltinbulat, S. (2016) 'Biometric Retina Identification Based on Neural Network', *Procedia Computer Science*, 102(August), pp. 26–33. doi: 10.1016/j.procs.2016.09.365.

Simpson, A. K., Roesner, F. and Kohno, T. (2017) 'Securing vulnerable home IoT devices with an in-hub security manager', *2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017*, pp. 551–556. doi: 10.1109/PERCOMW.2017.7917622.

Triggs, R. (2022) *How fingerprint scanners work — Optical, capacitive, and other variants*. Available at: https://www.androidauthority.com/how-fingerprint-scanners-work-670934/ (Accessed: 15 December 2022).

Yathavi, T. *et al.* (2020) 'Development of Auto Tracking and Target Fixing Gun using Machine Vision', *2020 International Conference on System, Computation, Automation and Networking, ICSCAN 2020*. doi: 10.1109/ICSCAN49426.2020.9262451.

eISSN 1303-5150