Cloud-Based Biometric-Enhanced ATM Powered by Deep Learning

R. Vidhya and S. Gokila

Abstract Automatic teller machines (ATMs) are the most common way to withdraw cash from a user's account. It offers a quick and convenient way to access one's funds. However, the technology used to authenticate the user and authorize the transaction has somewhat remained unchanged. The advances in computer vision technologies have made it reliable than ever before. Utilizing these computer vision-based technologies combined with fingerprint-based authentication-based technologies in ATMs makes the system fool-proof and robust. With an additional eye watching over, the user can carry out the transaction in complete confidence.

Keywords Authentication · Biometrics · Face detection · Face recognition · Neural networks

1 Introduction

Automatic teller machines (ATMs) as we know commonly were introduced in the early 1950s in the UK. A unique code was issued to the users with which a maximum of $10 could be withdrawn. The concept of a PIN (personal identification number) was introduced in 1970 to have a reliable way of authorizing the users. Methods to authenticate and authorize a user are something you are, something you know and some- thing you have, and ATM card comes under the category of 'something you have'. A PIN is generally four numbers long in most banks and is asked

R. Vidhya (✉)
Department of Computer Science and Engineering,
Sri Krishna College of Technology, Coimbatore, Tamil Nadu, India

S. Gokila (✉)
Department of Computer Science and Engineering,
Hindusthan College of Engineering and Technology, Coimbatore, Tamil Nadu, India

A. Ramu et al. (eds.), *International Conference on Computing, Communication, Electrical and Biomedical Systems*, EAI/Springer Innovations in Communication and Computing, https://doi.org/10.1007/978-3-030-86165-0_12

every time a user tries to carry out a transaction combining that with an ATM card; it covers both 'something you have' (the card itself) and 'something you know'. Even though it is considered secure, it does not take into account the fact that most ATM centres are in a public setting. In public setting a shoulder surfing attack is very simple. And the fact that PIN is only four numbers long makes it easier for the attacker to remember it. A skimming device may be attached to the machine which strips the card details with which the prospective attacker can recreate the card and since the PIN is known to them, making a fraudulent transaction becomes easier [1–3].

2 Technological Survey

There are two main artefacts required to carry out a transaction: the ATM card and the PIN that the user knows.

2.1 Artefacts

EMV Card EMV can be abbreviated as Europay, MasterCard and Visa which refer to the companies that came up with the early standards in 1995. Recently the standard was acquired by EMVCo, LLC who defines and manages the standards since. It is most commonly known to us as ATM card. According to Wikipedia an ATM card is as the name suggests, usually a plastic card issued by a bank to its customer which allows them to access the ATMs. The cards have a magnetic stripe that stores data related to the card (unique card number) and so on and have an additional security mechanism in the form of a CVV number. Card verification value or CVV in short is usually a three-digit number used to validate the card during online transactions. Also printed on the card are the card holder's name and the expiry date. Nowadays chip-based card has been replacing the magnetic strip cards. While they are secure, it takes a lot of time to read and process.

PIN It is a four-digit number that a user chooses while activating the card. It is kept at four digits so that it is easier to remember. It acts as the second layer of protection in the existing implementation.

Operation of ATM Machines The basic functionality of an ATM machine can be illustrated in Fig. 1. The existing implementation relies on two factors: possession of both the card and remembering the access code. The functionality can be briefly elucidated as below. The user walks into an ATM centre and inserts the card when prompted, then the user is asked for the amount and then finally the amount is dispatched after the PIN is entered by the user.

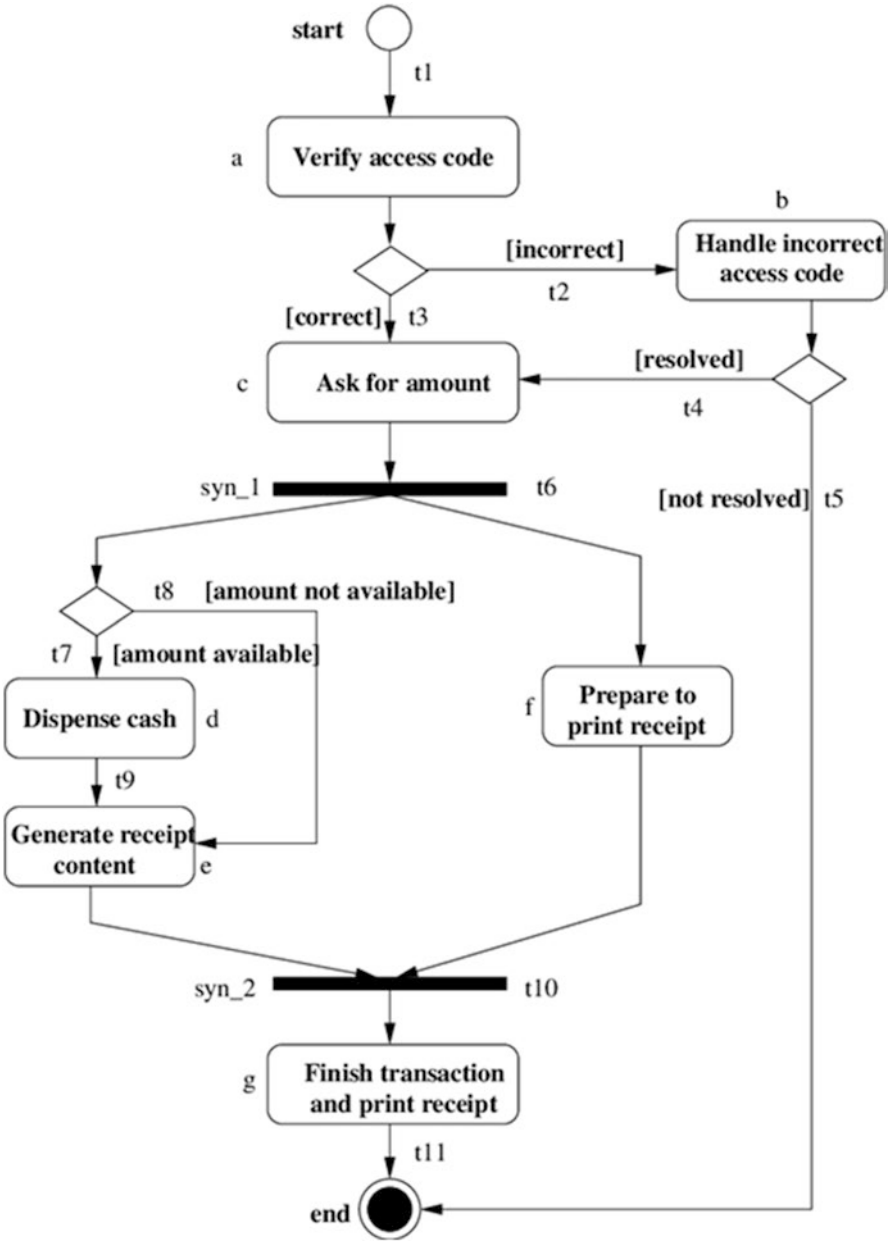

Fig. 1 UML diagram of ATM working [4]

3 Shortcomings with the Existing Implementation

The mere possession of both the card and the pin by an individual allows them to access the funds. ATM does not ensure that the person carrying the card is the one who is authorized to do so. If by any chance a person gets access to another person's card, there are many ways to know the PIN. The one situation when the current implementation holds its ground is when it comes to brute force attacks. An attack can be classified as brute force if it involves repeatedly trying to submit a value usually the password by putting together all the possible combinations. An evolved variant of brute force attacks uses a predefined dictionary which contains the most commonly used passwords which are tried first. While four-digit number is easier to brute force with today's computing power, there is restriction on how many attempts can be made before the card gets blocked. Because of this restriction, attackers generally try a more focused brute force attack utilizing social engineering. To accomplish this the attacker first identifies the victim and gathers as much information about them as possible. Then the attacker tries to come up with the combination the victim is most likely to use, for example, their birthdays or anniversaries or their ZIP code (0101, 0205 and so on). Ultimately all variants of brute force attacks have a little chance of success; hence the PIN is collected targeting and luring the victims with offers of a huge reward only to collect sensitive information like PIN in the end.

In the age of rapid information exchange, where everyone has access to the Internet, attacks are very easy. Phishing is one common practice. It is a targeted attack carried out on a particular set of people with the aim to extract sensitive information which can be their banking information, Social Security Number or any data that can be used to personally identify the person from them by reaching out to them by some medium like telephone, email and social media to mention a few while posing as genuine people from reputable institutions [5]. Old people are especially vulnerable due to a lack of awareness. Because of this they are targeted the most. Even if the attacker is unable to get the PIN, many cards nowadays use NFC to carryout pin-less transactions with which the attacker could withdraw the amount.

4 System Development

4.1 Overview of the Proposed Implementation

Our implementation creates a secure transaction layer between the existing ATM system and the user. At a higher level, the functionality can be divided across multiple modules as illustrated in Fig. 2.

To improve security and efficiency, the ATM starts to read facial data as soon as a user enters the ATM centre. By doing this, the ATM can detect a person's presence and get the user interface (UI) ready so that the user can interact with it immediately. From the security aspect, gathering facial data helps with the following:

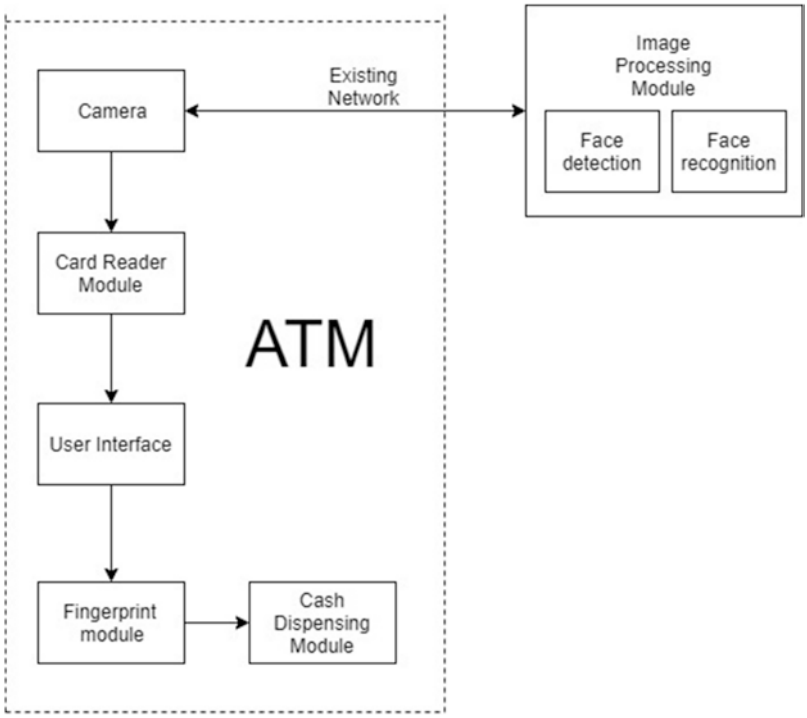

Fig. 2 Module-level functionality diagram

- Detect and identify malicious activity, and thwart maple is miscreants fixing a skimming device into the card reader that retrieves the card data once it is swiped.
- Identify if there are more people inside the ATM centre than allowed.
- Raise alarm if someone attempts to cover the face which could indicate some kind of unusual activity.
- Act as the first layer of security by identifying the user.

The actual processing of the gathered facial data happens remotely using the existing infrastructure set up by the bank which ensures that compatibility with the existing implementation is maintained. Image processing happens independently while the user interacts with the UI. Thus the UI always remains responsive. The user proceeds with the transaction inputting the amount required and so on; finally the user ID prompted to provide their fingerprint. Only if all the conditions are met, the transaction will get completed.

4.2 Web Camera

A webcam is a video camera retrofitted with circuitry that allows it to be exclusively used with a personal computer or a laptop. They use the USB (Universal Serial Bus) interface to communicate with the host. At the heart of a webcam is an image sensor

that is either made of CMOS (complementary metal oxide semiconductor) or CCD (charged coupling devices). Above the image sensor lies the lens which is either plastic or glass. Webcam produces a continuous stream of video and should always be connected with the internet [6].

4.3 Convolutional Neural Network-Based Image Classification

A convolutional neural network (CNN) is a class of deep learning neural networks [7]. Figure 3 shows layers in a convolutional neural network.

A neuron is the smallest unit of a neural network, and a collection of such neurons make up a neural network. In neural network these neurons are grouped together as layers, and the layers are connected to the subsequent layer. CNN or convolutional neural networks were proposed by Yann LeCun in 1988. It is a special architecture of artificial neural networks. In mathematical terms a convolution is when we take two functions f and g and perform a mathematical operation which produces another function h that describes how each function is modified by one another. Here we convolve the learnt data and the input data using 2D convolutional layers; this characteristic makes it ideal for 2D image processing.

Figure 4 shows what we perceive versus what a computer sees. To a computer an image is just an array of pixels which is of the same dimension as the image. Each element in the array contains a number from 0 to 255 indicating the pixel intensity at each point. The image is then passed through a series of connected layers where a small calculation is carried out at each layer. The convolution layer is always the first. The image (matrix of pixels) is given as the input to the first layer. Let us say this is the original pixel value function f, and then a smaller matrix is selected from

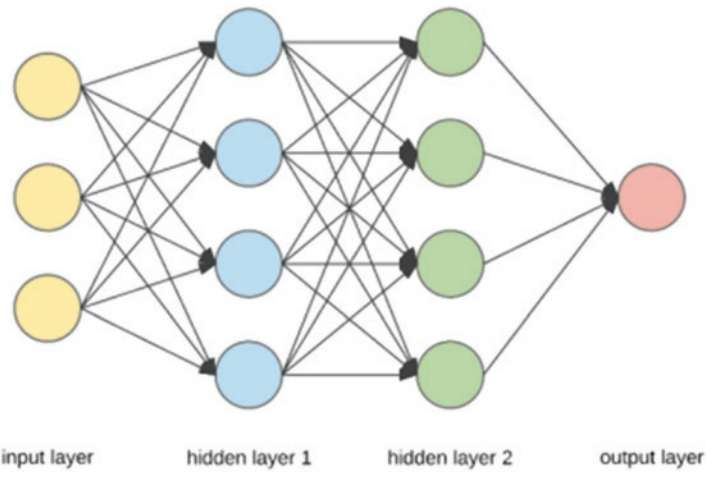

Fig. 3 Layers in a convolutional neural network

Fig. 4 What we perceive versus what a computer sees

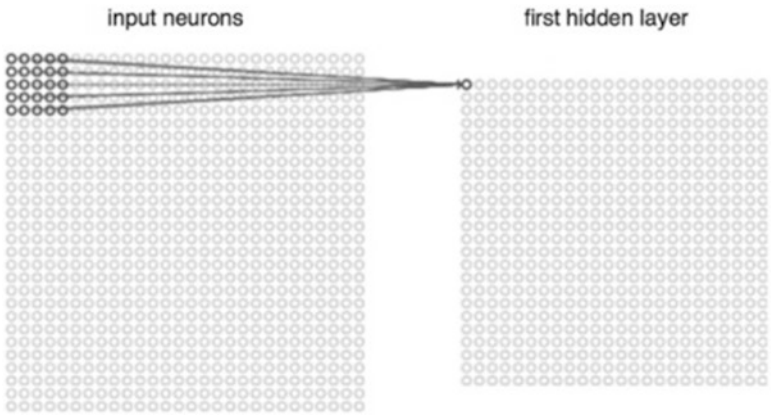

Fig. 5 Filter calculation to obtain a single value

the array which is called the filter which produces the convolution. Let us call it function g. Now function f is multiplied with function g and summed to produce a single value. This operation is analogous to us humans identifying the different features in an image like the face, hands, etc. This process is illustrated in Fig. 5.

4.4 Facial Detection

Face detection is a subset of machine learning that utilizes image processing technologies to carry out object class detection to identify human faces in digital images. An object class detection system aims to identify the different classes of features present in an image. Our implementation aims to utilize the existing infrastructure set up in the banks. To demonstrate this project utilizes third-party services provided by Amazon Web Services [8].

4.5 Face Recognition

Similar to face detection, face recognition uses image processing to identify a person's face, where its difference is that while face detection only aims to find faces in an image, a face recognition system attempts to establish the identity of the person(s) in the image. To achieve this each person's face is classified based on the facial feature points [9].

Figure 6 shows feature-based face detection. The face possesses. The most commonly used feature is the pupillary distance that calculates the distance between two pupils in a face. When combined with other modes of authentication, it becomes very reliable and hassle-free; the two most commonly used methods are bilinear interpolation and improved linear discriminant analysis [10]. Figure 7 shows working of a face recognition system.

4.6 Fingerprint Identification

The fingers of every human being have a unique pattern formed due to the ridge like structure of the skin. Evolutionally these ridges help us grip onto things. The ridge patterns are unique even between identical twins. This uniqueness makes it an ideal method to identify individuals. The process of conducting a fingerprint identification on a person is called dactyloscopy. In earlier days thumb impressions were checked by persons with nothing more than a magnifying glass. Nowadays with advances in computing technologies, it is automated. There are two ways to carry

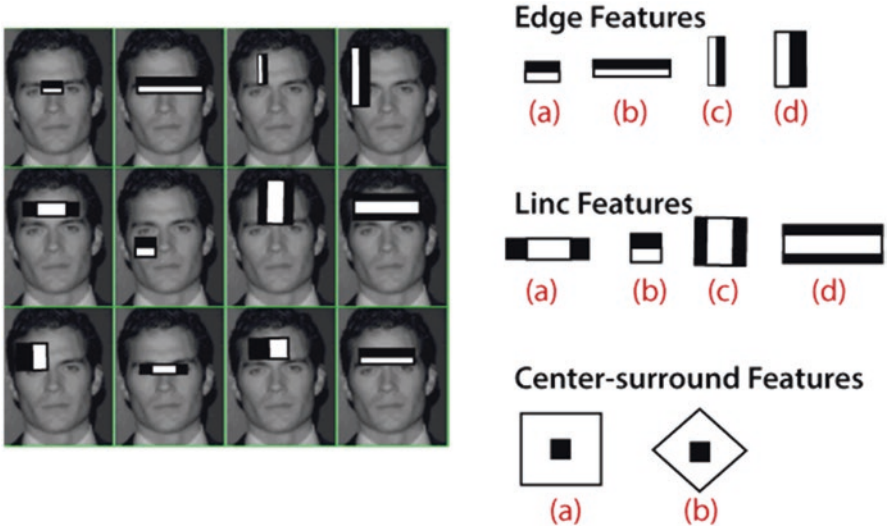

Fig. 6 Feature-based face detection

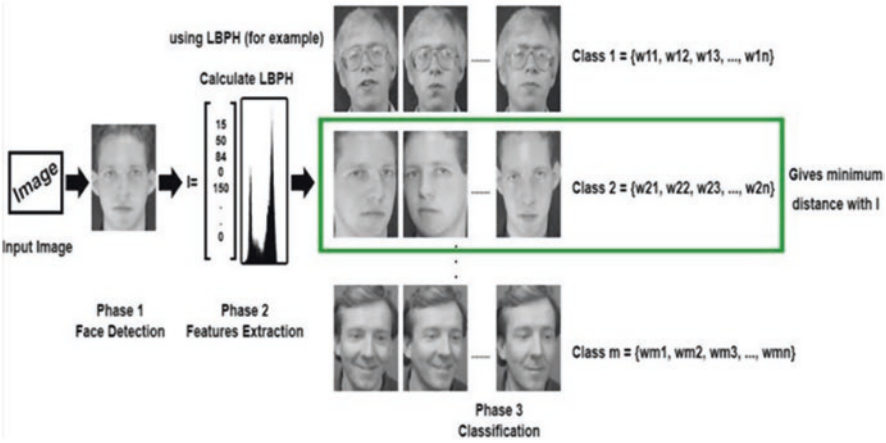

Fig. 7 Working of a face recognition system

out dactyloscopy: pattern matching and minutiae-based matching. A pattern matching simply tests if two images have a similar pattern, whereas minutiae-based matching tries to identify the minutiae points [11]. Figure 8 shows fingerprint identity.

4.7 Minutiae-Based Fingerprint Sensor

A minutiae-based fingerprint scanner works by comparing the minutiae points specifically the location and direction of each point. There are two methods to achieve this: using optical sensors and using capacitive sensors. In optical sensors, the CMOS sensor clicks a picture of the ridge patterns in the computer that analyses it. In capacitive scanners the distance between two ridges is measured as there exists a difference in capacitance since one part is raised and conductive, while the other part is not [12–15]. Fingerprint identity working is shown in Fig. 9.

5 Conclusion

This paper has demonstrated how the existing ATM setup can be enhanced in both the security aspect and in the usability aspect. The exponential growth in computing power has allowed running such complex deep learning tasks simpler and more efficient. Compared to the models of the yesteryears, today's models are smarter and more faster which allow for very low false-positive detections required when dealing with bank transactions.

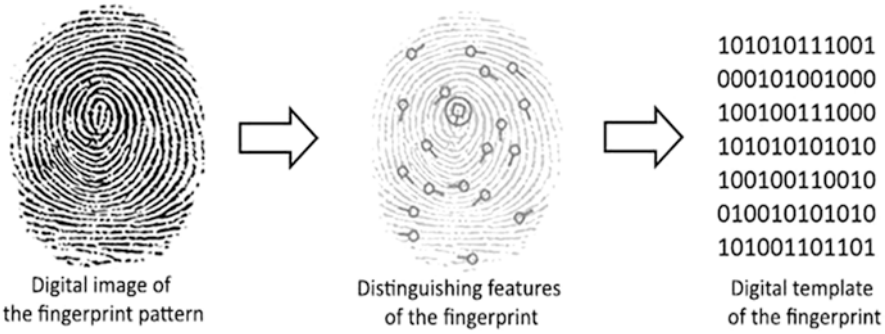

Fig. 8 Fingerprint identity

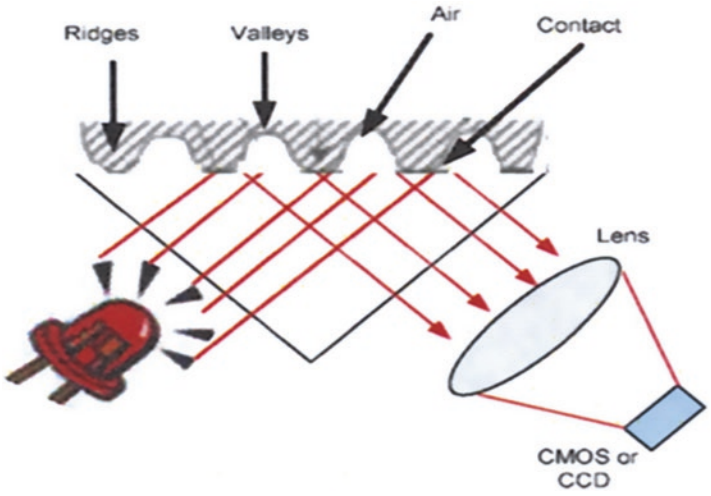

Fig. 9 Fingerprint identity working

References

1. Kumar, D.A., Iniyan, B., Askar, M.A., Ajay, A., Ambika, R.: Face recognition based new generation ATM machine. In: 5th International Conference on Advanced Computing & Communication Systems (ICACCS), pp. 938–943 (2019)
2. https://www.scienceabc.com/eyeopeners/why-are-atm-card-pins-usually-just-4-digit-long.html
3. Iddiqui, A.T.: Biometrics to control ATM scams: a study. In: International Conference on Circuits, Power and Computing Technologies [ICCPCT-2014], pp. 1598–1602 (2014)
4. Chen, M., Mishra, P., Kalita, D.: Efficient test case generation for validation of UML activity diagrams. Des. Autom. Embed. Syst. **14**(2), 105–130 (2010)
5. Thabit, F., Alhomdy, S., Jagtap, S.: A new data security algorithm for the cloud computing based on genetics techniques and logical-mathematical functions. Int. J. Intell. Netw. **2**, 18–33 (2021)

6. Devikanniga, D., Ramu, A., Haldorai, A.: Efficient diagnosis of liver disease using support vector machine optimized with crows search algorithm. In: EAI Endorsed Transactions on Energy Web, p. 164177 (Jul. 2018). https://doi.org/10.4108/eai.13-7-2018.164177
7. Srinivasa Rao, D., Berlin Hency, V.: Performance evaluation of congestion aware transmission opportunity scheduling scheme for 802.11 wireless LANs. Int. J. Intell. Netw. **2**, 34–41 (2021)
8. Titan, X.: Face recognition system and it's application. In: First International Conference on Information Science and Engineering, pp. 1244–1245 (2009)
9. Muhammad, R.S., Younis, M.I.: The limitation of pre-processing techniques to enhance the face recognition system based on LBP. Iraqi J. Sci. **58**(1B), 355–363 (2017)
10. https://en.wikipedia.org/wiki/Fingerprint
11. https://www.gemalto.com/govt/inspired/biometrics
12. https://en.wikipedia.org/wiki/Webcam
13. https://www.explainthatstuff.com/fingerprintscanners.html
14. Memon, S., Sepasian, M., Balachandran, W.: Review of finger print sensing technologies. In: IEEE International Multitopic Conference, pp. 226–231 (2008)
15. https://medium.com/@ksusorokina/image-classification-with-convolutional-neural-networks-496815db12a8