Machine Learning

**Biometrics of the fingerprint recognition**

Magnus Cardell, Elif Ilaria Yurtseven, & Mazen Abusharkh

horizontal line

# Introduction

The human body is by nature a standardized form with distinctive characteristics. The concept of having, for example, two arms, two legs, and a face, is said to be innate human characteristics. The form and function of these, however, vary immensely throughout a human population. Extracting the unique identifiers from a standard form is one of the key components in Biometrics. The iris of an eye, the fingerprint of a palm, or the pitch and volume of a voice, are all examples of possible unique identifiers. As privacy concerns about personal information and integrity are on the rise today, there is an incentive to find a fast, reliable, and affordable product that can be integrated into everyday life[[1]](#footnote-0). One prevalent biometric security product used today is the fingerprint scanner. In this case study, we will explore this technique and how it is used with machine learning algorithms.

# Role

When a fingerprint scan is sent to be verified, the system takes a biometric sample and checks it against a database of templates. Before the sample can be compared, however, there must be a number of preparing steps. First the training phase, where the user scans their fingerprint often multiple times so that the computer can learn the distinctive features based on image pattern recognition [[2]](#footnote-1). This stage also involves smaller pre-processing steps where the data is cleaned of noise artifacts, cropped, and signal enhanced[[3]](#footnote-2). To effectively store this data and use it for comparison, feature selection and extraction is used to define fingerprint *minutiae* which give you the unique structural data of the lines of a finger. In the comparison, the fingerprint is then compared to the database where the computer classifies whether or not to authenticate the data[[4]](#footnote-3).

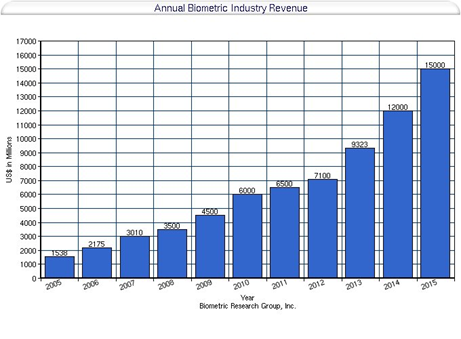
As described so far, the computer has been taught using supervised learning. The training data has a known outcome and a model is prepared through a training process. There are however practical uses of implementing unsupervised learning. In this semi-supervised learning, the computer has to learn the structure of the landmarks to solve the desired outcome. For example, after identifying landmark locations from all images in a training set, features around the points are extracted to get a structural account of the distribution of these points. By letting the computer find unique points, the template model would become smaller and use lesser but more accurate parameters.[[5]](#footnote-4)

# Growth

The market for automated fingerprint identification systems and fingerprint biometric technologies accounts for the greatest share of the global biometrics market and is forecast to continue to be the main source of overall market revenues. This sector was valued at $5 billion in 2012, nearly $10 billion in 2015[[6]](#footnote-5) and the Biometric System Market is estimated to reach a worth of $32.73 billion by 2022.[[7]](#footnote-6)  
Global strategies business report regarding Fingerprint Biometrics analysis announces that there are key driving and inhibiting forces in the Fingerprint Biometrics market:

* Tightening security measures in defense, customs, and border protection; where the driving force is the increase in threat or terrorist attacks and racism and the inhibitors are issues with fingerprint capturing.
* Growing adoption in the banking and financial services sector; where the driving force is security compulsions of government and law enforcement services and the inhibitor is growing competition from alternative biometric technologies.
* Rising prominence in immigration control and travel document verification; where the driving force is growing focus of business on safety and security of physical assets and the inhibitor is the forgery of fingerprints.[[8]](#footnote-7)

Industrial growth in Fingerprint Biometrics is the growing biometric investment in government and enterprise sectors to support national/civil ID, e-Governance, e-passports, law enforcement, access control and user authentication as well as in smartphones because of growing concerns over data integrity and security. Fingerprint identification technology is the oldest and most widely used biometric technology due to the unique patterns in each unique fingerprint. The increasing deployment of access control systems by building owners is further creating a strong business case for this market. In addition, 3D biometrics have become an important area of research and development.  
The United States is the largest worldwide market while the Middle East is predicted to be the fastest growing market with a CAGR (compound annual growth rate) of 14.5%. The biometric system market is expected to be worth US$32.73 billion by 2022. Below is the annual biometric industry revenue graph:



# Advancements

Fingerprint biometric systems have been going through what could be called evolutionary advancement since the beginning of the 21st century. The advancement in this field is based on three main patterns of fingerprint:

* Arch: The ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger.
* Loop: The ridges enter from one side of a finger, form a curve, and then exit on that same side.
* Whorl: Ridges form circularly around a central point on the finger.

These patterns are important in order to understand the advancement in Fingerprint Biometrics concerning both hardware and algorithms. The hardware advancement of the field went from optical imaging to ultrasonic and capacitance imaging now considered fastest and most accurate method.  
  
The major algorithmic advancements took place between the years 2001 and 2012, through the advancements in hardware technologies. In 2001, university students one from Hong Kong and three from Italy presented a new fingerprint classification algorithm based on two machine learning approaches: support vector machines (SVMs), and recursive neural networks (RNNs). RNNs were trained on a structured representation of the fingerprint image. They were also used to extract a set of distributed features which could be integrated into the SVMs. SVMs were combined with a new error correcting code scheme which, unlike previous systems, could also exploit information contained in ambiguous fingerprint images. In 2012, two students from the Informatics and Telematics Institute in Greece presented one of the latest updates on the algorithmic level of the fingerprint biometrics that is a multimodal of four machine learning algorithms for the fusion of several biometrics modalities. The algorithms examined are Gaussian Mixture Models (GMMs), Artificial Neural Networks (ANNs), Fuzzy Expert Systems (FESs), and Support Vector Machines (SVMs). The fusion of biometrics leads to security systems that exhibit higher recognition rates and lower false alarms compared to unimodal biometric security systems. Supervised learning was carried out using a number of patterns from a well-known biometrics database, and the validation took place with patterns from the same database which were not included in the training dataset. The comparison of the algorithms revealed that the biometrics fusion system is superior to the original unimodal systems and also other fusion schemes found in the literature.

# Problems

Despite the long history of using fingerprints, some key concerns still remain about the accuracy of identification, the usability of fingerprint systems in different situations, acceptance by the users, and other privacy concerns. One of the most important factors in the success of a biometric system is its accuracy. This is a measure of how well the system is able to correctly match the biometric information from the same person and avoid falsely matching biometric information from different people. In addition to accuracy, the speed of operation of a biometric system will be important for its eventual success. If it takes too long to enroll and/or verify participants, the result will be frustrated users and slow business processes. Also, as was mentioned previously, failures to enroll are often a serious problem when deploying biometric systems, and yet they have not received as much attention as matching failures. Failures to enroll can be caused by missing or damaged biometric characteristics, poor user training, poor devices, etc. All these problems are now solved or nearly solved with a new fingerprint recognition technology called ultrasonic fingerprint sensors.

Another area that must be considered is privacy. Depending on the place of deployment, it is likely that any biometric service involving the public would be covered by privacy legislation, which means that a privacy impact assessment would have to be completed and methods put in place to protect the privacy of the users. The organization bioprivacy.org has produced some tools that may be useful for doing impact assessments for biometric deployments. In addition, the Ontario Privacy Commissioner looked at a biometric deployment scenario when Toronto proposed an anti-double-dipping scheme [4]. They required that such a system have the following characteristics:

* Requiring the biometric scan to be encrypted
* Restricting the use of the encrypted finger scan only to authentication of eligibility, thereby ensuring that it is not used as an instrument of social control or surveillance
* Ensuring that an identifiable fingerprint cannot be reconstructed from an encrypted finger scan stored in the database
* Ensuring that a latent fingerprint (i.e., picked up from a crime scene) cannot be matched to an encrypted finger scan stored in a database
* Ensuring that an encrypted finger scan cannot itself be used to serve as a unique identifier
* Ensuring that an encrypted finger scan alone cannot be used to identify an individual (i.e., in the same manner as a fingerprint can be used)
* Ensuring that strict controls are in place as to who may access the biometric information and for what purpose
* Requiring the production of a warrant or court order prior to granting access to external agencies such as the police or government departments
* Ensuring that any benefits data (i.e., personal information such as the history of payments made, etc.) are stored separately from personal identifiers such as name, date of birth, etc.[[9]](#footnote-8)

# 

# Conclusion

The main reason we use biometrics security systems is because biometric systems use a characteristic of the user that is generally universal, stable, and unique. And fingerprints is the most common example for biometric security systems, and those biometric security systems are receiving a lot of attention because of their potential to reliably identify people based on a near-universal physical characteristic. Fingerprint-based security systems are becoming small and inexpensive and, as a result, they are being deployed in a wide range of situations and applications including cellular phones and laptop computers, automobile and building doors, and border-crossing and high-security military applications. Interestingly, biometric security systems are everywhere, replacing the conventional username and password combinations, the door security personnel, and the heavy metal keys. Nowadays, a lot of the world’s population have used fingerprint scanners for one reason or another. Biometric authentication is one of many machine learning approaches that changed and will keep changing the world around us. Generally, biometry has impacted the world positively, but it still generated some new concerns, such as privacy and reliability.

# Summary of Self-Driving Cars

Autonomous cars are self-driving cars capable of driving themselves without human input thanks to their obstacle detection unit which includes various types of cameras and a radar detection unit in order to identify track, pedestrians, bicycles, and even road signs. They generally use Bayesian Simultaneous Localization and Mapping (SLAM) algorithms, which fuse data from multiple sensors and an offline map into current location estimates and map updates and RTLS (Real Time Locating System) beacons for localisation. They use sensors like lidar, stereo vision, GPS and IMU (Inertial Measurement Unit). Visual object recognition uses machine vision algorithms including neural networks.

The main advantage of autonomous cars is the decrease in accidents caused by driver errors such as reaction time and distractions. However there are many potential concerns regarding self-driving cars, such as the acceptance by the user, the ability to be hacked, the possibility that those cars might not work with different types of roads (such as unpaved side roads), and their effect on economics. Many companies around the world are working on optimizing certain aspects of the self driving car such as the likelihood of a software bug or incompatibility or possible negative short-term economical effects and affordability in various countries.

**Bibliography**

**Albert Ali Salah**, *Machine Learning for Biometrics*, Centre for Mathematics and Computer Science (CWI), 2012, <http://oai.cwi.nl/oai/asset/13758/13758A.pdf>

**Masahiro Kawagoe**, *Fingerprint Pattern Classification,* Pattern Recognition, Volume 17, Issue 3, 1984, Pages 295-303

**Patrick, Andrew S.** "Fingerprint Concerns: Performance, Usability, and Acceptance of Fingerprint Biometric Systems." Andrew Patrick. National Research Council of Canada, 21 Apr. 2015. Web. 12 Feb. 2017.

**Ratha, Nalini K., and Venu Govindaraju.** *Advances in Biometrics: Sensors, Algorithms and Systems*. London: Springer-Verlag London Limited, 2008. Web. 11 Feb. 2017.

**Yao, Yuan, Gian Luca Marcialis, Massimiliano Pontil, Paolo Frasconi, and Fabio Roli.** *A New Machine Learning Approach to Fingerprint Classification.* AI\*IA 2001: Advances in Artificial Intelligence Lecture Notes in Computer Science (2001): 57-63. Web.

**Damousis, I. G., and S. Argyropoulos.** *Four Machine Learning Algorithms for Biometrics Fusion: A Comparative Study.* Applied Computational Intelligence and Soft Computing 2012 (2012): 1-7. Web.

**Rawlson King.** *Biometric Research Note: Commercial Applications for Biometrics Growing.* BiometricUpdate. N.p., 26 Sept. 2012. Web. 12 Feb. 2017.

*Fingerprint Biometrics Market Trends.* Fingerprint Biometrics Market Trends. N.p., n.d. Web. 11 Feb. 2017.

*Biometric System Market worth 32.73 Billion USD by 2022.* N.p., n.d. Web. 10 Feb. 2017.

1. Salah, Machine Learning for Biometrics [↑](#footnote-ref-0)
2. Kawagoe, Fingerprint pattern classification [↑](#footnote-ref-1)
3. Salah, Machine Learning for Biometrics [↑](#footnote-ref-2)
4. Ibid [↑](#footnote-ref-3)
5. Ibid [↑](#footnote-ref-4)
6. Rawlson King, Biometric Research Note: Commercial Applications for Biometrics Growing. [↑](#footnote-ref-5)
7. Biometric System Market worth 32.73 Billion USD by 2022. [↑](#footnote-ref-6)
8. Fingerprint Biometrics Market Trends. [↑](#footnote-ref-7)
9. Patrick, Fingerprint Concerns: Performance, Usability, and Acceptance of Fingerprint Biometric Systems, usability and acceptance issues. [↑](#footnote-ref-8)