Artificial Intelligence in Biometrics and Face Detection

J.Amey Aditya Achar

Bachelors of Engineering (Information Science and Engineering)

RNS Institute of Technology

OPEN ACCESS

Volume : 6

Special Issue : 1

Month : August

Year: 2018

ISSN: 2321-788X

Impact Factor: 3.025

Citation:.
Amey Aditya Achar. "Artificial Intelligence in Biometrics and Face Detection." *Shanlax International Journal of Arts, Science and Humanities*, vol. 6, no. S1, 2018, pp. 47–50.

DOI:
https://doi.org/ 10.5281/zenodo.1403575

Abstract

In 1956 John McCarthy first coined the term Artificial Intelligence, he defined it as "the science and engineering of making intelligent machines", and development of computer systems able to perform tasks normally requiring human Intelligence. Biometrics is a technical term for measurements and calculations, it refers to metrics related to human characteristics. With the wide spread of AI touching every possible field, advancements in the field of Biometrics has come a long way. In this paper we aim at introducing the readers to the basic principles of AI in Biometrics, performance of Biometric Systems in terms of false match rate (FMR), failure to enroll rate (FER), equal error rate (ERR), which have reduced extensively after the use of AI. Its application in the banking industry, explaining the use of Iris Recognition, for easier and safer withdrawal of money, in National Security in terms of Skynet: China's best Surveillance System, which uses Face Recognition technology to its full potential. After describing the applications, we define Biometrics of Intent, which surpasses the traditional scope and ambition of this Technology, a new era of Biometrics, one where cognitive sciences and neurobehavioral insights such as heart rates, breathing, eye movement, will be integrated into screening process, which help identify potentially dangerous individuals.

Keywords: Biometrics and Artificial Intelligence; Biometrics of Intent; Artificial Intelligence and Banking; Artificial Intelligence in National Security; Face Recognition; Biometric Systems

Introduction

Biometrics is a technical term for measurements and calculations, it refers to metrics related to human characteristics. It defines a person's identity based on the statistical analysis of their physical and behavioral characteristics. It is mainly used for surveillance or to grant access. There are broadly two types of biometric identifiers, based on physiological or behavioral characteristics. Face recognition, fingerprint scanner, iris recognition, DNA matching are examples of physiological biometrics, they are based on the composition of an individual. Behavioral biometrics depends on the unique ways in which individual acts, their gestures, walking patterns etcetera. The earliest applications of biometrics dates back to 1907, where the Hungarian police for first time used the fingerprint on a wine glass at the crime scene to solve a case. The next big step was in the creation of identification systems and database management in 1960. After these, followed the first real time facial recognition is 1991, with iris scanner in 1995 and biometric passports with RFIDs in 2006.

Today this same technology has reached great heights, in the names of Touch ID, Iris Recognition, Voice Assistants, and Infrared Cameras which help in faster and real time applications of facial recognition.

Artificial Intelligence was proposed decades ago with an attempt to develop intelligent algorithms which could mimic the visual cortex of the brain. Up until now, these were implemented as artificial neural networks which were too simple in terms of their structure and number layers to tackle complex real world problems like biometric recognition. In recent years, with the introduction of powerful and affordable GPUs and with the availability of large volumes of labelled data led to the emergence of Deep Learning as state of the art approach. Applications of Deep Learning include Natural Language Processing (NLP), computer vision, information retrieval and finance. Biometrics Recognition has been one of the most successful application of deep learning. This paper aims at introducing some applications of biometrics and Artificial intelligence in tackling real world problems, and building stronger security systems.

Performance of Biometric Systems

Performance of biometric systems is based on few metrics. False Match Rate (FMR) also called as False Acceptance Rate is a measure of the percent of inputs invalidly accepted. The system gives a match score, which is the probability of the similarity between the input pattern and a template in the database. If the score is greater than the threshold, the input is treated as genuine. False non-match rate (FNMR) is the probability that the system fails to detect the match between the input and the template in the database. It is a measure of valid inputs incorrectly rejected. The performance can be plotted in a ROC (Receiver Operator Characteristic) in a DET (Detection Error trade-off) plot. The DET curve gives uniform treatment to the two kinds of errors, and uses logarithmic scale for the two axes, which spreads out the plot and better recognizes diverse well performing frameworks, and for the most part creates plots that are near direct. In general, the biometric system sets a threshold, for an input to be identified as a valid match, i.e. how close it should be to be considered as a match. If the threshold value is higher, the FMR reduces, but FNMR increases, conversely, if threshold value is reduced, FNMR decreases, but FMR increases. Determination of the correct value of threshold is one application of Artificial intelligence in these systems.

Application of neural networks include face recognition, computer vision, Natural Language Processing (NLP). The most successful application of deep learning models is in biometric recognition. Biometrics in particular has tremendously improved with new models starting to emerge. Advancements in Computer vision make it possible to accept any kind of input, without the worry about the quality, hence reducing False Enroll Rate. Advancements in convolution neural networks, which is a biologically inspired model, have immensely helped in making the better performing facial recognition models.

Safer withdrawal of Money through Iris Recognition

Iris recognition is a method of identifying ring shaped patterns within the eye of human being which have complex patterns and varying colors that are visible upon close inspection. It is carried out, by gathering high resolution images of the pupil using digital cameras working at visible or infrared wavelength, and then using a specialized program to compare the subject's iris pattern and match with images stored in the database. The Biometric Iris Recognition technology is being used in more than 1000 ATM machines in financial institutions in Chicago and Montreal in lieu of debit cards. Iris recognition is most viable in the banking industry for the following reasons. Iris doesn't degrade with aging, it has more than 266 degree of rotation, which serves a pool of distinct

features associated to one individual, which improves the reliability of the biometric system, and the likelihood of damage or scratches to the iris is minimum as is it protected behind the eyelids, cornea and aqueous humor.

Iris recognition technology consists of three basic steps:

- Image capture: A high resolution image of the subject's eye must be captured, which can be automated or manually done, but it must be ensured that the iris is in proper focus and a clear image is generated.
- Locating the iris and optimizing the image: First the iris recognition framework enhances on the concentration and clarity of the picture. Then the boundaries of the eyes and the center of the pupil are identified and the analyzed for suitable feature extraction and analysis. The optimized image is converted into encoded structure features of the iris, which are formed by applying Daugman's rubber sheet model, which can be used to match the biometric templates in the database.
- Template storage and matching: The encoded structural features of the iris are stored in the database at the time of enrollment, and at the time of identification, the structural feature can be matched with the biometric templates stored in the database.

National Security through Face Recognition

A facial recognition device is one that takes an image or a video in real time and compares it to a set of available faces in the database and tries to create a match of the individual in it. The structure, shape and proportions of the face are compared. The distance between the eyes, size of the nose and jaw, the area surrounding the cheek bones are also compared. The mega-city of Chongging, in Southwest China uses this feature of biomimetic infused with artificial intelligence through a $2.6 billion project by installing 500,000 cameras across the entire city making it one of the world's largest security surveillance system. Deep learning technology used in the software improves the system by about 500% when compared to conventional systems. New algorithm that combines the features of machine learning and deep learning method, suppresses the error and enable recognition of individual in situations which was difficult using conventional systems (like the face from the side, part of a face covered by sun glasses etc.). The demographics of the crowd can also be identified using these systems, so they are not limited to only dealing with hard identities.

Biometrics of Intent

The present biometrics, however go way beyond speech, voice images or fingerprints. They are able to analyze different information and end point cooperation for example dexterity, weight, hand tremors, navigation and other finger gestures. The objective of biometrics of intent is to push the biometrics identification techniques to another wilderness where covert security innovation would examine people's minds to decide whether they harbor any malicious intent. This ability can be used by the national security or military forces to easily identify the enemies prior to any action. With this technology being fruitful in reality, the "biometrics of intent" for instance could help decide if the restless looking man at the airport is just having a bad day or is walking around with the intent to kill his manager. Studies on test subjects' behavioral responses in term of electroencephalographic (EEG - measures the electrical activity in the brain) and functional magnetic resonance imaging (FMRI - measures the neural blood flow), heart rates on viewing positive, negative, and neutral images help analyze the emotional state of an individual. With all the available data, one can use it to feed it into any Artificial Intelligence model, which is capable of detecting anomalies, and variations in the data, which would put a clear distinction in detecting

an individual with malicious intent. The ultimate goal that can be reached is to set up a databank of individuals' typical psychophysiological and behavioral responses to different mental states and utilize it to separate the physiology of intent mental states.

The concept of biometric of intent can be applied towards personal privacy and security towards sensitive information. The concept is based on analysis of behavioral biometrics: Key Interval Time (KIT) data through the use of artificial intelligence techniques as an effective means of identifying and distinguishing humans from one another. Every individual has a significant key stroke pattern, which can be exploited to associate it as an identification of that particular individual.

Nudata is a biometrics and behavioral analytics company that identifies its users based on the users' interaction with their products. BehavioSec is another company that uses machine learning in order to detect fraud for customers.

Conclusion

Due to the relatively recent advances in computation technologies, the concept of Artificial Intelligence has finally escaped the fantasies of mathematicians to become a major aspect of modern businesses and even lifestyles - from Youtube's AdSense detecting policy breaches in uploaded videos to Siri. Artificial Intelligence has helped solve several real world problems and continues to grow in application by the hour, making possible things that for decades have been passed off as hopeless fantasies, and this is merely the dawn of artificial intelligence technology. Who knows what wonders the future might hold?

References

Al-Assam Hisham and Sellahewa Harin, "Deep Learning – The new kid in Artificial Intelligence", Biometrics Institute, www.biometricsinstitute.org/news/deep-learning-the-new-kid-in-artificial-intelligence

Crisisboom, "Canadian Defence scientists probe 'biometrics of intent' ", Crisisboom, 16 March 2011, crisisboom.com/2011/03/16/biometrics-of-intent/

Crisisboom, "China – Security System on Steroids for Mega-City", Crisisboom, 09 March 2011, crisisboom.com/2011/03/09/china-security-system/

Purgason Benjamin, Hibler David, R.2012, "Security Through Behavioral Biometrics and Artificial Intelligence", Christopher Newport University, *Newport News*, Virginia, USA

Rouse Margaret, "Biometrics", Search Security, Tech Target, December 2017, searchsecurity.techtarget.com/definition/biometrics

Thakkar Danny, "An overview of Biometric Iris Recognition Technology and its Application Areas", Bayometric, Bayometric, www.bayometric.com/biometric-ir*is-recognit*on-application/