DGT301

**Facial recognition signal processing**

Nguyen Thanh Anh Duy – SE150090

Ho Thanh Thai – SE150350

Tran Ngoc Xuan Tin – SE150422

**Abstract**

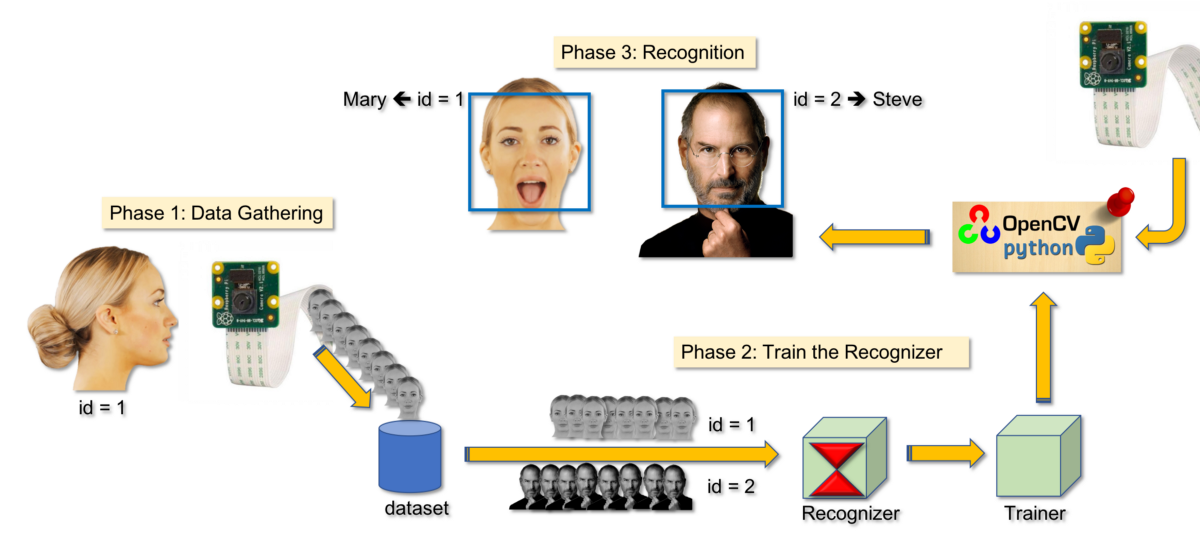
The invention relates to a digital signal processor (DSP)-based face detection method. The method comprises the following steps of: intercepting images from a dynamic video; extracting key information; and finding characteristic points by using the key information according to a topological relation between an entire face and each part based on the integrity attribute of a model by an image processing measure so as to finish overall face detection. A system hardware part consists of a front-end image acquisition part, an information processing part and a back end, wherein a charge coupled device camera with infrared image pick-up function is adopted by the front-end image acquisition part; a BF533 processor is adopted by the information processing part; and the back end connects a television with a DSP platform and directly displays a face detection result.

Table of Contents

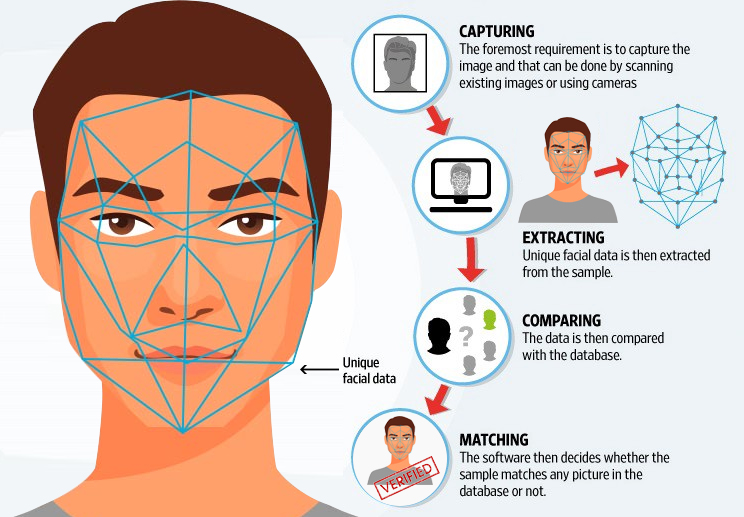
1. Introduction4
2. Technical requirements6
   1. Technical requirements for code reality6
   2. Technical requirements for application6
3. Analyze and explain the algorithms applied7
4. Application scope of the solution9
   1. Biometrics9
      1. Drivers Licenses9
      2. Entitlement Programs9
      3. Immigration9
      4. National ID10
      5. Passports10
      6. Voter Registration10
      7. Welfare Fraud10
   2. Information Security11
      1. Desktop Log-on11
      2. Application Security11
      3. Database Security11
      4. File Encryption12
      5. Intra-net Security12
      6. Internet Access12
      7. Medical Records13
      8. Secure Trading Terminals13
   3. Law Enforcement and Surveillance13
      1. Advanced Video Surveillance13
      2. CCTV Control14
      3. Portal Control14
      4. Post-Event analysis14
      5. Shoplifting and Suspect Tracking and Investigation15
   4. Smart Cards15
      1. Stored Value Security15
      2. User Authentication16
   5. Access Control16
      1. Facility Access16
      2. Vehicular Access17
5. Introducing some real products on the market18
6. Conclusion21
7. **Introduction to identity features**

Human activity is a major concern in a wide variety of applications such as video surveillance, human computer interface, face recognition, and face image database management. And machine face recognition is a research field of fast increasing interest. The strong need for user-friendly systems that can secure our assets and protect our privacy without losing our identity in a sea of numbers is obvious. At present, one needs a Personal Identification Number (PIN) to get cash from an ATM, a password for a computer, a dozen others to access the internet, and so on. Although extremely reliable methods of biometric personal identification exist, e.g., fingerprint analysis and retinal or iris scans, these methods rely on the cooperation of the participants, whereas a personal identification system based on analysis of frontal or profile images of the face is often effective without the participant’s cooperation or knowledge. Phillips described in the advantages/disadvantages of different biometrics.

We implemented a fully automatic DSP-based face recognition system that works on video. Our system consists of a face detection and tracking block, a skin tone extract block, a face normalization block, and face classification block.



**Figure 1.** Face detection system



**Figure 2.** Face region segmentation

1. **Technical requirements**
   1. Technical requirements for code reality

* Face detection
* Face analysis
* Converting the image to data
* Finding a match
  1. Technical requirements for application
* Textural features around 14 fiducial points
* Shape features of eye and eyebrows
* Searching time – 5 seconds per query image against a database of size 5000
* Limits of PIE variation:
  + Pose variation – 20%
  + Illumination variation – 20% of relative illumination variation
  + Expression variation – can tolerate deformation caused by natural expressions

1. **Analyze and explain the algorithms applied**

**Face Detection**, as the first step of the entire process, face detection affects greatly the overall system performance. In fact, a successful face detection is prerequisite to the success of following face recognition and verification tasks. Next, we apply 8-connected component labelling in the image to capture blobs and find the candidates of eye region. Finally, face detection completes by normalizing the face region to a standard size of 32 x 32 pixels.

Normalization of a face region reduces the effect of variation in the distance and location.

**Feature Extraction**, the extraction of feature vectors in face images is essentially a compression of a large image into a small vector. We used PCA [1] as feature extractor. Let the training set of M face images be . The average face of the training set is . Each face differs from the average by the vector . This set  is then subject to PCA, to produce a set of orthogonal vectors and their associated eigenvalues which best describe the distribution of the data. These eigenvectors can be thought of as a set of features that together characterize the variation among face images.

**Classification**, the classification is one of the most important components in a face recognition/verification system. Let us briefly describe the high-performance classifier, SVM [2]. The SVM provides a good generalization in pattern classification problems without any domain knowledge by the structural risk minimization method. If we assume that the input space is linearly separable for simplicity, the decision hyperplane is defined by equation (\*) in a high dimensional space  (\*), where x is a training pattern vector and  are the parameters that determines the hyperplane. The constraint given by equation (\*\*) must be satisfied to ensure that all training patterns are correctly classified  (\*\*), where  is a given data with . Because this simple model of SVM, called a maximal margin classifier, can not be applied to real applications, we adapted the dual objective function as  (\*\*\*), where  is slack variable and  is Lagrange coefficient. However, one problem is that it takes too much computation to solve this dual objective function. So, several approaches, such as Chunking, Decomposition and SMO (Sequential Minimal Optimization) have been proposed [3]. The Chunking algorithm uses the fact that the value of quadratic form is the same if you remove the row and column of the matrix that correspond to zero Lagrange multipliers. Therefore, Chunking drastically reduces the size of the matrix from the number of training examples squared to approximately the number of non-zero Lagrange multipliers squared.

The Decomposition algorithm shows that a large QP (Quadratic Problem) can be broken down into a series of smaller QP subproblems. As long as at least one example that violate KKT (Karush-Kuhn-Tucker) conditions is added to the examples for the previous subproblem, each step reduces the overall objective function and maintains a feasible point that obey all of the constraints. The main advantage of this decomposition is that it suggests algorithms with memory requirements linear in the number of training examples and linear in the number of support vectors. SMO is a simple algorithm that quickly solves the QP problem in SVM without any extra matrix storage and without invoking an iterative numerical routine for each subproblem. At every step, SMO choose two Lagrange multipliers to jointly optimize, finds the optimal values for these multipliers, and updates the SVM to reflect the new optimal values. We use the Decomposition algorithm considering the limitation of memory on DSP.

1. **Application scope of the solution**
   1. Biometrics
      1. Drivers Licenses

For many years, the Federal Bureau of Investigation (FBI) and U.S. Immigration and Customs Enforcement (ICE) have asked states to use their own face (or facial) recognition systems to search photos in their department of motor vehicles (DMV) databases. They have also obtained photos from state DMV databases through automated systems such as Nlets Photo Sharing, state networks such as Cal-Photo, or by simply requesting photo-sharing.

This use of DMV photos for law enforcement and immigration enforcement purposes is part of a larger context in which local, state, and federal law enforcement agencies, including ICE, have long relied on driver’s license databases to obtain information about drivers and car owners, including their addresses.

* + 1. Entitlement Programs

Face recognition is poised to become one of the most pervasive surveillance technologies, and law enforcement’s use of it is increasing rapidly. On the horizon, law enforcement would like to use face recognition with body-worn cameras, to identify people in the dark, to match a person to a police sketch, or even to construct an image of a person’s face from a small sample of their DNA.

This has led to the development of unproven, inaccurate systems that will impinge on constitutional rights and disproportionately impact people of color.

* + 1. Immigration

Facial recognition technology uses computer algorithms to scan and map the distinguishing features of a person’s face and then compares the resulting map to maps of pictures in the person’s passport, his visa, and in the galleries that CBP maintains.

Galleries include photographs captured by CBP during inspections, from passports and visas, and from other sources, such as the Automated Targeting System, which provides maps of faces in law enforcement and intelligence databases.

* + 1. National ID

Facial verification, which works by scanning someone’s face and matching it with a database image, is already used widely to unlock smartphones and access bank accounts, but Singapore is the first state to use it in a national ID scheme.

* + 1. Passports

While no one suggests that you’ll ever be able to travel without your ID – or, internationally, without your passport – on you, the day is approaching quickly when you rarely, if ever, will have to show those pieces of identification to anyone during your travels. Instead, your face will become you ID, or your passport.

* + 1. Voter Registration

Innovatrics has years of experience in providing trusted, scalable, and fully customizable solutions for creating biometric registries for elections and other citizen services. Leveraging top-performing fingerprint and face recognition algorithms, we can guarantee secure and fast identification and verification.

* + 1. Welfare Fraud

New facial recognition software has helped authorities detect dozens of attempts by fraudsters to claim welfare benefits using multiple identities over recent months.

The system involves comparing photographs of applicants captured during the registration process with all photographs held on the Department of Social Protection’s database.

* 1. Information security
     1. Desktop Log-on

Microsoft face authentication in Windows 10 is an enterprise-grade identity verification mechanism that’s integrated into the Windows Biometric Framework (WBF) as a core Microsoft Windows component called Windows Hello. Windows Hello face authentication utilizes a camera specially configured for near infrared (IR) imaging to authenticate and unlock Windows devices as well as unlock your Microsoft Passport.

* + 1. Application Security

Facial recognition systems include two huge and diverse applications. One aims at detecting a person, and is currently used in various surveillance applications, such as CCTV cameras. Another ensures that a person is successfully recognized, referring to biometric applications, such as mobile phones or smart home locks.

* + 1. Database Security

Facial biometrics system has been used as a measure of securities in the topmost institutions and workplaces to ensure that there is no scope of any vandalism. Just by a set of algorithms, the software does geometric and photometric recognition within seconds.

Its non-contact nature is the best thing about it in the sense that a person through facial recognition, even in a crowded place can be recognized, given that his ../images are saved in the database.

* + 1. File Encryption

Facial recognition technology turns your face into code that can be archived and traded among strange and suspect parties. Civil rights groups are already forecasting a near future where police use of facial recognition to track protesters will discourage people from hitting the streets. The face is only one of several methods that companies specializing in biometric identification technology are developing at a rapid pace. The Kansas-based company Stone Lock, for example, boasts that it uses infrared imagery to reduce your facial measurements into a unique and encrypted biometric signature data file.

Nobody could reconstruct your unique facial measurements, except the corporation that keeps your face in its lockbox. It’s time we conspire to shield our meat sacks from such intrusions and reclaim what encryption means in the context of biometric technology.

* + 1. Intra-net Security

When it comes to intranet security, the stakes have never been higher. Your intranet is no longer just a tool for communication and collaboration.

* + 1. Internet Access

In 2014, Facebook announced its Deep Face program, which can determine whether two photographed faces belong to the same person, with an accuracy rate of 97.25%. In June 2015, Google went one better with Face Net. Using an artificial neural network and a new algorithm, the company from Mountain View has managed to link a face to its owner with almost perfect results.

* + 1. Medical Records

Patient verification by unique identification is an important procedure in health care settings. Risks to patient safety occur throughout health care settings by failure to correctly identify patients, resulting in the incorrect patient, incorrect site procedure, incorrect medication, and other errors. To avoid medical malpractice, radio-frequency identification (RFID), fingerprint scanners, iris scanners, and other technologies have been implemented in care settings. The drawbacks of these technologies include the possibility to lose the RFID bracelet, infection transmission, and impracticality when the patient is unconscious.

* + 1. Secure Trading Terminals

The Vision Labs Luna POS terminal supports both normal card transactions and biometric facial recognition payments. For a biometric transaction, the terminal scans the customer's face and sends the template to the payment service provider or bank for identification. The facial data is not saved. Vision Labs says that with Covid-19 accelerating the move to contactless payments and banks now starting to use facial recognition to authorize online payments, its terminal is launching at an opportune time.

* 1. Law enforcement and surveillance
     1. Advanced Video Surveillance

The face image in a passport is an only data to be used for personal authentication worldwide, regardless of nationality. In addition, the face image recognition offers a unique advantage compared to other personal authentication technologies because it enables to authenticate people from a distant location such as personal identification through surveillance cameras.

* + 1. CCTV Control

While the application of facial recognition within both public and private spheres continues to draw criticism from those who see it as a threat to civil rights, this technology has become extremely commonplace in the lives of iPhone users.

Similarly, CCTV is a well-established security measure that many of us are familiar with, whether through spotting images displayed on screens in shops, hotels and offices, or noticing cameras on the side of buildings.

History has taught us that it is human nature to fear the unknown, especially if it seems that it may change life as we know it.

* + 1. Portal Control

Embed facial recognition into your apps for a seamless and highly secured user experience. No machine-learning expertise is required. Features include face detection that perceives facial features and attributes—such as a face mask, glasses, or face location—in an image, and identification of a person by a match to your private repository or via photo ID.

* + 1. Post-Event analysis

The recent rise of virtual events has emphasized the need for and value of strong event data, and thanks to virtual platforms, collecting and leveraging that data has never been easier. These platforms enable planners and marketers to capture more robust engagement data than what is normally collected at physical events, including metrics like session views, the duration of those views, number of visits to virtual booths, and more. However, facial analysis promises to offer even more specific and useful attendee data for both virtual and live events. In today’s climate, another advantage of facial analysis for live events is that it works very well with face masks, which isn’t the case when it comes to facial recognition.

It is simple to deploy and can provide rich data for both event organizers and exhibitors/sponsors. In addition, Zenus can be utilized in a similar way for virtual events using the video feed from a Zoom meeting, Google Meet call, etc. and is working on being able to further support hybrid events. In a post-Covid future, the technology could be deployed in an even greater capacity at live events.

* + 1. Shoplifting, Suspect Tracking and Investigation

Facial recognition is the only way to prevent shoplifting before it actually happens. It is crucial to prevent theft, as most violent retail altercations happen after somebody has been caught in the act.

Systems that have this technology can identify previous offenders based on whether their faces’ data points match with ones in a shoplifter database. Then, the system automatically notifies the store’s security team when a match is found.

Often, simply offering customer service to a known shoplifter will deter them from stealing – in most cases, they will simply leave the store when they know they are being watched. By using proactive facial recognition technology, you will reduce violent crime alongside theft.

* 1. Smart cards
     1. Stored Value Security

While many people interact with facial recognition merely as a way to unlock their phones or sort their photos, how companies and governments use it will have a far greater impact on people’s lives. When it’s a device you own or software you use, you may be able to opt out of or turn off facial recognition, but the ubiquity of cameras makes the technology increasingly difficult to avoid in public.

* + 1. User Authentication

Authentication plays a central role in boosting an organization’s security posture. It helps enable an organization to keep its systems secure by permitting only authenticated users (or processes) to access the protected resources, such as computer systems, networks, databases, websites and other network-based applications or services.

Passwords are the more traditional form of authentication, but they constitute a weak form of protection; users are prone to bad password practices, such as reusing passwords, using predictable passwords, or even sharing passwords with others. To combat this issue, more companies are leveraging artificial intelligence and machine learning technologies, such as deep learning-based techniques, to develop better and more secure authentication approaches. AI/ML algorithms have been shown to bolster cybersecurity by protecting devices against cyber-attacks and preventing fraudulent activities.

* 1. Access control
     1. Facility Access

Latest generation access control and door intercom systems are now increasingly adopting face recognition for highly secure authentication and keyless door entry.

The access control system uses AI algorithms to convert the image of the face into what is effectively a series of 'co-ordinates' - accurately pinpointing the distances between eyes, nose, mouth, ears, etc. - to create a unique identifying string of numbers which is stored in the system's database.

A face recognition-based system will use access control end-points featuring integrated, high-resolution cameras which will provide a live face scan of the individual at the door or gate.

* + 1. Vehicular Access

Face recognition is finding its way into the new generations of cars in an attempt to increase safety and convenience. From car ignition to theft prevention – there are countless possibilities of using facial recognition in cars. Such as:

* Unlocking the car with your face
* Personalized in-cabin experience
* Keeping the driver focused and safe
* Child protection
* Creating better and safer vehicles

1. **Introducing some real products on the market**

* **Amazon** previously promoted its cloud-based face recognition service named Rekognition to law enforcement agencies.
* **Apple** uses facial recognition to help users quickly unlock their phones, log in to apps, and make purchases.



**Figure 3.** Apple’s Face ID on iPhone

* **British** **Airways** enables facial recognition for passengers boarding flights from the US.
* **Cigna**, a US-based healthcare insurer, allows customers in China to file health insurance claims which are signed using a photo, rather than a written signature, in a bid to cut down on instances of fraud.
* **Coca-Cola** has used facial recognition in several ways across the world. Examples include rewarding customers for recycling at some of its vending machines in China, delivering personalized ads on its vending machines in Australia, and for event marketing in Israel.
* Since 2019, **Facebook** has made the feature opt-in as part of a drive to become more privacy focused. Facebook provides information on how you can opt-in or out of face recognition here.

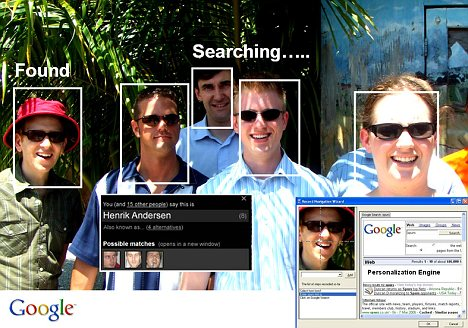


**Figure 4.** Facebook application

* **Google** incorporates the technology into Google Photos and uses it to sort pictures and automatically tag them based on the people recognized.
* **MAC** **make-up**, uses facial recognition technology in some of its brick-and-mortar stores, allowing customers to virtually "try on" make-up using in-store augmented reality mirrors.
* **McDonald’s** has used facial recognition in its Japanese restaurants to assess the quality of customer service provided there, including analyzing whether its employees are smiling while assisting customers.
* **Snapchat** is one of the pioneers of facial recognition software: it allows brands and organizations to create filters which mold to the user’s face — hence the ubiquitous puppy dog faces and flower crown filters seen on social media.



**Figure 5.** Snapchat application



**Figure 6.** Google application

1. **Conclusion**

In this paper, a new feature extraction method for a real-time face recognition system is proposed. We represent a face detection system by using a chrominance component of skin tone and face recognition system which combines PCA and LDA. Our face detection method detects skin regions over the entire image, and then generates face candidates based on the spatial arrangement of these skin patches. Our algorithm constructs maps of eye and mouth to detect the eyes, mouth, and face region. The PCA and LDA method presented here is a linear pattern recognition method. Compared with nonlinear models, a linear model is rather robust against noise and most likely will not over-fit. Although it is shown that distribution of face patterns is complex in most cases, linear methods are still able to provide cost effective solutions. Especially, the results of several experiments in real life show that the system works well and is applicable to real-time tasks. In spite of the worst case, the complete system requires only about 100 ms per a frame. The experimental performance is achieved through a careful system design of both software and hardware for the possibility of various applications.

**References**

[1] Turk, M., Pentland, A.: Eigenfaces for Recognition. Journal of Cognitive Neuroscience, 3 1 (1991) 77-86 6

[2] Cristianini, N., Shawe-Taylor, J.: An Introduction to Support Vector Machines. Cambridge University Press (2000) 6

[3] Scholkopf, B., Burges, C., Smola, A.: Advances in Kernel Methods – Support Vector Learning. MIT Press (1998) 7