Global Journal of Computer Science and Technology
Graphics & Vision
Volume 13 Issue 4 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Robust Automatic Face Recognition

By Roshan Kavuri, Sani Kommu Vasav & Ramisety Sravani
J.B. Institute of Engineering & Technology, India

Abstract - The crux of the character identification problem is to exploit the relations between videos and the associated texts in order to label the faces of characters with names. It has similarities to identifying faces in news videos. However, in news videos, candidate names for the faces are available from the simultaneously appearing captions or local transcripts. While in TV and movies, the names of characters are seldom directly shown in the subtitle or closed caption, and script/screenplay containing character names has no time stamps to align to the video. According to the utilized textual cues, we roughly divide the existing movie character identification methods into three categories In this Robust Face-Name Graph Matching for Movie Character Identification is used to detect the face of movie characters and the Proposed system is taking the minimum time to detect the face. In this one we can do it in a minute process.

Keywords : image processing, face recognition biometrics, pattern recognition, pixels, psychophysics.

GJCST-F Classification: I.4.8

Strictly as per the compliance and regulations of:

Robust Automatic Face Recognition

Roshan Kavuri [α], Sani Kommu Vasav [σ] & Ramisety Sravani [ρ]

Abstract - The crux of the character identification problem is to exploit the relations between videos and the associated texts in order to label the faces of characters with names. It has similarities to identifying faces in news videos. However, in news videos, candidate names for the faces are available from the simultaneously appearing captions or local transcripts. While in TV and movies, the names of characters are seldom directly shown in the subtitle or closed caption, and script/screenplay containing character names has no time stamps to align to the video. According to the utilized textual cues, we roughly divide the existing movie character identification methods into three categories In this Robust Face-Name Graph Matching for Movie Character Identification is used to detect the face of movie characters and the Proposed system is taking the minimum time to detect the face. In this one we can do it in a minute process.

Keywords : image processing, face recognition biometrics, pattern recognition, pixels, psychophysics.

I. Introduction

Traditionally, the management of identity was satisfactorily and principally achieved by connecting attributed identifiers with biographical identifiers that were anchored in existing and ongoing local social relations. As populations have grown, communities have become more transient, and individuals have become more mobile, the governance of people (as populations) required a system of identity management that was considered more robust and flexible. Also passwords and PINs are hard to remember and can be stolen or guessed; cards, tokens, keys and the like can be misplaced, forgotten, purloined or duplicated; magnetic cards can become corrupted and unreadable. However, an individual's biological traits cannot be misplaced, forgotten, stolen or forged.

Biometric technologies have emerged as promising tools to meet these challenges of Identification, based not only on the faith that "the body doesn't lie," but also on dramatic progress in a range of relevant technologies. Biometric-based technologies include identification based on physiological characteristics (such as face, fingerprints, finger geometry, hand geometry, hand veins, palm, iris, retina, ear and voice) and behavioural traits (such as gait, signature and keystroke dynamics). Face recognition appears to offer several advantages over other Identification, based not only on the faith that "the body doesn't lie," but also on dramatic progress in a range of relevant technologies. Biometric-based technologies include identification based on physiological characteristics (such as face, fingerprints, finger geometry, hand geometry, hand veins, palm, iris, retina, ear and voice) and behavioural traits (such as gait, signature and keystroke dynamics). Face recognition appears to offer several advantages over other biometric methods, Almost all these technologies require some voluntary action by the user, i.e., the user needs to place his hand on a hand-rest for fingerprinting or hand geometry detection and has to stand in a fixed position in front of a camera for iris or retina identification.

However, face recognition can be done passively without any explicit action or participation on the part of the user, thus to this need and using observations of human psychophysics, face recognition as a field emerged.

Advantages:

- Very fast and accurate.
- No need of any extra manual effort.
- No fever of data loss.
- Just need a little knowledge to operate the system.
- Can handle large database.
- Low error rate in retrieval of images.
- Increased efficiency in verification and identification of images.

Disadvantages:

The methods used to recognize the characters in the existing system are taking too much time for detection and performance is limited in complex scenes.

- This system has failed to demonstrate promising results in case of huge variation in the appearance of each character.
- It is very critical to detect the exact characters as the system is not efficient enough to provide accuracy above 90%.
- The error rate of the system is comparatively high in change of any external conditions.
- In the proposed process the time taken for detecting face in minimum (min) time only in windows processed

II. Face Recognition Process

Facial recognition research is a subfield in a larger field of pattern recognition research and technology. Pattern recognition technology uses statistical techniques to detect and extract patterns from

Author α σ ρ : Department of Information Technology J.B. Institute of Engineering & Technology, Hyderabad Andhra Pradesh, India.
E-mails : roshan.kavuri@gmail.com, sanikommuvasavireddy@gmail.com, rsravani@gmail.com

data in order to match it with patterns stored in a database. The data upon which the recognition system works (such as a photo of a face) is no more than a set of discernable pixel-level patterns for the system, that is, the pattern recognition system does not perceive meaningful "faces" as a human would understand them. Nevertheless, it is very important for these systems to be able to locate or detect a face in a field of vision so that it is only the image pattern of the face (and not the background "noise") that is processed and analyzed.
The two main approaches to face recognition are

1. *Geometric*

The geometrical approach uses the spatial configuration of facial features. That means that the main distinguishing features of the face such as the eyes, nose and mouth are first located and then faces are classified on the basis of various geometrical distances and angles between features.

2. *Photometric*

On the other hand, the photometric approach uses templates of the facial features .It is a statistical approach that distil an image into values and compare the values with templates to eliminate variances.

a) Face Recognition Solutions Tasks

FRS can typically be used for three different tasks, or combinations of tasks:

- Verification
- Identification
- Watch list

i. *Verification ("Am I the identity I claim to be?")*

Verification or authentication is the simplest task for a FRS. An individual with a pre-existing relationship with an institution (and therefore already enrolled in the reference database or gallery) presents his or her biometric characteristics (face or probe image) to the system, claiming to be in the reference database or gallery (i.e. claiming to be a legitimate identity). The system must then attempt to match the probe image with the particular, claimed template in the reference database. This is a one-to-one matching task since the system does not need to check every record in the database but only that which corresponds to the claimed identity (using some form of identifier such as an employee number to access the record in the reference database). There are two possible outcomes: (1) the person is not recognized or (2) the person is recognized.

ii. *Identification ("Who am I or What is my identity?")*

Identification is a more complex task than verification. In this case, the FRS is provided a face to attempt to match it with a biometric reference in the gallery (or not). This represents a one-to-many problem. In addition, we need to further differentiate between closed-set identification problems and open-set identification problems. In a closed-set identification problem we want to identify a person that we know is in the reference database or gallery (in other words for any possible identification we want to make we know beforehand that the person to be identified is in the database). Open-set identification is more complex in that we do not know in advance whether the person to be identified is or is not in the reference database. The outcome of these two identification problems will be interpreted differently. If there is no match in the closed-set identification then we know the system has made a mistake (i.e., identification has failed (a false negative)). However in the open-set problem we do not know whether the system made a mistake or whether the identity is simply not in the reference database in the first instance. Real-world identification applications tend to be open-set identification problems rather than closed-set identification problems.

iii. *Watch list ("is this one of the suspects we are looking for?")*

The watch list task is a specific case of an open-set identification task. In the watch list task, the system determines if the probe image corresponds to a person on the watch list and then subsequently identifies the person through the match (assuming the identities of the watch list are known). It is therefore also a one-to-many problem but with an open-set assumption. When a probe is given to the system, the system compares it with the entire gallery (also known in this case as the watch list).

b) Steps in Face Recognition Process

The facial recognition process normally has four interrelated phases or steps. The first step is face detection, the second is normalization, the third is feature extraction, and the final cumulative step is face recognition. These steps depend on each other and often use similar techniques. Each of these steps poses very significant challenges to the successful operation of a FRS.

i. *Detecting a Face*

Detecting a face in a probe image may be a relatively simple task for humans, but it is not so for a computer. The computer has to decide which pixels in the image is part of the face and which are not. In a typical passport photo, where the background is clear, it is easy to do, but as soon as the background becomes cluttered with other objects, the problem becomes extremely complex.

ii. *Normalization*

Once the face has been detected (separated from its background), the face needs to be normalized. This means that the image must be standardized in terms of size, pose, illumination, etc., relative to the images in the gallery or reference database. To normalize a probe image, the key facial landmarks must be located accurately. Using these landmarks, the

normalization algorithm can (to some degree) reorient the image for slight variations. Such corrections are, however, based on statistical inferences or approximations which may not be entirely accurate. Thus, it is essential that the probe is as close as possible to a standardized face.

iii. *Feature extraction and recognition*

Once the face image has been normalized, the feature extraction and recognition of the face can take place. In feature extraction, a mathematical representation called a biometric template or biometric reference is generated, which is stored in the database and will form the basis of any recognition task. It is important for successful recognition that maximal information is retained in this transformation process so that the biometric template is sufficiently distinctive.

To improvise the system and provide additional features, the following algorithms are used:

c) ECGM Algorithm

ECGM algorithm is being used to detect the faces in the video and to reduce the noises in the complex scenes. ECGM is a powerful tool for graph matching with distorted inputs. It has various applications in pattern recognition and computer vision. Through error correcting graph matching, we can define appropriate graph edit operations according to the noise investigation and design the edit cost function to improve the performance.

i. *Eigen Faces using PCA*

The PCA technique converts each two dimensional image into a one dimensional vector. Each component (eigenface) represents only a certain feature of the face, which may or may not be present in the original image. A probe image is compared against a gallery image by measuring the distance between their respective feature vectors. For PCA to work well the probe image must be similar to the gallery image in terms of size (or scale), pose, and illumination. It is generally true that PCA is reasonably sensitive to scale variation.

III. Overal Description

a) Product Perspective

This application is useful for face name matching in videos. It can be further developed to enhance security by using surveillance cameras in conjunction with face recognition system.

Currently it is gaining support as a potential tool for recognizing individuals in organizations where it can be used for attendance management system. Facial recognition is already in use in many law enforcement areas. Software has also been developed for computer networks and automated bank tellers that use facial recognition for user verification purposes.

This product is aimed to provide a best fitted engine to enroll, verify and identify face and name data at a high speed and very low error rate. As the input devices, web cam, scanner or any other image acquisition device can be used where user feeds input through this image acquisition device while processed biometric information is stored in an internal database. Product will do the comparison between internal database and given inputs by the user at identification.

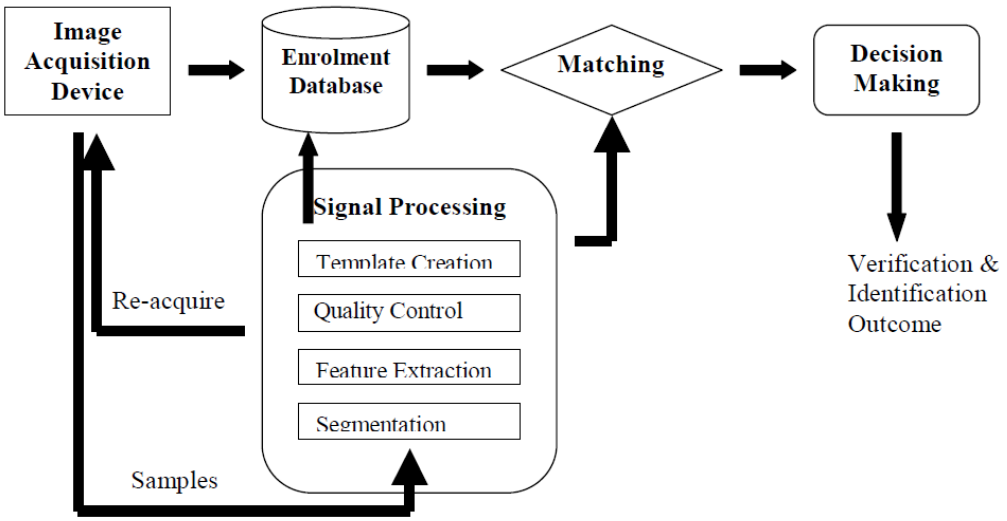

Figure 1 : High Level System description diagram

b) Product Features

Simultaneous multiple faces processing. The biometric face recognition system performs fast and accurate detection of multiple faces in live video streams and still images.

Live face detection. A conventional face identification system can be easily cheated by placing a photo of another person in front of a camera. The face recognition system is able to prevent this kind of security

breach by determining whether a face in a video stream belongs to a real human or is a photo.

Face image quality determination. A quality threshold can be used during face enrolment to ensure that only the best quality face template will be stored into database.

Tolerance to face posture. A face recognition system has certain tolerance to face posture that assures face enrolment convenience: rotation of a head can be up to 10 degrees from frontal in each direction (nodded up/down, rotated left/right, tilted left/right).

Multiple samples of the s amen face. Biometric template record can contain multiple face samples belonging to the same person. These samples can be enrolled with different face postures and expressions, from different sources and in different time thus allowing improving matching quality.

Identification capability. Face recognition system functions can be used in 1-to-1 matching (verification), as well as **1-to-many** mode (identification).

Fast face matching. The JUSTLOOK 3.2 face template matching algorithm compares **100,000 faces per second**.

Compact face features template. A face features template occupies only **2.3 Kilobytes**, thus our applications can handle large face databases**.**

Features generalization mode. This mode generates the collection of the generalized face features from several images of the same subject. Then, each face image is processed, features are extracted, and the collections of features are analyzed and combined into a single generalized features collection, which is written to the database. This way, the enrolled feature template is more reliable and the face recognition quality increases considerably.

i. *Time Attendance System*

Face Recognition Solution's **time attendance system** can be used to track the time spent by the individual in a particular premise. This biometric solution is exclusively used for managing the time related data. The biometric time attendance system is built to work on different premises without any extra hassles.

Biometric time attendance system is based on **face recognition technology.** With the usage of the biometric time attendance system, it eliminates the need of the paper register which was in use earlier for recording the attendance along with the time.

IV. Access Control System

Access control system is designed to work in different premises. If you are searching for a security system that can provide the protection from the access of the secured areas or resources then the Face Recognition Solution's access control system is the perfect solution. Since access controlling mechanism is a day to day phenomenon and therefore protection of the various resources is a vital act.

V. Visitor Management System

Face Recognition Solution's Visitor Management System deals with the security provided at various premises from the unauthenticated or unwanted visitors. This electronic solution can overcome the various shortcomings that used to be faced by the primitive security methods for checking the visitors at a particular premise.

VI. System Design

Design is the first step in the development phase for any techniques and principles for the purpose of defining a device, a process or system in sufficient detail to permit its physical realization. Once the software requirements have been realized, analyzed and specified the software design involves three technical activities design, coding, generation and testing that are required to build and verify the software.

a) Design Goals

The definition of goals is the first step of system design, it defines the qualities that our system should focus on many design goals can be inferred from the non function requirements or from the application domain, other will have to the elicited from the Client, it is necessary to state them explicitly such that every important design decisions can be made consistently following the same set of criteria.

The following are the design goals for the current system:

i. *Reliability*

The application should be reliable in keeping the data secure during computation of the orders.

ii. *Fault Tolerance*

The application should handle all the expected faults that a user is highly probable to commit.

iii. *Security*

It should never compromise on the security of orders and data. Once it fails to maintain security to the orders/data, the application becomes a worthless bauble.

iv. *Modifiability*

It should be easy to be understood. The design and implementation should not be too complex for another person to understand it. It should be feasible for modification.

System design is transition from a user oriented document to programmers or data base personnel. The design is a solution, how to approach to the creation of a new system. This is composed of several steps. It provides the understanding and procedural details necessary for implementing the system recommended in the feasibility study. Designing goes through logical and physical stages of development, logical design reviews the present physical system, prepare input and

output specification, details of implementation plan and prepare a logical design walkthrough.

VII. Conclusion & Future Enhancements

The main aim of the paper is to overcome the drawbacks of previous system by using the machine based face identification process. We have shown that the proposed two schemes are useful to improve results for clustering and identification of the face tracks extracted from uncontrolled movie videos. From the sensitivity analysis, we have also shown that to some degree, such schemes have better robustness to the noises in constructing affinity graphs than the traditional methods.

A third conclusion is a principle for developing robust character identification method: intensity alike noises must be emphasized more than the coverage alike noises.

In the future, we will extend our work to investigate the optimal functions for different movie genres.

Another goal of future work is to exploit more character relationships, e.g., the sequential statistics for the speakers, to build affinity graphs and improve the robustness.

Any face recognition system could not provide 100% efficiency till now but this system would provide improved efficiency up to 90% and decline in error rate. The Future enhancements of this paper include the following:

The face-name matching technique should be developed in live video surveillance

By detecting face the details of the person should be displayed with in very low time interval.

The project can be extended to detect faces even in case of external items like spectacles, cap, helmet, etc.

The system can be extended to match even if the person or individual are in disguise or in case of age progression.

References Références Referencias

1. J. Stall amp, H.K Ekenek and R.Stirfelhagen “video based face recognition on real world data “ICCV, 2007, pp 1-8.
2. J. Yang and A. Hauptmann, “multiple instance learning for labelling faces in broad casting news video,” in ACM INT Conf Multimedia 2005, pp 31-40.
3. O. Arandjelovic and R. Cippolla “automatic cast listing in feature-length films with anisotropic manifold space” in CVRP (2), 2006 PP 1513 -1520.
4. D. Raman S. Baker and S. Akkad “Leveraging archival video for building face datasets” in ICCV, 2007 pp1-8.
5. http://www.pages.drexel.edu/~sis26/Eigenface%20Tutorial.htm
6. http://sun.aei.polsl.pl/~mkawulok/stud/fr/lect/07.pdf

This page is intentionally left blank