Simulation Modelling Practice and Theory 65 (2016) 72–80

Contents lists available at ScienceDirect

Simulation Modelling Practice and Theory

journal homepage: www.elsevier.com/locate/simpat

Multiple granularity fused mobile forensics algorithm

Z. Wei [a,b], R. Zhao [c,*]

[a] Department of Computer Science and Technology, Tongji University, Shanghai, China
[b] Key Laboratory of Embedded System and Service Computing, Ministry of Education, Tongji University, Shanghai, China
[c] The Third Research Institute of the Ministry of Public Security, Shanghai, China

ARTICLE INFO

Article history:
Available online 2 May 2016

Keywords:
Face recognition
Bionic pattern recognition
Biometric feature
Mobile forensics

ABSTRACT

With the rapid development of Internet of Things and mobile computing platforms, many intelligent applications are implemented as mobile services, such as pattern recognition algorithms. This paper proposes two kinds of multiple granularity feature-based person recognition algorithms for forensics applications, which fuse biometric feature and face recognition algorithms into two kinds of strategies. A bionic pattern recognition based face recognition algorithm is also proposed. Experimental results show that the proposed algorithm has a satisfied recognition precision and low time complexity in many forensics scenarios, which could be conducted on mobile forensics devices with high efficiency.

1. Introduction

The development of Intelligence techniques provides a great convenience for forensics. Meanwhile, faster communication infrastructure brings high efficiency for many industry sectors, including forensics. Computation and communication were two distinct concepts. They are now integrated in all large information systems and infrastructures. The latest information infrastructure that integrates Internet of Things (IoT), cloud computing environments and Big Data considers both computing and communication quantifiable resources that offer flexible levels of performance and quality on demand [1]. Forensics system disposed with IoT architecture and Big Data analysis is a future developing trend.

Due to the pervasive applications of intelligent video surveillance network, for the purpose of human tracking, vehicle tracking, event detection, etc., it has become an important research direction of forensics. Existing video surveillance systems are mostly based on traditional network. With the rapid improvement of IoT and mobile computing platforms, more and more intelligent applications are expected to be disposed on IoT system and mobile terminals. However, the computing capacity is a bottleneck for many complicated intelligent applications [2], especially for some intelligent video analysis applications. This paper focuses on the fusion of face feature and soft biometric feature aiming at mobile forensic applications. The whole system is divided into front and back ends, connecting through internet, and based on Bay Trail IoT platform.

Automatic face recognition in forensics can be traced back to 1966 when the first paper was published by Bledsoe [3]. With the high coverage rate of surveillance cameras worldwide, the progression of robust and fast face recognition techniques in videos play more and more important role in law enforcement agencies. Compared to general automated face recognition, forensic face recognition has a higher performance requirement, because it normally works on facial images captured under noisy conditions, and it must be liable for legal procedures.

* Corresponding author. Tel.: +86 13817544956; fax: +86 2169589359.
E-mail addresses: zhihua_wei@tongji.edu.cn (Z. Wei), zhaorui1@126.com (R. Zhao).

http://dx.doi.org/10.1016/j.simpat.2016.02.007
S1569-190X(16)00026-5/

Generally, face recognition algorithms follow a similar process, including face detection, alignment, appearance normalization, feature representation [4-5], feature extraction [6-7], and matching [8].

Face detection is the prerequisite of face recognition. Yang et al. [9] summarized the various methods into four categories: knowledge-based methods, feature invariant methods, template matching methods and appearance-based methods. Knowledge-based methods use pre-defined rules to determine a face based on human experience; feature invariant methods try to seek the face structure features which are robust to pose and lighting variations; template matching methods use pre-defined face templates to judge whether the given image is a face; appearance-based methods learn face models from a training set which including enough representative face images and then perform detection. In general, appearance-based methods had been showing superior performance to the others. For example, the seminal work by Viola and Jones [10] has made face detection practically feasible in real world applications such as digital cameras and photo organization software. More attention has been given to boosting-based face detection schemes, which have evolved as the actual standard of face detection in real-world applications [10]. However, it still has limitations on mobile computing platforms.

In ideal conditions, many latest methods are likely to obtain satisfied results, and the process could make a fairly right decision without requiring any human interaction. However, illumination and pose variations are among the crucial factors that may and actually do hinder the correct recognition. Marsico et al. [11] evaluated some of the most popular and well-established algorithms for face recognition (principal component analysis (PCA), LDA, ICA, and SVMs) to assess the feasibility of real world face recognition in uncontrolled setting using data drawn from Facebook. Their results shows that none of the algorithms evaluated was robust.

In order to obtain more reliable evidence, forensic face recognition results is often fused with other biometric feature to enforce the judgment. Many interests focus on how to compensate for the main degradations found in uncontrolled scenarios. For example, Brendan F. et al. studied the influence of demographics on the performance of face recognition algorithms [12]. Pedro T. et al. studied the influence of distance on the performance of biometric recognition and its fusion strategies with face recognition [13]. Large amount of observations reflect that the ancillary information such as soft biometrics can contribute to improve and compensate the degraded performance of forensic systems [13].

Above all, single face recognition algorithms are hard to satisfy the real requirements for forensics precision. For real applications, combing other information to improve forensic precision and efficiency is an effective way. Moreover, previous researches mainly focus on algorithm simulations on PCs. With the performance improvement of mobile platforms, some researches pay more attentions on intelligent applications on mobile services. For example, Z. Wei et al. proposed a kind of forensics system based on hybrid features, which integrated face recognition and biometric features [14]. Its idea is conducting biometric recognition first to form a candidate set and then face recognition algorithm was working on the candidate set. The simple integration way brought a fast and effective forensics results. However, this kind of simple combination may bring the problem of loss of samples in biometric recognition process. This paper tries to work out a multiple granularity framework to integrate face recognition and biometric feature for forensics application. This framework should satisfy both precision requirement and complexity limitation on mobile computing platform.

The rest of the paper is organized as follows. Section 2 presents the overall architecture of the mobile forensics system. Section 3 addresses the face recognition algorithm. Section 4 gives the biometric feature recognition algorithm and fusion strategies. Section 5 introduces the experiments and results analysis. Section 6 concludes and gives the future research directions.

2. Multiple granularity mobile forensics system architecture

The architecture of the proposed mobile forensics system is based on Granular Computing (GrC) idea, which is a new computing paradigm to solve massive complex problems by simulating the human mind [15]. It enables us to map the complexities of the world around us into simple theories that are computationally tractable to reason in [16]. It also integrates human-oriented and machine-oriented studies to design human-inspired machines and systems for problem solving. Its central idea is to represent information and knowledge at multiple levels of granularity, to process it based on such a multilevel granular structure, to reasoning at multiple levels of abstraction, and to explore variable levels of schematic and approximate solutions of problems, from qualitative and symbolic to quantitative and numeric [17].

We developed the framework based on GrC theory. The overall architecture is shown in Fig. 1, where an image captured by the camera in a mobile device is input to the system. The face detection model as a preprocessing model will detect whether there is a person. The forensic process is designed in two granularity levels. The first level is the biometric model, which predicts the biometric features such as age, skin color, and gender, ensuring they are consistent with the candidate image set. The first level is called coarse granularity recognition. The second level is a refined recognition process, at which face recognition model works in the candidate set. Only when there is no well-matched images in this set, the search algorithm begins to conduct on the other images in the gallery database. The final decision will be made based on the fused results of two granularity levels. The design of each model is introduced as follows. The fusion methods will be discussed in Section 4.

(1) Face detection model: For the forensics application, the face detection in this paper is not only locating an outline of a face in given images, but also the accurate locations of detailed facial features such as eyes, nose and mouth are necessary for sub-sequential face recognition and biometric feature prediction. The multi-level facial feature location