Chapter 2
A Fingerprint Forensic Tool for Criminal Investigations

Gian Luca Marcialis
University of Cagliari, Italy

Fabio Roli
University of Cagliari, Italy

Pietro Coli
Arma dei Carabinieri, Italy

Giovanni Delogu
Arma dei Carabinieri, Italy

ABSTRACT

In this chapter, the authors describe the software module developed in the context of a joint research work between the Department of Electrical and Electronic Engineering of the University of Cagliari, and Raggruppamento Carabinieri Investigazioni Scientifiche (Scientific Investigation Office) of the "Arma dei Carabinieri", that is the militia maintained by the Italian government for police duties. Aim of the joint research work has been the study of state of the art on methods and algorithms for automatic analysis of latent fingerprint images and for fake fingerprints identification. The result of this research has been the development of a prototype software tool, whose aim is to help the human expert in analyzing latent fingerprints collected during investigations. This software exhibits several features which are not present in standard AFIS tools. Advanced modules for fingerprint image processing, comparison among fingerprints, and, finally, a module for discriminating fake latent fingerprints from "live" ones, characterize this tool. With the term "fake latent fingerprints", we mean latent fingerprint images released on the crime scene by a "stamp" reproducing a certain true fingerprint.

DOI: 10.4018/978-1-60566-836-9.ch002

INTRODUCTION

The exploitation of latent fingerprints for criminal investigation, from the first years of the previous century, has become one of the most important steps in forensic applications. The "proof" value of a fingerprint released in the crime scene has been appreciated in many occasions. Recently, the computer has been added as an important instrument for dactiloscopists, which are the human experts working on the analysis of latent fingerprint images.

The chapter topic is the computer aided latent fingerprint analysis, which has been done, so far, with the help of well-known Automatic Fingerprint Identification System[1] (AFIS) (Lee & Gaensslen, 1992; Komarinski, 2005). This software improved the efficiency of human experts in processing fingerprint images notably. Main "job" of AFISs is to retrieve a set of fingerprint images, stored in wide international data bases, "similar" to that found in the crime scene. This is done by "minutiae matching" (Komarinski, 2005; Jain et al., 1997). However, current AFISs do not take into account that the latent fingerprint analysis has made several steps ahead from their introduction in scientific police offices.

In general, the forensic fingerprint analysis is performed through the following steps:

1. The latent fingerprint is detected and several approaches aimed to its separation from the background are applied. These approaches consist in enhancing the fingerprint shape through the use of physical procedures or chemical substances (Lee & Gaensslen, 1992), as powders or fluorescent substances.
2. The enhanced fingerprint is photographed in order to capture a sufficient large number of images of it. This analysis can adopt a multi-wave length approach (different UV wave lengths are used), that is, several photos of the same surface are taken at different wave lengths (Berger et al., 2006). If the surface is not plane, it can happen that an image is blurred in some parts. Thus, several photos obtained by setting different focus of the camera's lens are necessary, and the result is that each photo contains only some sharp parts of the fingerprint (Burt et al., 1982; Burt, 1983; Burt & Adelson, 1983; Burt, 1992).
3. Insertion of the best image of the latent fingerprint in the AFIS data base.
4. Searching for the nearest images on the basis of the minutiae detected by the human expert on the fragment.
5. Final technical report about the individual operations performed on the fingerprint fragment.

During this analysis, and especially on step 2, many operations cannot be performed by AFISs. Moreover, the human operator is not able to jointly exploit multiple images captured at different wavelengths. AFIS cannot help him in this task. On the other hand, combining such information could be very useful in order to obtain a clear latent fingerprint image, separated from the more or less complex background.

Another aspect that forensic investigations did not yet take into account is the possibility of faking a fingerprint, which has been shown some years ago by several researchers (Talheim et al., 2002; Matsumoto et al., 2002; Ligon, 2002; Coli et al, 2007). In other words, it has been shown that, independently on the subject will, it is possible to "capture" its fingerprint and reproduce the related shape on a material as silicone or gelatine (Matsumoto et al., 2002). This can be done by constraining the subject to put his finger on a plasticine-like material. Otherwise, it is possible to enhance his latent fingerprint on the surface where it has been released, with the same methods used by the scientific police officers. So far, additional hardware to the electronic sensor, or image processing and pattern recognition approaches,