Forensic Science International 262 (2016) 84–96

Contents lists available at ScienceDirect

Forensic Science International

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

The use of fingerprints available on the web in false identity documents: Analysis from a forensic intelligence perspective

Carlos Magno Alves Girelli [a,b,*]

[a] Laboratory of Carbon and Ceramic Materials, Department of Physics, Federal University of Espirito Santo, 29075-910 Vitoria-ES, Brazil
[b] Identification Group, Federal Police Department of Brazil, 29114-670 Vila Velha-ES, Brazil

ARTICLE INFO

Article history:
Received 20 July 2015
Received in revised form 28 January 2016
Accepted 22 February 2016
Available online 4 March 2016

Keywords:
Fingermark
False document
Web
Reversal
AFIS
Forensic intelligence

ABSTRACT

Fingerprints present in false identity documents were found on the web. In some cases, laterally reversed (mirrored) images of a same fingerprint were observed in different documents. In the present work, 100 fingerprints images downloaded from the web, as well as their reversals obtained by image editing, were compared between themselves and against the database of the Brazilian Federal Police AFIS, in order to better understand trends about this kind of forgery in Brazil. Some image editing effects were observed in the analyzed fingerprints: addition of artifacts (such as watermarks), image rotation, image stylization, lateral reversal and tonal reversal. Discussion about lateral reversals' detection is presented in this article, as well as suggestion to reduce errors due to missed HIT decisions between reversed fingerprints. The present work aims to highlight the importance of the fingerprints' analysis when performing document examination, especially when only copies of documents are available, something very common in Brazil. Besides the intrinsic features of the fingermarks considered in three levels of details by ACE-V methodology, some visual features of the fingerprints images can be helpful to identify sources of forgeries and modus operandi, such as: limits and image contours, fails in the friction ridges caused by excess or lack of inking and presence of watermarks and artifacts arising from the background. Based on the agreement of such features in fingerprints present in different identity documents and also on the analysis of the time and location where the documents were seized, it is possible to highlight potential links between apparently unconnected crimes. Therefore, fingerprints have potential to reduce linkage blindness and the present work suggests the analysis of fingerprints when profiling false identity documents, as well as the inclusion of fingerprints features in the profile of the documents.

1. Introduction

According to the criminal database of the Brazilian Federal Police (BFP), more than 7000 cases involving false documents are investigated annually by that law enforcement agency [1]. Such statistics would become so much higher if considered the criminal cases investigated by the 27 state polices of Brazil.

When persons bearing supposedly false documents are arrested, the seized documents are sent to the forensic division to be examined. The analysis aim to verify the authenticity of the document based mainly on features of the substrate. When the criminal activity is detected after the offender has gone, generally only copies of the false documents are available for the investigation, resulting in the impossibility of conducting regular forensic analysis on the original questioned documents. Fingerprint examination may be helpful for detecting forgeries, especially when dealing with copies of documents, given that in Brazil identity (ID) documents usually display the fingerprint (right thumb) of the bearer.

In late 2014, while searching on AFIS for a suspicious fingerprint present in false ID document, experts from BFP in the state of Espirito Santo obtained HIT decisions with fingerprints from false documents that have been used in different states of Brazil, some of them located so far from the others. In general, no additional intelligence work was done with respect to the links created inside the AFIS by making HIT decisions. The results of the comparisons were solely focused on specific investigation process and the subsequent trial.

Intrigued by the unlikely connection between those criminal cases from so far apart locations, the experts decided to go beyond the routine task. They performed search for the suspicious fingerprint image on the web, considered the most likely source

* Correspondence address: Grupo de Identificação, Superintendência Regional de Polícia Federal no Espírito Santo, Rua Vale do Rio Doce, 01, São Torquato, Vila Velha-ES, CEP 29114-670, Brazil. Tel.: +55 27 3041 8089; fax: +55 27 3041 8064.
E-mail addresses: girelli.cmag@gmail.com, girelli.cmag@dpf.gov.br

http://dx.doi.org/10.1016/j.forsciint.2016.02.041
0379-0738/

for independent forgers have obtained a same fingerprint image. The search was successful; they found websites containing that fingerprint used in multiple false documents [2]. The finding caused great surprise, given that all the experts of that Identification Group had more than ten years of experience and they had never thought to search for fingerprints on the web before.

The present study was designed to verify whether fingerprints available on the web besides that already identified have been used to forge ID documents in Brazil and, if so, how often this has happened. Furthermore, considering that BFP has recently detected some cases of laterally reversed (mirrored) fingerprints on false ID documents [2,3], and that such reversals have also been used in recent research of other authors [4], all procedures performed in the present study were applied for both fingerprints obtained from the web and their lateral reversals.

Some image editing effects observed in the fingerprints obtained from the web will be discussed with regard to their detection by the AFIS search. In this sense, a suggestion to improve the workflow when searching for lateral reversals on AFIS will be presented.

Also, this web-based study will be analyzed from a forensic intelligence perspective. In simple terms, the intelligence activity can be briefly defined as the result of a process aiming to transform raw data into a form suitable for making decisions [5]. Forensic intelligence occurs when such activity is carried out by law enforcement agencies in an accurate, usable and timely manner, obtaining information from traces and forensic case data to support tactical, operational and strategic decisions, especially in models such as intelligence-led policing [6–8]. Instead of focusing on each individual criminal case and in the use of its evidences solely for court purposes, forensic intelligence is based on a multi-case focus and a broader approach. The aim is to uncover potential links that may lead to the identification of common sources and series of crimes, allowing authorities to better understand crimes and use resources in a proactive manner [8].

Some examples of the use of forensic intelligence are given elsewhere [5,9–12]. Rossy et al. [9] have described the integration of retrospective dataset extracted from a common database shared by Swiss police forces, concluding that forensic outcomes have a great potential to detect crime series. Morelato et al. [5] have discussed the use of forensic case data in intelligence-led policing, presenting as example the illicit drug profiling performed in Australia and in Europe, in particular in Switzerland. A novel forensic intelligence model based on systematic profiling of false ID document was proposed by Baechler, Ribaux and Margot [10], aiming to uncover links, patterns and trends based on visual features of false documents. The application of such method to different types of seized documents has led those authors to conclude that it has a great potential to diminish linkage blindness and to develop analysis capacity at the strategic, operational and tactical levels [10]. In a follow-up research, Baechler et al. [11] have presented further results from the application of the profiling method to seized ID documents, giving more details about the comparison process and metrics used in the method. A transversal model comparing illicit drugs and false ID documents monitoring from a forensic intelligence perspective was presented by Morelato et al. [12], aiming to generalize the use of the method to break barriers between apparently separate fields of study in forensic science and intelligence, among other considerations.

In Brazil, profiling of illicit drugs has been done [13–16], but there is still no profiling of false documents for forensic intelligence purposes. Fingermarks and documents are generally examined by different experts from different divisions and no forensic intelligence work has been developed with respect to fingerprints present on false documents. One goal of this work is to present some features of fingerprints that have been used in false ID documents with potential to highlight possible links between criminal cases, justifying the addition of fingerprint analysis in the profiling activity as well as the inclusion of fingerprints features in the profile of the false ID documents.

2. Materials and methods

2.1. Web search and image editing

Fingerprints images were obtained by searching on Google Images website. After typing 'impressão digital' ('fingerprint' in Portuguese language), the first displayed 100 fingerprint images in JPEG format were saved. Image resolutions ranged from 72 to 762 ppi, the most common incidences being 96 ppi ($n = 49$) and 300 ppi ($n = 20$).

The images were edited using Adobe Photoshop in order to remove watermarks, texts, logo marks and any artifacts considered extrinsic to the fingerprints, such as for instance those displayed in Fig. 1. After clean up the images and orientate the fingerprints with the fingertips facing up, the samples were identified by numbers from '01' to '100' and are presented in Fig. 2.

2.2. AFIS search

All the 100 fingerprints displayed in Fig. 2 were inserted, one by one, in the BFP AFIS. Because of the different sizes and resolutions of the images, it was necessary to adjust the scales following an operational procedure developed by fingermark experts from BFP [17]. The procedure consists in marking a distance perpendicular to 11 ridge lines close to the nuclei region and attributes a length of 5 mm to that distance. Although the statistical study performed by those researchers [17] has concluded that there are limitations associated to the method and it should not replace the use of a scale when photographing fingermarks, its use can be helpful as a last resource for adjusting the scale in the lack of other reference with known dimension on the image.

The adjusted-scale fingerprints were auto-encoded by the system with no human manual mark-up of minutiae. A list of 15 candidates was presented by the system at the end of the search and HIT decisions were based not only on the number of minutiae, but on the whole set of features in agreement, as established by international standards [18–21]. Anyway, only for information, the numbers of minutiae in agreement for each pair of matched fingerprints were in the range 15–100.

The first comparisons performed in AFIS were made between the fingerprints themselves. Matched fingerprints were grouped together in groups numbered by G-01, G-02, G-03 and so on. The group G-01 was filled with the fingerprint # 01 and all the others resulting from a HIT decision with fingerprint # 01; G-02 was filled with fingerprint # 02 (or the next in line if fingerprint # 02 have

Fig. 1. Examples of artifacts present in fingerprints available on the web. The contrast between artifacts and fingerprints were highlighted using Adobe Photoshop for better visualization.