Sample research paper on a critique on digital influences in fingerprint analysis...

Law, Criminal Justice

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

Arunabha Banerjee

Senior Associate, Corporate & Compliance Solutions, Thomson Reuters

Abstract

With the changing needs of time, forensic analysis of fingerprint in administering criminal justice has undergone a sea change. The process has experience intense digitalization of late with the inception of Automated Fingerprint Information System in an attempt to facilitate speed, efficiency and convenience. However, the automation has been hampered by numerous setbacks, as evident in some recent high profile cases. This article seeks to delve into the nuances of use of digital methods in evidentiary analysis of fingerprints and suggest an effective way forward, which suits the interests of all parties concerned.

Keywords: Fingerprint, identification, image, latent, IAFIS, AFIS, FBI, Daubert, Mitchell, Mayfield

Introduction

Fingerprint identification is primarily based on viewing all the ridges within a fingerprint and then classifying them into loops, arches, and whorls. Each of these can be further divided into sub-patterns. The final step involves finding and mapping the location of shapes and contours. Matching fingerprints imply that the pattern, sub-pattern, and at least some of the shapes and contours roughly correspond with each other. The American fingerprint system has developed over the years through nationalization, computerization, and digitization. Initially, the law enforcement used inked fingerprint cards. Eventually, the databases became so large that manual searches became next to impossible. In Automated Fingerprint Information System (AFIS) technology, the files are generally split into computerized criminal files and manually maintained civil files. Within the last 10 years, new shapes and contours have been incorporated into the identification process including sweat pores, ridge width, shape, path deviation, and their governance. (Cherry, 2007). In less than 15 minutes AFIS can sift through computerized images of fingerprints and prepare a list of possible matches. (Schwinghammer, 2005).

The FBI's Integrated Automated Fingerprint Information System (IAFIS) approximately 130, 000 employment background and criminal checks are completed by using IAFIS and its regional Automated Fingerprint Identification System (AFIS) counterparts. (Cherry, 2006).

However, in spite of the improved process efficiency, the question that needs to be answered here is whether speed and convenience compromised on accuracy? The digital methods are marked by several disadvantages. The

resolution of the computer images are severely compromised while scanning the photographic images to fit them into the screen. Errors may also creep in during the process of linking the prints to specific individuals and storing the prints in digital databases prone to hacking. Stored images are vulnerable to manipulation. (Cherry & Meyer, 2004).

Judicial approach

In Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U. S. 579 (1993), the court held that the prosecution needs to establish the foundation for the formula used to enhance and transform fingerprint images. The Court noted that Rule 702 of Federal Rules of Evidence retained mandatory " gatekeeping" requirement laid down in Frye v. United States, 293 F. 1013 (D. C. Cir. 1923). But the new standard was " reliability" rather than " general acceptance." The Court explained how the " reliability" of evidence might be demonstrated using (a) testing, (b) peer review and publication, (c) error rate and standards controlling technique, and (d) general acceptance. The government attempted to establish the efficacy of AFIS for the first time in United States v. Mitchell, 199 F. Supp. 2d 262, 263 (E. D. Pa. 2002).

In Mitchell, a study jointly conducted by Lockheed Martin and the FBI purported to demonstrate the uniqueness of fingerprint patterns. The study used AFIS and 50, 000 fingerprints of the same pattern type, comparing each print with itself and with the other 49, 999. The AFIS generated a " similarity score" for each comparison. The study found that prints compared to themselves always generated higher similarity scores than comparison with

other prints. The probability of existence of two identical complete fingerprints was 1 in 1097. (Cole, 2004).

Efficacy of AFIS – Glaring Instances

The automated system, however, has serious flaws. Thomas Bush III, the Assistant Director of Criminal Justice Information Services at the FBI, conceded that the system had missed a fingerprint attribution for Jeremy B. Jones, a serial killer, on three occasions. The IAFIS computer system failed to match the images in the database to the new images produced each time Jones was re-arrested. IAFIS takes shortcuts to save time. For example, IAFIS analyzes only the index fingers. If the prescreening yields a very low score, a non-match decision is made without analyzing the images of the other fingers. The system therefore fails to identify the source of the fingerprint patterns that produced the latent image. (Cherry, 2006).

The flaws came to the fore in a series of high profile cases, including that of Brandon Mayfield. Mayfield had been arrested for leaving fingerprints in the Madrid bombing case. Partial latent fingerprints were found on plastic bags containing detonator caps. Digital images were provided to FBI for scrutiny. The FBI fed the data intoit Integrated Automated Fingerprint Identification System (IAFIS) for review. (Cherry & Meyer, 2004). The FBI ran the print through its computers and came up with fifteen possible matches. (Schwinghammer, 2005). The FBI asserted that the bombing print was a match for the print of one of those fifteen. However, a later review revealed that the identification was flawed on grounds of the image being below par in terms of quality. (Cherry & Meyer, 2004).

Roger Benson and Miguel Espinoza also found themselves on the receiving end of similar misfortune. Benson was imprisonedfor 43 days. He had beenassigned a print numberwhich was also linked to William Lee Kellogg, a felon with criminal history. Espinoza, who ran a restaurant in Medford, Oregon, found his number assigned to a murderer. Espinoza was wrongly identifiedas a murderer during an administrativedue diligence. The town council accordingly proceeded to revoke his license. (Cherry & Meyer, 2004).

Critical observations

The grave miscarriage of justice inflicted on these unfortunate victims stands well documented. The attorney should file a discovery motion requesting the disclosure of the original image and all computer-derived images. After obtaining all the images, the attorney can have them reviewed by an imaging expert to identify any problems such as equipment distortions, electronic enhancements and color. (Cherry & Meyer, 2004).

The main reason behind the requirement of such a detailed scrutiny is the possibility of errors at every major step in forensic analysis, including scanning, clean-up, indexing etc. Scanners have been found inadequate in providing perfect representation of the fingerprint images. The operator may delete certain pixels. If there is a later enhancement it amounts to two alterations compromising on the quality of evidence. As seen in a number of cases, prints may get wrongly attributed to innocent individuals. Most computer hard drives, serving as databases for fingerprint images, are vulnerable to hacking, making them to prone to easy manipulation in the hands of computer invaders. The fingerprint images may inadvertently get

distorted while obtaining print outs from devices which operate on the “ best-fit” principle.(Cherry, 2006).

Conclusion - The way forward

In light of all these issues, the subject clearly merits a detailed critical study by a qualified neutral third party. Fingerprint identification witnesses testify that their work has an error rate of zero. The judiciary has tended to rely on these assertions to form its opinions. However, our experiences suggest that such credence is far from deserved and needs to be earned to withstand tests of admissibility. (Schwinghammer, 2005). Also, the current situation demands framing of distinct professional standards to get rid of existing ambiguities. (Cherry & Meyer, 2004).

However, in spite of all the above shortcomings, there appears to be some light at the end of the tunnel. There are some promising signs that the administration and courts are showing a more critical attitude towards digital methods. Under the current US-Visit system, two exemplar fingerprints as well as a photograph to verify the identity are being used. In close cases, human examiners are checking the identification. The agency may further upgrade its system in future to require a match of all 10 prints.(Cherry, 2006). This also falls in line with Henry Fauld’s suggestion over a century ago. (Schwinghammer, 2005). Fauld wanted the law enforcement not to rely on one-print matches, as they do not sufficiently corroborate the link to the correct person. He also wanted specialized experts to undertake fingerprint examinations instead of police officers who can be potentially biased in their analysis. For all our apprehensions regarding outdated theories, this classical

piece of thought may just turn out to be the difference between an innocent capture and a rightful arrest of the guilty. There appears to be a definite promise in the road ahead.

References

Cherry, M. (2007). HOW WE CAN IMPROVE THE RELIABILITY OF FINGERPRINT IDENTIFICATION. Champion, 36, 38& 52.

Schwinghammer, K. (2005). FINGERPRINT IDENTIFICATION: HOW " THE GOLD STANDARD OF EVIDENCE" COULD BE WORTH ITS WEIGHT. American Journal of Criminal Law, 265, 280, 281 &282.

Cherry, M. (2006). A CAUTIONARY NOTE ABOUT FINGERPRINT ANALYSIS AND RELIANCE ON DIGITAL TECHNOLOGY. Champion, 27, 29, 30 & 33.

Cherry, M, & Meyer, L. (2004). DOES THE USE OF DIGITAL TECHNIQUES BY LAW ENFORCEMENT AUTHORITIES CREATE A RISK OF MISCARRIAGES OF JUSTICE?. Champion, 24, 26, 27-28& 29.

Cole, S. A. (2004). GRANDFATHERING EVIDENCE: FINGERPRINT ADMISSIBILITY RULINGS FROM JENNINGS TO LLERA PLAZA AND BACK AGAIN. American Criminal Law Review, 1189, 1215 & 1218-1219.