available at www.sciencedirect.com

SCIENCE DIRECT®

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

Digital Investigation

Paradigm shift in document related frauds: Characteristics identification for development of a non-destructive automated system for printed documents

Gaurav Gupta[a,*], *Chandan Mazumdar*[a,1], *M.S. Rao*[b,2], *R.B. Bhosale*[c,3]

[a]*Department of Computer Science and Engineering, Centre for Distributed Computing, Jadavpur University, Kolkata 700032, India*

[b]*Directorate of Forensic Science, Ministry of Home Affairs, Govt. of India, Block No. 9, 8th Floor, C.G.O. Complex, New Delhi 110003, India*

[c]*Government Examiner of Questioned Documents, Directorate of Forensic Science, Ministry of Home Affairs, Govt. of India, Ramanthapur, Hyderabad 500003, India*

ARTICLE INFO

Article history:
Received 12 February 2005
Revised 27 January 2006
Accepted 30 January 2006

Keywords:
Scanned and printed document
Conventional Document Fraud (CDF)
Digitized Document Fraud (DDF)
Fraud and forgery
Digital forensics
Digital forensic in Conventional Document Frauds

ABSTRACT

In today's advanced and highly changing technological environment, the question of authorship of a document often transcends to the more traditional means of inscription. It now needs to be looked into from the perspective of involvement of complex digital technologies comprising Computer Systems, Software Programs, Scanners and Printers. The impact and threat of Digitized Document Frauds like counterfeiting of currency, stamps, judicial papers, educational certificates, degrees, cheques, will, property papers, licenses, security passes, badges, immigration and visa documents including the fraudulent generation of, or alteration in, commonly used documents on the economy and society are inevitable and growing; hence our *Forensic Readiness* is crucial. This work identifies the peculiar characteristics for the development of a non-destructive automated system for efficiently detecting and fixing the origin of the questioned documents by linking them to the scanner and printer used. This in turn may help establish the authorship of the questioned documents. This work is the first general experimental study for investigating Digitized Document Frauds in a forensically sound manner in the light of Locard's principle of information exchange, individuality principle, cause–effect principle and the principle of comparison.

* *Corresponding author*. Tel.: +91 33 24146209, +91 9830560678 (mobile); fax: +91 33 24146209.
E-mail addresses: gaurav1980@gmail.com, http://www.cdcju.org.in (G. Gupta), chandanm@vsnl.com (C. Mazumdar), msrnd@rediffmail.com (M. S. Rao)
[1] Tel.: +91 33 24619846.
[2] Tel.: +91 11 24362676.
[3] Tel.: +91 9440486339.

1742-2876/$ – see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.diin.2006.01.009

1. Introduction

''One can not come into contact with an environment without changing it in some way.''

–Exchange Principle, now called Contact Traces, first articulated by Edmond Locard in 1910.

This is still an age of hardcopy documents, and a paper-less world is still a distant dream. We depend on these printed documents in many of our encounters with the complexities of modern life. Hardly a day goes by without some document playing a crucial part in the life of every one of us. Therefore, it is of no surprise that criminals expend significant effort and resources to create fraudulent documents.

Document manipulation and tampering have seen a paradigm shift in the form of Digitized Document Frauds (DDF). Digitized Document Fraud is defined as the process of scanning any conventional document, editing the scanned image to get the desired changes using image processing software and finally printing the document using printer. Examples of DDF include generating fake currency, stamp papers, and other documents like educational certificates, degrees, cheques, will, property papers, licenses, immigration and visa documents, security passes and badges. One of the famous and recent frauds is the billion dollar fake stamp paper scandal, which rocked India in 2004; this highlights the burning problem of misuse of digital technology in Conventional Document Frauds. The other famous cases include generation of fake postal stamps, which are generally used only once, thus costing heavily to the exchequer, fake transcripts and experience certificate generation for availing of over privileges in educational and private institutes to name a few.

The use of sophisticated computerized systems capable of producing high quality hardcopies makes the job of criminals much easier and safer than the conventional ways of tracing, imitating and tampering of documents due to the former being extremely difficult to detect using conventional mechanisms, as the output is almost the same as the real document. Because the fraudulently generated documents are so realistic, there are less chances of the forger being caught, making Digital Document Fraud a low-risk high-gain venture.

The objective of this study is to detect and attribute the document to the machine and tool used for its generation. Until now there were no well-defined procedures and guidelines to forensically link the crime to the perpetrator in Digitized Document Fraud cases. Our work is based on the following principles (Chisum and Turvey, 2000; Chisum, 1999; DeForest et al., 1983; Saferstein, 1998; Inman and Rudin, 2001):

1. Locard's Exchange Principle of Evidence, which states ''One can not come into contact with an environment without changing it in some way''.
2. Individuality principle, which states that no two objects are identical. It is often the case that two objects cannot be told apart, but they are not identical. If the two objects are distinguishable, it is obvious that they are not from the same source. However, if they are indistinguishable, they need to be examined in more detail to determine whether they are from the same source.
3. Every effect has a cause. The cause must precede the effect.
4. Principle of comparison is based on the theory of comparison of questioned information with the genuine (original) one and with suspects (if available) using existing tools and technology. It states that we can almost always detect and fix the culprit if enough of all genuine, questioned and suspected material is available; also the innocence can be proved, in case of false implications.

In the light of above-mentioned principles this study tries to identify the characteristics unique to a scanner/printer. This analysis of characteristics will lead to linking of crime to the criminal. The identified peculiar characteristics can serve as investigatory leads to determine the origin of a document and thus help ascertain the authorship of the documents under question.

This paper explores the role that scanners/printers play in the generation of fraudulent documents. The identified characteristics are specific to printers and scanners and differ considerably even within the same make and same model number. These characteristics are universal and may help in addressing the following issues about the document in question:

1. Is the document in question genuine or fake?
2. Which type of scanner/printer has been used to generate a fraudulent document?
3. Providing clues to locate the suspected scanners and printers.

This forms the basis for the development of a non-destructive automated system for efficiently detecting and fixing the origin and thus authorship of questioned documents. Our findings are effective even in the scenario where an intelligent criminal destroys digital evidence from the storage media of computer system and only the fake document is available to establish and link the crime to the criminal. Provided the proposed methodology can be generalized, its efficiency and reliability of results could help digital investigators combat this growing threat to economy and society.

2. Previous work

Detection of tampering in digital images could be useful when the remnant-scanned image is available in storage system. The Popescu (2004), Luxen and Forstener (2002), Fridrich et al. (2005), Farid (2002), Popescu and Farid (in press-a), Fridrich (2005), Farid and Lyu (2003), Popescu (2005), Popescu and Farid (in press-b) could provide vital information regarding the malicious editing in the scanned image. These could help in pinpointing the details of the changes in the fraudulently generated document. But intelligent criminals can destroy information from the Computer Systems.