COMPUTATIONAL INTELLIGENCE IN IDENTIFYING COUNTERFEIT DOCUMENTS

[1]L. AMUDHA, [2]T. M. NITHYA,[3]J. RAMYA
[1]Assistant Professor, [2]Assistant Professor, [3]Assistant Professor,
[1]Department of Computer Science and Engineering,
[1] K.Ramakrishnan College of Engineering, Tiruchirappalli, Tamil Nadu, India

Abstract - Digital Forensics is a branch of forensic science that encompases the recovery and investigation of details found in digital devices. Digital Evidence is information found among a variety of electronic devices like CD, pen drive, hard disk or even mobile phones that is useful in legal systems. The use of digital evidences in criminal and civil investigations is taking a major role in recent years. These evidences are equivalent to fingerprints, DNA pattern or iris pattern that is unique for any person. There is still some limitation, where the digital evidence may be misleading. Anyhow, at the end it is the court to decide whether the digital forensic evidence of that investigation is reliable or not. Also with the increasing prevalence of mobile phones, forensic evidences collected from mobile devices are becoming an invaluable source of evidence. This paper shows digital forensics in a different perspective, and analyses the existing methods of digital forensics. The results are checked with all the existing methods and appropriate matching for specific type of forensic evidence like PAN number, Voter ID, AAthar card, etc.with a forensic method.

IndexTerms-Digital forensics, doctoring, investigation, evidence, fraudulent, automated tools.

I. INTRODUCTION ABOUT DIGITAL FORENSICS

There are many variations of digital forensics like Computer Forensics, Mobile Device Forensics, Network Forensics, Database Forensics, Multimedia Forensics, and Cloud Forensics. Nowadays there are many criminal activities related to duplicating documents. Digital or counterfeit documents have increased and not enough tools are available for identifying such documents. Fig 1 shows that confidential information may be inside a computer system or documents shared across the network. Following sections has a discussion about the methods to identify such documents.

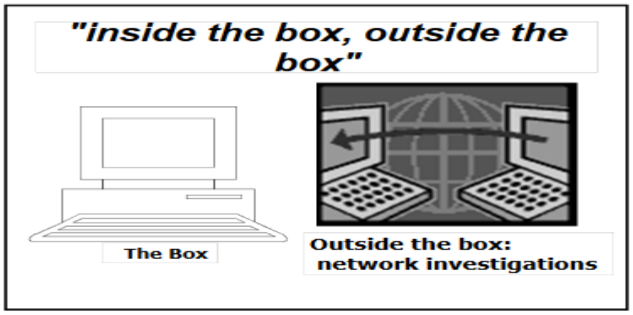
"inside the box, outside the box"
The Box
Outside the box: network investigations

Fig.1 Two major types of secured data

II. ROLE OF MOBILE PHONES IN DIGITAL CRIME

With the wide spread usage of mobile phones, the vulnerability of the information in the device also has rapidly increased. The smartphone users, nowadays does all their private transactions through these handheld devices[3]. The level of security available for these personal and highly secure information is a great challenge in recent days. The possibilities of threat includes theft of personal information, copyright misuse, improper usage of IP addresses, money laundering and many others.

Today corruption and crimes are prevalent in the country at all places. Most of the criminals use documents particularly digital documents that can be easily generated or modified. Digitized document frauds are therefore increasing widely. The following table depicts the types of forensics cases and problem domains where scope of fraudulent activity is more dominating. Computer Forensics Are Used In The Following Investigations

Table 1 List of forensics

Hacking	Obscene Publication
Paedophiliac Rings	Defamation
Immigration Fraud	Narcotics Trafficking
Credit Card Cloning	Software Piracy
Electoral Law	Forgery
Perjury	Sexual Harassment
Murder	Divorce
Data Theft	Fraud

There are 5 reasons why documents are used in criminal investigations and forensics as a strong evidence. Digital forensics documents have the following features.

1. They are ACCURATE
2. They are QUICK
3. Avoids NON-COMPLIANCE
4. Maintains CONSISTENCY
5. Long-term AFFORDABILITY

III. COUNTERFEIT DOCUMENTS

The need for computationally intelligent digital forensic tool has increased a lot in the recent years, since there are many criminal cases related to duplicating IDs, Driving Licenses, Passports, Digital Signatures, ATM cards and even Academic Certificates that are created with very little effort(refer Fig 3). Authenticity of digital documents in legal issues is being a great challenge in recent times.

The following table (Table 2) indicates the sources of evidences that can be used at the offenders side.

Table 2 Sources of Evidence in Offender's computer

1	–	Accessed And Downloaded Images
2	–	Documents
3	–	Chat Sessions
4	–	User Log Files

3	–	Internet Connection Logs
4	–	Browser History And Cache Files
5	–	Email And Chat Logs
6	–	Passwords & Encryption Key

Digital photographs were not acceptable as evidence simply because of the fact, which might have been doctored. These doctoring might not be detectable in naked eye. It is comparatively simple to do changes in a scanned document with the large range of available software and a little knowledge of how to use the features in the software.

To detect such doctored images we might need sophisticated software tools that are able to look at the images as a whole and identify any possible changes in the overall image. A number of tools are nowadays available to identify the fake digital document that makes the cybercrime work a little easier. Fig 2. shows the traditional method and automated method of identifying doctored images in the forensic document

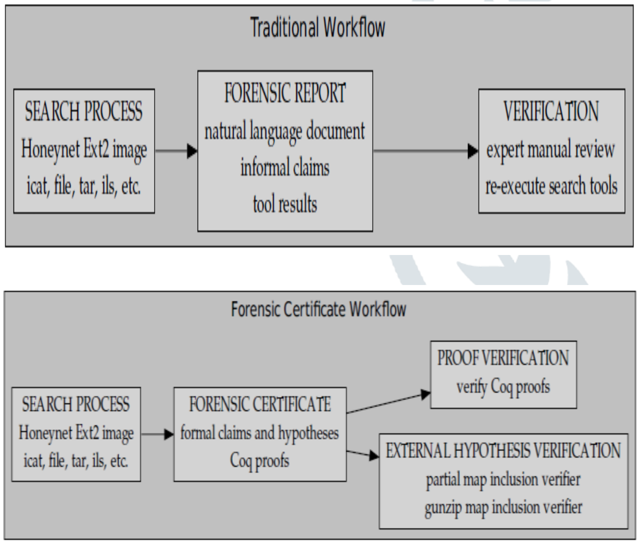

Fig 2. Traditional and automated method for identifying image doctoring

Fig. 3 Image of a forensic evidence

Many Graphic design applications aid in this case. Any how these applications leave some traces of clues to identify the fraudulent documents. More advanced digital forensic tools are required to identify such counterfeit documents with higher degree of accuracy.

Investigators must be able to identify a counterfeit document that leads to serious crime by acquiring an accurate understanding of how these documents are generated. What type of software is used? To help the investigation process, software tools could be used that generates identifies the tools and techniques along with the date of creation of the documents.

Recently there is a lot of improvement in Digital Image Forgery Detection, Analysis of Electronic Signatures, Digital Droplets, Cloud Computing, Digital Forensic Tools, and Forensic Document Examination. Still there is huge scope for research analyst to develop more standard and accurate software to identify the history of such forged documents.

IV. EXISTING METHODS TO IDENTIFY COUNTERFEIT DOCUMENTS

To ensure that documents are genuine and to identify a rightful owner, a document verification system would be the most accurate tool. Document verification systems may be office-based or remotely accessed. They will enable a wider and more consistent scrutiny of documents than manual verification process.

Software/Hardware tools that are available for counterfeit detection and verification checks thoroughly from simple to extremely complex features. Choosing the right tool depends upon the circumstances at any point of transaction. Based on the type of devices available, the method of image doctoring is categorized as Visible Verification, Micro printing, InfraRed, Magnetic, UltraViolet.

The major point of concern is to decide whether or not a “human decision” is mandatory to make an authentication. The first category, Visible Verification, requires a person to determine authentication. All other categories are machines with logical programming that identifies the genuineness of the document.

V. FORENSIC CERTIFICATE MODEL

There are severe consequences for errors in digital forensics. The model presented here (Fig 4) proposes a method for more accurate counterfeit and real document identification.

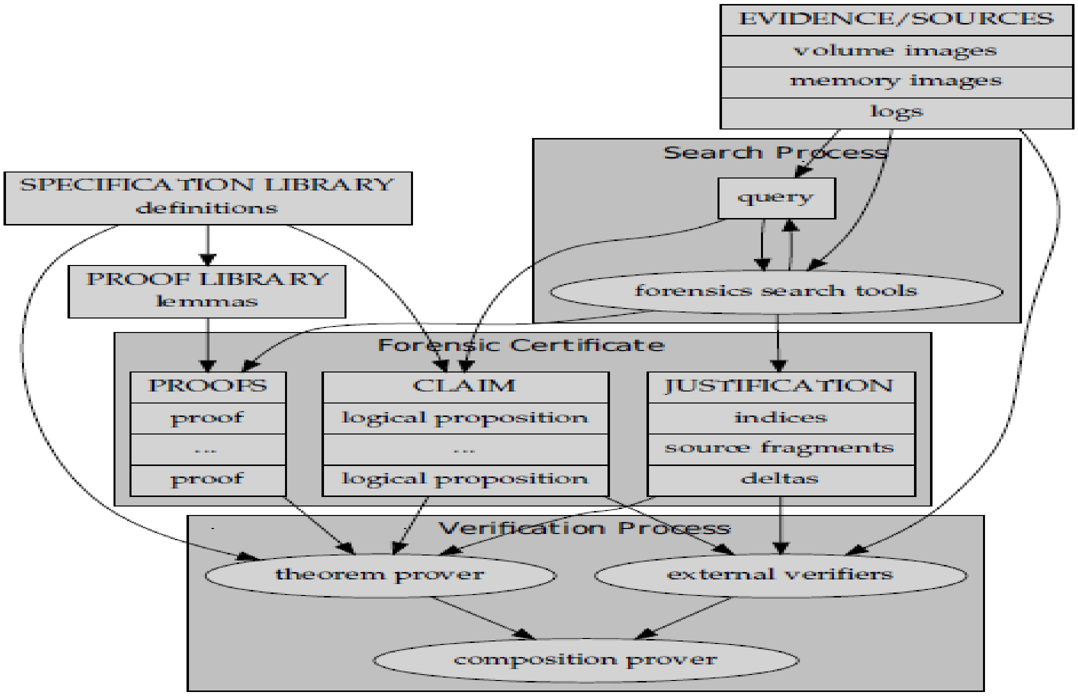

Fig.4 Fake document Identification

Any digital document that is suspected to be a counterfeit document undergoes a series of steps to identify whether any graphical changes are made to it. Results obtained are compared with the internal logs about the original person and if any deviation occurs, then the software concludes that counterfeit measures are applied to the document.

VI. CONCLUSION

Automated software tools can be integrated as part of the verification or scanning hardware to identify the duplicated document thereby ensuring correctness at all stages of verification. System generated digital forensic evidence is effective in addressing cases where counterfeit document editing is more likely related to graphical applications like CorelDraw and vector graphics.

REFERENCES

[1] User-generated digital forensic evidence in graphic design applications, Mabuto, E.K. ; Dept. of Comput. Sci., Univ. of Pretoria, Pretoria, South Africa; Venter, H.S.IEEE,Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on 26-28 June 2012,PP 195 – 200, 978-1-4673-1425-1.

[2] System-generated digital forensic evidence in graphic design applications,Enos Mabuto and Hein Venter, University of Pretoria, South Africa, Journal of Digital Forensics,2013, Security and Law, Vol.8(3),pp 71-86

[3] A Cloud-Focused Mobile Forensics Methodology, IEEE Journals & Magazines, IEEE CLOUD COMPUTING, Quang Do; Ben Martini; Kim-Kwang Raymond Choo,IEEE Cloud Computing,Year: 2015, Volume: 2, Issue: 4, Pages: 60 - 65

[4] Certificates for Verifiable Forensics Radha Jagadeesan, CM Lubinski, Corin Pitcher, James Riely, and Charles Winebrinner

[5] Evaluating Digital Forensic Tools (DFTs) Flavien Flandrin, Prof William J. Buchanan, Richard Macfarlane, Bruce Ramsay, Adrian Smales DePaul University, 2014 IEEE 27th Computer Security Foundations Symposium

[6] B. Carrier, “Digital forensics tool testing images.” SourceForge, 2010. [Retrieved 28 April 2012].

[7] W. Buchanan, “Advanced security and network forensics,” 2011.

[8] Y. Guo, J. Slay, and J. Beckett, “Validation and verification of computer forensic software tools - searching function,” Journal of Digital Investigation, vol. 6, pp. 12–22, 2009.

[9] D. V. Forte, "The responsibilities of an incident responder," Network Security, vol. 2010, pp. 18-19, 2010.

[10] C. M. S. Steel and C.-T.Lu, "Impersonator identification through dynamic fingerprinting," Digital Investigation, vol. 5, pp. 60-70, 2008.