A Survey in Modern Techniques in Digital Forensic Evidence in Graphics Design Applications

Muna E. M. Ahmed Elsheik
Princess Noura University, College of computer Science and Information, Information System Department, KSA

Memaahmed@gmail.com

Abstract. Digital forensics syndicates computer science theories, including computer architecture, applications, operating systems, file systems, software engineering, and computer networking as well as legal procedures that describe criminal and civil litigation, cyberlaw, and rules of evidence.

This paper explores the modern techniques innovated in gathering digital forensic evidence from certain design application that proof counterfeit image or document was formed. The extrapolation is created by linking digital forensic information gathered with the imaginable deeds established such as scanning, printing, editing, saving, importing, exporting the fake documents or images. The file generated by the particular graphic application is analyzed to accumulate the digital forensic information that concludes if the system is used for designing counterfeit document or image.

Keywords: Graphic design applications Digital evidence, Digital forensic

1. INTRODUCTION

Computer graphics application can be used to forged documents and images such as fingerprint image, palmprint image, IDs document, passports, certificates licenses .etc. conversely, the use of any graphics design applications creates behind traces of digital evidence that can used during a digital forensic exploration. The modern digital tools investigate a system to find digital evidence but do not investigate a system dedicated for creating forged image and documents created through the use of graphic application. A digital forensic investigation generally consists of four phases: acquisition, examination, analysis and reporting U.S. National Institute of Justice (2001). Assuming that an individual is suspected of creating counterfeit documents, the regular process of acquisition is tracked. The phases of acquisition and reporting are generally similar in diverse cases; hence the prominence is on the examination and analysis phases.

This paper recognizes the modern techniques for digital traces left over when certain graphic design applications had been used. The tracing process achieved by correlating the probable activities taken during document creation with the traces left behind. The foundation of potential evidence referred to above equates to the results of possible actions (i.e., document scanning, editing, saving and printing) taken during document creation. Most of this evidence would originate from the application log files, denoted to as system-generated evidence.

The rest of the paper is organized as follows: Section two introduce overview on digital forensics and digital forensics evidence, section three define the image and video forensic analysis. In section three graphic design applications and document counterfeit. While Section four is an evaluation and discussion of the evidence extracted from the graphic design applications. Finally Section five serves as conclusion to this paper.

2. OVERVIEW

Digital forensics was defined as the use of systematically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate illegal actions shown to be disruptive to planned operations DFRWS. (2001). .The term digital forensics cover all application from database management system to computer network to mobile and computerized and portable devices Cohan, F. (2010). This is followed by developing new techniques and tools for digital forensic which cover different field database, multimedia, malware, network, communication forensic U.S. National Institute of Justice (2001). Meanwhile, digital evidence is defined as any hardware, software or any data that can be used to prove one or more of the “who, what, when, where, why and how” of a security incident. Digital evidence consists entirely of sequences of binary values called bits F. Cohan,(2010,). Traces left behind from the use of an application or operating systems are referred to as digital forensic artifacts. Application artifacts left by installed applications can be an excellent source of potential evidence when performing an analysis. An artifact, however, does not become evidence unless its ability to prove a fact has been established Altheide, C., & Carvey, H. (2011) Zelkowitz, (2009). but in this area of research focusing in graphic design application is infrequent. which is a particular area that is nearly always exploited for the purpose of creating counterfeit documents and images. Most research work that has been undertaken up till now has concentrated on image forensics, which is the kind of investigation that is able to determine whether or not an image as been forged or tempered. Researcher in Lien, C. C. (2010). proposed a method that uses a pre-calculated resampling weighting table to detect periodic properties in error distribution within an image. The errors in the distribution within an image are used to determine if the image has been forged. a method to detect contrast enhancement and addition of noise in jpeg compression images is proposed in Cohan, F. (2010). Changes in contrast and noise within an image are determined through the use of an algorithm that calculates pixel values within the image. The values are then used to detect forgery within the image. In T.j Gardern, (2007), researcher introduced a method that determines characteristics associated within digital still camera images to determine the origin of the image. The characteristics are compared to the exact replicas and derivate of other statistical images to detect forgery. These, and other related work focus on determining forgery using statistical data within the image. Very little of the research carried out to date has specifically investigated the ways and means in which documents are counterfeited. These ways also include the methods and procedures that can be used to detect such activities from graphic design applications, which is the focus of this paper. How and where evidence is located differs, depending on the crime being investigated, the platform (operating systems) and the application used to commit the crime.

All digital evidence belong can be categorized by three types of evidence first category, exculpatory evidence refer to evidence prove or demonstrate to the someone is not guilty or of alleged crime. The second category, inculpatory evidence is the evidence supports particular allegation theory or hypotheses the last category is the evidence of tampering which is the evidence reveal that the system was tampered adjusted with the purpose of avoiding consequent tracing and identification T.j Gardern, T.M Anderson(2007)..

In the Farhood N.D (2013) the author discuss Digital Forensic Trends and Future where the study has two phases. First phase the data collection process started with keyword analysis in order to identify the focus of each article studied. Second phases Topics Covered in the Journals as in figure 1. The collected keywords were then grouped into broad category topics based on their representation to accommodate most of the topics identified in recent digital forensics such as forensic, forensics tool, file forensic image forensics video forensics analysis and etc. in this study we focus in image and video analysis meanly in graphical applications.

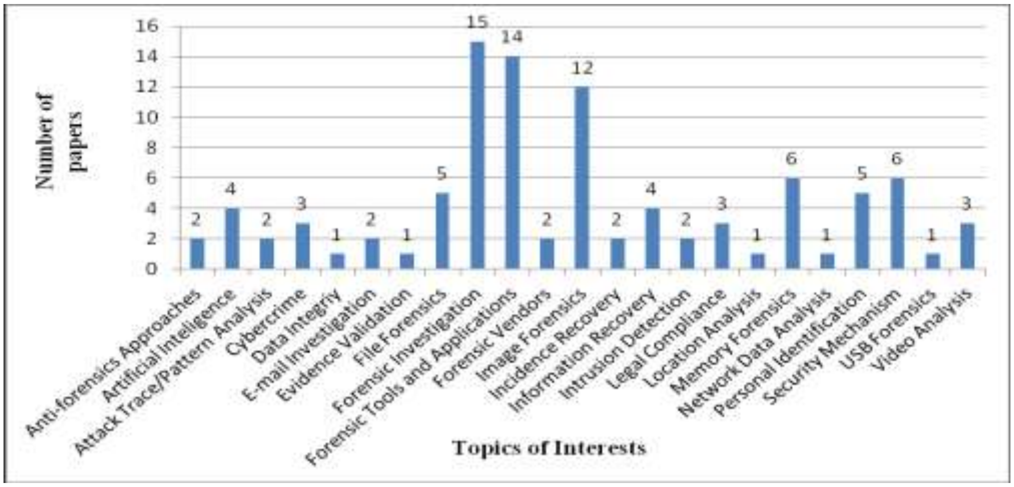

Fig 1: Interested Topics in Forensics **Farhood N.D (2013)**

3. Image and Video Forensic Analysis

Authors are strongly encouraged to follow the principles of sound technical writing, as found in Ref. 1, for example. In addition, good English usage is essential. Authors whose native language is not English may wish to collaborate with a colleague whose English skills are more advanced. A spell checker can be helpful to discover misspelled words, but authors should also proofread their papers carefully prior to submission. Manuscripts that do not meet acceptable English standards or lack clarity may be rejected.

3.1 Image Forensic Analysis

image forensic used Image scrutiny to expose the information using the image support machine with decision fusion techniques M.-J. Tsai, C (2012) The researcher recommends a model that identifies the foundation model or device of an image by using the support vector machine approach along with decision fusion procedures. Where the feature selection algorithms considered as features in optimal subsets are generated in a series of inclusion and exclusion steps and count based aggregation as the algorithm of decision fusion. The trained model is built where test images is fed into the trained model to predict the camera source model.
As the imaging scrutiny being enhanced, J. Santamaría (2011), contributes reviewing the state-of-the-art image cataloging methods that lays the basics on evolutionary computation and analyzes the 3D modelling of forensic objects. The paper includes different evolutionary approaches in order to signify the wide variety of techniques within the EC. Other author in] A. Rocha (2010) presents image meta-description approach suitable for diverse image inference presentations named as progressive randomization (PR). This method is based on

agitations on the values of the Least Significant Bits of images that makes it different from the state-of-the-art algorithms.

With the extremely innovative application, the forensic tool is intelligent to differentiate between the forged and actual image. In W. Lu, W. Sunn,(2011),"demonstrate that By using multi resolution decomposition and higher order local autocorrelations *(HLACs*) image features are extracted and determine if it is actual or forged . The researcher suggests Two dimensional discrete wavelet transformation (2D-DWT), a powerful multi resolution analysis tool. The signal characteristics in detail can be localized in different position, orientation and scale and multi resolution decomposition contains many intrinsic characteristics of natural images and fake images. They are used and as by right of the inner product lemma of higher order autocorrelation, the feature extraction and SVM are joined and the computation complexity is decreased significantly. In image analysis, the image can be detected and located the replica regions with rotation, using an effectual and strong passive authentication techniques G. Liu, J. Wang, (2011).It uses circle wedge and the Hu moments for detection and position. In this technique Gaussian pyramid is used for putrefaction and to overwhelmed the possible distortion caused by JPEG compression and noise contamination, produced sub-image in low frequency is chosen. The sub-image is divided into many circle wedges overlapping each other and from them the features of Hu moments are extracted. Here, the circle-wedge mode and the Hu moments are able to eliminate the effect of rotation.

As Noise degradation causes failure to blind fake detection approaches, in M. Taylor, (2011) the author suggests a model that divides a suspected image into different partitions with consistent noise levels. However, the authentic images also can contain various isolated regions with very different variations, which make the proposed method a supplement to other forgery detection methods rather than a standalone forgery detector. The proposed method is not able to find the corrupted regions, when the noise degradation is very small ($\sigma < 2$). In Z. He, W. Sun, (2011), author proposes to apply an approximate run length based scheme in order to use image splicing the common form of image tampering. Proposed pattern only computes run lengths on the edge pixels and what makes it better is that splicing normally introduces extra edges to the image. This technique introduces to a threshold t. If the absolute value of the difference of two neighboring pixels' grayscale value is not greater than the threshold t, the two pixels are considered as they are in an approximate run. This technique needs further research on the fluctuation of grayscale values of consecutive pixels that tends to be more dramatic in an image with complex texture. Hence makes the authentic images and the spliced one less distinguishable.

The exposure to a new extraction algorithm as proposed by the author in W. Li, Y. Yuan (2009) is talented to excerpt the block artifacts grids (BAG) and then anomalous BAGs due to interpolate or concealing objects can be detected with a marking procedure by copy–paste operations. The author suggests that with extracting weak horizontal and vertical edges with periodicity of 8 separately and then combining them the BAGs are found. In J. S. Okolica (2011), the paper includes all the existing surveys and references that directly deal with blind image forensics. the paper suggests that in order to detect image forgery, it does not require any other prior information about the image, for detecting image forgery. Nevertheless**,** this method only implies that leaving the "ideal" lab conditions and applying the existing methods to real-life applications, higher rate of false positives are considered than reported. Lack of automation is another drawback of existing methods. To localize the forgery, existing methods need to have knowledge of various modification regions containing some inconsistencies. Many of the existing methods deals only with JPEG and compression properties.

The image of computer produced and real image can be distinguished based on human visual system. In H. Farid ,(2012), it defines a series of psychophysical experiments that used images of changeable resolution, JPEG compression, and color to explore the capability of observers. From the experiments directed, it reveals that the image is in fact photographic when an observer believes it to be photographic that can be expressed as the following conditional probability,

$$P\ (I = \text{photo} \mid R = \text{photo}) \qquad (1)$$

where R denotes the user response and I the image category.
By replacing “photo” with “CG”, the conditional probability that an image is CG if an observer says it is CG,

$$P\ (I = CG \mid R = CG) \qquad (2)$$

However, the precisions stated in the paper are a junior bound on human performance, unlike time rendering technologies; observer performance can likely be improved. To classify the source camera-model of a digital image, F. Daryabar (2012) utilizes traces of demos icing operation in digital cameras and using two approaches and defining a set of image characteristics which are used as features in scheming classifiers that differentiate between digital camera models. the paper identifies demos icing artifacts associated with different camera-models. Two methods namely Expectation–Maximization algorithm that analyzes the correlation of each pixel value to its neighbors and analysis of inter-pixel differences are used to detect and classify the traces of interpolation operation in images. It is expected that the use of combined method would eliminate some of the false-positives due to mismatch of the reference pattern.

3.2 Video Forensic Analysis

Digital forensic analysis uses many tools that can be applied, whether it is a software tool or hardware tool. Samsung providing the device like digital video recorder (DVR) to perform an analysis in imaging digital forensic W. S. van Dongen,(2008).The device designed with two disjointed hard disk to execute particular recording and testing. It is also for minimizing the error occurs during the video forensic investigation. This device is able to compress the video recorded in the form of MPEG-4 format and store in the video file. moreover; it is adept to transfer the video into a PC (Samsung 2005) in real-time connection. The investigation of video recorded can refer to the time and date stated on the image display. The primary and secondary hard disks are divided into three partitions. The first partition is “ect” whixh is used to store event and system log file. The second partition is “bin” directory which contains operating system executable files. The third partition is “root” directory that is used for bookkeeping files for example “. db” and “.eve” files. Therefore, the history of logged files will be recorded in hard disks accordingly. In addition, Closed Circuit Television (CCTV) also is an effective way in providing an image’s features for digital forensics investigation N. R. Poole, (2009). The video data will be extracted before it can gain access to manufacturer’s application software. The image will be stored on the CCTV disk as well as digital video recorder. However, the disk must not overload with data in order to provide the best result of the initial investigation. The papers stated in this theme contain the related issues with privacy regarding the structure of the hard disk. The information about the structure may be a copyrighted information which should be available on the manufacturer side only and not for other parties. The history in the log file may reveal user activity that may be private to the user and should be accessible by other person,
Few researches and investigation in fake and forged video has been done. next few year this will a rich area in video forensic analysis.

4. Graphical Application and Document Counterfeit

Many graphic design applications are currently available in the industry; however, Adobe Systems Incorporated is regarded as the largest software maker in the graphic design software category Adobe Systems Incorporated owns software technologies that are used for online transactions, business applications and social technologies Tech Specs (2011), this make researchers in the forensic evidence deliberate in using adobe applications to extract forged images information and analysis. Any one of the adobe applications such as adobe Illustrator, adobe Photoshop, and adobe acrobat can be used for document editing. Therefore it is necessary to conduct an exclusive examination for potential digital forensic evidence.

In Enos K. (2012), ” author were carried out various experiments in order to search for pertinent evidence in graphic design applications. Experiments were conducted on Adobe applications. The experiments were directed in two parts. The first part study digital forensic artifacts created in graphic design applications where the cause of the potential evidence is mainly system-generated with results mostly from registry analysis, application log file analysis and system pre fetch file analysis. The second part of the experiments, which includes inspection of user-generated files, highlights results from file content identification and inspection. the analysis for forensic artifacts was conducted on a Windows 7 platform graphic design applications can be used for creating counterfeit documents, firstly three techniques are used to gather digital forensic information related to graphic design applications. These techniques are the registry analysis, application log file analysis and system prefetch file analysis each disclose information that can be of digital forensic importance. All this digital information can be correlated to constitute the digital evidence related to graphic design applications. Moreover, it is possible for a digital forensic investigator to conduct an in-depth analysis of files generated from graphic design applications. For user generated file examination the investigator is able to verify the identity of a file type through content identification using file signatures. Also an investigator is able to know which metadata can be extracted from user generated files from graphic design applications. Enos M, Hein V(2014). Revisiting the problem “graphic design applications can be used to create fraudulent documents” and having acquired the necessary digital forensic artifacts, a digital forensic investigator is able to deduce activities associated with the creating of fraudulent documents.

5. Conclusion

In last decades the digital forensic evidence become interested area of research. Graphical applications can be used to develop forged images and videos at the same time can help to analyze and investigate the digital evidence. The paper cover the image and video analysis , overview in techniques used in digital evidence and graphical application used in digital evidence. The survey limited in using adobe application where a side from the five techniques, registry analysis, application log file analysis, system prefetch analysis, content identification (signature verification) and content examination (metadata extraction) were discussed above, more techniques can be tested for future work to gather digital forensic information related to the use of graphic design applications. Future work can be conducted by carrying out in detecting inserted images for example videos, fingerprints, bar codes in counterfeit and documents images this should be exercise on other graphic design applications..

References

U.S. National Institute of Justice (2001). Electronic Crime Scene Investigation Guide: A Guide for First Responders DFRWS. (2001). A roadmap for digital forensic research. Digital Forensic Research Workshop, p. 16.
Cohan, F. (2010). Towards a science of digital forensic investigation. IFIP Advances Digital Forensics VI, China, p. 17-35.
F. Cohan,(2010,) "Towards a science of digital forensic investigation", IFIP Advances Digital Forensics VI, China, pp. 17-35.
Altheide, C., & Carvey, H. (2011). Digital Forensics with Open Source Tools. Elsevier, MA USA p. 2.
Zelkowitz, M. V. (2009). Advances in Computers Information Security. Academic Press, Elsevier.
Lien, C. C. (2010). Fast forgery detection with the intrinsic resampling properties. *Journal of Information Security*, *1*(1), 11-22.
Stamm, M. C. (2009). Forensic detection of image tampering using intrinsic statistical fingerprints in histograms. *APSIPA Annual Summit and Conference*, Japan, 563-572.
T.j Gardern, T.M Anderson(2007), "Criminal Evidence principle and cases", CA,USA, Wardsworth,
pp37

Farhood N.D, Ali , Ramlan M, Nor F, Farid D, (2013)," Digital Forensic Trends and Future" International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(2): 48-76 The Society of Digital Information and Wireless Communications.

M.-J. Tsai, C.-S.Wang, J. Liu, and J.-S.Yin, (2012), "Using decision fusion of feature selection in digital forensics for camera source model identification," *Computer Standards & Interfaces*, vol. 34, pp. 292-304.
J. Santamaría, O. Cordón, and S. Damas(2011), "A comparative study of state-of-the-art evolutionary image registration methods for 3D modeling," *Computer Vision and Image Understanding*, vol. 115, pp. 1340-1354.
A. Rocha and S. Goldenstein,(2010) "Progressive randomization: Seeing the unseen," *Computer Vision and Image Understanding*, vol. 114, pp. 349-362.
W. Lu, W. Sun, F.-L.Chung, and H. Lu,(2011),"Revealing digital fakery using multiresolution decomposition and higher order statistics," *Engineering Applications of Artificial Intelligence*, vol. 24, pp. 666-672.
G. Liu, J. Wang, S. Lian, and Z. Wang, (2011), "A passive image authentication scheme for detecting region-duplication forgery with rotation," *Journal of Network and Computer Applications*, vol. 34, pp. 1557-1565
M. Taylor, J. Haggerty, D. Gresty, and T. Berry(2011), "Digital evidence from peer-to-peer networks," *Computer Law & Security Review*, vol. 27, pp. 647-652.
Z. He, W. Sun, W. Lu, and H. Lu, (2011), "Digital image splicing detection based on approximate run length," *Pattern Recognition Letters*, vol. 32, pp. 1591-1597.
W. Li, Y. Yuan, and N. Yu,(2009) "Passive detection of doctored JPEG image via block artifact grid extraction," *Signal Processing*, vol. 89, pp. 1821-1829.
J. S. Okolica and G. L. Peterson,(2011), "Windows driver memory analysis: A reverse engineering methodology," *Computers & Security*, vol. 30, pp. 770-779.
H. Farid and M. J. Bravo,(2012), "Perceptual discrimination of computer generated and photographic faces," *Digital Investigation*, vol. 8, pp. 226-235.

F. Daryabar, A. Dehghantanha, HG. Broujerdi, (2012),"Investigation of Malware Defence and Detection Techniques," International Journal of Digital Information and Wireless Communications**(**IJDIWC**),** volume 1, issue 3, pp. 645-650.

W. S. van Dongen,(2008), "Case study: Forensic analysis of a Samsung digital video recorder," *Digital Investigation*, vol. 5, pp. 19-28.

N. R. Poole, Q. Zhou, and P. Abatis,(2009), "Analysis of CCTV digital video recorder hard disk storage system," *Digital Investigation*, vol. 5, pp. 85-92.

Tech Specs, www.adobe.com, Accessed 22 June2011.

Enos K. Ma,Hein S. Venter (2012)" Analyzing Registry, Log Files, and Prefetch Files in Finding Digital Evidence in Graphic Design Applications", The ISC Int'l Journal of Information Security, Volume 4, Number 2 (pp. 137{150).

Enos M, Hein V(2014)," SYSTEM-GENERATED DIGITAL FORENSIC EVIDENCE IN GRAPHIC DESIGN APPLICATIONS" Journal of Digital Forensics, Security and Law, Vol. 8(3).