A GENERALIZE OVERVIEW ADAPTION OF DIGITAL FORENSICS PROCESS

[1]Prof. Parag R Wadnerkar, [2]Dr Ajay B Gadicha
[1]Head & Professor, Mechanical Engineering Department
P. R. Pote College of Engineering and Management, Amravati.
[2]Head & Associate Professor, Department of Artificial Intelligence and Data Science P. R. Pote College of Engineering and Management, Amravati.

Abstract:
Digital forensics is defined as the process of conserving definitive retrieving and chronicle computer evidence for adoption by a court. It is the science of finding evidence in digital media such as computers, mobile phones, servers or networks. It equips the investigative team with the best techniques and tools to solve complex digital cases. Digital Forensics assists the forensic team in analyzing, decisive definitive and averting digital evidence found on
different types of electronic devices. This chapter covers various aspects of digital forensics, its process, function and variables affecting crime scene analysisIn this chapter, we are also emphasizing the advantages and disadvantages of digital forensics.
Keywords: **Digital forensics, crime scene investigation.**

1. Introduction

Digital forensics (sometimes known asvirtual forensic technology) is a department of forensic technology encompassing the healing and research of material observed in virtualdevices, frequentlyaboutpc crime. The term virtual forensics becomeat the beginning used as a synonym for laptop forensics however has increased to coverthe investigation of all devicescapable of storing digitalinformation. With roots in theprivate computing revolution of the past due tothe 1970s and early 1980s, the fielddevelopedhaphazardlyat some stage in the 1990s, and it was not till the early twenty-first century that national regulations emerged. The technical component of researchis divided into numerous sub-branches, regarding the type ofdigitalgadgets involved; computer forensics, community forensics, forensic information evaluation, and mobile device forensics.

The regular forensic method encompasses the seizure, forensic imaging (acquisition) and analysis of digital media, and the manufacturing of a record into gathered proof. As nicely as figuring out direct evidence of a crime, virtual forensics can be used to attribute proof to unique suspects, verify alibis or statements, decidethe intent, perceivesourcesor authenticate documents.

Literature Review:

An efficient method for detection and localization of anomalies in videos is depicted in this paper. Using fully convolutional neural networks (FCNs) and temporal data, a pre-trained supervised FCN is transferred into an unsupervised FCN ensuring the detection of (global) anomalies in scenes. Experimental results on two benchmarks suggest that detection and localization of the proposed method outperforms existing methods in terms of accuracy and processing speed. Besides this, it is a solution for overcoming limitations in training samples used for learning a complete CNN. This method enables us to run a deep learning-based method at a speed of about 370 fps. Altogether, the proposed method is both fast and accurate for anomaly detection in video data [1, 4].

Sr. No.	Author	Year	Method used	Methodology used	Conclusion
01	Li et. al. [1]	2014	Convolutional Neural Networks	Tracking with deep track, CUDA-PTX	It employs a CNN architecture and a structural loss function that handles multiple input cues and class-specific tracking.
02	Hrishikesh Bhaumik,Siddhartha Bhattacharyyaa, Mausumi Das Natha, Susanta Chakraborty [24] (ELSEVIER)	2016		Hybrid soft computing techniques	The systems have increased in robustness, efficiency and effectiveness as compared to earlier used traditional approaches. It also helped to reduce user interaction and manual annotation to a great extent.
03	Shi-Zhe Chen, Chun-Chao Guo,Jian-Huang La [22]	2016	Traditional and CNN-based method	Deep cnn	Formulate the person re-identification task as a learning-to-rank problem. Extensive experimental results clearly demonstrate the effectiveness of our proposed approach
04	Antonio C. Nazare Jr., William Robson Schwartz [30] (ELSEVIER)	2016	Smart Surveillance Framework (SSF)	Framework 1 user modules 2 SSF kernel	Smart Surveillance Framework (SSF) allows the simultaneous execution of multiple user modules that can be developed independently since they have communication and synchronization through a shared memory, which contributes to the scalability and flexibility.
05	Shao et. al. [14] IEEE transaction	2016	Big Data	LDA, KNN, fuzzy clustering	By a combination of snapshot images, original surveillance videos and unusual events, valuable clues can be found out much easier, which thus helps the police boost their investigation efficiency.
06	Revathi and Kumar [5] SPRINGER	2016	Deep learning-based anomy detection (DLAD)	Background Estimation (BE) Module, an Object Segmentation (OS) Module, a Feature	Better error rate of 0.75% and precision of 85%

				Extraction (FE)Module, and an Activity Recognition (AR) Module	
07	Sabokroua et. al. [4]	2017	Deep learning - Fully Convolutional neural network (FCN)	AlexNet	Proposed method is both fast and accurate for anomaly detection in video.
08	Chang and Tay [2]	2017	Spatiotemporal architecture	ConvLSTM	Detects Abnormal events but it may produce more false alarms as compared to other evnts
09	Thanh Vu et. al. [3]	2017	Restricted Boltzmann machine (RBM)	ConvAE	RBMs are trained to capture different image statistics localized at different regions. This framework is readily generalized to a more powerful deep unsupervised abnormality detection framework.
10	Sinha et. al. [11] IEEE, International Conference on Intelligent Computing and Control (I2C2)	2017	Deep Learning	Convolutional Neural Networks(CNN), Restricted Boltzmann,Machines (RBM) and Autoencoders, Recurrent Neural Networks and Extreme Learning.	This paper summarizes and gives an idea to the new researchers to explore more in the vast yet young area of Deep learning.
11	Muhammad et. al. [12] IEEE Access	2018	CNN	GoogleNet	This paper improved the flame detection accuracy, but the number of false alarms is still high and more research is required.
12	Bajestani et. al.[7]	2018	Faster R-CNN	Object Detection	This method improves the true positive with the tradeoff of trivial false positive.
13	Manisha Kaushal a, Baljit S. Khehra b, Akashdeep Sharma [28] (ELSEVIER)	2018	Soft computing	Neural network Fuzzy Logic Neuro-fuzzy Hybrid	Various soft computing based approaches for moving object detection and tracking in videos. Article provides various techniques along which scope, pros, cons and the limitation associated with each of them
14	Huang et. al.[6] SCOPUS-	2018	Restricted Boltzmann machine (RBM)	SCL	It improves the average accuracy of multimodal deep representation by

	HINDAWI				2.65%
15	Nasir et. al. [15] ELSEVIER	2018	Fog Computing		
16	Muhammad et. al.[21] IEEE	2018	Video summarization	a fast probabilistic and lightweight algorithm	Experimental results verify the efficiency, security, and robustness of proposed algorithm compared to other image encryption methods.
17	Munir et. al. [9] IEEE Access	2018	Convolutional Neural Networks	DeepAnT	Evaluation of DeepAnT on 10 different data sets comprising of 433 time series in total and provided a detailed comparison with 15 state-of-the-art anomaly detection methods.
18	Raahat Devender Singh, Naveen Aggarwal [23] (SPRINGER)	2018		Passive-blind technique Inter-frame forgery detection	Presents a repository of information regarding the kinds of tamper attacks a video can suffer from and a comprehensive source of references for the passive-blind techniques proposed for detecting attacks
19	Sultani et. al. [8] IEEE Xplore	2018	Multiple instance learning (MIL)	Deep MIL Ranking Model, binary SVM classifier	A new large-scale anomaly dataset consisting of a variety of real world anomalies is introduced.
20	Alberto Castillo, SihamTabik, Francisco P´erez, Roberto Olmos, and Francisco Herrera [27] (ELESEVIER)	2018	Deep learning	DaCoLT- a brightness guided preprocessing approach	This paper proposed a brightness guided preprocessing approach. DaCoLT model shows a high potential even in low quality videos and provides satisfactory results as an automatic alarm system.
21	Bouindour et. al. [10] Applied sciences MDPI	2019	Convolutional Neural Networks	Matlab	This method is robust, takes into account rare normal events present in the trainingphase. Besides, it can be incorporated in online CCTV.
22	James A.D. Camerona, Patrick Savoiea , Mary E. Kayea , Erik J.	2019	CNN based algorithms	GoogLeNet , AlexNet VGG16,ResNet50, SSD	This work has highlighted some of the practical challenges of designing a processing system for a

	Scheme [26] (ELESEVIER)				CNN-based automated surveillance system using off-the-shelf hardware and open-source algorithms.
23	Jianyu Xiao , Shancang Li , Qingliang Xu (IEEE)	2019	Deep learning	Object detection and tracking	Proposed a framework for video based digital forensics investigation, useful for anti-crime or fast response when crime activities or behaviors are detected
24	Summra Saleema, Aniqa Dilawari , Ghani Khana, Razi Iqbal c, Shaohua Wand, Tariq Umer [29] (ELSEVIER)	2019	Deep Convolution Neural Networks (CNN).	Feats-rich model encodes the visual contents to visual and facial features using CNN architecture.	It is a framework for generating multi-line textual descriptions for video captioning. Feats-rich model extends feature matrix to visual (2-D and 3-D) and facial features. Spatio-temporal characteristics are encompassed by employing deep neural networks.
25	Sreenu and Durai [13] SPRINGER OPEN ACCESS	2019	Big Data	ImageNet2012, PASCAL VOC, Frames Labeled In Cinema (FLIC), Leeds Sports Pose (LSP)	Methods analyzing crowd behavior were discussed.

Goals of PC crime scene investigation

Here are the fundamental destinations of utilizing Computer crime scene investigation:

- It assists with recuperating, dissecting, and protecting PC and related materials in such a way, that it causes the examination office to introduce them as proof in an official courtroom.
- It assists with proposing the rationale behind the wrongdoing and personality of the fundamental guilty party.
- Structuring systems at a speculated wrongdoing scene which causes you to guarantee that the advanced proof acquired isn't debased.
- Information procurement and duplication: Recovering erased records and erased parcels from advanced media to extricate the proof and approve them.
- Causes you to recognize the proof rapidly and permits you to evaluate the potential effect of the malevolent movement on the person in question delivering a PC measurable report which offers a total report on the examination procedure.
- Protecting the proof by following the chain of authority.

2. Process of Digital Forensics

Digital forensics entails the following steps that are explained below:

➢ Identification: This is the first step in forensic medicine. The identification process largely consists of such things as what evidence exists, where it is stored and ultimately how far away it is stored. Electronic data carriers can be personal computers, mobile phones, PDAs, etc.

➢ Preservation: It consists of stopping humans from using virtual devices so that digital evidence isn't always tampered with.

➢ Analysis: In this step, investigationmarketers reconstruct fragments of facts and draw conclusions based totally on evidence found. However, it'd take numerous

iterations of the exam to support a particular crime theory.

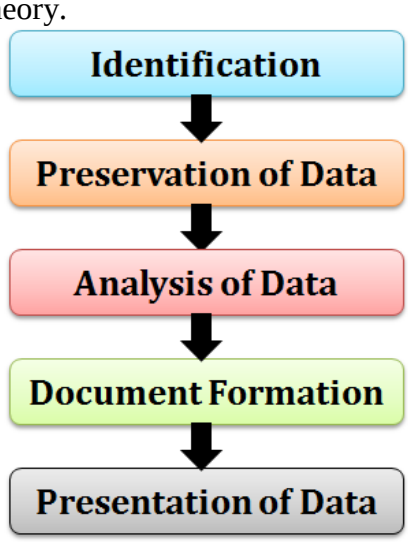

Figure 1: Process of digital forensics

➢ Documentation: In this technique, a report of all of the visible statisticsought to be created. It can be used to recreate and visualize a crime scene. This includes proper documentation of the crime scene, as well as photographing, sketching and mapping the crime scene.

➢ Presentation: In this final step, the technique of summarization and clarification of conclusions is done.

3. Difficulties looked through Digital Forensics

Here, are full-sizeproblems looked at with the aid of the Digital Forensic:

- The enlargement of PCs and extensiveutilization of internetaccess
- Simple accessibility of hacking instruments
- Absence of physicalproof makes indictment troublesome.
- The largedegree of more room in Terabytes makes these investigations troublesome.
- Any innovative changes require an update or adjustments to arrangements.

4. Model Uses of Digital Forensics

In late time, enterpriseassociations have appliedautomaticprison sciences in the following a sort of cases:

- Licensed innovation robbery
- Mechanical reconnaissance
- Business questions
- Misrepresentation examinations
- Improper usage of the Internet and email inside theworking environment
- Fabrications related issues

5. Advantages of Digital criminal sciences

Here, are some advantages of Digital criminal sciences

- To guarantee the honesty of the PC framework.
- To deliverevidencein the court, this can spark off the field of the guilty party.
- It encourages the agencies to catch massiveinformation if their PC frameworks or systems are undermined.
- Proficiently finds cybercriminals from anywhereon the planet.
- Assists with ensuring the association's cash and significant time.
- Permits to concentrate, process, and decipher the verifiable proof, so it demonstrates the cybercriminal activityinside the court.

6. Detriments of Digital Forensics

Here, are sizable cons/downsides of using Digital Forensic

- Advanced proofstatedin court. In any case, its mileshave to be proven that there's no altering.
- Creating electronic records and placing away them is an amazingly luxurious undertaking.
- Lawful specialists ought to have huge PC data.
- Need to create authentic and persuading evidence.
- In the occasion that the instrumentapplied for automaticcriminologyisn't always as per indicated gauges, at that point in thelegit courtroom, the evidencemay be opposed via equity.
- Absence of specialized informationby way of the examining reputable probably might not offer the proper outcome.

7. Conclusion

The preservation, recognition, extraction, and recording of evidence that can be used in a court of law are known as digital forensics. Identification, preservation, analysis, documentation, and presentation make up the digital forensics process. Disk forensics, network forensics, wireless forensics, database

forensics, malware forensics, email forensics, memory forensics, and other kinds of digital forensics exist. Thus, we draw the conclusion that 1) intellectual property theft and 2) industrial espionage are instances where digital forensic science can be used. 3) Conflicts at work; 4) fraud inquiries.

References

[1] Sundresan Perumal; Norita Md Norwawi; Valliappan Raman; Internet Of Things(IoT) Digital Forensic Investigation Model:Top-Down Forensic Approach Methodology; IEEE Fifth International Conference on Digital Information Processing and Communications (ICDIPC)**2015**, DOI:10.1109/ICDIPC.2015.7323000

[2] Kwaku Kyei; PavolZavarsky; Dale Lindskog; Ron Ruhl; A Review and Comparative Study of Digital Forensic Investigation Models; ICDF2C Digital Forensics & Cyber Crime; **2012,**https://doi.org/10.1007/978-3-642-39891-9_20

[3] Harleen Kaur and Khairaj Ram Choudhary, "Digital Forensics: Implementation and Analysis for Google Android Framework," Springer International Publishing Switzerland 2017 I.M. Alsmadi et al. (eds.), Information Fusion for Cyber-Security Analytics, Studies in Computational Intelligence 691, DOI 10.1007/978-3-319-44257-0_13.

[4] What is Digital Forensics? History, Process, Types, Challenges; <https://www.guru99.com/digital-forensics.html>

[5] Digital forensics; https://en.wikipedia.org/wiki/Digital_forensics

[6] Shaonian Huang, Dongjun Huang, Xinmin Zhou at "Learning Multimodal Deep Representations for Crowd Anomaly Event Detection", Hindawi, Mathematical Problems in Engineering, Volume 2018, Article ID 6323942, 13 pages, https://doi.org/10.1155/2018/6323942.

[7] Mohammad Farhadi Bajestani,Seyed Soroush Heidari Rahmat Abadi, Seyed Mostafa Derakhshandeh Fard, Roozbeh Khodadadeh at "AAD: Adaptive Anomaly Detection through traffic surveillance videos"29 Aug 2018

[8] Aqas Sultani, Chen Chen, Mubarak Shah at "Real-world Anomaly Detection in Surveillance Videos"

[9]. MOHSIN MUNIR, SHOAIB AHMED SIDDIQUI, ANDREAS DENGEL, AND SHERAZ AHMED at "DeepAnT: A Deep Learning Approach for Unsupervised Anomaly Detection in Time Series" January 7, 2019, IEEE access, Digital Object Identifier 10.1109/ACCESS.2018.2886457.

[10]. Samir Bouindour, Hichem Snoussi, Mohamad Mazen Hittawe and Nacef Tazi and Tian Wang 3, "An On-Line and Adaptive Method for Detecting Abnormal Events in Videos Using Spatio-Temporal ConvNet", 21 February 2019, Appl. Sci. 2019, 9, 757; doi:10.3390/app9040757.

[11]. Rajat Kumar Sinha,Ruchi Pandey,Rohan Pattnaik, "Deep Learning For Computer Vision Tasks: A review", International Conference on Intelligent Computing and Control 2017

[12] Khan Muhammad, Jamil Ahmad, Irfan Mehmood, Seungmin Rho and Sung Wook Baik, "Convolutional Neural Networks Based Fire Detection in Surveillance Videos", April 23, 2018, Digital Object Identifier 10.1109/ACCESS.2018.2812835.

[13]. G. Sreenu and M. A. Saleem Durai, "Intelligent video surveillance: a review through deep learning techniques for crowd analysis", April 23, 2018. Digital Object Identifier 10.1109/ACCESS.2018.2812835

[14]. Zhenfeng Shao, Jiajun Cai, Zhongyuan Wang, "Smart Monitoring Cameras Driven Intelligent Processing to Big Surveillance Video Data", Published in IEEE Transactions on Big Data 2018 DOI:10.1109/TBDATA.2017.2715815

[15]. Mansoor Nasir, Khan Muhammad, Jaime Lloret Mauri, Arun Kumar Sangaiah, Muhammad Sajjad lessPublished in J. Parallel Distrib. "Fog computing enabled cost-effective distributed summarization of surveillance videos for smart cities", Comput. 2019 DOI:10.1016/ j.jpdc.2018.11.004

[16]. Francesco Turchini,Lorenzo Seidenari,Tiberio Uricchio, and Alberto Del Bimbo, "Deep Learning Based Surveillance System for Open Critical Areas", Received: 3 August 2018; Accepted: 4 October 2018; Published: 11 October 2018, 3, 69; doi:10.3390/inventions3040069.

[17]. Cheng-Bin Jin,Shengzhe Li,and Hakil Kim, " Real-Time Action Detection in Video Surveillance using Sub-Action Descriptor with Multi-CNN"

[18]. Francesco Turchini,Lorenzo Seidenari,Tiberio Uricchio and Alberto Del Bimbo, "Deep Learning Based Surveillance System for Open", Critical Areas, Received: 3 August 2018; Accepted: 4 October 2018; Published: 11 October 2018, 3, 69; doi:10.3390/inventions3040069.

[19]. J. Ahmad, K. Muhammad, and S. W. Baik, ''Data augmentation-assisted deep learning of hand-drawn partially colored sketches for visual search,'' PLOS ONE, vol. 12, no. 8, p. e0183838, 2017.

[20]. K. Muhammad, J. Ahmad, and S. W. Baik, ''Early fire detection using convolutional neural networks during surveillance for effective disaster management,'' Neurocomputing, vol. 288, pp. 30–42, May 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/ S09252312 17319203

[21]. K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. H. Ge Wang, and S. W. Baik, ''secure urveillance framework for IoT systems using probabilistic image encryption,'' IEEE Trans. Ind. Inform., doi: https://doi.org/10.1109/TII.2018.2791944

[22]. S.-Z. Chen, C.-C. Guo, J.-H. Lai, "Deep ranking for person re-identification via joint representation learning", IEEE Transactions on Image Processing 25 (5) (2016) 2353–2367.

[23] Raahat Devender Singh, Naveen Aggarwal, "Video content authentication techniques: a comprehensive survey," Multimedia Systems (2018) 24:211–240, DOI: 10.1007/s00530-017-0538-9.

[24] Jianyu Xiao, Shancang Li , And Qingliang Xu, "Video-Based Evidence Analysis and Extraction
in Digital Forensic Investigation," Special Section On Deep Learning: Security And Forensics Research Advances And Challenges, Date Of Publication April 26, 2019, Date Of Current Version May 7, 2019, DOI: 10.1109/Access.2019.2913648.

[25] Hrishikesh Bhaumika, Siddhartha Bhattacharyyaa, Mausumi Das Natha, Susanta Chakraborty, "Hybrid soft computing approaches to content based video retrieval: A brief review," Appl. Soft Comput. J. (2016), Elsevier,
http://dx.doi.org/10.1016/j.asoc.2016.03.022