A REVIEW PAPER ON DATA FORENSIC

Bharathi Kannan B, Assistant Professor, Department of Computer Science & Engineering, Galgotias University

ABSTRACT

Over the past few decades, we have seen information technology go through several stages of development. Early on, we saw the evolution of VLSI technologies, networking infrastructure, and multimedia compression and coding schemes. Later, we saw the rise of effective multimedia content search and retrieval. As a consequence, digital material and multimedia gadgets have grown common. Once technology has moved in this manner, we will encounter a critical issue which we will then have to contend with, and that is the problem of ascertaining whether content, devices, and intellectual property are being used by authorised users for legitimate purposes, and being able to accurately and with a high degree of certainty prove it. Forensic methods and technologies are used to recreate digital material to answer who has done what, when, when, and how. The purpose of this study is to provide a review of the progress that has been made in the information forensics field over the previous decade, including descriptions of concepts, methodology, most current methods, and areas of application.

KEYWORDS: Data, Forensic, Technology, Information

INTRODUCTION

The lifespan of every technology has an expiration date. In the 1970s, advancements in VLSI gave rise to a new technological revolution that created smaller, quicker electronic systems. Since that time, global developments in high-speed networking and wireless infrastructure have occurred. Development of multi-media compression techniques and systems accelerated with the 1990s introduction of broadband communication and computer infrastructure. Many industry standards were established because to this, including JPEG, MPEG-1/2/4, and H.26x. Following this, we found ourselves on the hunt for and categorising material as it spread over the internet [1-4]. The emphasis of research and development (R&D) shifted to online search, and major commercial web search providers (Google and Yahoo) arose. Naturally, there is now a major challenge, which is to include information, devices, and intellectual assets and provide for secure, forensic evidence gathering to establish strong evidence against perpetrators.

Digital content's broad usage has led to a variety of new information security problems. At the threat of altering, falsifying, and redistributing digital materials [6-9], attackers may inflict huge damage. Because of this, the government, business, and social entities that use digital information must think carefully about the long-term effects of their decisions. Several cryptographic encryption and authentication approaches have been developed to protect communication infrastructures while preventing illegal access to digital information. Decryption happens after delivery, and hence after security measures have been applied [10-

12]. Given that information is sent without any direct control over how it is utilised or processed, there is nothing in the way of corrective measures available. While these solutions can't prevent media material from being altered or faked before to cryptographic encryption or signing, they can at least stop that from happening while the cryptographic algorithm is used. Digital information that comes from an unknown or untrusted source often impacts people's lives in crucial ways. Forgers and information attackers may fabricate convincingly realistic fakes when this occurs [13].

DATA FORENSIC

This birth of the area of information forensics is in reaction to the increase in the requirement to verify the trustworthiness of multimedia material. A somewhat novel use of forensics involves forensic examination of digital multimedia material without using other than the digital material itself. The scope of the reconstruction process strives to be as extensive as possible, in an effort to understand what, when, where, and how everything has been done to the material. Even if the information passes through many devices and processing, each processing step has an impact on the information's state. Forensic investigation depends on traces, which are referred to as intrinsic fingerprints. While there have been various forensic ways to detect tampering using invisible traces that appear in multimedia information during capture and processing, nowadays, forensic approaches have only just begun to investigate this phenomenon [14-17].

In addition, security measures such as digital watermarks are externally created. By using an invisible data embedding methodology, these security measures are often built into information content and so cannot be detected by end users. In these instances, we use the term extrinsic fingerprints. While a good deal of work from about the year 2000 had addressed methods for embedding extrinsic information to confirm copyright or validate host media data's integrity, a majority of that work focused on adding external data instead. In the last decade, there has been much study on enhancing classical robust watermarking so that new and different types of traceable fingerprints may be applied, each with unique information and able to connect to particular acquisition devices [18-20].

DETECTION AND PROCESSING

In many cases, unknown or untrusted audiovisual material provides critical information. A questionable picture or video that is broadcast by a foreign government, such as a terrorist film, may have substantial political or military significance. In order for media portrayed in this medium to be believed, the processing that it has experienced must first be identified and determined to be real. Researchers have created many forensic approaches that work independently of external security measures, therefore the multimedia material may have had no embedded security protections before processing. These strategies use features of the digital information itself to accomplish their goals [21-24]. Tracing a multimedia file's processing history, detecting tampering, and identifying forgeries may be categorised into five broad categories, according on the methodology in which they function. Classifiers based on machine learning that learn a large number of picture statistics are part of this. When used together, the different forensic methods may accurately detect a broad range of kinds of forgery and processing processes.

CONCLUSION

Information forensics principles have seen numerous uses, including for rooting out tampering, identifying the origins of items, and pinpointing the time and location of items. Thus far, the research community has depended on individual research groups' empirical testing of various methodologies, frequently with a small-scale dataset, to illustrate and compare performances. "So yet, no forensics hypothesis has been developed." A sound understanding of forensics begins with basic principles. To this end, you should also introduce the concept of "forensicability" for equipment, channels, and processing systems. The foundations of forensic analysis may be formalised using three specific theories, which are the theory of detection, the theory of classification, and machine learning. By providing the community with a more basic knowledge of what device, channel, or processor options can or cannot be inferred forensically, the theories on forensicability help the community gain an unprecedented but critical awareness of individual or combinations of options [25-28].

REFERENCES

1. Agarwal, S., Perry, H. B., Long, L.-A., & Labrique, A. B. (2015). Evidence on feasibility and effective use of mHealth strategies by frontline health workers in developing countries: Systematic review. *Tropical Medicine and International Health*, *20*(8), 1003–1014. https://doi.org/10.1111/tmi.12525
2. Ahas, R., Aasa, A., Roose, A., Mark, U., & Silm, S. (2008). Evaluating passive mobile positioning data for tourism surveys: An Estonian case study. *Tourism Management*, *29*(3), 469–486. https://doi.org/10.1016/j.tourman.2007.05.014
3. Atchley, P., Atwood, S., & Boulton, A. (2011). The choice to text and drive in younger drivers: Behavior may shape attitude. *Accident Analysis and Prevention*, *43*(1), 134–142. https://doi.org/10.1016/j.aap.2010.08.003
4. Bernardi, P., Cavagnaro, M., Pisa, S., & Piuzzi, E. (1998). SAR distribution and temperature increase in an anatomical model of the human eye exposed to the field radiated by the user antenna in a wireless LAN. *IEEE Transactions on Microwave Theory and Techniques*, *46*(12 PART 1), 2074–2082. https://doi.org/10.1109/22.739285
5. Carroll, J. K., Moorhead, A., Bond, R., LeBlanc, W. G., Petrella, R. J., & Fiscella, K. (2017). Who uses mobile phone health apps and does use matter? A secondary data analytics approach. *Journal of Medical Internet Research*, *19*(4). https://doi.org/10.2196/jmir.5604
6. Carter, B., Rees, P., Hale, L., Bhattacharjee, D., & Paradkar, M. S. (2016). Association between

portable screen-based media device access or use and sleep outcomes a systematic review and meta-analysis. *JAMA Pediatrics*, *170*(12), 1202–1208. https://doi.org/10.1001/jamapediatrics.2016.2341

7. Christensen, H. C., Schüz, J., Kosteljanetz, M., Poulsen, H. S., Thomsen, J., & Johansen, C. (2004). Cellular Telephone Use and Risk of Acoustic Neuroma. *American Journal of Epidemiology*, *159*(3), 277–283. https://doi.org/10.1093/aje/kwh032
8. Erogul, O., Oztas, E., Yildirim, I., Kir, T., Aydur, E., Komesli, G., Irkilata, H. C., Irmak, M. K., & Peker, A. F. (2006). Effects of Electromagnetic Radiation from a Cellular Phone on Human Sperm Motility: An In Vitro Study. *Archives of Medical Research*, *37*(7), 840–843. https://doi.org/10.1016/j.arcmed.2006.05.003
9. Firth, J., Cotter, J., Torous, J., Bucci, S., Firth, J. A., & Yung, A. R. (2016). Mobile phone ownership and endorsement of “mhealth” among people with psychosis: A meta- Analysis of cross-sectional studies. *Schizophrenia Bulletin*, *42*(2), 448–455. https://doi.org/10.1093/schbul/sbv132
10. Gao, S., Liu, Y., Wang, Y., & Ma, X. (2013). Discovering spatial interaction communities from mobile phone data. *Transactions in GIS*, *17*(3), 463–481. https://doi.org/10.1111/tgis.12042
11. Gutiérrez, J. D.-S., de Fonseca, F. R., & Rubio, G. (2016). Cell-phone addiction: A review. *Frontiers in Psychiatry*, *7*(OCT). https://doi.org/10.3389/fpsyt.2016.00175
12. Hall, C. S., Fottrell, E., Wilkinson, S., & Byass, P. (2014). Assessing the impact of mHealth interventions in low- and middle-income countries - what has been shown to work? *Global Health Action*, *7*(1). https://doi.org/10.3402/gha.v7.25606
13. Hardell, L., Carlberg, M., Söderqvist, F., Mild, K. H., & Morgan, L. L. (2007). Long-term use of cellular phones and brain tumours: Increased risk associated with use for ≥10 years. *Occupational and Environmental Medicine*, *64*(9), 626–632. https://doi.org/10.1136/oem.2006.029751
14. Herrera, J. C., & Bayen, A. M. (2010). Incorporation of Lagrangian measurements in freeway traffic state estimation. *Transportation Research Part B: Methodological*, *44*(4), 460–481. https://doi.org/10.1016/j.trb.2009.10.005
15. Hou, C., Carter, B., Hewitt, J., Francisa, T., & Mayor, S. (2016). Do mobile phone applications improve glycemic control (HbA&lt;&gt;1c&lt;&gt;) in the self-management of diabetes? A systematic review, meta-analysis, and GRADE of 14 randomized trials. *Diabetes Care*, *39*(11), 2089–2095. https://doi.org/10.2337/dc16-0346
16. Iribarren, S. J., Cato, K., Falzon, L., & Stone, P. W. (2017). What is the economic evidence for mHealth? A systematic review of economic evaluations of mHealth solutions. *PLoS ONE*, *12*(2). https://doi.org/10.1371/journal.pone.0170581
17. Khurana, V. G., Teo, C., Kundi, M., Hardell, L., & Carlberg, M. (2009). Cell phones and brain tumors: a review including the long-term epidemiologic data. *Surgical Neurology*, *72*(3), 205–214. https://doi.org/10.1016/j.surneu.2009.01.019
18. Kung, K. S., Greco, K., Sobolevsky, S., & Ratti, C. (2014). Exploring universal patterns in human home-work commuting from mobile phone data. *PLoS ONE*, *9*(6).

https://doi.org/10.1371/journal.pone.0096180

19. Lee, S. H., Nurmatov, U. B., Nwaru, B. I., Mukherjee, M., Grant, L., & Pagliari, C. (2016). Effectiveness of mHealth interventions for maternal, newborn and child health in low- and middle-income countries: Systematic review and meta-analysis. *Journal of Global Health*, *6*(1). https://doi.org/10.7189/jogh.06.010401
20. Liang, X., Zheng, X., Lv, W., Zhu, T., & Xu, K. (2012). The scaling of human mobility by taxis is exponential. *Physica A: Statistical Mechanics and Its Applications*, *391*(5), 2135–2144. https://doi.org/10.1016/j.physa.2011.11.035
21. Martin, C. K., Han, H., Coulon, S. M., Allen, H. R., Champagne, C. M., & Anton, S. D. (2009). A novel method to remotely measure food intake of free-living individuals in real time: The remote food photography method. *British Journal of Nutrition*, *101*(3), 446–456. https://doi.org/10.1017/S0007114508027438
22. Pappalardo, L., Simini, F., Rinzivillo, S., Pedreschi, D., Giannotti, F., & Barabási, A.-L. (2015). Returners and explorers dichotomy in human mobility. *Nature Communications*, *6*. https://doi.org/10.1038/ncomms9166
23. Rice, E., Rhoades, H., Winetrobe, H., Sanchez, M., Montoya, J., Plant, A., & Kordic, T. (2012). Sexually explicit cell phone messaging associated with sexual risk among adolescents. *Pediatrics*, *130*(4), 667–673. https://doi.org/10.1542/peds.2012-0021
24. Stopczynski, A., Sekara, V., Sapiezynski, P., Cuttone, A., Madsen, M. M., Larsen, J. E., & Lehmann, S. (2014). Measuring large-scale social networks with high resolution. *PLoS ONE*, *9*(4). https://doi.org/10.1371/journal.pone.0095978
25. Whittaker, R., Mcrobbie, H., Bullen, C., Rodgers, A., & Gu, Y. (2016). Mobile phone-based interventions for smoking cessation. *Cochrane Database of Systematic Reviews*, *2016*(4). https://doi.org/10.1002/14651858.CD006611.pub4
26. Wilson, F. A., & Stimpson, J. P. (2010). Trends in fatalities from distracted driving in the United States, 1999 to 2008. *American Journal of Public Health*, *100*(11), 2213–2219. https://doi.org/10.2105/AJPH.2009.187179
27. Wilson, F. P., Shashaty, M., Testani, J., Aqeel, I., Borovskiy, Y., Ellenberg, S. S., Feldman, H. I., Fernandez, H., Gitelman, Y., Lin, J., Negoianu, D., Parikh, C. R., Reese, P. P., Urbani, R., & Fuchs, B. (2015). Automated, electronic alerts for acute kidney injury: A single-blind, parallel-group, randomised controlled trial. *The Lancet*, *385*(9981), 1966–1974. https://doi.org/10.1016/S0140-6736(15)60266-5