DATA FORENSICS ANALYSIS ON BIOMETRIC IMAGES USING BENFORD'S LAW AND SUPPORT VECTOR MACHINE ALGORITHM

By

ALSAADI HUSSAM HUSSEIN HAMID

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia in Fulfillment of the Requirements for the Degree of Master of Science

January 2024

IPM 2024 2

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Science

DATA FORENSICS ANALYSIS ON BIOMETRIC IMAGES USING BENFORD'S LAW AND SUPPORT VECTOR MACHINE ALGORITHM

By

ALSAADI HUSSAM HUSSEIN HAMID

January 2024

Chairman : Muhammad Aslam bin Mohd Safari, PhD
Institute : Mathematical Research

The manipulation of biometric data has become a prominent topic, leading to the development and exploration of methods for detecting such manipulation. This study utilizes a combination of Benford’s law, an image quantization to analyze the fingerprint images processing associated with biometric data. The aim is to propose a mechanism for detecting data manipulation, particularly when one biometric sample is substituted for another in an application, whether intentionally or unintentionally. The study focuses on differentiating between biometric samples and investigating the modification of fingerprint images. To achieve this, the Benford legal difference scale is applied to fingerprints digitally obtained, industrially created fingerprints, contactless acquired fingerprints to search for separation modes. Benford’s law has been successful in determining the alteration of landscape images in previous studies, and this study combines Benford’s law elements with a SVM (Support Vector Machine) to identify malicious alterations in JPEG fingerprint images. The proposed strategy is intended to safeguard against internal threats.

Keywords: Benford's law, Fingerprint, JPEG, SVM

SDG: GOAL 9: Industry, Innovation and Infrastructure, GOAL 11: Sustainable Cities and Communities, GOAL 17: Partnerships for The Goals.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
sebagai memenuhi keperluan untuk ijazah Master Sains

ANALISIS FORENSIK DATA PADA IMEJ BIOMETRIK MENGGUNAKAN HUKUM BENFORD DAN ALGORITMA MESIN VEKTOR SOKONGAN

Oleh

ALSAADI HUSSAM HUSSEIN HAMID

January 2024

Pengerusi : Muhammad Aslam bin Mohd Safari, PhD
Institut : Penyelidikan Matematik

Manipulasi data biometrik telah menjadi topik yang menonjol, membawa kepada pembangunan dan penerokaan kaedah untuk mengesan manipulasi tersebut. Kajian ini menggunakan gabungan hukum Benford, pengkuantitian imej untuk menganalisis pemprosesan imej cap jari yang berkaitan dengan data biometrik. Tujuannya adalah untuk mencadangkan mekanisme untuk mengesan manipulasi data, terutamanya apabila satu sampel biometrik digantikan dengan yang lain dalam aplikasi, sama ada secara sengaja atau tidak sengaja. Kajian ini memberi tumpuan kepada membezakan antara sampel biometrik dan menyiasat pengubahsuaian imej cap jari. Untuk mencapai matlamat ini, skala perbezaan hukum Benford digunakan pada cap jari yang diperoleh secara digital, cap jari yang dibuat secara industri, cap jari yang diperoleh tanpa sentuhan untuk mencari mod pemisahan. Hukum Benford telah berjaya dalam menentukan pengubahan imej landskap dalam kajian terdahulu, dan kajian ini menggabungkan elemen hukum Benford dengan SVM (Mesin vektor sokongan) untuk mengenal pasti pengubahan berniat jahat dalam imej cap jari JPEG. Strategi yang dicadangkan bertujuan untuk melindungi daripada ancaman dalaman.

Kata Kunci: Cap jari, JPEG, SVM, Undang-undang Benford

SDG: MATLAMAT 9: Industri, Inovasi, dan Infrastruktur, MATLAMAT 11: Bandar dan Komuniti Lestari, MATLAMAT 17: Perkongsian untuk Matlamat.

ACKNOWLEDGEMENTS

First of all, I thank God Almighty for giving me the strength and determination to undertake this study.

And to my family who stood with me in the most difficult circumstances I went through, especially when I was first infected with the Coronavirus in 2021, after which I was about to bid farewell to this life and go to its final resting place, and also to everyone who prayed to God for my recovery and release from this ordeal.

Many thanks to Dr Muhammad Aslam bin Mohd Safari (Department of Mathematics and Statistics) for encouragement, continuous guidance, supervision, continuous scientific assistance, and editing of the manuscript. Thanks also to Assistant Professor T.S. Dr. Mohammad Lutfi bin Othman (Department of Electrical and Electronic Engineering).

I would like to express my deep appreciation and great thanks to Dr. Nur Sumirah Mohd Dom, the institute's coordinator, and I will never forget my thanks and appreciation to my supervisor, with whom I lost contact a whole year ago because she helped me at beginning study at the prestigious UPM University.

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the degree of Master of Science. The members of the Supervisory Committee were as follows:

Muhammad Aslam bin Mohd Safari, PhD
Senior Lecturer
Faculty of Science
Universiti Putra Malaysia
(Chairman)

Mohammad Lutfi bin Othman, PhD
Associate Professor, Ts Ir.
Faculty of Engineering
Universiti Putra Malaysia
(Member)

ZALILAH MOHD SHARIFF, PhD
Professor and Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 12 September 2024

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

DCT	Discrete Cosine Transformation
e-MRTDs	electronic Machine-Readable Travel Documents
GBL	Generalized Benford Law
IDCT	Inverse DCT
JPEG	Joint Photographic Expert Group
SVM	Support Vector Machine
TIFF	Tag Image File Format
UPM	Universiti Putra Malaysia

CHAPTER 1

INTRODUCTION

1.1 Premise

Biometric authentication has become ubiquitous in our daily lives, granting access to everything from smartphones to secure buildings. This widespread adoption hinges on the inherent uniqueness of individual biometric data (e.g., fingerprints, iris patterns). While the convenience and security benefits of biometrics are undeniable, the sensitive nature of this data necessitates robust verification methods. Ensuring the integrity of biometric systems is paramount to safeguarding personal information and financial security.

This study investigates the impact of different image compression techniques on the efficacy of biometric recognition systems. A biometric image, initially stored in the secure Tag Image File Format (TIFF), will be subjected to compression using various Joint Photographic Expert Group (JPEG) compression algorithms. The goal is to determine the optimal balance between image quality, essential for accurate biometric identification and file size reduction for efficient storage and transmission.

Rapid advancements in technology have made biometric systems an essential part of our everyday existence. For identification or authentication purposes, these systems rely on the intrinsic uniqueness of our biological traits, such as iris scans, fingerprints and facial features. Due to each fingerprint's or iris's uniqueness and high level of dependability for identification, biometrics' fundamental distinctiveness serves as its main strength. However, biometric systems security is critical. Robust security measures are necessary to guarantee the integrity of the system and prevent unauthorized access, especially considering the sensitive nature of the data they manage. One of the most important facets of biometric security is brought to light by this study on image compression. We can provide a path towards the creation of more resilient and secure biometric systems by merging these insights with cutting-edge algorithms such as Support Vector Machines (SVMs) and anomaly detection methods through Benford's law.

In the domain of biometrics, where unique biological characteristics are utilized for identification and verification purposes, the ability to distinguish between various fingerprint types holds paramount importance. Fingerprint analysis serves two primary functions:

a) Verification (1: 1 matching): This process establishes whether a claimed identity aligns with the presented fingerprint. In simpler terms, it confirms if an individual is indeed who they purport to be.

b) Identification (1: N matching): This method identifies an individual or determines the source of a captured biometric sample by comparing it against a vast database containing numerous fingerprint records.

It is crucial to navigate these applications while prioritizing data privacy concerns. Furthermore, fingerprints possess the potential for broader applications beyond identification and verification. Optically captured fingerprints, for instance, can be utilized to construct a comprehensive biometric database for a nation. This database can then be leveraged to bolster national security by expediting criminal investigations and potentially minimizing the overall crime rate.

This study investigates the application of Benford’s law for analyzing and differentiating between various biometric image formats. The research focuses on both grayscale and color images compressed using the JPEG technique. Benford’s law, introduced by Frank Benford in 1938, offers a well-established method for data assessment and tamper detection. Also known as the first-digit law or the "odd-numbers" law, it specifically examines the leading digit (most significant digit [MSD]) of numerical data. This law suggests a logarithmic distribution for the leading digit probabilities within a set of natural numbers (1 to 9). As described by Iorliam et al. (2022), natural data sets exhibit a logarithmic distribution for the leading digit frequencies. Critically, this law is expected to hold true for authentic organically occurring numerical data. Conversely, manipulated data or random values are likely to deviate from this expected distribution.

While traditionally associated with forensic accounting, Benford’s law has recently demonstrated potential in image forensics. Existing research suggests that pixel-domain image representations may not adhere to the law, while those transformed into the DCT domain exhibit better alignment. This finding, as highlighted by Gonzalez-Garcia and Pastor (2009), represents a significant advancement in the application of Benford’s law for image analysis.

This study aims to build upon these findings by examining the applicability of Benford’s law to various biometric image formats, particularly those compressed using JPEG. The analysis will explore potential correlations between image format and leading digit distribution, with a focus on identifying potential indicators of image tampering.

1.2 Study Background

Biometric data alteration by digital means poses a serious risk that may be used for a variety of unlawful actions, both online and offline. The basis for many criminal and terrorist operations is this manipulation. Biometric identifiers, which are extremely distinctive to each person and are used to confirm ownership of legal documents or access to certain services, include fingerprints and iris scans. Particularly targeting these identifiers, criminals and terrorists modify them to enable illicit actions that may have detrimental effects on public safety and financial security.

Using counterfeit fingerprints to obtain unauthorized access to systems or data while hiding the real identity of the offender is a frequent strategy. In order to identify and avoid fingerprint manipulation, researchers are including more electronic elements into fingerprint recognition systems, especially in electronic Machine-Readable Travel Documents (e-MRTDs) (Satapathy, 2020). The same essential ideas are still communicated in this updated form, which makes use of simpler, clearer language. Additionally, it offers a citation to back up the assertion of improvements in e-MRTD security.

The increasing sophistication of digital manipulation techniques poses a growing challenge to the security of biometric identification systems, particularly fingerprints stored in e-MRTDs. Recent research suggests that incorporating double-identity biometrics into e-MRTDs could be a promising approach to thwart attempts to bypass security through altered fingerprints (Hildebrandt & Dittmann, 2015). This method involves correlating and comparing a single biometric template with data from two individuals. For instance, double-identity facial recognition could detect inconsistencies indicative of tampering. However, it's important to acknowledge the limitations of this approach. A recent study demonstrated the creation of specialized synthetic fingerprints, known as double-identity fingerprints, that could be enrolled in e-MRTD systems (source to be added). These fingerprints are meticulously crafted by combining features from two separate individuals. Notably, a successfully enrolled double-identity fingerprint grants access to the system without revealing the identities of those involved in the forgery. Additionally, alternative methods of tampering with fingerprint sensors exist, potentially leading to inconclusive readings or bypassing identification altogether.

To enhance fingerprint identification and combat forgeries, researchers are turning to Benford’s law, a statistical fingerprint of real data. This approach capitalizes on the natural distribution of leading digits found in genuine fingerprints. Studies like those by Hildebrandt & Dittmann (2015) have shown success in detecting manipulated data using Benford’s law divergence values. Satapathy (2020) further explored its potential by tackling the emerging threat of "double-identity fingerprints," which combine elements from multiple individuals. Their solution, integrating generalized Benford’s law with a Support Vector Machine, analyzes leading digit distributions in fingerprint data. This method is particularly attractive due to its simplicity, as it leverages readily available features and avoids complex pre-processing, making it a time-efficient weapon against sophisticated forgery techniques.

The discipline of computational image processing is always looking for novel approaches to identify changes and tampering with biometric fingerprints. In an attempt to detect forgeries, previous studies have investigated a variety of picture formats. Nevertheless, combining machine learning methods with generalized Benford’s law is a very interesting line of inquiry. Researches have shown how successful this method is for a variety of image processing applications. Continuing this pace, this work examines changes to optically derived biometric fingerprints. Here, our special goal is to differentiate real fingerprints from those that have been artificially created. By concentrating on optically obtained data, we may take use of the innate statistical characteristics.

1.3 Problem Statement

The significant problem of identifying faked and manipulated biometric fingerprints is examined in this thesis. This issue is becoming more and more serious and threatens the integrity of security systems. Traditional biometric verification systems, especially those that use fingerprints in e-MTDs, are becoming more and more susceptible to hacking due to the widespread use of sophisticated digital manipulation techniques. By concentrating on the vital problem of distinguishing between real and artificially created fingerprints, this study seeks to strengthen detection techniques. In order to accomplish this goal, a brand-new strategy that combines sophisticated machine learning methods—SVM in particular—with a revised application of generalized Benford's law is presented. The accuracy of biometric identification systems might be greatly improved by using this combination strategy.

1.4 Objectives

Based problem statement, three objectives are proposed which are illustrated as follows:

a) To enhance the generalized Benford's law for optically acquired fingerprints and synthetically generated double identity fingerprints.

b) To obtain the DCT coefficients in the spatial domain for the fingerprints.

c) To implement SVM to enhance the accuracy of the system.

1.5 Significance of Research

This study is aimed to highlight features of double identity fingerprints, which can be used to detect the alterations, tampering and fraud in optically generated fingerprints. Therefore, the findings of this study will be helpful in various real-life application, such as e-MRTD fingerprint processing, biometric fingerprint devices and other forensic application of fingerprint analysis.

1.6 Scope of Research

The aim of the research is to detect the alterations for optically acquired fingerprints and synthetically generated double identity fingerprints by applying generalized Benford's law incorporated with support vector machine algorithm, thereby some specific important parameters for defining the scope of research are:-

a) Acquired fingerprints will only be of index finger and thumb, since these are the mostly used approach in majority of the electronic documentation.

b) Fingerprints will be acquired from the students associated with University of Putra Malaysia (UPM).

c) The double identity fingerprints (synthetically generated fingerprints) will be generated by combining two different person's fingerprints from the optically acquired fingerprints.

d) Standard definition of generalized Benford's law is used in order to avoid any confusion.

e) Computational facilities of the research include UPM computational laboratory and personal computer.

f) For Result validation, comparison and evaluation has been realized using internationally recolonized and publicly available data set "FVC2000".

1.7 Organization of Research

Chapter 1 is the prologue to the postulation. It discusses the issue foundation, issue articulation, targets and related research questions.

Chapter 2 presents a survey of the writing, zeroing in on the biometric legal, improvement and ramifications of Benford's regulation as well as a detail conversation into the fingerprints examination.

In Chapter 3 the exploration system has been examined. It incorporates the information assortment strategy, populace and test choice systems, review variable and examination instrument legitimacy and information investigation techniques.

Chapter 4 presents an itemized survey of the information examinations, including distinct insights and inferential investigations. The distinct measurements will be nitty gritty on reaction rate and segment qualities of the review. In the meantime, the pre-test examinations, factor examination, structure condition demonstrating and the numerous mediating tests by Hayes and Scharkow (2013) will be introduced.

Chapter 5 is the last part of this thesis that highlights examination and discusses the future and scholastic meaning of the exploration both in hypothetical and commonsense field. At last, the suggestions and restrictions of the review will likewise be introduced in this section

REFERENCES

Aamo, I., & Caleb, S. F. (2017). On the use of Benford's law to detect JPEG biometric data tampering. *Journal of Information Security, 8*(3), 240-256.

Abdulrahman, A. K., & Ozturk, S. (2019). A novel hybrid DCT and DWT based robust watermarking algorithm for color images. *Multimedia Tools and Applications, 78*(12), 17027-17049.

Abrams, O., Goos, P., & Vandehey, P. (2009). Benford's Law for skewed and truncated distributions. *Insurance: Mathematics and Economics, 44*(2), 166-173.

Ahmed, S. B., Razzak, M. I., & Alhaqbani, B. (2016). The minutiae based latent fingerprint recognition system. In *Proceedings of the International Conference on Internet of Things and Cloud Computing* (pp. 1-9).

Al-ani, M. S., & Al-Aloosi, W. M. (2013). Biometrics fingerprint recognition using discrete cosine transform (DCT). *International Journal of Computer Applications, 69*(6).

Al-Bandawi, H., & Deng, G. (2019). Classification of image distortion based on the generalized Benford's law. *Multimedia Tools and Applications, 78*(18), 25611–25628.

Ali, S., Ganapathi, I., & Prakash, S. (2018). Robust technique for fingerprint template protection. *IET Biometrics, 7*.

Amornraksa, T., & Tachaphetpiboon, S. (2006). Fingerprint recognition using DCT features. *Electronics Letters, 42*(9), 1-7.

Andrea, C., Lucio, B., Mario, M., & Domenico, P. (2019). Newcomb–Benford law and the detection of frauds in international trade. *Proceedings of the National Academy of Sciences, 116*(1), 106–115.

Angelopoulos, C., Bedard, A., Katz, J. O., Karamanis, S., & Parissis, N. (2004). Digital panoramic radiography: An overview. *Seminars in Orthodontics, 10*(3), 194-203.

Ashok, Jammi, Shivashankar, Vaka, & Mudiraj, P. V. G. S. (2018). An overview of biometrics. *International Journal on Computer Science and Engineering*.

Barabesi, L., Cerioli, A., & Perrotta, D. (2021). Forum on Benford's law and statistical methods for the detection of frauds. *Statistical Methods & Applications, 30*, 767-778.

Berger, A., & Hill, T. P. (2015). *An introduction to Benford's law*. Princeton University Press.

Bonettini, N., Bestagini, P., Milani, S., & Tubaro, S. (2021). On the use of Benford’s law to detect GAN-generated images. In *25th International Conference on Pattern Recognition (ICPR), January, 2021* (pp. 5495-5502). IEEE.

Czyżewski, A., Hoffmann, P., Szczuko, P., Kurowski, A., Lech, M., & Szczodrak, M. (2018). Analysis of results of large-scale multimodal biometric identity verification experiment. *IET Biometrics, 8*.

del Acebo, E., & Sbert, M. (2005). Application of Benford's law for digital image forensics. *Journal of Digital Forensic Security, 1*(2), 15-26.

Egghe, L., & Guns, R. (2012). Applications of the generalized law of Benford to informetric data. *Journal of the American Society for Information Science and Technology, 63*(8), 1662-1665.

Feng, J., Jain, A. K., & Ross, A. (2010, August). Detecting altered fingerprints. In *20th International Conference on Pattern Recognition, August, 2010* (pp. 1622-1625).

Gies, S. V., Piquero, N. L., Piquero, A. R., Green, B., & Bobnis, A. (2021). Wild, wild theft: Identity crimes in the digital frontier. *Criminal Justice Policy Review, 32*(6), 592-617.

Gonzalez-Garcia, M. J., & Pastor, M. G. C. (2009). Benford’s law and macroeconomic data quality. *International Monetary Fund*.

Hammad, B. T., Ali, K. M., Al-Rawi, S. S., & Ahmed, I. T. (2012). The use of two transform methods in fingerprints recognition. *Journal of University of Anbar for Pure Science, 6*(2).

Hand, D. J. (2009). *Handbook of statistical methods*. London: Chapman and Hall/CRC.

Heidari, M., James Jr, H., & Uzuner, O. (2021, April). An empirical study of machine learning algorithms for social media bot detection. In *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)* (pp. 1-5). IEEE.

Hildebrandt, M., & Dittmann, J. (2015, March). Benford’s law based detection of latent fingerprint forgeries on the example of artificial sweat printed fingerprints captured by confocal laser scanning microscopes. *Media Watermarking, Security and Forensics, March, 2015*, 9409:77-86. SPIE.

Hürlimann, W. (2015). Benford's law in scientific research. *International Journal of Scientific and Engineering Research, 6*(7), 143-148.

Iorliam, A., orGEM, E., & Shehu, Y. I. (2022). An investigation of Benford's law divergence and machine learning techniques for intra-class separability of fingerprint images. *Gazi University Journal of Science Part A: Engineering and Innovation, 9*(3), 211-224.

Iorliam, A., Ho, A., Poh, N., & Shi, Y. Q. (2014). Do biometric images follow Benford's law? In *2nd International Workshop on Biometrics and Forensics (IWBF)*.

Izenman, A. J. (2008). *Modern multivariate statistical techniques (Vol. 1)*. New York: Springer.

Jain, A. K., & Kumar, A. (2010). Biometrics of next generation: An overview. *Second Generation Biometrics, 12*(1), 2-3.

Li, F., Han, S., Zhang, H., Ding, J., Zhang, J., & Wu, J. (2019, February). Application of Benford's law in data analysis. In *Journal of Physics: Conference Series (Vol. 1168, No. 3, p. 032133)*. IOP Publishing.

Li, W., Guo, Q., Jakubowski, M., & Kelly, M. (2012). A new method for segmenting individual trees from the LiDAR point cloud. *Photogrammetric Engineering & Remote Sensing, 78*(1), 75-84.

Luque, B., & Lacasa, L. (2009). The first-digit frequencies of prime numbers and Riemann zeta zeros. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, 465*(2107), 2197-2216.

Makrushin, A., Kraetzer, C., Neubert, T., & Dittmann, J. (2018, June). Generalized Benford's law for blind detection of morphed face images. In *Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security* (pp. 49-54).

Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). *Handbook of fingerprint recognition (Vol. 2)*. London: Springer.

Miao, D., Tang, Q., & Fu, W. (2007). Fingerprint minutiae extraction based on principal curves. *Pattern Recognition Letters, 28*(16), 2184-2189.

Miller, S. J. (Ed.). (2015). *Benford's law*. Princeton University Press.

Moulton, P., & Liu, F. (2018). A quick and easy approach to financial fraud detection.

Mustafa, W. A., Yazid, H., Khairunizam, W., Jamlos, M. A., Zunaidi, I., Razlan, Z. M., & Shahriman, A. B. (2019, June). Image enhancement based on discrete cosine transforms (DCT) and discrete wavelet transform (DWT): A review. *IOP Conference Series: Materials Science and Engineering, 557*(1), 012027.

Nayak, C., Simon, S. H., Stern, A., Freedman, M., & Sarma, S. D. (2007). Non-Abelian Anyons and Topological Quantum Computation. *Cornell University publication, 1*, 1-73.

Pérez-González, F., Heileman, G. L., & Abdallah, C. T. (2007, September). Benford's law in image processing. In *IEEE International Conference on Image Processing* (pp. I-405). IEEE.

Piciucco, E., Maiorana, E., & Campisi, P. (2017). Biometric fusion for palm-vein-based recognition systems. In *Digital Communication. Towards a Smart and Secure Future Internet: 28th International Tyrrhenian Workshop, TIWDC 2017, Palermo, Italy, September 18-20, 2017, Proceedings 28* (pp. 18-28). Springer International Publishing.

Pietronero, L., Tosatti, E., Tosatti, V., & Vespignani, A. (2001). Explaining the uneven distribution of numbers in nature: The laws of Benford and Zipf. *Physica A: Statistical Mechanics and its Applications, 293*(1-2), 297-304.

Qadir, G., Zhao, X., Ho, A. T., & Casey, M. (2011, May). Image forensic of glare feature for improving image retrieval using Benford's Law. In *2011 IEEE International Symposium of Circuits and Systems (ISCAS)* (pp. 2661-2664). IEEE.

Randa, R., & Reyns, B. W. (2020). The physical and emotional toll of identity theft victimization: A situational and demographic analysis of the National Crime Victimization Survey. *Deviant Behavior, 41*(10), 1290-1304.

Satapathy, G. (2020). Generalized Benford's law for fake fingerprint detection. In 242–246.

Shehu, A. I. O. E. Y. I. (2022). An investigation of Benford's law divergence and machine learning techniques for intra-class separability of fingerprint images.

Scott, P. D., & Fasli, M. (2001). Benford's law: An empirical investigation and a novel explanation. Unpublished manuscript.

Talukder, K. H., & Harada, K. (2010). Haar wavelet based approach for image compression and quality assessment of compressed image. *arXiv preprint arXiv:1010.4084*.

Tan, L. T., de Leeuw PhD, A., Remi Nout, M. D., Simon Duke, M. B. B. S., Lars Fokdal, M. D., Alina Sturdza, M. D., ... & Pötter, R. (2019, July). Image-guided adaptive radiotherapy in cervical cancer. *Seminars in Radiation Oncology, 29*(3), 284-298.

Tiribuzi, M., Pastorelli, M., Valigi, P., & Ricci, E. (2012, November). A multiple kernel learning framework for detecting altered fingerprints. In *Proceedings of the 21st International Conference on Pattern Recognition (ICPR2012)* (pp. 3402-3405). IEEE.

Vishnu, U. (2021). Deepfake detection using Benford's law and distribution variance statistic. *GAN, 8*(10).

Walia, G. S., Jain, G., Bansal, N., & Singh, K. (2019). Adaptive weighted graph approach to generate multimodal cancelable biometric templates. *IEEE Transactions on Information Forensics and Security, 15*, 1945-1958.

Wallace, G. K. (1992). The JPEG still picture compression standard. *IEEE Transactions on Consumer Electronics, 38*(1), xviii-xxxiv.

Waller, A., & Zhao, X. (2017). Using Benford's law divergence and neural networks for classification and source identification of biometric images. *2017, 1*, 88–105.

Yao, H., Mao, F., Qin, C., & Tang, Z. (2021). Dual-JPEG-image reversible data hiding. *Information Sciences, 563*, 130-149.

Yoon, S., Feng, J., & Jain, A. K. (2012). Altered fingerprints: Analysis and detection. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 34*(3), 451-464.