BOOK CHAPTER | *"Fake is Fake – Whether Deep or Shallow"*

Biometric Spoofing and Deepfake Detection

Yaw Amoah-Yeboah
Digital Forensics & Cyber Security Graduate Programme
Department Of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: nanayawamoahyeboah@gmail.com
Phone: +233245399268

ABSTRACT

Biometrics have increasingly become most suited mechanisms for identification and authentication in the use of diverse technologies and systems. However, much they prove to be more robust than other identification and authentication mechanisms, there is also an upsurge with privacy and security concerns. With AI being at the forefront of our technological advancement, it has been to our advantage and also, somehow to our detriment. People are constantly deriving ways to either trick biometric sensors to crack and bypass these authentication protocols. The practice of these nefarious activities ranges from creating fake videos or images for spreading hate, political expediency, embarrassing celebrities etc. This paper seeks to delve to the nooks and crannies of the subject matter to provide a vivid understanding in this regard and also throws light on a few areas where there exists the need for more research.

Keywords: Biometrics, Spoofing, Deepfakes, Deepfake Detection, Africa, Cybersecurity.

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Yaw Amoah-Yeboah (2022): Biometric Spoofing and Deepfake Detection
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 279-284
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P45

1. INTRODUCTION

Biometrics refers to the metrics related to human characteristics and traits. The term biometrics is originated from Greek words, bios and metron, literally meaning —measurement of life (Aleena and Chthra, 2015) [1]. These characteristics can be broadly grouped in three: Biological, Morphological and Behavioral. Amongst these three groups, the Morphological is widely used in most technologies and systems due to its easy accessibility as its forms the structure of the body. The use of these features as deemed as unique and different from person to person provides and concise procedure from telling others apart. As a system penetration, whether allowed or black-hacked have become a negative normalcy, faking biometrics to gain access to systems is one of the attacks. Through this means, intruders produce synthetics like fake silicon fingerprints, iris images or carefully designed face masks. These forms or attacks are referred to as spoofing.

Deepfakes have been some predominant techniques used as biometric spoofs. The term "Deepfake" is derived from "Deep Learning" and "Fake," and it describes specific photorealistic video or image contents created with DL's support. This word had been named after a Reddit user in late in late 2017, who applied deep learning methods for replacing a person's face in pornographic videos using another person's face and created photorealistic fake videos. To generate such counterfeit videos, two neural networks: (i) a generative network and (ii) a discriminative network with a FaceSwap technique are used (Oberoi, 2021; Hui, 2021) [2][3].

1.1 Background of The Study

It is not enough for people to know the prevalence of such a menace. It is important to have participating stakeholders understand the bits and pieces of the narrative. This can be done if there are papers throwing bright light on the topic. This paper also looks at providing where there are lack of researches on which most papers on either biometric spoofing or deepfake detection ignore.

2. RELATED LITERATURE

Biometric Spoofing

Traditional authentication mechanisms which primarily was solely focused on verifying the identity of the user usually relied on what the user has (e.g., phones or security tokens) and or what the user knows (e.g., security questions, PINs, passwords etc.) (Jain, Ross et Prabhakar, 2004) [17]. Due to the researchers' extensive recommendation of using biometrics as the robust means of both identification and authentication purposes (Stan Z, 2009; Chingovska et al 2014, Stallings et al 2012) [4] [5] [6], technologies and systems are breaking the ice to replace the traditional approaches aforementioned. According to Marasco and Sherab (2016) [7], a sensor spoofing attack is *an attempt to circumvent a biometric system by forging the trait of an authorized person and presenting it to the sensor* and most biometric traits can be mimicked or forged with the right knowledge and appreciable effort (Gupta et al, 2014; Matsumoto et al, 2002) [8][9].

Biometric Spoofing Detection

Most researchers through their papers have articulated clearly the use of multimodal biometric authentication procedures as one of the best means to shield against spoofing attacks. Chris Burt (2019) [10], issued a position statement on www.biometricsupdate.com that attackers may still do everything they can to gain access to such systems. This leaves much to be desired. Since then, several investigations and researches have been done on biometric spoofing including the recent documentary on Netflix titled Coded Bias where MIT media researcher Joy Buolamwini's computer science studies uncovered that her face was unrecognizable in many facial recognition programs and she was motivated to find out why.

With many researches done and several ongoing, spoofing detectability has broadly been recommended to be included in the design of every authentication of these systems (Zoppi et al, 2020) [11]. This is so biometric comparisons aren't enough. Certain approaches for anomaly detections like Full Reference Image Quality Measurements (FR IMQs), Distortion Specific

Approaches, Natural Science Statistics Approaches can be used (Aleena and Chthra, 2015) [1]. Also, an AI model can be implemented using the classification technique where artificial feed forward neural networks are used (Arashloo et al, 2017) [12].

Deepfake Detection

With increase in deep learning technology, we have seen advancements in video editing and forgery but there is also positive development in analysing one's interview performance (Pathar et al, 2019) [13]. In current crisis, work from home culture is increasing, people are not meeting face to face which gives them chances for making forgery or deepfaking (identity tampering) in their video stream. In this scenario, recruiters might anticipate for a single application or service that will do the behavioural analysis of a candidate along with forgery detection (Nirnay et al, 2021) [18]. Rossler et al [14] introduced a vast video dataset to train the media forensic and Deepfake detection tools called FaceForensic in March 2018. Several methods and their respected performance have been assessed over time.

To use physical indications, for example, eye blinking as features in detecting Deepfake, Li, et al (2019) [15] proposed a long-term recurrent convolutional network (LRCN). Their method highlighted that the total eye blinking of an individual in Deepfake videos is always lower than in real videos. It can easily extract from the eye areas based on six eye landmarks and use them as features. On the other hand, Rana and Sung (2020) [16] proposed a deep ensemble learning strategy, namely, DeepfakeStack, to detect Deepfake by analysing multiple deep learning models. The concept behind DeepfakeStack is to train a meta-learner to top base-learners with pre-trained experience. It provides an interface for fitting the meta-learners on the base learners' prediction and demonstrates how an ensemble method executes the role of classification.

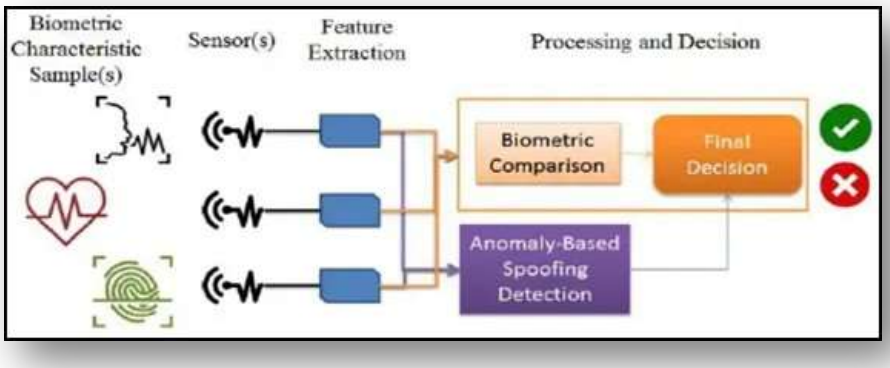

Figure 1: General Runtime support offered by Spoofing Detectability: Spoofing Detection module.

3. IMPLICATIONS FOR ONLINE SAFTEY

By and large, most people, if not all have become a citizen of the digital world. And as Maslow's theory will have it, security is certainly a need in this regard. Online safety has rather become a brazen topic for all and sundry. Deepfakes are not only carried out for financial gains; some are carried out to incite conflicts and cause certain degrees of embarrassment.

This poses a huge risk to users of online resources. It can be used to produce video calls for actions ranging from requesting money for bills to be paid, speaking ill of one's religion to asking for a mob action to be meted out to people (Francesca et al, 2020) [21]. Deepfakes as a cyber-crime is really a cancer. In reality, stopping an attack before it has begun — essentially intelligence gathering — won't always be possible. The scope of this problem is also enormous: the sheer wealth of information available about almost anybody online via social networks makes anybody a viable target of such a crime. As such, the requirement for methods of detecting these crimes, be it deepfakes or biometric spoofing, in situ are more important now than ever

4. CYBERCRIME PROSECUTION/PREVENTION IN AFRICA

Diverse taskforces comprising government, industry and civil groups have been set up to deal with cyber security at the three levels of legal, policy and regulation. Also, Computer Emergency Response Teams (CERTs) have been set up in different East and West African states to fight cybercrime with other collaborative partners such as ITU and EACO.
In West African countries, led by ECOWAS, policies have been initiated in capacity-building, prioritising cybercrime issues and developing networks across the borders as a definite way in fighting cybercrime (Quarshie and Odoom, 2012) [19].

According to the 2019 Symantec report on Cybercrime and Cyber Security Trends in Africa [20], a cursory overview of some countries of Africa in terms of specific criminal law provisions on cybercrime and electronic evidence suggests that by April 2018:

- 11 States seemed to have basic substantive and procedural law provisions in place (Botswana, Cameroon, Côte d'Ivoire, Ghana, Mauritania, Mauritius, Nigeria, Senegal, Tanzania, Uganda and Zambia) although implementing regulations may still be missing in one or the other country.
- A further 12 States seemed to have substantive and procedural law provisions partially in place (Algeria, Benin, Gambia, Kenya, Madagascar, Morocco, Mozambique, Rwanda, South Africa, Sudan, Tunisia and Zimbabwe).

5. RESEARCH FINDINGS

It is abundantly clear from the related literature that a vast amount of research has been done on both biometric spoofing and deepfake detection and its various application in the technology industry cannot be over emphasized. Deep learning is at the forefront of deepfake detection as many datasets provide this approach the appreciable cognitive ability to achieve this feat at a remarkable level. Also, the used of classification models through various neural network algorithms can be one of the surest ways of detecting deepfakes and hence can be emphatically stated that deep learning models are far better and outperform non-deep learning models. The use of multimodal biometric approach for authentication, adds a layer to prevent biometric spoofing. It goes to buttress the eloquent importance of the utilization of the 2FA process for ensuring that the sanctity of any system is protected. One of such multimodal biometric approaches can be facial recognition and the fingerprint.

6. CONCLUSION

This paper threw light on biometrics and the very essence why biometrics are widely used for identification and authentication. It also brought to fore the relatable literature as there is on biometric spoofing and deepfake detection subject matters and what researchers and academics have uncovered. With several approaches to combat the occurrences of these two menaces, it is evidently clear, from the researches done over time that the one surest way of doing this is through the implementation of deep learning models

7. RECCOMENDATION FOR POLICY AND PRACTICE

This paper recommends the following for best practices in circumventing biometric spoofs and detecting deepfakes:

1. Implementing biometric authentication systems, biometric comparisons are not enough; liveness detection algorithms should also be incorporated.

2. Biometrics should only answer the question "WHO ARE YOU" in any authentication protocol and actions to the statement "PROVE IT" should be through something you have or something you know. In cases where these cannot be implemented, multimodal biometrics can be employed.
3. Deep Learning applications on neural network models are the surest way of detecting deepfakes. Refined and new datasets must be added to the old to improve the model's predictability index or score.

8. DIRECTION FOR FUTURE WORKS

This paper provides the basis for understanding the bits and pieces of biometric spoofing and deepfake detection. There are limitations to this study. This includes the limited resources of relatable literature and a considerable expansion on the way and manner different neural network models can be implemented to detect deepfakes. Further research could be undertaken on a comparison on the various neural network models. An empirical study is also needed to investigate the factors of successful implementation.

REFERENCES

1. Aleena T.S, Chithra K, "Spoofing Protection for Biometric Systems", IJSTE Volume 1, Issue 10/060, pp 299-302, 2015.
2. G. Oberoi, "Exploring DeepFakes," https://goberoi.com/exploring-deepfakes-20c9947c22d9, last accessed: 2021/1/4
3. J. Hui, "How deep learning fakes videos (Deepfake) and how to detect it," https://medium.com/how-deep-learning-fakes-videos-deepfakes-and-how-to-detect-it-c0b50fbf7cb9, last accessed: 2021/1/4
4. Li, Stan Z. Encyclopedia of Biometrics: I-Z. Vol. 2. Springer Science & Business Media, 2009

5. I. Chingovska, A. Anjos, and S. Marcel, “On the effectiveness of local binary patterns in face anti-spoofing”, in Proc. IEEE Int. Conf. Biometric Special Interest Group, Sep. 2012, pp. 1– 7
6. Stallings, W., Brown, L., Bauer, M. D., & Bhattacharjee, A. K. (2012). Computer security: principles and practice (pp.978-0). Upper Saddle River, NJ, USA: Pearson Education
7. Marasco, E., Shehab, M., & Cukic, B. (2016, October). A Methodology for Prevention of Biometric Presentation Attacks. In 2016 Seventh Latin-American Symposium on Dependable Computing (LADC) (pp. 9-14). IEEE
8. Gupta, P., Behera, S., Vatsa, M., & Singh, R. (2014, August). On iris spoofing using print attack. In 2014 22nd International Conference on Pattern Recognition (pp. 1681-1686). IEEE
9. Matsumoto, T., Matsumoto, H., Yamada, K., and Hoshino, S. Impact of artificial "gummy" fingers on fingerprint systems. In Proc. of SPIE Opt. Sec. Counterfeit Deterrence Tech. IV, pages 275-289, 2002
10. C Burt, Spoof attacks top this week biometrics and digital ID news (2019) [Online] biometricupdate.com/201911/spoof-attacks-top-this-weeks-biometrics-and-digital-id-news
11. Zoppi, T., Ceccarelli, A., Salani, L., & Bondavalli, A. (2020). On the educated selection of unsupervised algorithms via attacks and anomaly classes. Journal of Information Security and Applications, 52, 102474
12. Arashloo, Shervin Rahimzadeh, Josef Kittler, and William Christmas. "An anomaly detection approach to face spoofing detection: A new formulation and evaluation protocol." IEEE access 5 (2017): 13868-13882
13. Rohit Pathar; Abhishek Adivarekar;Arti Mishra; Anushree Deshmukh, “Human Emotion Recognition using Convolutional Neural Network in Real Time”, Chennai, India, ICIICT, 2019
14. Andreas Rössler, Davide Cozzolino, Luisa Verdoliva, Christian Riess, Justus Thies, Matthias Nießner,“ FaceForensics++: Learning to detect Manipulated Facial Images”, New York, United States, arXiv.org, 2019
15. Y. Li and S. Lyu, “Exposing Deepfake videos by detecting face warping artifacts,” in IEEE CVPR Workshops, 2019
16. S. Rana, M Nobi, B Murali and A.H. Sung, “Deepfake Detection: A Systematic Literature Review”, IEEE Access, 2020.
17. Jain AK, Ross A, Prabhakar S (2004) An introduction to biometric recognition. Circuits and Systems for Video Technology. IEEE Transactions 14: 4-20.
18. Khajuria, N., Chavadekar, R., Dhote, A., & Chavhan, S. (2021). Forensic Tool for Deepfake Detection and Profile Analysis.
19. Osborn Quarshie, H., Quarshie, H. O., & Odoom, A. M.-. (2012). Fighting Cybercrime in Africa. Computer Science and Engineering, 2(6), 98–100. https://doi.org/10.5923/J.COMPUTER.20120206.03
20. Moctar Yedaly, Souhila Amazouz, Auguste K. Yankey (2019), Cybercrime & CyberSecurity Trends In Africa, Symnatec Corporation