A Taxonomy on Biometric Security and Its Applications

Aditya Bakshi and Sunanda Gupta

Abstract

In modern times, pioneering works in the field of face recognition have seen the new development in biometric technology. A greater spectrum with modalities such as iris, face, fingerprints, signature, or hand has been largely deployed, and highly accurate systems using these modalities have been designed too. Recently, a critical issue has been addressed that affects the path of technological evolution in biometrics, i.e., spoofing, which is very resistant to biometric technology through external attacks. Spoofing is different from other IT security solutions as it is a purely biometric vulnerability. With the help of a sensor, an illegitimate user fools the biometric system by treating it as a genuine one using a synthetic forged version refers to as spoofing. The researchers and developers of the biometric community have worked a lot in suggesting and emerging different security methods. The main objective of this paper is to deliver an inclusive outline of the emerging field of anti-spoofing that has been carried out over the last decade. The work covers concepts, procedures, or advanced techniques that largely positioned face modality and also explains the future aspect in the field of biometric security.

Keywords

Biometrics • Anti-spoofing • Face • Attacks • Security

1 Introduction

For the last 40 years, revolutionary works on the face recognition system (i.e., automated system) have been done (Bledsoe, 1964; Kelly, 1970; Davis et al., 1952), and for developing an accurate biometric security system, a continuous progress has been done. Biometric traits such as iris, voice, and fingerprints modalities have been used for detection purposes nowadays. Every technology has its own time to prove its worth. For improving the performance of biometric systems (Jain et al., 2006), there are many areas such as image processing, computer vision, and pattern recognition in which researchers from different fields work for designing innovative new techniques. For example, the new security biometric paradigm can be designed as "forget about cards and passwords, you are your own key" (Guardian, 2013). Forensics, border and access control, surveillance, or online commerce are the diverse activities in biometrics too.

For the improvement in the recognition performance and scenario of constant expansion, a new area of concern is rising in biometric technology. The resilience against outside threats in biometrics has been developed that possess great challenges that have draws an attention by researchers. It is believed that airports, laptops, or mobile phones are not only examples of biometric security, but in day-to-day life, users become more familiar with this security mechanism. Therefore, in each year the deployment of biometric systems keeps growing as the general public easily understands the security weaknesses in their systems. Apart from the face, there are other biometric systems fingerprints or irises that fool users too because it is very easy to get the detailed guidance with tutorial videos on creating fake masks.

Many real operational applications have been designed as attacks cannot be restricted in the theoretical or academic sphere. The prime example for biometric security is new iPhone 5S fingerprint reader which is vulnerable to many attacks (Guardian, 2013). Other attacks such as face

A. Bakshi (✉) · S. Gupta
Department of Computer Science and Engineering, Shri Mata Vaishno Devi University, J and K, Katra, India
e-mail: addybakshi@gmail.com

S. Gupta
e-mail: sunanda.gupta@smvdu.ac.in

P. K. Singh et al. (eds.), *Innovations in Information and Communication Technologies (IICT-2020)*,
Advances in Science, Technology & Innovation,
https://doi.org/10.1007/978-3-030-66218-9_24

recognition (Register, 2008; The CNN, 2010) attempt from hacking groups, from actual illegal cases (Tech Crunch, 2009), or even from security-specific conferences (Duc and Minh, 2009) where live demonstrations have been shown by the user for biometric security.

In literature, spoofing is well explained with low-cost and tech features publically which are shown in different ways, but these features are not vulnerable in all biometric modalities (Rasa, 2013; Galbally et al., 2011; 2011; Matsumo et al., 2002; Hennebert et al., 2007; Mjaaland et al., 2010; Chen et al., 2005; Alegre et al., 2012; Bin et al.. 2009; Akhtar et al., 2012). Therefore, for detection, necessary countermeasures can be incorporate to such an extent that systems are robust to these attacks (Tome et al., 2014). However, examples like encryption, digital signature, or watermarking are not effective in today's scenario as imitating these threats is not easy in security mechanisms. As a result, for detecting biometric systems, i.e., differentiate between fake and real samples, precise countermeasures have been required. A significant amount of research has been conducted in biometric security that is ensured in good publications in international journals and conferences. With the development of new anti-spoofing algorithms and systems, researchers make the system harmless for real-time applications. Face, fingerprints, and iris are the most popular and mature modalities that are the most of spoofing mechanism. At this moment, to explain the strong picture and advancements, a diverse and dedicated work in the anti-spoofing field is need for an hour today.

2 Background Study and Literature

The basic terminology used in the case for spoofing has not reached a general agreement by the biometric community. Therefore, lots of ongoing efforts and proposals have been explained for combined and consistent classification for vulnerabilities in spoofing. The ability of an illegitimate user that fools the biometric system and recognize as a genuine user by presenting in front of the sensor as a synthetic forged version of the original biometric user. These types of attacks are referred to as direct attacks. The process of impersonating different users to make a novel unpretentious personality using an artificial trait is referred to as spoofing.

Different scenarios for spoofing attacks that have been conceived on the type of biometric system are as follows (i) Verification system: In the best mutual incident, a duplicate copy of the true user is presented at the time of the authentication part. The registered actual pattern of the real user is acquired and matched in this phase. (ii) A closed set of Verification system/Identification system: Spoofing can be performed by producing a new identity for actual users that can be used by other users to enter the system later at the enrollment stage too. (iii) Identification system in open set: Using the spoofing artifact, a new identity has been created in a watch list to avoid further loss of information.

2.1 State-Of-The-Art in Face Anti-Spoofing

The principal idea for selecting the face biometric as anti-spoofing survey is following:

- The group, i.e., International Biometric Group (IBG), tells face is the most organized biometric in terms of market quota right after at world level after fingerprints (International Biometrics Group, 2008). The most important ID documents such as pictures on biometric passport (Gipp et al., 2007) or national ID cards (2013). DNI Electronico, 2013) adopted the same pattern. The highest potential biometric traits nowadays are faces that impact the financial and societal point of view.
- Also very large amount of spoofing related published work has been conducted for face recognition together with the fingerprint trait.

In this section, common face spoofing techniques summary is presented. After that, a review of diverse mechanisms has been presented against spoofing security.

The three types of anti-spoofing techniques with biometric system block diagram is shown in Fig. 1.

2.1.1 Face Spoofing

In an enormous majority of recognized societies, the use of facial masks has been recognized for centuries. The trends to change one's self physical appearance are the most modern version used by the attackers. For example, the use of silicon artifacts or other methods is becoming more and more popular these days. These can be easily performed or implemented due to the availability of progressive expertise, its reasonable cost, and its swiftness. Although, many algorithms have been developed for robust facial surgery changes (Aggarwal et al., 2012; Sun et al., 2013). But, the problem of recognizing a person in automatic face authentication systems (Singh et al., 2010) is still an open challenge. Even, by wearing regular make-up (Dantcheva et al., 2013), face-based biometric systems may be outwitted. The three main types of attacks that have been used by the attackers to carry out spoofing attacks:

Photograph Attacks: In a photograph attack, a photograph of the genuine user is presented in front of the recognition system for attempting fraudulent access. The attacker captures a photograph of the user by himself using a digital camera. But most of the time, the attacker retrieved the user picture from the Internet which was taken by the attacker

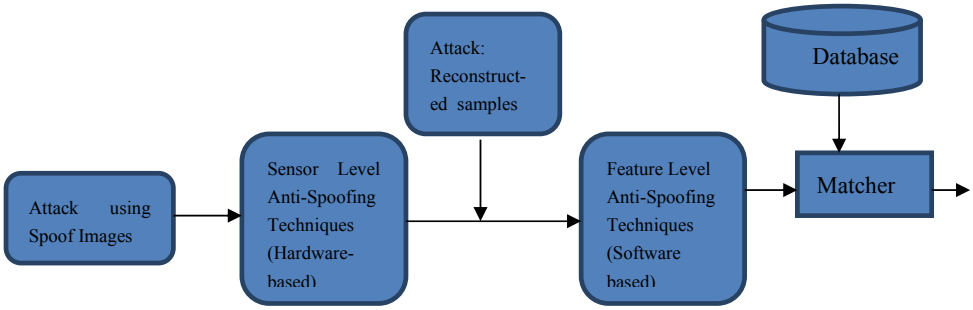

Fig. 1 Block diagram of the biometric system with types (three) of anti-spoofing techniques

using a digital camera, or even retrieved from popular online social networks available today (Li et al., 2014). The image used for attack purposes may be from digital-photograph attacks (i.e., use of a digital device such as notepad and mobiles) or attacks from printed on a paper (Galbally, 2010a; Anjos and Marcel , 2011a). Photographic masks are the more innovative type of photograph attack these days. In these masks, eyes and mouth have been shown very clear as shown in high-resolution printed photographs. These help the imposters to attack on assured movements in the face such as eye blinking can be copied easily.

Video Attacks. Replay attacks are the other name of video attacks. Video attacks are a version of the spoofed photographs in a more sophisticated way. In this case, the attacker plays a video of the real client using mobiles, notebook, or laptop (Chingovska et al., 2012; Zhang et al., 2012) but does not use a still image. Furthermore, the development in face spoofing attacks is appeared frequently and detection is very difficult.

Mask Attacks. Mask attacks use 3D disguise of the real client's face for spoofing mechanism that increases the difficulty for accurate countermeasures. Moreover, the use of depth clues for finding a solution in the other two types of attacks becomes inefficient against a complete 3D face configuration. Although, it is a very great idea that has been circulating easily in the biometric system by copying the face mask of a different user but still (Kim et al., 2009) these attacks are not that much common than the previous two categories. With the attainment of the mask-specific datasets (Erdogmus and Marcel, 2013a; Kose and Dugelay, 2013), face-mask spoofing has been used thoroughly with different materials and sizes of masks (Erdogmus and Marcel, 2014; Erdogmus and Marcel, 2013b).

In today's generation, large databases of realistic masks posed great technical and economic difficulty that addressed the scarcity of research work in the field of face spoofing. But, recent emergence in most of the companies where 3D face models may be found for a rational value has lessened its difficulty.

2.1.2 Face Anti-spoofing

A physical insurgency under the ages of the TABULA RASA European project engrossed on the study of spoofing attacks in biometric systems. In the last three years, lots of experiments have been done in this technology which was out of the box for more than a decade. The achievement and circulation of numerous face spoofing databases motivate the researchers for the development of new security mechanisms against these attacks. For effective countermeasures, more emphasis is on the designing of a robust system, not on topics for data procurement which attracts the researchers (Li et al., 2014; Chingovska et al., 2012; Zhang et al., 2012; Kose and Dugelay 2013). This is the main reason that lots of recent publications were there for numerous methods in 2D face anti-spoofing. For face recognition systems (i.e., 3D structure) against attacks on mask, artifacts are a capable study for new security algorithms which is also initiated.

In the next sections, a review of face anti-spoofing and its challenges have been addressed. It is generally witnessed that when anti-spoofing approaches are verified under different circumstances for which they were considered, loss of accuracy is a significant issue across databases. The weaknesses of such methods are used by the strengths of others (Chingovska, et al., 2013) (Chakka et al., 2011) but by mixing many balancing algorithms usually give great results. Also, for the detection of video-based attacks, some liveness detection systems have been considered using the face analysis and context-based analysis with head poses of 2D images (Marsico et al., 2012; Wang et al., 2013). From different acquired samples, non-facial information has many advantages such as scenes with motion features, (Kim et al., 2011) recapturing process used for estimating the noise in an image (Silva Pinto et al., 2012), use of popular local binary patterns (LBP) for sequential evidence existing in series of videos (Freitas Pereira et al., 2012), etc. Table I shows the attacks on the face biometrics investigated.

Saha et al., (2012) presented a hardware-based computer vision algorithm using the Xilinx hardware development platform as well Mathworks Matlab and corresponding transmission crypto channel between multiple FPGA platforms for developing a hardware-software co-design

environment. As designs of application-specific integrated circuits (ASICs) and digital signal processors (DSP) have been successfully implemented by the engineers, but field programmable gate array (FPGA) combining the key advantages of ASICs and DSPs is a very powerful hardware device for rapid prototyping. Asaduzzaman, Abu, et al.. (Asaduzzaman et al.. 2015) proposed a CUDA-accelerated image processing method for loading of the pixel's bytes in a one-dimensional array with length equal to matrix width * matrix height * bytes per pixel which is the key step of an algorithm. Kaur et al.. (2012) presented distributed image processing algorithms using dynamic data for a particular application under various distributed environments. The performance analyses can also be done for a distributed image processing framework through distributed control. Akhtar, Zahid, et al., (2012) proposed robust multi-modal systems with serial and parallel fusion modes and their comparative analysis for spoofing attacks. As evaluation for the robust multi-modal system has not yet been investigated for serial fusion mode so for empirical investigation for finding the different vulnerability for real spoofing attacks.

3 Applications in Biometric Security

The exploitation of face videos (i.e., both spatial and temporal information) has shown very good results by dynamic anti-spoofing schemes. However, examples like applications for passport design, etc., these schemes cannot give fruitful results as there is only one face image of the user is present. Moreover, even getting the high accuracy for facial analysis with nonconsecutive frames, there are scenarios where detection cannot be done easily such as applications on video surveillance. This section explains different spoofing applications which are used by the illegitimate user for accessing the system in the field of biometric security.

One of the applications explained by the researchers is the physical entrance of the Indian currency. The economy of each country including India is affected by fake currency detection which is a very serious issue. It can be implemented either by changing its physical appearance or use of chemical properties (Rathee 2016). One of the security features of Indian currency is its authentication, but capturing various features such as security thread, intaglio printing

Table 1 Different face biometrics attacks

References	Feature type	Approach	Database
Galbally 2010b)	Face	Proposed a two face recognition systems for indirect attacks for testing the vulnerabilities based on Bayesian adaption using a hill-climbing attack algorithm	XM2VTS database
Kapur and Baregar 2013)	Face + SIFT	Presented the security of an image using image steganography and image stitching that can be achieved by using any electronic mode. Using k nearest method, parts are stitched together. The quality of the image is greatly improved by implementing SIFT features	Live database
Anjos and Marcel 2011b)	Face + Motion	The author presented a novel technique for spoofed identities such as photographs those by-pass 2D face recognition systems very easily. So, to find out the solution and designing a protocol, a motion-based algorithm that detects correlations between the scene context and the person's head movements is implemented	PRINT-ATTACK database
Chakka 2011)	Face	The author explained the competition of 2D face recognition systems for spoof identities, and a unique evaluation method is used by comparing the performance between different advanced algorithms on the similar database	Mask database
Hemalatha and Wahi 2014)	Face + liveness detection	Author presented a face recognition system against spoof attacks This paper explained the outline to the face biometric system, face spoofing attacks, and liveness detection that is helpful for identification (authentication) application	Live database
Pan 2011)	Face + color texture	Proposed a generalization of color texture-based face anti-spoofing mechanism for finding a robust face PAD solution for attack-specific and countermeasures based solely on color texture analysis	Replay attack database
Boulkenafet et al., 2018)	Face + eye blinking	Proposed an anti-spoofing face recognition system against photograph attack and a real-time liveness detection approach by explaining impulsive eye blinks which is a non-intrusive mechanism. The proposed model shows the effectiveness of our approach and after an extensive set of experimentation, it presents how it outperforms the cascaded Adaboost and HMM in the task of eye blink detection	Blinking video database

(continued)

Table 1 (continued)

References	Feature type	Approach	Database
Pan 2007)	Face	Proposed a continuous authentication mechanism for smartphone users using facial attributes. The author uses binary attribute classifiers for training that provides compact visual descriptions of faces	MOBIO and AA01
Samangouei et al. 2017)	Face + texture	Proposed countermeasures in the mask database that developed using both 2D data (texture images) and 3D data (3D scans). Moreover, the baseline technique for both 2D and 3D face recognition has already been used for analysis of mask spoofing	Mask database
Goswami and `Face recognition captcha.', 2012)	Face	Explored a face recognition-based CAPTCHA for potential high-level attacks. To understand the CAPTCHA, the complex background is inserted that can be placed with the same subject where clients can effectively discover one set of human face pictures	AR face database
Yu 2019)	Face + kernel features	Proposed a diffusion-based kernel matrix model for face liveness detection. As different verification systems and face recognition are vulnerable to video spoofing attacks, the proposed model uses anisotropic diffusion in a video to enhance the edges of each frame and extract the video features using diffusion kernel (DK) features	Replay attack database
Nguyen 2008)	Face	Proposed an automatic layer extraction method for face synthesis and editing and its applications. The human faces can be viewed as a composition of several different layers with different categories of objects too. The proposed method shows that the tasks such as beard removal (virtual shaving), beard synthesis, and beard transfer are explained very clearly	Live database
Galbally and `Hill-climbing attack to an eigenface-based face verification system.', 2009)	Face	Proposed an evaluation of Eigen face-based verification system using the XM2VTS database. The proposed hill-climbing attack algorithm of an Eigen face-based approach with Bayesian adaption is used to test the vulnerability for face recognition	XM2VTS database

(RBI logo), and documentation mark, different image processing procedures have been applied. So, the conclusive score of all the three features has been bonded to differentiate between actual and false currencies that make the system more robust and accurate.

Another application is also related to currency, i.e., counterfeit currency. Because of the rapid adoption and adaptation, forgers are becoming tougher to find (Ahmed 2014). So, one of the effective methods in terms of cost, reliability, and accuracy is easily available for the detection of fake user. This can be achieved by extracting existing features of banknotes such as micro-printing, optically variable ink (OVI), water-mark, iridescent ink, security thread, and ultraviolet lines using OCR (Optical Character recognition), contour analysis, face recognition, speeded up robust features (SURF) and Canny Edge & Hough transformation algorithm of Open CV.

The other application is protection against the use of low entropy passwords in consumer storage devices. Also, all the stored confidential information from a removable storage device can be easily retrieved by stolen passwords from the devices (Amin 2017). So, a common verification and key concession protocol have been implemented to protect the confidential information in the device of the user. An algorithm, i.e., Burrows-Abadi- Needham (BAN) logic is used for the security analysis.

Recently, the research and development community has gained considerable attention in the field of fog and mobile edge computing. The problems of security and privacy of biometric can be solved using edge computing that plays a vital role in saving critical private information. The information of software content that is easy to copy and distributed has been solved using zero-watermarking (Abdul et al., 2017). Also, data can be secured with visual cryptography that can be shared from multiple sources. So, a security mechanism for biometric face images has been developed which adversely impacts the visual quality of the image.

4 Future Scope

The problems and challenges that have been addressed in biometrics could help other researchers to work in this field. Although, detecting the recent developments and consequences from the different future models would show a path for different in future directions.

First, the absence of interoperability is the major shortcomings in existing anti-spoofing techniques that need to be examined in the future across databases. However, many algorithms have been designed to attain accuracy nearby 100% but when the difficult dataset is transformed their performance drops significantly. Therefore, it is clear that no superior anti-spoofing technique is designed to date. The results show a curious message that may be learned: No existing anti-spoofing system. The environment of the attack situations and acquisition settings has been changed from one particular protection method to another. Therefore, best fusion approaches have to be developed using liveness detection techniques to achieve greater performance over diverse spoofing information (Freitas Pereira et al., 2013; Galbally et al., 2014).

Second, the equilibrium between safety and suitability is another theoretical problem in spoofing field. The most reason for deploying and developing biometrics is its security dimension that cannot be denied. Fields related to forensics should also be considered that could impact the spoofing. It is also possible to include temporal information in systems that are working with face videos. Video attacks can also be used for video attack measures.

Renowned Sherlock Holme's short stories are prime evidence in fake fingerprint forensic. The possibilities of spoofing attacks in the coming future can be predicted effectively. In years to come, detection of spoofing can gain a lot of significance and assets.

5 Conclusion

Nowadays, in the next-generation system, the role of biometrics and its technologies has improved severely. So, a need for securing the system is an important aspect. It might be identified that in spoofing detection, lots of work and advancements have been done, but evolution of different offensive practices would make spoofing attacks more and more sophisticated. In this paper, a different aspect of biometric security has been explained with a background and literature survey for spoofing detection. Lots of application and future aspects of biometric security have also been covered. This will help to motivate the researchers to work in this field that helps the user to differentiate between fake and real users. So, protection against direct attacks is still a big challenge that energizes the new generation to enhance the work in designing secure biometric systems in the coming years.

References

Bledsoe W.W. (1964). *The model method in facial recognition*. Panoramic Res., Inc., Palo Alto, CA, USA, Tech. Rep. PRI:15,

Kelly, M.D. (1970). Visual identification of people by computer, Stanford AI Project, Stanford, CA, USA, Tech. Rep. AI-130.

Davis, K. H., Biddulph, R., & Balashek, S. (1952). Automatic recognition of spoken digits. *J. Acoust. Soc. Amer., 24*(6), 637642.

Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: A tool for information security. *IEEE Transformation Information Forensics Security, 1*(2), 125143.

The Guardian. (2013). *iPhone 5S Fingerprint Sensor Hacked by Germany's Chaos Computer Club*. (Online). Available: www.theguardian.com/technology/2013/sep/22/apple-iphone-ngerprint-scanner-hacked.

The Register. (2008). *Get Your German Interior Minister's Fingerprint Here*. (Online). Available: https://www.theregister.co.uk/2008/03/30/german_interior_minister_ngerprint_appropriated/

The CNN. (2010). *Man in Disguise Boards International Flight*. (Online). Available: https://edition.cnn.com/2010/WORLD/americas/11/04/canada.disguised.passenger/PRA Laboratory. (2013).

Fingerprint Spoofing Challenge, YouTube. (Online). Available: https://www.youtube.com/watch?v=vr0FmvmWQmM.

Discovery Channel. (2011). *Mythbusters: Fingerprints Cannot be Busted, YouTube*. (Online). https://www.youtube.com/watch?v=3Hji3kp-i9kChaos Computer Club Berlin. (2013).

Tech Crunch. (2009). *Woman Uses Tape to Trick Biometric Airport Fingerprint Scan*. (Online). Available: https://techcrunch.com/2009/01/02/woman-uses-tape-to-trick-biometric-airport-ngerprint-scan/ BBC News. (2005).

Malaysia Car Thieves Steal Finger. (Online). Available: https://news.bbc.co.uk/2/hi/asia-pacic/4396831.stm.

Duc, N. M., Minh, B. Q. (2009). *Your Face is NOT Your Password*. Face Authentication Bypassing Lenovo, Asus,Toshiba. San Francisco, CA, USA: Black Hat.

Tabula, R. (2013). *Tabula Rasa Spoofing Challenge*. (Online). Available: https://www.tabularasa-euproject.org/evaluations/tabula-rasaspoong-challenge-2013.

Galbally, J., Fierrez, J., Alonso-Fernandez, F., & Martinez-Diaz, M. (2011). Evaluation of direct attacks to fingerprint verification systems. *Telecommunication System, 47*(3–4), 243–254.

Galbally, J., et al. (2010a). An evaluation of direct attacks using fake fingers generated from ISO templates. *Pattern Recognition Letters, 31*(8), 725732.

Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S. (2002). Impact of artificial gummy fingers on ngerprint systems. In *Proceedings on SPIE, Optical Security Counterfeit Deterrence Technology IV*, vol. 4677, pp. 275–289.

Hennebert, J., Loeffel, R., Humm, A., Ingold, R. (2007). A new forgery scenario based on regaining dynamics of signature. In *Proceedings IAPR International Conference Biometrics (ICB)*, pp. 366–375.

Mjaaland, B.B., Bours, P., Gligoroski, P. (2010). Walk the walk: Attacking gait biometrics by imitation. In *Proceedings 13th International Conference Information Security (ISC)*, 2010, pp. 361–380.

Chen, H., Valizadegan, H., Jackson, C., Soltysiak, S., Jain, A.K. (2005). Fake hands: Spoong hand geometry systems. In *Proceedings Biometrics Consortium Conference (BCC)*.

Alegre, F., Vipperla, R., Evans, N., Fauve, B. (2012). On the vulnerability of automatic speaker recognition to spoofing attacks with artificial signals. In *Proceedings European Signal Processing Conference (EUSIPCO)*, pp. 3640.

Bin, Q., Jian-Fei, P., Guang-Zhong, C., Ge-Guo, D. (2009). The anti-spoofing study of vein identification system. In *Proceedings International Conference Computer Intelligence Security (ICCIS)*, pp. 357360.

Akhtar, Z., Fumera, G., Marcialis, G.L., Roli, F. (2012). Evaluation of serial and parallel multi biometric systems under spoofing attacks. In *Proceedings IEEE 5th International Conference Biometrics, Theory, Application System (BTAS)*, pp. 287–288.

Tome, P., Vanoni, M., & Marcel, S. (2014). *"On the vulnerability of finger vein recognition to spoofing", in Proc."* Biometrics Special Interest Group (BIOSIG): IEEE Int. Conf.

IBG. (2008). Biometrics market and industry report 2009–2014. *International Biometrics Group*, Virginia, USA, Tech. Rep.

Gipp, B., Beel, J., & Rössling, I. (2007). *ePassport: The World's New Electronic Passport*. Scotts Valley, CA, USA: CreateSpace.

Ministerio del Interior, Gobierno de Espana. (2013).DNI Electronico.

Aggarwal, G., Biswas, S., Flynn, P.J., Bowyer, K.W. (2012). A sparse representation approach to face matching across plastic surgery,'' in Proc. Workshop Appl. Comput. Vis. (WACV), pp. 118–119.

Sun, Y. Tistarelli, M., Maltoni, D. (2013). Structural similarity based image quality map for face recognition across plastic surgery,'' in Proc. IEEE Conf. Biometrics, Theory, Appl. Syst. (BTAS), Sep./ Oct. 2013, pp. 1–8.

Singh, R., Vatsa, M., Bhatt, H. S., Bharadwaj, S., Noore, A., & Nooreyezdan, S. S. (Sep. 2010). Plastic surgery: A new dimension to face recognition. *IEEE Trans. Inf. Forensics Security, 5*(3), 441–448.

Dantcheva, A., Chen, C., Ross, A. (2013). Can facial cosmetics affect the matching accuracy of face recognition systems? In *Proceedings IEEE 5th International Conference Biometrics, Theory, Applicaion Systems (BTAS)*, pp. 391–398.

Li, Y., Xu, K., Yan, Q., Li, Y., Deng, R.H. (2014). Understanding OSN-based facial disclosure against face authentication systems. In *Proceedings ACM Asia Symposium Information Computer Communication Security (ASIACCS)*, pp. 413–424.

Anjos, A., Marcel, S. (2011). Counter-measures to photo attacks in face recognition: A public database and a baseline. In *Proceedings IEEE International Joint Conference Biometrics (IJCB)*, pp. 1–7.

Chingovska, I., Anjos, A., Marcel, S. (2012). On the effectiveness of local binary patterns in face anti-spoong. In *Proceedings IEEE International Conference Biometrics Special Interest Group (BIOSIG)*, pp. 1–7.

Zhang, Z., Yan, J., Liu, S., Lei, Z., Yi, D., Li, S.Z. (2012). A face antispoofing database with diverse attacks. In *Proceedings of IAPR International Conference on Biometrics (ICB)*, pp. 26–31.

Kim, Y., Na, J., Yoon, S., & Yi, J. (2009). Masked fake face detection using radiance measurements. *J. Opt. Soc. Amer., 26*(4), 760–766.

Erdogmus, N., Marcel, S. (2013). Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect. In *Proceedings IEEE Biometrics, Theory, Application System (BTAS)*, pp. 1–6.

Kose, N., Dugelay, J.L. (2013). On the vulnerability of face recognition systems to spoong mask attacks. In *Proceedings IEEE International Conference Acoustics Speech Signal Process. (ICASSP)*, pp. 2357–2361.

Erdogmus, N., & Marcel, S. (Jul. 2014). Spoong face recognition with 3D masks. *IEEE Trans. Inf. Forensics Security, 9*(7), 1084–1097.

Erdogmus, N., Marcel, S. (2013). Spoong 2D face recognition systems with 3D masks. In *Proceedings International Conference Biometrics Special Interest Group (BIOSIG)*, pp. 1–8.

Chingovska, I., et al. (2013). The 2nd competition on counter measures to 2D face spoofing attacks. In *Proceedings IAPR International Conference Biometrics (ICB)*, pp. 1–6.

Chakka, M.M., et al. (2011). Competition on counter measures to 2-D facial spoofing attacks. In *Proceedings IEEE International Joint Conference Biometrics (IJCB)*, pp. 1–6.

de Marsico, M. M., Nappi, D. R. , Dugelay, J. (2012). Moving face spoofing detection via 3D projective invariants. In *Proceedings IEEE International Conference Biometrics (ICB)*, pp. 73–78.

Wang, T., Yang, J., Lei, Z., Liao, S., Li, S.Z. (2013). Face liveness detection using 3D structure recovered from a single camera. In *Proceedings IEEE/IAPR International Conference Biometrics (ICB)*, pp. 1–6.

Kim, Y., Yoo, J.H., Choi, K. (2011). A motion and similarity-based fake detection method for biometric face recognition systems. In *Proceedings IEEE International Conference Consumer Electronics (ICCE)*, pp. 171–172.

da Silva Pinto, A., Pedrini, H., Schwartz, W., Rocha, A. (2012). Video based face spoofing detection through visual rhythm analysis. In *Proceedings 25th Conference Graphics Patterns Images (SIBGRAPI)*, pp. 221–228.

de Freitas Pereira T., Anjos, A., de Martino, J.M., Marcel, S. (2012). LBP-TOP based countermeasure against face spoofing attacks. In *Proceedings International Workshop Computer Vis.ion Local Binary Pattern Variants (ACCV)*,pp. 1–12.

Saha, Sangeet, Satyabrata Maity, and Suman Sau. "A brief experience on journey through hardware developments for image processing and its applications on Cryptography." arXiv preprint arXiv:1212.6303 (2012).

Asaduzzaman, A., Martinez, A., Sepehri, A. (2015). A time-efficient image processing algorithm for multicore/manycore parallel computing. SoutheastCon 2015. IEEE.

Kaur, S., Manisha, B. *Review Paper on Image Processing in Distributed Environment*.

Akhtar, Z. (2012). Evaluation of serial and parallel multibiometric systems under spoofing attacks. In *2012 IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS). IEEE.*

Galbally, J. (2010). On the vulnerability of face verification systems to hill-climbing attacks. *Pattern Recognition, 43*(3), 1027–1038.

Kapur, J., & Baregar, A. J. (2013). Security using image processing. *International Journal of Managing Information Technology (IJMIT), 5*(2), 13–21.

Anjos, A., Sébastien, M. (2011). Counter-measures to photo attacks in face recognition: a public database and a baseline. In *2011 international joint conference on Biometrics (IJCB).* IEEE.

Murali Mohan, C. (2011). Competition on counter measures to 2-d facial spoofing attacks. In *2011 International Joint Conference on Biometrics (IJCB). IEEE.*

Hemalatha, S., Amitabh, W. (2014). A study of liveness detection in face biometric systems. *International Journal of Computer Applications, 91*(1).

Pan, G. (2011). Monocular camera-based face liveness detection by combining eyeblink and scene context. *Telecommunication Systems, 47*(3–4), 215–225.

Boulkenafet, Z., Komulainen, J., & Hadid, A. (2018). On the generalization of color texture-based face anti-spoofing. *Image and Vision Computing, 77,* 1–9.

Pan, G. (2007). Eyeblink-based anti-spoofing in face recognition from a generic webcamera. In *2007 IEEE 11th International Conference on Computer Vision. IEEE.*

Samangouei, P., Patel, V. M., & Chellappa, R. (2017). Facial attributes for active authentication on mobile devices. *Image and Vision Computing, 58,* 181–192.

Goswami, Gaurav, "Face recognition captcha." 2012 IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS). IEEE, 2012.

Yu, C. (2019). Diffusion-based kernel matrix model for face liveness detection. *Image and Vision Computing, 89,* 88–94.

Nguyen, M. H. (2008). *Image-based shaving*. Computer graphics forum. Vol. 27. No. 2. Oxford, UK: Blackwell Publishing Ltd.

Galbally, J. (2009). Hill-climbing attack to an eigenface-based face verification system. In *2009 First IEEE International Conference on Biometrics, Identity and Security (BIdS). IEEE.*

Rathee, N. (2016). Feature fusion for fake Indian currency detection. In *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom). IEEE.*

Ahmed, Z. (2014). Image processing based Feature extraction of Bangladeshi banknotes. In *The 8th International Conference on Software, Knowledge, Information Management and Applications (SKIMA 2014)*, IEEE.

Amin, R. (2017). A software agent enabled biometric security algorithm for secure file access in consumer storage devices. *IEEE Transactions on Consumer Electronics, 63*(1), 53–61.

Abdul, W., et al. (2017). Biometric security through visual encryption for fog edge computing. *IEEE Access* 5 (2017): 5531–5538.

de Freitas Pereira, T., Anjos, A., De Martino, J.M., Marcel, S. (2013). Can face anti-spoong countermeasures work in a real world scenario? In *Proceedings IEEE International Confw Biometrics (ICB)*, pp. 1– 8.

Galbally, J., Marcel, S., & Fierrez, J. (Feb. 2014). Image quality assessment for fake biometric detection: Application to iris, ngerprint, and face recognition. *IEEE Transactions on Image Processing, 23*(2), 710–724.