SPOOF DETECTION: Application to Face Recognition

Aarti Sharma[1] Dr. Surender Dahiya[2]
[1]Ambala College Of Engineering And Applied Research Devsthali (Near Mithapur) Ambala
[2]Kurukshetra University, Kurukshetra Haryana, India

Abstract--- User authentication is an important step to protect information, and face biometrics plays an important role to recognize a person. Face biometrics is natural, easy to use, and universally acceptable. Recent work has publicized that face biometrics can be easily spoofed using cheap low-tech equipment. This paper introduces novel and appealing techniques to detect face spoofing using the motion, texture analysis, liveness detection. The key idea of the approach is to learn and detect the structure facial textures that characterize real faces but not fake ones.

Keywords: Anti-spoofing; Liveness detection; Countermeasure; Face recognition; Biometrics.

I. INTRODUCTION

Biometric recognition [1] is a natural and reliable solution to the problem of person recognition. It is more difficult to manipulate, share or forget these traits because biometrics identifiers inherent to an individual.

Biometrics offers certain advantages over traditional ways [2] follow as:-

- Non Repudiation- it is a way to guarantee that an individual who accesses a certain facility can't later deny using it.
- Negative Recognition – it is the process by which a system determines that a certain individual is indeed enrolled in the system although the individual might deny it.

A biometric recognition system consists of four main modules: (i) sensor (ii) feature extraction (iii) system database (iv) matcher module. Biometrics features can be categorized as physiological and behavioral traits. As in Figure 1. Shown below.

As one of the most popular applications of image analysis and understanding, face recognition has recently gained major attention. This is supported by the emergence of face recognition conferences such as the [3]International Conference on Audio and Video-Based Authentication (AVBPA) since 1997 and the International Conference on Automatic Face and Gesture Recognition (AFGR) since 1995, systematic empirical evaluations of face recognition techniques (FRT), including the FERET [Phillips et al. 1998b, 2000; Rizvi et al. 1998], FRVT 2000 [Blackburn et al. 2001], FRVT 2002 [Phillips et al. 2003], and XM2VTS [Messer et al. 1999] protocols. The problem of machine recognition of human faces continues to appeal researchers from areas such as image processing, pattern recognition, neural networks, computer vision, computer graphics, and psychology.

2000; Rizvi et al. 1998], FRVT 2000 [Blackburn et al. 2001], FRVT 2002 [Phillips et al. 2003], and XM2VTS [Messer et al. 1999] protocols. The problem of machine recognition of human faces continues to appeal researchers from areas such as image processing, pattern recognition, neural networks, computer vision, computer graphics, and psychology.

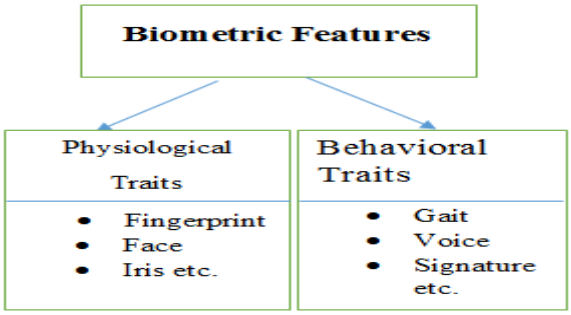

Fig. 1: Traits of Biometric

The problem of machine recognition of faces [4] can be defined as follows: given still or video images of a scene, identify or verify one or more persons in the scene using a stored database of faces. The solution to the problem includes segmentation of faces (face detection) from cluttered scenes, feature extraction from the face regions, recognition, or verification (Figure 2). In identification problems, the input to the system is an unknown face, and the system reports back the determined identity from a database of known individuals, whereas in verification problems, the system needs to confirm or reject the claimed identity of the input face.

Among the different threats analyzed, the direct or spoofing attacks have motivated the biometric community to study the vulnerabilities against this type of fraudulent actions in traits such as the fingerprint [5], the face [6], the signature [7], or even the gait [8] and multimodal approaches [9].

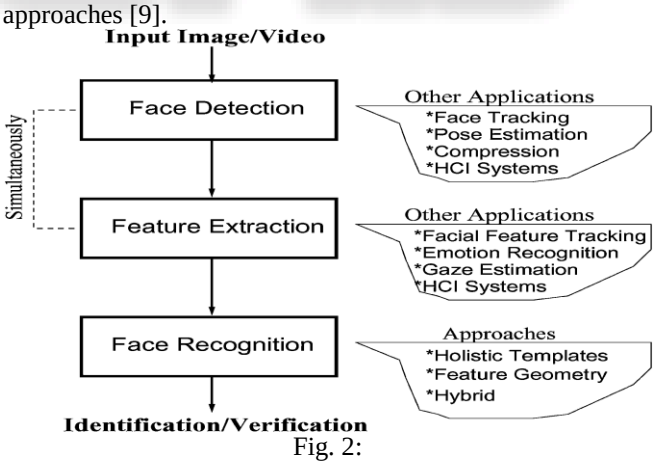

Fig. 2:

II. LETRATURE REVIEW

Face recognition systems can be easily spoofed using a simple photograph of the enrolled person's face, which may be displayed in hard-copy or on a screen. For 2-D face recognition systems Anti-spoofing can be broadly classified in 3 categories with respect to the clues used for attack detection: motion, texture analysis and liveness detection. In motion analysis clues are generated when 2D counterfeits are presented to the system input camera, for example photos or video clips. 2D objects motion is different that of real human faces which are 3-D objects, in many cases and

these deformation patterns are base for spoof detection. For example, [10] presents the Lambertian reflectance model to differentiate between the 2-D face images used during an attack and a real (3-D) face, in enrollment. The latent reflectance information of images captured in both cases using either a variational retinex-based method or a far simpler difference-of-gaussians [11] based approach is estimated and an equation is derived. It is the first work on literature to offer a publicly available database for the development of spoofing counter-measures. [12] Explore a technique to estimate liveness based on a short sequence of images using a binary detector that calculates the trajectories of specific parts of the face given to the input sensor using a simplified optical flow analysis followed by heuristic classifier. [13] Introduce a method for fusing scores based on concurrently, the 3-D face motion scheme introduced on the previous work and liveness properties such as eye-blinks or mouth movements. Texture analysis counter-measures are based on texture patterns such as printing failures or overall image blur that may look unnatural when exploring the input image data. [14] proposes a method for print-attack detection by 2-D Fourier spectra comparing the hard-copies of client faces and real accesses. In [15] the author proposes a method based on micro-textures present on the paper using a linear SVM classifier [16]. Drawback of this method that input image needs to be reasonably sharp.

It explores a real-time liveness detection that uses an undirected conditional random field framework to model the eye-blinking that relaxes the independence assumption of generative modelling and state dependence limitations from hidden Markov modelling use the publicly available PRINT-ATTACK database and its companion protocol with a motion-based algorithm that identifies correlations between the person's head movements and the scene context which can be used to compare to other counter-measure techniques.

[17] proposed a new IQA scheme based on the concept of gradient similarity. Gradients convey important visual information containing structural and contrast changes which affects the image quality. Luminance changes also affect the image quality. Finally, the effects of these changes are integrated via an adaptive method to obtain the overall image quality score.The effectiveness of the proposed IQA scheme has been demonstrated with six public benchmark IQA databases.

[18] address the problem of detecting face spoofing attacks by inspecting the potential of texture features based on Local Binary Patterns (LBP) and their variations on three types of attacks: printed photographs, and photos and videos displayed on electronic screens of different sizes.A publicly available face spoofing REPLAY-ATTACK database containing all above 3 types of attacks.

[19] presented an approach Inspired by image quality assessment, characterization of printing artifacts and by differences in light reflection, for antispoofing based on learning the micro-texture patterns that differentiate live face images from fake images. Furthermore, reflected light from human faces and prints is different in many ways because a human face is a complex non rigid 3D object whereas a photograph is a planar rigid object. In this approach the micro-texture patterns are encoded into an enhanced feature histogram using multi-scale local binary patterns (LBP). In addition, the texture features are used for spoofing detection as well as for face recognition. This provides a unique feature space for coupling spoofing detection and face recognition.

[20] present multibiometric, multi attack and software-based fake detection method. By adding liveness assessment through the use of image quality assessment security of biometric recognition frameworks is enhanced.The experimental results, attained on publicly available data sets of fingerprint, iris, and 2D face using 25 general image quality features extracted from one image. All these results validate the "quality-difference" hypothesis formulated as "It is expected that a fake image captured in an attack attempt will have different quality than a real sample acquired in the normal operation scenario for which the sensor was designed."

III. Threats Of The Biometric System

There are different types of threats [21] to the biometric system which are explained as:-

- Circumvention:- An attacker gains access to the system protected by biometric authentication.
- Repudiation:- An individual who accesses a certain facility can later deny using it.
- Collusion:- A user with wide super user privileges.
- Coercion:- An attacker forces a legitimate user to access the system.
- Denial of service:- An attacker corrupts the biometric system so that legitimate user can't use it.

IV. Spoofing Attacks

Spoofing attacks are one of the security traits that biometric recognition systems are proven to be vulnerable to. When spoofed, a biometric recognition system is bypassed by presenting a copy of the biometric evidence of a valid user. Spoofing attack is the action of outwitting a biometric. Sensor by presenting a counterfeit biometric evidence of a valid user [22]. It is a direct attack to the sensory input of a biometric system and the attacker does not need previous knowledge about the recognition algorithm. Most of the biometric modalities are not resistant to spoofing attacks: the biometric systems are usually designed to only recognize identities without concern whether the identity is live or not. Despite the existence of very sophisticated biometric authentication and verification systems nowadays, implementing anti-spoofing schemes for them is still in its infancy.

Depending on the biometric modality being attacked, fabricating fake biometric data can have different levels of difficulty.

A. Spoofing Related Risks

- Fake artifacts being used to mount attacks against existing enrollments in order to gain unauthorized access.
- Fake artifacts being used to enroll and authentication in a biometrics system.
- Fake artifacts being used to mount attacks against existing enrollment in order to gain unauthorized access to the resource protected by biometric system.
- These are the results of attacks- due to inability of the biometrics system to ensure liveness.

V. ANTISPOOFING METHODS FOR FACE BIOMETRICS

Face recognition systems can be easily spoofed using a simple photograph of the enrolled person's face, which may be displayed in hard-copy or on a screen. For 2-D face recognition systems Anti-spoofing can be broadly classified in 3 categories with respect to the clues used for attack detection: motion, texture analysis and liveness detection.

1. In motion analysis clues are generated when 2D counterfeits are presented to the system input camera, for example photos or video clips. 2D objects motion is different that of real human faces which are 3-D objects, in many cases and these deformation patterns are base for spoof detection. For example, [23] presents the Lambertian reflectance model to differentiate between the 2-D face images used during an attack and a real (3-D) face, in enrollment. The latent reflectance information of images captured in both cases using either a variational retinex-based method or a far simpler difference-of-Gaussians [24] based approach is estimated and an equation is derived.
2. Texture analysis counter-measures are based on texture patterns such as printing failures or overall image blur that may look unnatural when exploring the input image data. [25] proposes a method for print-attack detection by 2-D Fourier spectra comparing the hard-copies of client faces and real accesses. In [26] the author proposes a method based on micro-textures present on the paper using a linear SVM classifier [27]. Drawback of this method that input image needs to be reasonably sharp.
3. Liveness detection is to determine if the biometrics data is being captured from a legitimate , live user who is physically present at the point of acquisition. [28] Explore a technique to estimate liveness based on a short sequence of images using a binary detector that calculates the trajectories of specific parts of the face given to the input sensor using a simplified optical flow analysis followed by heuristic classifier. Introduce a method for fusing scores based on concurrently, the 3-D face motion scheme introduced on the previous work and liveness properties such as eye-blinks or mouth movements.

Real-time liveness detection that uses an undirected conditional random field framework to model the eye-blinking that relaxes the independence assumption of generative modelling and state dependence limitations from hidden Markov modelling.

Specific liveness detection measures vary from technology to technology, but all liveness detection technique fall in to three categories (Fig.3):-

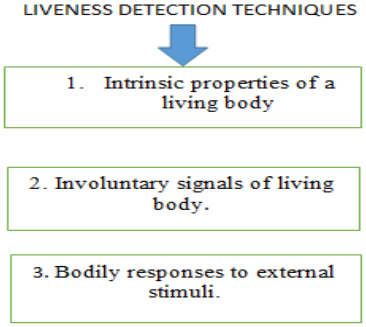

Fig. 3: Liveness Detection

VI. CONCLUSION

The study of the vulnerabilities of biometric systems against different types of attacks has been a very active field of research in recent years [2]. Spoofing is a real concern with regard to security of biometric system. More and more successful spoofing attempts are being published. It is possible to combat spoofing attacks with liveness detection testing but all of these countermeasures come at certain price often affecting user convenience, hardware prices.

REFERENCES

[1] S.Kent and L.Millett. Who Goes There? Authentication Technologies through the Lens of Privacy. National Academy Press,2003.
[2] S.Prabhakar, S.Pankanti, and A.K.Jain. Biometric Recognition: Security And Privacy Concerns. IEEE Security And Privacy Magazine, 1(2):33-42, March-April 2003.
[3] C. L. Fancourp, L.Bogoni, K. J. Hanna, Y. Guo, R. P. Wildes, N. Takahashi and U. Jain. In Fifth International Conference on on Audio and Video-Based Authentication (AVBPA), USA 1997.
[4] S.Z. Li and Anil K. Jain, editors. Handbook of Face Recognition. Springer- Verlag, 2005.
[5] J. Galbally, R. Cappelli, A. Lumini, G. G. de Rivera, D. Maltoni, J. Fierrez, et al., "An evaluation of direct and indirect attacks using fake fingers generated from ISO templates," Pattern Recognit. Lett., vol. 31,no. 8, pp. 725–732, 2010.
[6] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," in Proc. IEEE IJCB, Oct. 2011, pp. 1–7.J. Hennebert, R. Loeffel, A. Humm, and R. Ingold, "A new forgery scenario based on regaining dynamics of signature," in Proc. IAPR ICB, vol. Springer LNCS-4642. 2007, pp. 366–375.
[7] J. Hennebert, R. Loeffel, A. Humm, and R. Ingold, "A new forgery scenario based on regaining dynamics of signature," in Proc. IAPR ICB, vol. Springer LNCS-4642. 2007, pp. 366–375.
[8] A. Hadid, M. Ghahramani, V. Kellokumpu, M. Pietikainen, J. Bustard, and M. Nixon, "Can gait biometrics be spoofed?" in Proc. IAPR ICPR, 2012, pp. 3280–3283.
[9] Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Evaluation of serial and parallel multibiometric systems under spoofing attacks," in Proc. IEEE 5th Int. Conf. BTAS, Sep. 2012, pp. 283–288.
[10] X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," Computer Vision ECCV 2010, vol. 6316, pp. 504-517, 2010.
[11] Y. Li and X. Tan, "An anti-photo spoof method in face recognition based on the analysis of fourier spectra with sparse logistic regression," in Chinese Conference on Pattern Recognition, 2009.
[12] K. Kollreider, H. Fronthaler, and J. Bigun, "Nonintrusive liveness detection by face images," Image and Vision Computing, vol. 27, no. 3, pp. 233-244, 2009.
[13] "Verifying liveness by multiple experts in face biometrics," in Computer Society Conference on

Computer Vision and Pattern Recognition Workshops. IEEE, 2008, pp. 1-6.
[14] J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of fourier spectra," in In Biometric Technology for Human Identification, 2004, pp. 296-303
[15] J. Bai, T. Ng, X. Gao, and Y. Shi, "Is physics-based liveness detection truly possible with a single image?" in International Symposium on Circuits and Systems. IEEE, 2010, p. 3425-3428.
[16] V. N. Vapnik, The nature of statistical learning theory. Springer, 1995.
[17] A. Liu, W. Lin, and M. Narwaria, "Image quality assessment based on gradient similarity," IEEE Trans. Image Process., vol. 21, no. 4, pp. 1500–1511, Apr. 2012.
[18] A. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in Proc. IEEE Int. Conf. Biometr. Special Interest Group, Sep. 2012, pp. 1–7.
[19] J. Maatta, A. Hadid, and M. Pietikainen, "Face spoofing detection from single images using micro-texture analysis," in Proc. IEEE IJCB,Oct. 2011, pp. 1–7.
[20] A. K. Jain and D. Zongker, "Feature selection: Evaluation, application, and small sample performance," IEEE Trans. Pattern Anal. Mach. Intell., vol. 19, no. 2, pp. 153–158, Feb. 1997.
[21] Manvjeet Kaur, Dr. Sanjeev Sofat & Deepak Saraswat,"Template and Database Security in biometrics systems" International Journal of Computer Applications (0975 – 8887) Volume 4 –No.5, July 2010.
[22] K. Nixon, V. Aimale, and R. K. Rowe, "Spoof detection schemes," Handbook of Biometrics, 2008.
[23] X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," Computer Vision ECCV 2010, vol. 6316, pp. 504-517, 2010.
[24] Y. Li and X. Tan, "An anti-photo spoof method in face recognition based on the analysis of fourier spectra with sparse logistic regression," in Chinese Conference on Pattern Recognition, 2009.
[25] J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of fourier spectra," in In Biometric Technology for Human Identification, 2004, pp. 296-303.
[26] J. Bai, T. Ng, X. Gao, and Y. Shi, "Is physics-based liveness detection truly possible with a single image?" in International Symposium on Circuits and Systems. IEEE, 2010, p. 3425-3428.
[27] V. N. Vapnik, The nature of statistical learning theory. Springer, 1995.
[28] K. Kollreider, H. Fronthaler, and J. Bigun, "Nonintrusive liveness detection by face images," Image and Vision Computing, vol. 27, no. 3, pp. 233-244, 2009.

