Detection of Fake Biometrics: Assessment of Image Quality in Face, Fingerprint

J. Madhavi[1], Giri Babu K[2]

[1]Assistant Professor, TKR College of Enginnering And Technology
[2]Assistant Professor, CVR College Of Engineering And Technology

Abstract:
Biometric authentication is difficult because it is difficult to distinguish between a genuine trait and a fake, self-made synthetic, or reconstructed sample. This calls for new, more effective protection measures. This paper describes a software-based fake detection method that can be used in multiple biometric systems to detect fraudulent access attempts. This system adds liveness assessment to biometric recognition systems in an easy-to-use, non-invasive way. It is intended to increase security. This method is easy to use and can be used in real-time. It works by combining 25 image quality features (i.e. it uses 25 general image quality features from one image (i.e., the same image used for authentication) to differentiate legitimate samples from counterfeit ones. The proposed method is superior to other state-of-the-art methods, according to experiments that used publicly available data for fingerprint, iris, and 2D faces. The analysis of biometric samples' general quality revealed valuable information that can be used to identify genuine traits from fake ones.

Keywords: Image quality assessment, biometrics, security, attacks, countermeasures.

INTRODUCTION:

Biometrics refers to the science and technology that measures and analyzes human body characteristics, such as fingerprints. Eye retinas and iris patterns, voice patterns, facial patterns, hand measurements, and voice patterns. It is used primarily for authentication. Many initiatives have been developed to ensure the security of the biometric systems. These initiatives reflect the importance of all parties involved in developing security systems to allow the rapid development of technology into practical use. This will allow them to fraudulently access the biometric system. Digital protection mechanisms that are used are ineffective as attacks are done in analog domains and interactions with the device are done using regular protocol.

For image processing applications like recognition, retrieval and classification, compression, restoration, and other similar fields, it is important to measure the quality of images. Images can be affected by different distortions. It is important to accurately rate the quality of the image. The traditional subjective rating method used to assess the image's quality was based on the time requirements. Experts are needed to evaluate image quality. This can be costly and time-consuming. Many image quality assessment algorithms exist today to determine the quality.

The image may not look the same as the original when it is displayed to the user. This happens because it has gone through multiple processes. There are many possible sources of distortion, including motion blurring, Gaussian Noise, sensor inadequacy and compression. It is also possible that the image has been subject to error during transmission. Images before they are stored or transmitted. A variety of methods have been developed to assess the quality of videos and images.

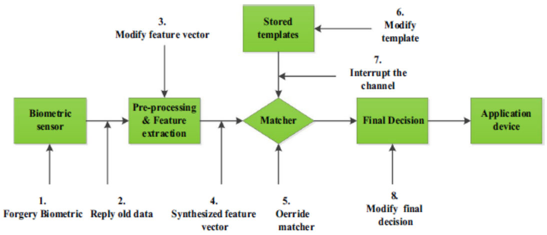

Figure 1: Attack points in the general biometric system

LITERATURE SURVEY

Paper Javier (Galbally Z.Wei 2014) introduced a new software-based multibiometric and multi attack protection method that aims to overcome some limitations. It cannot operate under diverse biometric systems or for different spoofing scenarios. The paper by Poonam Dabas Z.Wei (2013) introduced objective methods to measure the quality of images. The paper presented a method that focused on quality measures and an algorithm for modeling HVS (Human Visual System). The properties of HVS include perceived brightness and frequency response. HVS is used for processing input images.

This paper's Approach [9] is based upon the fact that digital media hide information by altering signal properties to introduce some degradation. This paper shows how adding a message or watermark to a digital media file can create unique artifacts that are detectable using Image Quality Measures. This paper shows that image quality assessments can be used to distinguish between stego-images and cover images.

IMAGE QUALITY ASSESSMENT FOR LIVENESS DETECTION

Image quality refers to the image's perceived image degradation. Imaging systems can introduce distortions or artifacts into the signal. This makes quality assessment a critical problem. Image quality can be measured in two ways. The subjective image quality assessment uses the mean opinion score (MOS). While algorithms evaluate quality, they are based on subjective evaluations. This is how an image is perceived by viewers. This is why the human visual system has a high degree of adaptation. The measurement of structural distortion must be accurate to approximate the perception of image distortion. This will make them more useful in real-world situations. Image quality can be measured in two ways.

The subjective image quality assessment uses the mean opinion score (MOS), which is a human-based method of evaluating quality. Algorithms are used to objectively evaluate quality. The diagram for IQA can be found. The measurement of structural distortion must be accurate to approximate the perception of image distortion in real-world situations.

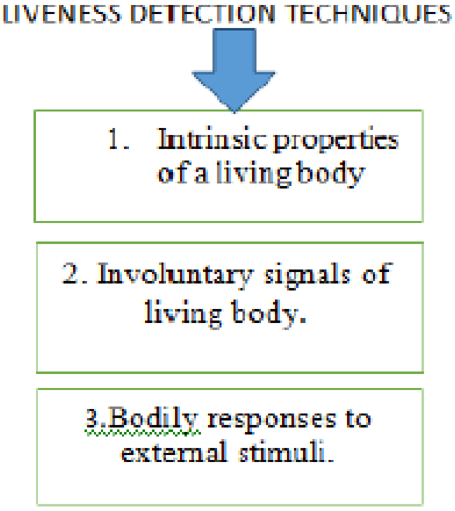
LIVENESS DETECTION TECHNIQUES
1. Intrinsic properties of a living body
2. Involuntary signals of living body.
3.Bodily responses to external stimuli.

Fig.2. Liveness detection

IMAGE QUALITY ASSESSMENT TECHNIQUES

1. Subjective Methods

Images are presented to several observers for subjective quality assessment. Each image is displayed to an observer who is asked to rate the image on a scale of 1-5. The subjective quality test takes into consideration three factors: illumination, viewing distance from the observer to display, and display properties.

2. Objective Methods

An objective method uses two images to determine the image quality. It is a quantitative approach that takes into account the intensity of two images, reference and distorted types. An objective method can be divided into three types: full-reference (reduced-reference), and no-reference (no-reference) based on the availability of a reference image. This allows us to calculate a number that indicates the image quality.

Reduced Reference (RR) models: This method does not use the original reference image center side by side. Some features from the original reference images are however extracted and used by the quality assessment system. This allows the assessment system to quantify the image's quality and help it evaluate its quality.

PROPOSED METHOD

The proposed system aims to improve the security of biometric recognition systems by adding liveness assessment quickly, easily, and without any intrusion, using image quality assessment.

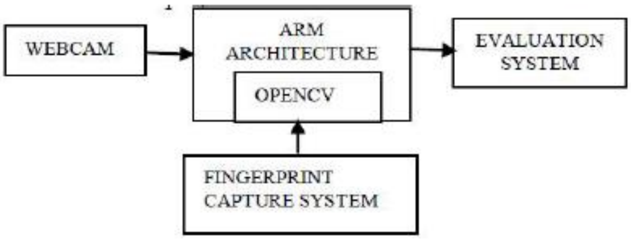

Fig.3 Architecture diagram for real-time recognition from a web camera

Face Recognition

This step allows us to determine who a person is based on a single facial image. We have used the Fisher algorithm to recognize faces. To recognize faces, the OpenCV function was used in the proposed system. OpenCV has many FaceRecognizer algorithms. We used the Fisher algorithm to recognize faces in our system. To verify the accuracy of the prediction or to determine if it is a mistake, face verification can be performed. Facial verification can be achieved by reconstructing facial images, then calculating the similarities between the reconstructed and input images. To perform these steps, we use OpenCV functions. We have thus used the Fisher faces algorithm. It requires a higher threshold, so we used a threshold of 0.7.

Proposed Fingerprint recognition method: Another biometric check is fingerprint. We have used OpenCV to fingerprint in the proposed system. We take the fingerprint of the person [18] at registration and verify it at verification time.

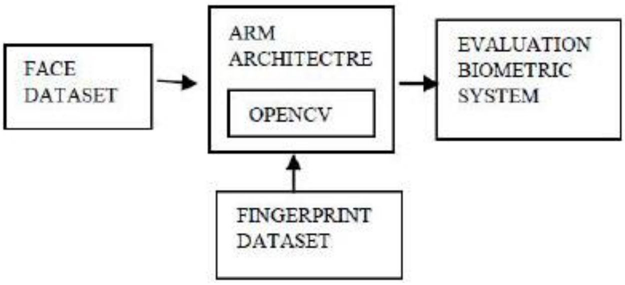

Fig 4: Architecture Diagram of Offline Recognition

VI. EXPERIMENTAL RESULTS

Proposed Face Recognition

The proposed system consists primarily of the following three steps for face recognition:

1. First, we need to create a database with multiple images of faces for each person.
2. Next, we will use the images from the database to identify faces and train the face recognition program.
3. The third step is to verify that the facial recognition software can recognize faces it was programmed for.

Dataset:

We used the publicly accessible AT &T "The Database of faces", also known as "The ORL Database of faces" in our proposed system. The database contains ten images of each subject. Images were taken at various times and with different lighting conditions. The facial expressions of the subjects (smiling or smiling open or closed eyes), as well as facial details like glasses or without glasses, were varied. The dark background was uniform and subjects were in front and upright positions.

Fig 5: Images of Fingerprint Dataset:

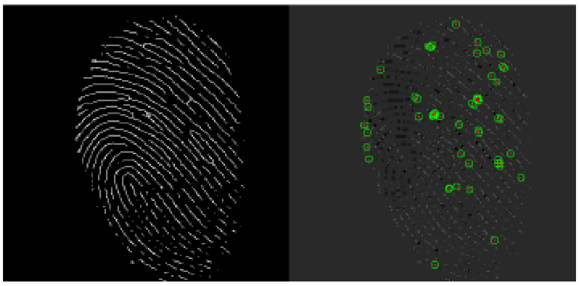

Fig 6: Comparison between thinned fingerprint and Harris corner response as well as the selected Harris corners.

Face Recognition:

We recommend that we take at least 15 images using the web camera to achieve better performance. The proposed system recognizes the face of the image taken by the camera with a similarity 93%. Fingerprint authentication was also successfully performed.

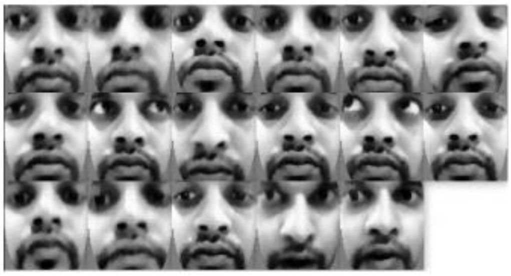

Fig: 7 Images captures from web camera

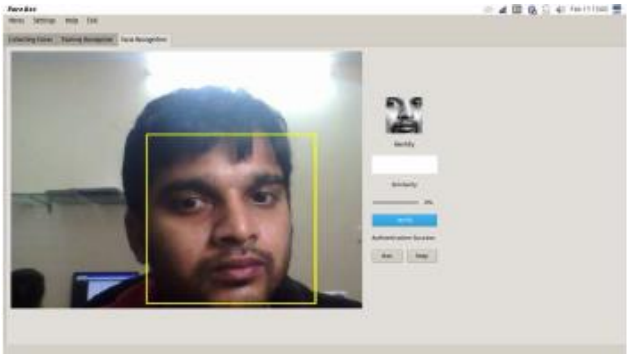

Fig 8: Image acquisition using web camera

Conclusion

It is clear that biometric security has been an active area of research over the past few years. The proposed system was evaluated using biometric modalities like fingerprint and face. This includes the use of publicly available databases as well as face images captured by webcam and fingerprint scanners with well-defined associated protocols. The system was successfully developed and tested using both offline and real-time recognition. The system was successfully tested and evaluated. The system uses publicly accessible data. Different algorithms are used to recognize different biometrics. Future work will be possible with the proposed work, such as using video quality measures to detect video attacks and further evaluation of other image-based modalities, like palm print.

REFERENCES:

1. Hadid A, Evans N, Marcel S, Fierrez J. Biometrics systems under spoofng attack: an evaluation methodology and lessons learned. IEEE Signal Process Mag. 2015;32:20–30.
2. Akhtar Z, Micheloni C, Foresti GL. Biometric liveness detection: challenges and research opportunities. IEEE Secu Priv. 2015;13:63–72.
3. Marcel S, Nixon MS, Li SZ. Handbook of biometric anti-spoofing. London: Springer London; 2014. p. 1–279.
4. Shahin MK, Badawi AM, Rasmy ME. A multimodal hand vein, hand geometry, and fingerprint prototype design for high-security biometrics. In: Proceedings of the 2008 Cairo International Biomedical Engineering Conference. IEEE; 2008. p. 1–6.
5. Rodrigues RN, Ling LL, Govindaraju V. Robustness of multimodal biometric fusion methods against spoof attacks. J Vis Lang Comput. 2009;20:169–79.
6. Jiang RM, Sadka AH, Crookes D. Multimodal biometric human recognition for perceptual human–computer interaction. IEEE Trans Syst Man Cybern Part C Appl Rev. 2010;40:676–81.
7. Gomez-Barrero M, Galbally J, Fierrez J. Efcient software attack to multimodal biometric systems and its application to face and iris fusion. Pattern Recognit Lett. 2014;36:243–53.
8. Das A, Pal U, Ferrer MA, Blumenstein M. A framework for liveness detection for direct attacks in the visible spectrum for multimodal ocular biometrics. Pattern Recognit Lett. 2016;82:232–41.
9. Kavitha P, Vijaya K. Optimal feature-level fusion and layered k-support vector machine for spoofing face detection. Multimed Tools Appl. 2018;77:26509–43.
10. Jain AK, Hong L, Kulkarni Y. A multimodal biometric system using fingerprint, face, and speech 1999; 10.
11. Komeili M, Armanfard N, Hatzinakos D. Liveness detection and automatic template updating using a fusion of ECG and fingerprint. IEEE Trans Inf Forensics Secur. 2018;13:1810–22.
12. Walia GS, Singh T, Singh K, Verma N. Robust multimodal biometric system based on optimal score level fusion model. Expert Syst Appl. 2019;116:364–76.
13. Chetty G, Wagner M. Multi-level liveness verification for facevoice biometric authentication. In: Proceedings of the 2006 Biometrics Symposium: special session on research at the biometric consortium conference. IEEE; 2006. p. 1–6.
14. Akhtar, Z., Micheloni, C., Piciarelli, C., Foresti, G.L.: MoBio; LivDet: Mobile biometric liveness detection. In: 2014 11th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS). pp. 187–192. IEEE (2014)
15. Gupta K, Walia GS, Sharma K. Multimodal biometric system using grasshopper optimization. In: 2019 international conference on computing, communication, and intelligent systems (ICCCIS); 2019. IEEE, p. 387–391.
16. Bao W, Li H, Li N, Jiang W. A liveness detection method for face recognition based on optical fow feld. In: Proceedings of 2009 international conference image analysing signal process; 2009. IASP 2009, p. 233–236.
17. Sahidullah M, Thomsen DAL, Hautamaki RG, Kinnunen T, Tan ZH, Parts R, Pitkanen M. Robust voice liveness detection and speaker verifcation using throat microphones. IEEE/ACM Trans Audio Speech Lang Process. 2018;26:44–56.
18. Kim W, Hong W, Kim T, Kim D, Lee M. RF sensor-based liveness detection scheme with loop stability compensation circuit for a capacitive fngerprint system. IEEE Access. 2019;7:152545–51.

19. Albakri G, Alghowinem S. The efectiveness of depth data in liveness face authentication using 3D sensor cameras. Sensors. 2019;19:1928.
20. Wang, Y., Cai, W., Gu, T., Shao, W., Li, Y., Yu, Y.: Secure Your Voice. In: Proceedings of ACM interactive, mobile, wearable ubiquitous technology, vol 3. 2019. p. 1–28.
21. Ma Li, Tan T, Wang Y, Zhang D. Personal identifcation based on iris texture analysis. IEEE Trans Pattern Anal Mach Intell. 2003;25:1519–33.
22. Chen R, Lin X, Ding T. Liveness detection for iris recognition using multispectral images. Pattern Recognit Lett. 2012;33:1513–9.
23. Parveen S, Ahmad S, Abbas N, Adnan W, Hanaf M, Naeem N. Face liveness detection using dynamic local ternary pattern (DLTP). Computers. 2016;5:10.
24. Boulkenafet Z, Komulainen J, Hadid A. Face spoofng detection using colour texture analysis. IEEE Trans Inf Forensics Secur. 2016;11:1818–30.
25. Agarwal R, Jalal AS, Arya K. A multimodal liveness detection using statistical texture features and spatial analysis. Multimed Tools Appl. 2020;79:13621–13645.
26. Sun L, Pan G, Wu Z, Lao S. Blinking-based live face detection using conditional random felds. In: Advances in Biometrics. vol. 4642 LNCS. Springer: Berlin, Heidelberg; 2007. p. 252–260
27. Zhao G, Pietik M. Patterns with an application to facial expressions. Most. 2007;29:1–14.
28. Wang L, Ding X, Fang C. Face live detection method based on physiological motion analysis. Tsinghua Sci Technol. 2009;14:685–90.
29. Chetty G. Biometric liveness checking using multimodal fuzzy fusion. In: 2010 IEEE world congress computational intelligence; 2010. WCCI, p. 1–8.
30. Komogortsev OV, Karpov A. Liveness detection via oculomotor plant characteristics: attack of mechanical replicas. In: Proceedings of 2013 international conference biology; 2013. ICB.
31. Singh AK, Joshi P, Nandi GC. Face recognition with liveness detection using eye and mouth movement. In: 2014 international conference on signal propagation and computer technology (ICSPCT 2014); 2014. IEEE, p. 592–597.
32. Somasundaram G, Cherian A, Morellas V, Papanikolopoulos N. Action recognition using global spatio-temporal features derived from sparse representations. Comput Vis Image Underst. 2014;123:1–13