IJAREEIE

e-ISSN: 2278-8875
p-ISSN: 2320-3765

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

Volume 10, Issue 12, December 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.282

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.282|

|| Volume 10, Issue 12, December 2021 ||

DOI:10.15662/IJAREEIE.2021.1012041

Fake Identification in Biometric System Using IQA

Abhijit Vijay Magdum[1], P.P.Belgali[2]

P.G Student, Department of Electronics Engineering, Shivaji University, Dr. J. J. M. C. O. E Jaysingpur, Kolhapur, India[1]

Professor, Department of Electronics Engineering, Shivaji University, Dr. J. J. M. C. O. E Jaysingpur, Kolhapur, India[2]

ABSTRACT: Now a day's different biometric systems like fingerprint, face, ear, palm, gait, voice, signature, iris, etc. are used worldwide to identify a person. There are various advantages of biometric system such as accurate identification, accountability, easy to use, time saving, versatility, scalability but it is having some disadvantages also. Disadvantages of biometric systems are high cost, people aversion of using a new system, lack of durability of biometric devices, spoofing attacks. This paper focused on method or technique which can be effectively used to overcome one of the disadvantage of biometric system that is spoofing. This method is live detection which will detect whether sample given to biometric system is live or artificially created. Proposed method uses Image quality assessment (IQA). The main objective is to enhance the security. This system is user friendly, cost efficient, less complex, time saving, faster and can be use for multibiometric system.

KEYWORDS: Biometrics, Image quality assessment, Liveness detection, Security, Spoofing attack

I.INTRODUCTION

Biometric systems have several advantages over traditional authentication systems. Biometric information cannot be acquired by direct covert observation. It is impossible to share and difficult to reproduced. It enhances user convenience as there is no need to remember long and random passwords. In spite their various advantages, biometric systems are vulnerable to attacks.

Types of attacks are
(i) Artificially created biometrics,
(ii) Attacking via input port,
(iii) Attacking at database.

In artificially created biometric usual attack methods are face mask, gummy fingers, a printed or contact lenses iris image. Liveness detection is efficient way to overcome these attacks. Liveness is a major attribute in individual's feature space but has low specificity by itself. It is dichotomy of the feature space into live and non-living. Since intruders will introduce a large number of spoofed biometric into system, liveness detection will enhance performance of a multimodal biometric system (spoof attack). Liveness detection reads claimant's physiological signs of life. Image quality assessment is the most important part of the proposed method which uses various image for quality measures.
With the help of image quality measures this system is able to differentiate between real (live) and fake (artificially created) biometric samples. Liveness Detection having two types first is hardware based and second is software based. In hardware based method, sensors are use. Fake detection rate of it is high but this method is complex and costly. In software based method IQA is used. Fake detection rate of this method is less comparative to hardware based method but it is cost efficient, faster, user friendly, easy to use and having good performance. For different biometric system different sensors are required in hardware based method whereas method present in this paper which is software based is applicable to all biometric systems. Hence software based method is always preferable to use.

II.PROPOSED WORK

The proposed system has two steps
(i) Feature extraction,
(ii) Classification.

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.282|

|| Volume 10, Issue 12, December 2021 ||

DOI:10.15662/IJAREEIE.2021.1012041

***(i)*Feature Extraction:** In this system considering image quality measures in which some are Full Reference (FR) and some are No Reference (NR) measures [3]. In FR measures, input biometric sample image and its Gaussian filtered (clean and undistorted) image are used. In NR measures, only input biometric sample is used. Then FR and NR measures are combine for final parameterization in which priorities will given to image quality measures.
***(ii)*Classification:** Further with the help of training data comparison will be done and input sample will be classified as real or fake. If input sample detected as real then only it will further go for recognition purpose to biometric system otherwise access will be denied.

a) Gaussian filtering:

The input image is filtered with a low pass Gaussian kernel filter to generate smoothed version of image.

b) Full reference features:

These features are obtained with reference to the image. The following features can be used for classification.

III. MOTIVATION

The given system is motivated in number of things such as, it consistently perform at different multi-biometric System. The given system is able to adapt multi-attack system. The proposed method is able to generalize different databases and attack scenarios.
The error rates achieved by the proposed system are very low. It helps to avoid fraud access in Industrial, Educational, and Government institutions. It gives high performance and high speed of execution.Due to this system it is able to consistently perform at a high level for different biometric traits, also it is able to adapt different types of attacks.

IV. BLOCK DIAGRAM

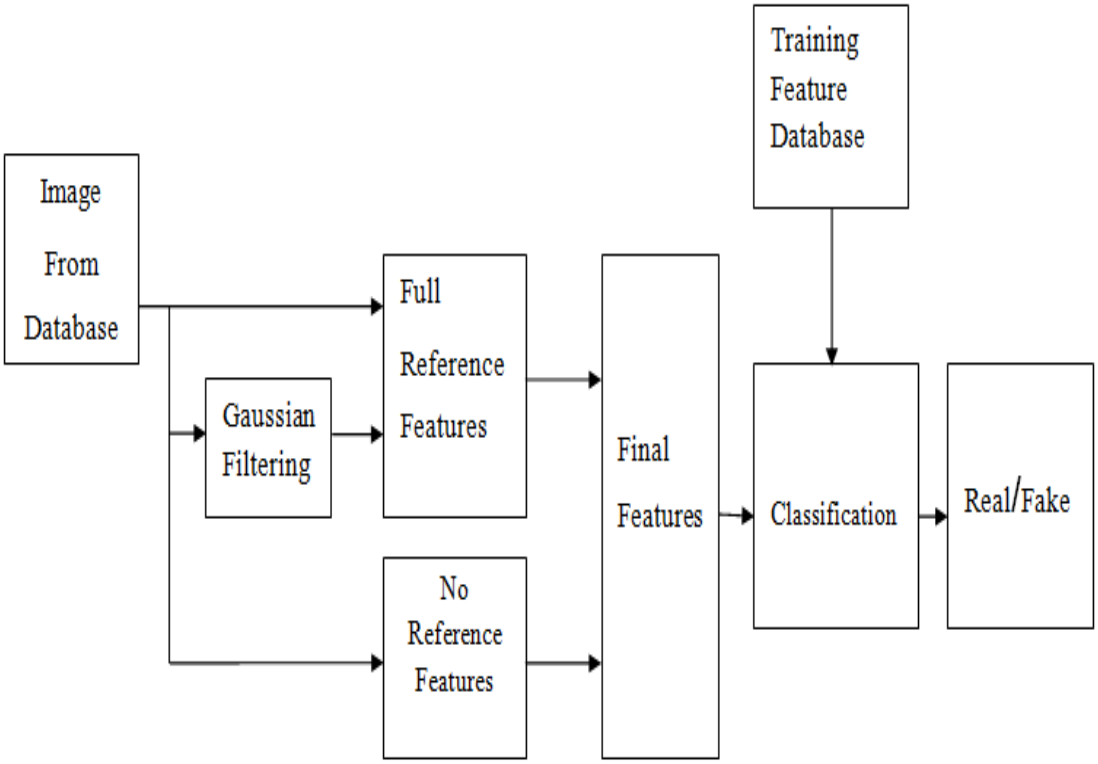


Fig.1 The General Diagram Of Proposed Method

| e-ISSN: 2278 – 8875, p-ISSN: 2320 – 3765| www.ijareeie.com | Impact Factor: 7.282|

|| Volume 10, Issue 12, December 2021 ||

DOI:10.15662/IJAREEIE.2021.1012041

V. FUTURE SCOPE

Future enhancement for this work can be
(i) Assessment for video quality measures for video attack similar to image quality measures,
(ii) Extension of image quality measures.

VI. CONCLUSION

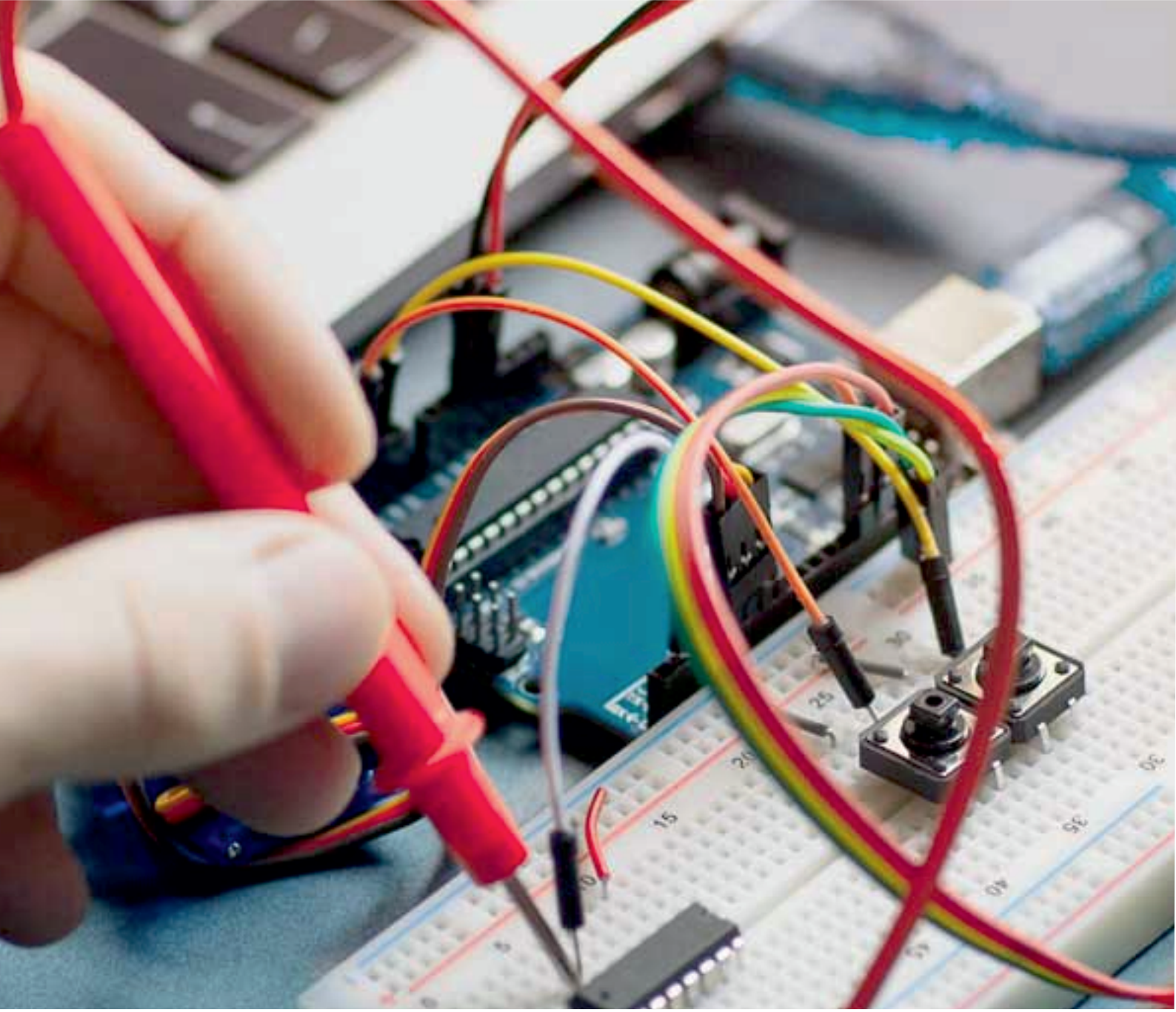
Proposed system is able to detect whether given biometric sample is real or fake. This system enhances security as well as can be use for multi-biometric systems. It is user friendly, cost effective, less complex, time saving and faster.

VII.ACKNOWLEDGEMENT

The authors would like to acknowledge the useful comments continuous support and encouragement by Prof. Mrs.P.P.Belgali

REFERENCES

1) A. Mittal, R. Soundararajan, and A. C. Bovik, “Making a ‘completely blind’ image quality analyzer,” IEEE Signal Process. Lett., vol. 20, no. 3,pp. 209–212, Mar. 2013.
2) D. Brunet, E. R. Vrscay, and Z. Wang, “On the mathematical properties of the structural similarity index,” IEEE Trans. Image Process., vol. 21, no. 4, pp. 1488–1499, Apr. 2012.
3) M. G. Martini, C. T. He wage, and B. Villarini, “Image quality assessment based on edge preservation,” Signal Process., Image Communiction., vol. 27, no. 8, pp. 875–882, 2012.
4) 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.
5) M. C. Stamm and K. J. R. Liu, “Forensic detection of image manipulation using statistical intrinsic fingerprints,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 492–496, Sep. 2010.
6) G.L.Marcialis, A.Lewicke, B.Tan, P.Coli, D.Grimberg,A.Congiu,et al.,“First international fingerprint liveness detection competition LivDet 2009,” in Proc. IAPR ICIAP, Springer LNCS-5716. 2009,pp. 12–23.
7) X. Zhu and P. Milanfar, “A no-reference sharpness metric sensitive to blur and noise,” in Proc. Int. Workshop Qual. Multimedia Exper., 2009, pp. 64–69.
8) Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, “Image quality assessment: From error visibility to structural similarity,” IEEE Trans. Image Process., vol. 13, no. 4, pp. 600–612, Apr. 2004.
9) Z. Wang and A. C. Bovik, “Mean squared error: Love it or leave it? A new look at signal fidelity measures,” IEEE Signal Process. Mag.,vol. 26, no. 1, pp. 98–117, Jan. 2009.
10) J. Zhu and N. Wang, “Image quality assessment by visual gradient similarity,” IEEE Trans. Image Process., vol. 21, no. 3, pp. 919–933, Mar. 2012.
11) M. A. Saad, A. C. Bovik, and C. Charrier, “Blind image quality assessment: A natural scene statistics approach in the DCT domain,” IEEE Trans. Image Process., vol. 21, no. 8,pp. 3339–3352, Aug. 2012.
12) H. R. Sheikh and A. C. Bovik, “Image information and visual quality,” IEEE Trans Image Process., vol. 15, no. 2, pp. 430–444, Feb. 2006.
13) Z. Wang, H. R. Sheikh, and A. C. Bovik, “No-reference perceptual quality assessment of JPEG compressed images,” in Proc. IEEE ICIP, Sep. 2002, pp. 477–480



INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 7.282

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

International Journal of Advanced Research

in Electrical, Electronics and Instrumentation Engineering

9940 572 462 6381 907 438 ijareeie@gmail.com

Scan to save the contact details