International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Fake Biometric Recognition Applicable to Fingerprint, Iris and Face Based On Image Quality Assessment

Nivi Varghese[1], Reshma Manohar[2]

[1]Final Year M. Tech. (Cyber Security), KMP College of Engineering, Perumbavoor, Kerala, India

[2]Assistant Professor, Department of Computer Science and Engineering, KMP College of Engineering, Perumbavoor, Kerala, India

Abstract: ***To guarantee the genuine vicinity of a genuine honest to goodness attribute as opposed to a fake self-fabricated engineered then again recreated specimen is a noteworthy issue in biometric validation, which requires the advancement of new and effective security measures. In this paper, we display a novel programming based fake recognition strategy that can be utilized as a part of different biometric frameworks to distinguish distinctive sorts of false get to endeavors. The goal of the proposed framework is to improve the security of biometric distinguishment structures, by including liveness appraisal in a quick, easy to use, and non-nosy way, through the utilization of picture quality appraisal. The proposed methodology introduces a low level of multifaceted nature, which makes it suitable for ongoing applications, utilizing 25 general picture quality peculiarities removed from one picture (i.e., the same gained for verification purposes) to recognize honest to goodness also impostor tests. The trial results, got on freely accessible information sets of finger impression, iris, and 2D face, demonstrate that the proposed system is very aggressive analyzed with other cutting edge methodologies and that the examination of the general picture nature of genuine biometric specimens uncovers profoundly significant data that may be productively utilized to separate them from fake characteristics.***

Keywords: Picture quality appraisal, biometrics, security, assaults, countermeasures

1. Introduction

Among the distinctive dangers dissected, the alleged direct then again parodying assaults have propelled the biometric group to study the vulnerabilities against this kind of fake activities in modalities, for example, the iris[4], the unique fingerprint mark[5] ,the face[6] , the mark , or even the step and multimodal methodologies. In these assaults, the interloper employments some kind of artificially created relic (e.g., sticky finger, printed iris picture or face veil), or tries to copy the conduct of the honest to goodness client (e.g., step, signature), to deceitfully get to the biometric framework. As this kind of assaults are performed in the simple space and the association with the gadget is carried out after the consistent convention, the regular computerized insurance instruments (e.g., encryption, advanced signature or watermarking) are not viable.

The previously stated works and other simple studies, have plainly demonstrated the need to propose and create particular security strategies against this danger. Along these lines, specialists have concentrated on the configuration of particular countermeasures that empower biometric frameworks to recognize fake examples and reject them, enhancing thusly the vigor and security level of the frameworks.

In the present work we propose a novel programming based multi-biometric and multi-assault security strategy which focuses to overcome some piece of these limits through the utilization of picture quality appraisal (IQA). It is not just proficient of working with a decent execution under distinctive biometric frameworks (multi-biometric) and for differing parodying situations, yet it likewise gives a decent level of insurance against certain non-satirizing assaults (multi-assault). Besides, being programming based, it exhibits the typical favorable circumstances of this sort of methodologies: quick, as it just needs one picture (i.e., the same specimen obtained for biometric distinguishment) to recognize whether it is genuine or fake; non-nosy; easy to use (straightforward to the client); shoddy and simple to install in as of now utilitarian frameworks (as no new bit of equipment is needed).

An included playing point of the proposed system is its speed what's more low intricacy, which makes it exceptionally appropriate to work on genuine situations (one of the coveted qualities of this sort of techniques). As it doesn't send any quality particular property (e.g., details focuses, iris position or face location),the processing burden required for picture handling objects is exceptionally decreased, utilizing just general picture quality measures quick to register, consolidated with extremely basic classifiers.

It has been tried on freely accessible assault databases of iris, finger impression and 2D face, where it has arrived at results completely similar to those got on the same databases and taking after the same exploratory conventions by more unpredictable characteristic particular top-positioned methodologies from the cutting edge.

2. Related Works

Lot of works are carried in earlier related to the above researched area.

2.1. A High Performance Fingerprint Liveness Detection Method Based On Quality Related Features

Another programming based liveness recognition methodology utilizing a novel unique mark parameterization in light of value related gimmicks is proposed. The framework is tried on an exceptionally difficult database containing more than 10,500 genuine and fake pictures procured with five sensors of distinctive advancements and covering an extensive variety of direct assault situations as far as materials and methods took after to create the sticky fingers. The proposed arrangement ends up being hearty to the multi-situation dataset, and presents a general rate of 90% accurately grouped examples. Moreover, the liveness identification system exhibited has the included point of interest over already considered procedures of requiring only one picture from a finger to choose whether it is genuine or fake. This last trademark furnishes the technique with exceptionally profitable gimmicks as it makes it less nosy, more easy to understand, quicker and diminishes its usage costs[2].

2.2. Evaluation of Direct Attacks to Fingerprint Verification Systems

The vulnerabilities of unique finger impression based distinguishment frameworks to direct assaults with and without the participation of the client are concentrated on. Two separate frameworks, one particulars based and one edge peculiarity built, are assessed in light of a database of genuine and fake fingerprints. Taking into account the finger impression pictures quality and on the outcomes accomplished on diverse operational situations, we acquire various factually critical perceptions with respect to the strength of the frameworks [3].

3. Proposed System

The utilization of picture quality evaluation for liveness recognition is roused by the supposition that: "It is normal that a fake picture caught in an assault endeavor will have diverse quality than a genuine example gained in the typical operation situation for which the sensor was outlined."

Expected quality contrasts in the middle of genuine and fake examples may include: level of sharpness, shading and luminance levels, neighborhood antiquities, measure of data found in both sort of pictures (entropy), structural mutilations or characteristic appearance.

Case in point, iris pictures caught from a printed paper are more inclined to be smudged or out of concentrate because of trembling; face pictures caught from a cell phone will presumably be over-covered or under-uncovered; and it is not uncommon that unique finger impression pictures caught from a sticky finger present nearby obtaining relics, for example, spots and patches. Besides, in a possible assault in which an artificially delivered picture is specifically infused to the correspondence channel before the gimmick extractor, this fake example will doubtlessly fail to possess a percentage of the properties found in regular pictures.

4. Principle of Proposed framework

The issue of fake biometric identification can be seen as a two-class arrangement issue where an information biometric test must be doled out to one of two classes: genuine or fake. The key purpose of the methodology is to discover a situated of discriminant characteristics which allows to construct a proper classifier which gives the likelihood of the picture "authenticity" given the removed set of gimmicks.

In the present work we propose a novel parameterization utilizing 25 general picture quality measures[1]. A general outline of the assurance methodology proposed in this work is demonstrated in Figure.1. With a specific end goal to keep its all-inclusive statement what's more effortlessness, the framework needs one and only include: the biometric test to be named genuine or fake (i.e., the same picture procured for biometric distinguishment purposes). Moreover, as the system works all in all picture without seeking for any quality particular properties, it doesn't require any preprocessing steps (e.g., unique finger impression division, iris identification or face extraction) before the processing of the IQ characteristics. This trademark minimizes its computational load. When the gimmick vector has been produced the specimen is named genuine (produced by a certified attribute) or fake (artificially created), utilizing some basic classifiers. Specifically, for our analyses we have considered standard executions in Mat lab of the Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA) classifiers

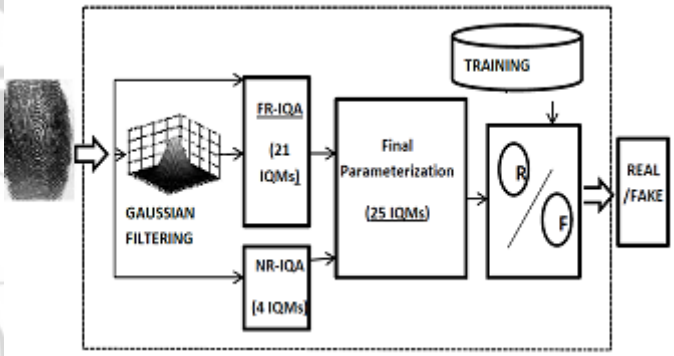

Figure 1: General method for biometric recognition based on image quality assessment

The assessment exploratory convention has been outlined with a two-fold objective:

- First, assess the "multi-biometric" measurement of the security system. That is, its capacity to accomplish a decent execution, contrasted with other characteristic particular methodologies, under distinctive biometric modalities. For this reason three of the most expanded picture based biometric modalities have been considered in the trials: iris, fingerprints also 2D face.
- Second, assess the "multi-assault" measurement of the assurance technique. That is, its capacity to distinguish not just mocking assaults, (for example, different liveness detection specific methodologies) additionally false get to endeavors done with manufactured or recreated examples.

In view of these objectives, and keeping in mind the end goal to attain to reproducible results, we have just utilized as a part of the test approval openly accessible databases with decently portrayed assessment conventions. This has permitted us to think about, in an target and reasonable way, the execution of the proposed framework with other existing cutting edge liveness discovery arrangements. The assignment in all the situations and examinations portrayed in the following segments is to consequently recognize genuine also fake examples.

For this reason we manufacture a 25-dimensional basic classifier in light of general IQMs[1]. Accordingly, in all cases, results are accounted for regarding: the False Genuine Rate (FGR), which accounts for the quantity of false specimens that were delegated genuine; also the False Fake Rate (FFR), which gives the likelihood of a picture originating from a certifiable specimen being considered as fake. The Half Total Error Rate (HTER) is figured as HTER = (FGR + FFR

5. Conclusion

In this setting, the present work has made a few commitments to the best in class in the field of biometric security, specifically:

1) it has demonstrated the high capability of picture quality evaluation for securing biometric frameworks against a mixture of assaults;
2) proposition and acceptance of another biometric insurance strategy;
3) reproducible assessment on numerous biometric characteristics taking into account openly accessible databases;
4) similar results with other already proposed assurance arrangements.

The present research likewise opens new potential outcomes for future work, including:

1) expansion of the considered 25-list of capabilities with new picture quality measures;
2) further assessment on other picture based modalities (e.g., palm print, hand geometry, vein);
3) consideration of worldly data for those cases in which it is accessible (e.g., frameworks working with face features);
4) utilization of feature quality measures for feature assaults (e.g., illicit access endeavors considered in the REPLAY-ATTACK DB);
5) examination of the gimmicks singular significance.

References

[1] Javier Galbally,Sebastien Marcel, and Julian Fierrez "Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition"IEEE Transactions On Image Processing, vol. 23, no. 2, February 2014.
[2] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "A high performance fingerprint liveness detection method based on quality related features," *Future Generat. Comput. Syst.*, vol. 28, no. 1,pp. 311–321, 2012.
[3] J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz, "Evaluation of direct attacks to fingerprint verification systems," *J. Telecommun. Syst.*, vol. 47, nos. 3–4, pp. 243–254, 2011.
[4] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security,"*EURASIP J. Adv. Signal Process.*, vol. 2008, pp. 113–129, Jan. 2008.
[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.

Author Profile

Nivi Varghese received the B.Tech degree in Computer Science from Mahatma Gandhi University Kottayam in 2013 and currently pursuing final year M. Tech degree in Computer Science and Engineering with specialization in Cyber Security from KMP College of Engineering, Perumbavoor.

Reshma Manohar received B.Tech in Computer Science from CUSAT in 2012 and M.Tech in Computer Science from Mahatma Gandhi University Kottayam in 2014 and currently working as assistant professor in KMP College of Engineering Perumbavoor in Computer Science and Engineering Department